

Administratorhandbuch zu Backup Exec 20.4

Rechtlicher Hinweis

Copyright © 2019 Veritas Technologies LLC. Alle Rechte vorbehalten.

Veritas und das Veritas-Logo sind Marken oder eingetragene Marken von Veritas Technologies LLC bzw. verbundener Unternehmen in den USA und anderen Ländern. Andere Bezeichnungen können Marken anderer Rechteinhaber sein.

Dieses Produkt enthält möglicherweise Software anderer Hersteller, für die Veritas einen entsprechenden Hinweis ("Programme anderer Hersteller") zur Verfügung stellen muss. Einige Programme anderer Hersteller werden über eine "Open Source"-Lizenz oder im Rahmen kostenloser Softwarelizenzen zur Verfügung gestellt. Die Lizenzvereinbarung, die der Software beiliegt, ändert keine Rechte oder Verpflichtungen, die Sie im Rahmen dieser Open Source- oder kostenlosen Softwarelizenzen haben können. Weitere Informationen finden Sie im Dokument mit dem Hinweis zu Programmen anderer Hersteller, das im Lieferumfang dieses Veritas-Produkts und auf folgender Webseite verfügbar ist:

<https://www.veritas.com/about/legal/license-agreements>

Das in diesem Dokument beschriebene Produkt wird unter Lizenzen vertrieben, die die Nutzung, Vervielfältigung, Distribution und Dekompilierung/Zurückentwicklung (Reverse Engineering) einschränken. Kein Teil dieses Dokuments darf in irgendeiner Form mit irgendwelchen Mitteln ohne schriftliche Einwilligung von Veritas Technologies LLC und von möglichen Lizenzgebern reproduziert werden.

Die Dokumentation wird ohne Mängelgewähr bereitgestellt. Alle ausdrücklichen und stillschweigenden Voraussetzungen, Darstellungen und Gewährleistungen, einschließlich der stillschweigenden Gewährleistung der Marktgängigkeit, Eignung für einen bestimmten Zweck oder Nicht-Beeinträchtigung, sind ausgeschlossen, außer in dem Umfang, in dem diese Haftungsausschlüsse als nicht rechtsgültig angesehen werden. VERITAS TECHNOLOGIES LLC IST IN KEINEM FALL ERSATZPFLICHTIG FÜR IRGENDWELCHE BEILÄUFIG ENTSTANDENEN ODER FOLGESCHÄDEN IN ZUSAMMENHANG MIT DER BEREITSTELLUNG, LEISTUNGSFÄHIGKEIT ODER VERWENDUNG DIESER DOKUMENTATION. Die in dieser Dokumentation enthaltenen Informationen können jederzeit ohne Ankündigung geändert werden.

Die lizenzierte Software und Dokumentation gelten als kommerzielle Computersoftware gemäß FAR 12.212 und unterliegen den eingeschränkten Rechten gemäß FAR, Abschnitt 52.227-19 "Commercial Computer Software - Restricted Rights" und DFARS 227.7202 ff "Commercial Computer Software and Commercial Computer Software Documentation" sowie etwaigen Nachfolgebestimmungen, ob von Veritas als "On Premises-" oder gehostete Dienste bereitgestellt. Jede Verwendung, Modifikation, Reproduktionsversion, Vorführung, Vorstellung oder Offenlegung der lizenzierten Software und Dokumentation seitens der US-amerikanischen Regierung darf ausschließlich in Übereinstimmung mit den Bestimmungen dieser Vereinbarung erfolgen.

Veritas Technologies LLC.
2625 Augustine Drive.
Santa Clara, CA 95054

<http://www.veritas.com>

Technischer Support

Der technische Support unterhält global Support-Center. Primäre Aufgabe des technischen Supports ist es, spezifische Fragen zu Produktmerkmalen und -funktionen zu beantworten. Der technische Support erstellt auch den Inhalt für die Online-Supportdatenbank. Der technische Support arbeitet mit den anderen Funktionsbereichen innerhalb der Firma zusammen, um Ihre Fragen rechtzeitig zu beantworten.

Es stehen folgende Support-Angebote zur Verfügung:

- Eine Vielzahl von Support-Optionen, mit denen Sie den entsprechenden Servicebedarf für Unternehmen aller Größen flexibel auswählen können.
- Telefon- und/oder Web-Support, der schnelle Antworten und aktuelle Informationen zur Verfügung stellt
- Upgrade-Zusicherung, die Software-Upgrades liefert
- Globaler Support, der basierend auf regionalen Geschäftsstunden oder einer Rund-um-die-Uhr-Basis bezogen werden kann
- Premium-Dienstleistungsangebote, die Account Management Services umfassen

Informationen zum Supportangebot finden Sie auf unserer Website:

www.veritas.com/support

Alle Supportleistungen werden in Übereinstimmung mit Ihrem Supportvertrag und der jeweils geltenden Richtlinie für technischen Support für Unternehmen erbracht.

Technischer Support

Kunden mit einem aktuellen Supportvertrag können unter folgender URL auf Informationen zugreifen:

www.veritas.com/support

Bevor Sie sich an den technischen Support wenden, prüfen Sie, ob die in der Produktdokumentation aufgeführten Systemanforderungen erfüllt sind. Außerdem sollten Sie auf den Computer zugreifen können, auf dem das Problem auftrat, falls es nötig ist, das Problem erneut zu provozieren.

Halten Sie folgende Informationen bereit:

- Produktversion
- Hardware-Daten
- Arbeitsspeicher, Speicherplatz und NIC
- Betriebs-system

- Version und Patch-Level
- Netzwerktopologie
- Router, Gateway und IP-Adresse
- Problembeschreibung:
 - Fehlermeldungen und Protokolldateien
 - Fehlerbehebung, die durchgeführt wurde, bevor Sie sich an den technischen Support wandten
 - Aktuelle Änderungen an Softwarekonfiguration und Netzwerk

Lizenzierung und Registrierung

Wenn Ihr Produkt Registrierung oder einen Lizenzschlüssel erfordert, rufen Sie die Website des technischen Support unter folgender URL auf:

www.veritas.com/support

Kundenservice

Informationen zum Kundenservice finden Sie unter folgender URL:

www.veritas.com/support

Der Kundenservice kann bei nicht-technischen Fragen helfen. Beispiele:

- Fragen zu Produktlizenzen und -seriennummern
- Aktualisieren persönlicher Angaben wie Anschrift und Name
- Allgemeine Produktinformationen (Funktionen, verfügbare Sprachen, lokale Anbieter)
- Neueste Informationen zu Produkt-Updates und -Upgrades
- Informationen zu Upgrade-Versicherung und Support-Verträgen
- Optionen für den technischen Support
- Nichttechnische Fragen zu vertriebsvorbereitenden Maßnahmen
- Probleme mit CDs, DVDs oder Handbüchern

Supportvertragsressourcen

Wenn Sie sich bezüglich eines vorhandenen Supportvertrags an uns wenden möchten, wenden Sie sich an das Team für Ihre Region:

Weltweit (ausgenommen Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

Inhalt

Technischer Support	4	
Kapitel 1	Einführung in Backup Exec	40
	Info zu Backup Exec	40
	Funktionsweise von Backup Exec	40
Kapitel 2	Installation	43
	Info zum Installieren von und den Lizenzierungsoptionen für Backup Exec	44
	Backup Exec - Vorinstallations-Checkliste	46
	Ausführen der Umgebungsprüfung vor Installation oder Upgrade von Backup Exec	48
	Microsoft SQL Server Express Edition-Komponenten, die mit Backup Exec installiert worden sind	50
	Systemanforderungen für Backup Exec	51
	Installieren von Backup Exec mithilfe des Installationsassistenten	55
	Installieren zusätzlicher Agents und Funktionen auf dem lokalen Backup Exec-Server	66
	Installieren von Backup Exec auf Remote-Computern über die Push-Installation	68
	Methoden für die Installation von Agent for Windows	77
	Installieren von Agent for Windows auf Remote-Computern über eine Push-Installation	78
	Updates für den Agent for Windows auf Remote-Computern installieren	84
	Installation von Agent for Windows in einem Active Directory-Netzwerk	87
	Installieren von Agent for Windows auf einem Remote-Computer über eine Eingabeaufforderung	92
	Installieren von Agent for Windows mithilfe eines Befehlsskripts	95
	Installieren von Remote Administrator	96
	Installieren von Remote Administrator über die Befehlszeile	98
	Ausführen des Remote Administrator	100

Installieren von Backup Exec über die Befehlszeile (Silent-Mode)	103
Befehlszeilen-Switches für die Installation von Backup Exec im Silent-Mode	104
Installationsparameterdateien erstellen und einsetzen	111
Info zum Installationsprotokoll	113
Anzeigen des Installationsübersichtsberichts	113
Reparieren von Backup Exec	114
Aktualisieren von Backup Exec mit Veritas Update	115
Anzeigen installierter Aktualisierungen	117
Deinstallieren von Backup Exec	118
Anzeigen von Lizenzinformationen	118
Backup Exec-Lizenzvertragsinformationen	119
Aktualisieren von abgelaufenen Wartungsverträgen	119
Verwalten von Lizenzvertragskundennummern	120
Infos zum Aktualisieren von Backup Exec	121
Upgrade-Checkliste für Backup Exec	124
Verwenden des Migrationsberichts, um zu bestimmen, wie sich vorhandene Aufträge nach einem Upgrade von einer früheren Version von Backup Exec geändert haben	125
Aufgaben nach der Installation	126
Deinstallieren von Backup Exec	127
Deinstallieren von Backup Exec mit der Befehlszeile	128
Deinstallieren der Backup Exec-Funktionen vom lokalen Backup Exec-Server	128

Kapitel 3	Erste Schritte	130
	Info zur Backup Exec-Administratorkonsole	130
	Herstellen einer Verbindung mit Veritas SaaS-Backup	134
	Anzeigen der Versionshinweise für Backup Exec	134
	Sperrern und Freigeben der Backup Exec-Konsole	134
	Sortieren, Filtern und Kopieren von Informationen in der Backup Exec-Administratorkonsole	135
	Anpassen von Ansichten in der Backup Exec-Administratorkonsole	139
	Konfigurieren der Registerkarte "Startseite"	139
	Konfigurieren des RSS Reader	147
	Erstellen eines Plans für die Notfallwiederherstellung (DPP)	148
	Erste Schritte mit Backups	151

Kapitel 4	Backups	153
	Vorbereitung für Ihr erstes Backup mit Backup Exec	155
	Verbessern von Backups in Backup Exec	156

Fehlerbehebung bei der Backup-Leistung	160
Erforderliche Benutzerrechte für Backup-Aufträge	165
Serverliste auf der Registerkarte "Backup und Wiederherstellung"	166
Hinzufügen von zu sichernden Servern zur Serverliste auf der Registerkarte "Backup und Wiederherstellung"	167
Entfernen eines Servers aus der Serverliste auf der Registerkarte "Backup und Wiederherstellung"	168
Erstellen einer Servergruppe	168
Ein- bzw. Ausblenden von Servergruppen auf der Registerkarte "Backup und Wiederherstellung"	170
Hinzufügen von Servern zu einer Servergruppe	170
Entfernen von Servern aus einer Servergruppe	171
Bearbeiten einer Servergruppe	171
Verschieben von Servern in die Gruppe "Ausrangierte Server"	172
Verschieben von ausrangierten Servern in die Gruppe "Alle Server"	173
Entfernen von Servergruppen aus Backup Exec	173
Sichern von Daten	174
Infos zum Sichern von Datenträgern, für die unter Windows die Deduplizierung aktiviert ist	184
Sichern und Wiederherstellen von Dateien der virtuellen Festplatte (VHD) von Microsoft in Backup Exec	185
Info zum Auswählen von zu sichernden Daten	186
Ändern der Reihenfolge, in der Backup-Quellen gesichert werden	192
Ausschließen von Dateien von Backups	195
Einschließen spezifischer Dateien mit der Backup-Auswahl eines Backup-Auftrags	198
Info zum Sichern von wichtigen Systemkomponenten	200
Shadow Copy-Dateisystemkomponenten von Backup Exec	204
Backup-Methoden in Backup Exec	205
Konfigurieren von Backup-Methoden für Backup-Aufträge	215
Ermittlung des Backup-Status von Dateien in Backup Exec	218
Konfigurieren von Backup Exec, um Dateien nach einem Backup automatisch zu löschen	222
Konfigurieren erweiterter Optionen für Backup-Aufträge	223
Ausführen des nächsten geplanten Backup-Auftrags vor seiner geplanten Zeit	225
Bearbeiten von Backup-Definitionen	226
Prüfung der Identifikationsdaten für Backup-Quellen	234
Ersetzen der Identifikationsdaten für eine Backup-Quelle	235
Erstellen neuer Identifikationsdaten für eine Backup-Quelle	236

Löschen ausrangierter oder nicht genutzter Backup-Quellen aus dem Teilfenster "Identifikationsdaten"	238
Wie die Joborganisation in Backup Exec arbeitet	239
Einschließen ein spezifisches Datum im Zeitplan für einen Backup-Auftrag	240
Durchführung von Backup-Aufträgen zu einem bestimmten Datum verhindern	242
Anzeigen aller geplanten Backup-Aufträge im Kalender	243
Hinzufügen einer Stufe zu einer Backup-Definition	244
Bearbeiten von Stufen	245
Manuelles Duplizieren von Backup-Sätzen bzw. Auftragsverläufen	246
Manuelle Ausführung von Probelaufaufträgen	251
Gesicherte Daten manuell überprüfen	252
Kopieren von Daten von einer virtuellen Bandbibliothek auf ein physisches Bandgerät mit DirectCopy	255

Kapitel 5

Wiederherstellungen	257
Methoden für das Wiederherstellen von Daten in Backup Exec	258
Suchen nach Daten zum Wiederherstellen	260
Wiederherstellen von Daten aus einem Server, einem Backup-Satz, einem Backup-Auftrag oder einem Speichergerät	261
Wiederherstellen von Dateisystemdaten	265
Vollständige Online-Wiederherstellung eines Microsoft Windows-Computers	267
Wiederherstellen des Systemstatus	268
Installieren eines Windows Server-Domänencontrollers in einer vorhandenen Domäne durch die Anwendung einer umgeleiteten Wiederherstellung	272
Wiederherstellen der Shadow Copy-Komponenten von Backup Exec	274
Wiederherstellen von Dienstprogrammpartitionen oder Unified Extensible Firmware Interface-Systempartition	275
Informationen zum Wiederherstellen verschlüsselter Daten	276
Info zur Wiederherstellung von NetWare SMS-Datenträger-Backups auf andere als SMS-Datenträger mit Backup Exec	277
Abbrechen eines Wiederherstellungsauftrags	277
Funktionsweise der Backup Exec-Kataloge	277
Konfigurieren der Standardoptionen für Kataloge	279
Verschieben der Backup Exec-Kataloge in einen neuen Ordner	283
Katalogisieren von Backup-Sätzen	284

Kapitel 6	Verwalten und Überwachen von Aufträgen	286
	So überwachen und verwalten Sie Aufträge in Backup Exec	286
	Informationen zur Auftragsüberwachung	289
	Anzeigen der Details zur Auftragsaktivität für aktive Aufträge	290
	Abbrechen eines aktiven Auftrags	291
	Aufträge anhalten	292
	Aufheben der Wartestellung von Aufträgen	294
	Anhalten der Auftragswarteschlange	295
	Fortsetzen einer angehaltenen Auftragswarteschlange	296
	Sofortiges Ausführen von geplanten Aufträgen	297
	Ändern der Priorität für geplante Aufträge	297
	Löschen von geplanten Aufträgen	299
	Wiederholen nur fehlgeschlagener Aufträge	300
	Führen Sie den Backup-Auftrag mit aktiviertem Debugging aus	301
	Informationen zum Auftragsverlauf	302
	Anzeigen des Verlaufs eines Auftrags	303
	Löschen eines Auftrags aus dem Auftragsverlauf	304
	Ausführen eines Auftrags über den Auftragsverlauf	305
	Wiederholt nur fehlgeschlagener Aufträge aus dem Auftragsverlauf	306
	Führen Sie den Backup-Auftrag mit aktiviertem Debugging im Auftragsverlauf aus.	307
	Anzeigen des Auftragsprotokolls	308
	Suchen nach Text im Auftragsprotokoll	309
	Drucken des Auftragsprotokolls	311
	Speichern des Auftragsprotokolls	312
	Verknüpfung des Auftragsprotokolls mit der Website des technischen Supports von Veritas	313
	So verwendet man Auftragsprotokolle mit vertikalen Anwendungen	314
	Konfigurieren von standardmäßigen Auftragsprotokolloptionen	314
	Fehlerbehandlungsregeln für fehlgeschlagene oder abgebrochene Aufträge	316
	Erstellen einer benutzerdefinierten Fehlerbehandlungsregel	317
	Aktivieren oder Deaktivieren von Fehlerbehandlungsregeln	318
	Löschen einer benutzerdefinierten Fehlerbehandlungsregel	319
	Aktivieren einer Fehlerbehandlungsregel für einen fehlgeschlagenen Auftrag	319
	Benutzerdefinierte Fehlerbehandlungsregel für wiederhergestellte Aufträge	320

Kapitel 7

Info zur Fehlerbehandlungsregel für Cluster-Failover	321
Liste von Auftragsstatus in Backup Exec	322
Festlegen von Auftragsstatus- und Wiederherstellungsoptionen	330
Warnmeldungen und Benachrichtigungen	333
Warnmeldungen und Benachrichtigungen in Backup Exec	334
Warnmeldungen in Backup Exec	336
Aktivieren der Anzeige aktiver Warnmeldungen und des	
Warnmeldungsverlaufs auf der Registerkarte "Startseite"	338
Eigenschaften für aktive Warnmeldungen	339
Anzeigen des Warnmeldungsverlaufs für einen Server oder ein	
Speichergerät	340
Löschen einer Warnmeldung aus dem Warnmeldungsverlauf	340
Kopieren der Warnmeldung in ein Dokument oder eine E-Mail	341
Filtern von Warnmeldungen	342
Anzeigen des Auftragsprotokolls für Warnmeldungen	343
Reagieren auf aktive Warnmeldungen	343
Manuelles Löschen aller Informationsmeldungen	344
Einrichten von Benachrichtigungen für Warnmeldungen	344
Konfigurieren von E-Mail- oder SMS-Benachrichtigungen für	
Warnmeldungen	345
Hinzufügen von Empfängern für die Benachrichtigung	348
Hinzufügen einer Empfängergruppe für Warnmeldungen	351
Entfernen eines Empfängers aus einer Gruppe	351
Deaktivieren von Warnmeldungen per E-Mail oder SMS für einen	
Empfänger	352
Bearbeiten der Benachrichtigungseigenschaften für Empfänger	353
Löschen von Empfängern	353
Konfigurieren von Warnmeldungskategorien	354
Zuweisen von bestimmten Warnmeldungskategorien an bestimmte	
Empfänger	356
Senden einer Benachrichtigung beim Abschluss eines Auftrags	357
Benachrichtigungsoptionen für Aufträge	357
Deaktivieren von Benachrichtigungen für eine bestimmte	
Meldungskategorie	358
Konfigurieren von Standardeinstellungen für Warnmeldungen	359
Aktivieren oder Deaktivieren von Popup-Warnmeldungen	361
SNMP-Traps für Backup Exec-Warnmeldungen	361
Installieren und Konfigurieren des SNMP-Systemdienstes	364
Installieren der Leistungszähler-Provider der	
Windows-Verwaltungsinstrumentation	365

Installieren des Windows-Verwaltungsinstrumentation-Providers für SNMP	365
Deinstallieren des WMI-Leistungszähler-Providers	366
Deinstallieren des Windows-Verwaltungsinstrumentation-Providers für SNMP	366

Kapitel 8	Plattenbasierter und netzwerkbasierter Speicher	367
	367
	Funktionen und Typen des plattenbasierten und netzwerkbasierten Speichers	367
	Speichertrendanalysestatus für Plattenspeicher und virtuelle Datenträger	369
	Festlegen von Schwellenwerten für geringen Speicherplatz auf plattenbasierten Speichern	371
	Konfigurieren von Festplattenspeicher	372
	Ändern des Speicherorts für ein Datenträgerspeichergerät	375
	Bearbeiten der Eigenschaften von Festplattenspeichern	376
	Wiederherstellen von Daten von einem erneut verbundenen oder eingelekten, plattenbasierten Speichergerät	383
	Konfigurieren des Plattenkassettenspeichers	384
	Bearbeiten der Eigenschaften von Festplattenkassetten	385
	Bearbeiten der Eigenschaften von Plattenkassetten	391
	Löschen abgelaufener Backup-Sätze auf plattenbasiertem Speicher durch Data Lifecycle Management (DLM)	393
	Backup-Sätze	401
	Ändern des Ablaufdatums von Backup-Sätzen auf plattenbasierten Speichergeräten	404
	Aufbewahren von Backup-Sätzen auf plattenbasierten Speichergeräten zum Vermeiden des Ablaufens	406
	Freigeben aufbewahrter Backup-Sätze auf plattenbasierten Speichergeräten	407
	Anzeigen des Inhalts oder der Eigenschaften von Backup-Sätzen	408

Kapitel 9	Cloud-basierte Speichergeräte	410
	Info zu Cloud-basierten Speichergeräten	410
	Cloud-Speicher von Amazon S3	411
	Anforderungen für die Konfiguration eines Cloud-basierten Speichers für Amazon S3	411
	Konfigurieren des Amazon-Cloud-Speichers	412
	Cloud-Speicher von Google	414

Anforderungen für die Konfiguration von Cloud-basierten	
Google-Speichergeräten	414
Konfigurieren des Speichers für Google Cloud Storage	415
Cloud-Speicher von Microsoft Azure	417
Anforderungen für die Konfiguration des Cloud-basierten	
Speichergeräts Microsoft Azure	417
Konfigurieren des Speichers für Microsoft Azure Cloud Storage	
.....	418
Privater Cloud-Speicher	420
Anforderungen für das Konfigurieren von privaten Cloud-basierten	
Speichergeräten	420
Erstellen einer Cloud-Instanz für eine private Cloud	422
Konfigurieren des Speichers für ein privates Cloud-basiertes	
Speichergerät	423
Anzeigen und Bearbeiten vorhandener Cloud-Instanzen für eine	
private Cloud	424
Löschen einer Cloud-Instanz für eine private Cloud	425
Informationen zu S3-kompatiblen Cloud-Speicher	426
Konfigurieren des S3-kompatiblen Cloud-Speichers mit Backup	
Exec	427
Bearbeiten der Eigenschaften eines Cloud-basierten Speichergeräts	
.....	428
Best Practices beim Einsatz von Cloud-basiertem Speicher	431
Ändern der Standardeinstellungen für Cloud-Speicher	432
Info zu Backup Exec™ CloudConnect Optimizer	434
Konfigurieren von Backup Exec™ CloudConnect Optimizer	435

Kapitel 10	Veraltete Backup-to-Disk-Ordner	439
	Veraltete Backup-to-Disk-Ordner	439
	Den Namen oder die Beschreibung eines veralteten	
	Backup-to-Disk-Ordners ändern	440
	Ändern der Einstellung für gepufferte Lesevorgänge für einen	
	veralteten Backup-to-Disk-Ordner	441
	Ändern des Speicherorts eines älteren Backup-to-Disk-Ordners	
	441
	Erneutes Erstellen eines veralteten Backup-to-Disk-Ordners	
	einschließlich des Inhalts	442
	Wiederherstellen von Daten aus einem veralteten	
	Backup-to-Disk-Ordner	443

Kapitel 11	Bandspeicher	446
	Support für Bandlaufwerke und Wechsler	447
	Hinzufügen oder Ersetzend von Geräten durch den Assistent für Hot Swap-Geräte	447
	Installieren von Bandgerätetreibern	449
	Bearbeiten von Bandlaufwerkseigenschaften	450
	Anzeigen von Statistiken zu Bandlaufwerken	457
	Wechsler in Backup Exec	457
	Anforderungen zum Einrichten der Wechsler-Hardware	458
	Inventarisieren von Wechslern beim Starten der Backup Exec-Dienste	459
	Barcoderegeln für einen Wechsler konfigurieren	459
	Initialisieren eines Wechslers beim Starten des Backup Exec-Dienstes	464
	Festlegen eines Reinigungsschachts	465
	Wechslerseigenschaften bearbeiten	465
	Erstellen von Wechslerpartitionen	466
	Bandlaufwerke in einer Wechslerpartition hinzufügen oder entfernen	468
	Erneute Zuweisung einer Schacht-Basisnummer für Wechsler	469
	Bearbeiten der Eigenschaften von Wechslerschächten	469
	Entfernen oder erneutes Konfigurieren von Wechslerpartitionen	470
	Verwalten von Bändern	472
	Standard-Mediensätze	473
	Überschreibschutzzeiträume und Anhängezeiträume in Mediensätzen	476
	Erstellen von Mediensätzen für Bänder	480
	Ändern des Überschreibschutz- oder Anhängezeitraums für einen Mediensatz	483
	Ändern des Namens und der Beschreibung eines Mediensatzes	485
	Ändern des Medienspeicher oder der Vaulting-Zeiträume für einen Mediensatz	485
	Löschen eines Mediensatzes	486
	Umbenennen eines Mediensatzes	487
	Medienüberschreibschutzstufen für Bandmedien	487
	Überschreiben der zugeordneten oder importierten Bandmedien	488
	So sucht Backup Exec nach überschreibbaren Medien in Bandlaufwerken	488

Anzeigen von Bändern, die von einem Auftrag genutzt werden	491
Kennzeichnen von Bandmedien	492
Info zum Kennzeichnen von importierten Bandmedien	494
So werden Barcodebezeichnungen Medienkennungen für Bänder	494
Umbenennen einer Bandmedienkennung	495
So werden WORM-Medien in Backup Exec verwendet	495
Standardmedienspeicher	496
Ändern des Namens oder der Beschreibung eines Medienspeichers	498
Erstellen von Medienspeicherregeln zum Verschieben von Speichermedien in und aus Medienspeichern	499
Aktualisieren des Bandmedienspeicherorts in Medienspeichern	500
Löschen eines Medienspeichers	500
Verschieben von Bandmedien in einen Speicher	501
Ausrangieren beschädigter Bandmedien	501
Löschen von Bandmedien	502
Band- oder Datenträgermedien löschen	502
Info zum Katalogisieren von Band- oder Plattenspeichermedien, die verschlüsselte Backup-Sätze enthalten	505
Verknüpfen von Bandmedien mit einem Mediensatz	505
Bearbeiten von Bandmedieneigenschaften	506
Rotationsstrategien für Bandmedien	508

Kapitel 12	Speichergerätepools	512
	Erstellen von Speichergerätepools	512
	Festlegen einer Standard-Auswahlmethode für ein Gerät in einem Speichergerätepool	515
	Anzeigen von Aufträgen, Auftragsverläufen und aktiven Warnmeldungen für einen Speichergerätepool	516
	Hinzufügen und Entfernen von Geräten in einem Speichergerätepool	517

Kapitel 13	Speichervorgänge	518
	Info zu Speicheraufträgen	519
	Übersicht über die Registerkarte "Speicher" in Backup Exec	520
	Verwenden des Assistenten "Speicher konfigurieren"	523
	Anzeigen von Details für mehrere Speichergeräte	526
	Senden einer Benachrichtigung beim Abschließen eines geplanten Speicherauftrags	526

Einen Speicherauftrag planen	527
Bearbeiten globaler Einstellungen für Speicher	535
Freigeben von Speichergeräten	544
Löschen von Speichergeräten	546
Ändern des Status eines Speichergeräts in "Online"	547
Umbenennen von Speichergeräten	547
Anzeigen von Aufträgen, Auftragsverläufen, Backup-Sätzen und aktiven Warnmeldungen für Speichergeräte	548
Katalogisieren eines Speichergeräts	548
Scannen eines Speichergeräts	549
Inventarisieren eines Speichergeräts	550
Inventarisieren und Katalogisieren von Speichergeräten	552
Ein Speichergerät anhalten und wieder starten	552
Deaktivieren und Aktivieren eines Speichergeräts	553
Initialisieren eines Wechslers	553
Formatieren eines Bands als WORM-Band	553
Spannen eines Bands	554
Formatierung eines Bandes in einem Bandlaufwerk	554
Auswerfen von Medien aus einer Plattenkassette oder einem Bandlaufwerk	555
Reinigen eines Wechslerlaufwerks	556
Importieren von Medien in Backup Exec	558
Exportieren von Medien und abgelaufenen Medien	566
Sperren und Freigen des vorderen Ladeschachts	569
Status von Backup Exec-Servern und Speichergeräten	576
So sehen Sie den Status des Sperrmodus für die Datenträgerspeicherung	579

Kapitel 14	Konvertierung in virtuelle Computer	581
	Funktionsweise der Konvertierung eines physischen Computers in einen virtuellen in Backup Exec	581
	Anforderungen für die Konvertierung in Aufträge für virtuelle Computer	590
	Gleichzeitig mit Backup-Auftrag in virtuellen Computer konvertieren	592
	Konvertierung in virtuellen Computer nach Backup-Auftrag	599
	Hinzufügen einer Konvertierung in eine virtuelle Computer-Phase zu einem Backup-Auftrag	607
	Konvertieren in einen virtuellen Computer von einem Zeitpunkt	614
	Erstellen einer einmaligen Konvertierung in einen virtuellen Computer	616

	Einstellungsstandardoptionen für die Konvertierung in Aufträge für virtuelle Computer	623
Kapitel 15	Konfiguration und Einstellungen	628
	Ändern der Standardeinstellungen für Backup-Aufträge	630
	Konfigurieren von Zeitplänen für Backup-Jobs	635
	Konfigurieren von Speicheroptionen für Backup-Aufträge	645
	Konfigurieren automatischer Testlaufaufträge für Backup-Aufträge	653
	Konfigurieren der automatischen Prüfung von Aufträgen	655
	Konfigurieren der Optionen für Instant GRT und Vollständige Katalogisierung zum Verbessern der Backup-Leistung von GRT-Aufträgen	656
	Konfigurieren von Advanced Open File-Optionen für Backup-Aufträge	664
	Konfigurieren der Auftragswiederaufnahme	667
	Konfigurieren von Befehlen vor oder nach Backup-Aufträgen	670
	Konfigurieren von Datei- und Ordneroptionen für Backup-Aufträge	676
	Standardmäßige Zeitplanoptionen für richtliniengesteuerte Aufträge und für Aufträge zum sofortigen Ausführen einstellen	685
	Ausschließen von Tagen vom Backup-Zeitplan für alle Backups	688
	Entfernen von Daten aus der Liste ausgeschlossener Tage	690
	Exportieren einer Liste von Daten, die aus allen Backups auf einem anderen Server ausgeschlossen sind	691
	Ändern der Standardeinstellungen	692
	Konfigurieren der Standardeinstellungen zum Sichern mehrerer Server oder Anwendungen	693
	Konfigurieren der Datenbankverwaltung und -sicherheit	694
	Exportieren des Backup Exec-Datenbankverschlüsselungscodes	698
	Aktualisieren von Backup Exec-Datenbankverschlüsselungscodes	700
	Konfigurieren der Verschlüsselung für die Verbindung zur Backup Exec-Datenbank	702
	Planen der Prüfung von Login-Konten durch Backup Exec	706
	Konfigurieren von Backup Exec, um Daten für Backup zu suchen	708
	Hinzufügen gefundener Server zur Liste von Servern in Backup Exec	710
	Backup-Netzwerke	711
	Netzwerk- und Sicherheitsoptionen für Backup Exec ändern	713
	Deaktivieren des Sperrmodus für Datenträgerspeicherung	721

Verwendung von Backup Exec mit Firewalls	722
Backup Exec-Anschlüsse	724
Backup Exec-Listener-Ports	726
Infos zum Aktivieren einer SQL-Instanz hinter einer Firewall	727
Verwendung von Verschlüsselung mit Backup Exec	727
Verwaltung von Verschlüsselungscodes	731
Erstellen von Verschlüsselungscodes	732
Ersetzen eines Verschlüsselungscodes	733
Löschen des Verschlüsselungsschlüssels	736
Granular Recovery Technology	737
Festlegen von Standardoptionen für Granular Recovery Technology	
festlegen (GRT)	744
DBA-initiierte Auftragsvorlagen	746
Erstellen DBA-initiierten Auftragsvorlagen	746
Bearbeiten von von DBA gestarteten Auftragsvorlagen	747
Löschen von DBA-initiierten Auftragsvorlagen	748
Speicheroptionen für von DBA gestartete Aufträge	748
Allgemeine Optionen für DBA-initiierte Aufträge	753
Netzworkoptionen für DBA-initiierte Aufträge	753
Duplizieren von Auftragseinstellungen für DBA-initiierte Aufträge	
.....	755
Konfigurieren der Einstellungen für Veritas™ Information Map	759
Backup Exec-Login-Konten	762
Erstellen von Backup Exec-Login-Konten	766
Bearbeiten von Backup Exec-Login-Konten	768
Ändern des Kennworts für ein Backup Exec-Login-Konto	770
Ersetzen von Backup Exec-Login-Konten	770
Löschen von Backup Exec-Login-Konten	771
Ändern des Backup Exec-Standard-Login-Kontos	772
Erstellen von neuen Backup Exec-System-Login-Konten	773
Kopieren von Login-Konto-Informationen auf einen anderen	
Backup Exec-Server	774
Testen von Login-Konten	775
Starten und Anhalten von Backup Exec-Diensten	776
Ändern der Identifikationsdaten für ein Dienstkonto	777
Ändern der Startoptionen für Backup Exec-Dienste	778
Konfigurieren von Überwachungsprotokollen	779
Anzeigen des Überwachungsprotokolls	780
Entfernen von Einträgen aus dem Überwachungsprotokoll	781
Speichern eines Überwachungsprotokolls in einer Textdatei	781
Kopieren von Konfigurationseinstellungen auf einen anderen Backup	
Exec-Server	782
Anzeigen von Servereigenschaften	783

Kapitel 16

Konfigurieren der Standardeinstellungen für das Backup	785
Berichte	792
Berichte in Backup Exec	792
Einen Bericht jetzt ausführen	794
Planen eines Berichts	794
Erstellen eines benutzerdefinierten Berichts	796
Hinzufügen oder Entfernen von Feldern für einen benutzerdefinierten Bericht	802
Ändern der Filter für einen benutzerdefinierten Bericht	802
Ändern der Art, wie Daten in einem benutzerdefinierten Bericht gruppiert oder sortiert werden	805
Ändern der Diagrammoptionen in den benutzerdefinierten Berichten	806
Vorschau von benutzerdefinierten Berichten	807
Kopieren eines benutzerdefinierten Berichts	807
Speichern eines Berichts	808
Drucken eines Berichts in der Backup Exec-Berichtsanzeige	809
Anzeigen abgeschlossener Berichte	810
Bearbeiten eines Berichts	810
Erneutes Ausführen eines abgeschlossenen Berichts	810
Löschen eines Berichts	811
Festlegen der Standards für Standard- und benutzerdefinierte Berichte	811
Anzeigen der Berichtseigenschaften	813
Liste von Backup Exec-Standardberichten	814
Bericht "Meldungsverlauf"	819
Bericht "Warnmeldungsverlauf nach Backup Exec-Server"	820
Bericht "Überwachungsprotokoll"	821
Bericht "Erfolgsrate von Backup-Aufträgen"	821
Bericht "Backup-Empfehlungen"	822
Bericht "Erfolgsrate des Backups von Ressourcen"	822
Bericht "Backup-Sätze nach Mediensatz"	823
Bericht "Backup-Umfang nach Ressourcen geordnet"	824
Bericht "Cloud-Speicherübersicht"	824
Bericht "Täglicher Geräteinsatz"	825
Bericht "Zusammenfassung zu Deduplizierungsgeräten"	826
Bericht "Zusammenfassung zur Deduplizierung"	827
Bericht "Gerätezusammenfassung"	827
Bericht "Zusammenfassung zum Datenträgerspeicher"	828
Bericht "Fehlerbehandlungsregeln"	829
Bericht "Ereignisempfänger"	830

Bericht "Fehlgeschlagene Backup-Aufträge"	831
Bericht "Auftragszusammenfassung"	832
Bericht "Verwaltete Backup Exec-Server"	833
Bericht "Medienüberwachung"	834
Bericht "Medienfehler"	835
Bericht "Für Wiederherstellung erforderliche Medien"	836
Bericht "Medienzusammenfassung"	836
Bericht "Medienspeicherinhalt"	837
Bericht "Medien zum Speicher verschieben"	838
Bericht "Vorgangsübersicht"	839
Bericht "Nächtliche Zusammenfassung"	841
Bericht "Problemdateien"	842
Bericht "Kürzlich beschriebene Medien"	842
Validierungsübersicht "Wiederherstellung bereit"	843
Bericht "Kürzlich geschützte Ressourcen"	844
Bericht "Ressourcenrisikoanalyse"	845
Bericht "Wiederherstellungssatz-Details nach Ressource"	845
Bericht "Medium aus Speicher abrufen"	846
Bericht "Wechslerinventar"	847
Bericht "Geplante Serverarbeitslast"	848
Bericht "Verfügbarkeit temporärer Medien"	849
Bericht "Probelaufergebnisse"	849

Kapitel 17	Sofortwiederherstellung in der Cloud	851
	Info zur Sofortwiederherstellung in der Cloud	852
	Überblick über die Registerkarte "Sofortwiederherstellung in der Cloud"	
	in Backup Exec	853
	Anforderungen zum Konfigurieren der Sofortwiederherstellung in der	
	Cloud in Backup Exec	856
	Vorkonfigurationen, die im Azure-Portal abgeschlossen werden müssen	
	856
	Vorbereiten der VMware- bzw. Hyper-V-Infrastruktur	857
	Konfigurieren von Azure-Ressourcen	857
	Anzeigen von Fehlerdetails	860
	Anzeigen der Konfigurationsdetails	860
	Anzeigen der Details zum virtuellen Computer	861
	Manuelles Aktualisieren der Ansicht virtueller Computer	861
	Aktivieren der Replikation virtueller Computer	862
	Verwalten der Replikation von virtuellen Computern	864
	Verwalten des Failover für einen virtuellen Computer	865
	Ändern des Abonnements oder des Recovery Services-Tresors	865
	Vorbereiten einer neuen Infrastruktur	866

	Entfernen einer konfigurierten Azure-Ressource aus Backup Exec	866
	Verlängern des Backup Exec-Zertifikats	867
Kapitel 18	GDPR Guard	869
	Info zu GDPR Guard	869
	Befehle der Backup Exec-Management-Befehlszeile (BEMCLI) zum	
	Importieren und Exportieren	871
	Unterstützte Typen gesicherter Daten	873
	Blockieren des Zugriffs auf gesicherte Elemente	874
	Wiederherstellen blockierter Elemente	875
	Best Practices zum Blockieren des Zugriffs auf gesicherte Elemente	
	mit GDPR Guard	876
Kapitel 19	Fehlerbehebung bei Backup Exec	879
	Fehlerbehebung von Hardware-bezogenen Problemen	880
	Fehlerbehebung auf Wechslern und Bandlaufwerken	883
	Weitere Informationen über Warn- und Fehlermeldungen	889
	Beheben von Fehlern beim Sichern in Backup Exec	889
	Fehlerbehebung bei ausgefallenen Komponenten in einem SAN	892
	Fehlerbehebung bei Offline-Speichergeräten in einem SAN	892
	Suchen von Hardwarefehlern in einem SAN	894
	Zurücksetzen des SAN	895
	Onlineschalten von Speichergeräten nach dem unsicheren	
	Entfernen eines Geräts in einem SAN	896
	Beheben von Fehlern mit der Installation von Backup Exec	897
	Fehlerbehebung beim Blockieren des Zugriffs auf gesicherte Elemente	
	mit GDPR Guard	897
	Fehlerbehebung bei der Sofortwiederherstellung in der Cloud in Backup	
	Exec	900
	Verbesserung der Leistung von Backup Exec	900
	Zugriff auf Veritas Online	901
	Durchsuchen der Veritas-Supportdatenbank	901
	Kontaktieren des technischen Support für Backup Exec	902
	Einsatz des Remote-Support	903
	Verwalten Ihrer Backup Exec-Support-Fälle	903
	Infos zu den BackupExec-Diagnosetools	903
	Ausführen des Hilfe-Tools "Veritas QuickAssist"	904
	Generieren einer Diagnosedatei zur Fehlerbehebung von Backup Exec	
	904
	Befehlszeilenparameter für eine Diagnosedatei	906

Kapitel 20

Ausführen des begather-Dienstprogramms, um Fehler bei Backup Exec-Komponenten auf Linux-Servern zu beheben	909
Verwenden von Backup Exec Debug Monitor zur Fehlerbehebung	910
Informationen zum Backup Exec Debug Tool	910
Verwenden von Backup Exec in Clusterumgebungen	911
Über Backup Exec und Cluster	912
Anforderungen zum Erstellen von Clustern für Backup Exec in einer Microsoft Cluster Server-Umgebung	913
Funktionsweise von Backup Exec in einer Microsoft Cluster Server-Umgebung	914
Voraussetzungen für die Installation von Backup Exec auf einem Microsoft Cluster Server	915
Installieren von Backup Exec auf einem Microsoft Cluster Server	916
Aktualisieren von Backup Exec in einem Microsoft-Cluster	917
Installieren zusätzlicher Backup Exec-Funktionen in einem Microsoft-Cluster	918
Deinstallieren von Backup Exec aus einem Microsoft-Cluster	919
Erstellen von Speichergerätepools für Microsoft Cluster Server	920
Festlegen eines anderen Failover-Knotens	920
Festlegen eines neuen zentralen Administrationsservers in einer Microsoft Cluster Server-Umgebung	922
Konfigurationen für Backup Exec und Microsoft Cluster Server	923
Cluster mit zwei Knoten und lokal angeschlossenen Speichergeräten	924
Cluster mit zwei Knoten und Bandgeräten an einem gemeinsamen SCSI-Bus	925
Konfigurieren eines gemeinsam genutzten SCSI-Busses für Bandgeräte	927
Cluster mit mehreren Knoten in einem Fibre Channel-SAN mit Central Admin Server Feature	929
Verwenden von Central Admin Server Feature mit Microsoft-Clustern und einem SAN	931
Info zur Sicherung von Microsoft Cluster Servern	932
Wiederherstellen von Daten in einem Microsoft Cluster	933
Notfallwiederherstellung eines Clusters	933
Verwenden von Simplified Disaster Recovery zum Vorbereiten einer Notfallwiederherstellung eines Clusters	934

Wiederherstellen von Knoten im Cluster mithilfe von Simplified Disaster Recovery	935
Wiederherstellen von Backup Exec in einem Microsoft-Cluster mithilfe von Simplified Disaster Recovery	936
Wiederherstellen des gesamten Clusters mithilfe der manuellen Notfallwiederherstellung	937
Wiederherstellen der Datendateien des Microsoft Clusters Servers	938
Wiederherstellen von Backup Exec in einem Microsoft-Cluster	938
Manuelles Verbinden zweier Cluster-Datenträgergruppen und Neusynchronisierung der Datenträger	939
Fehlerbehebungs-Cluster	940

Kapitel 21	Simplified Disaster Recovery	941
	Info zu Simplified Disaster Recovery	941
	Anforderungen für die Anwendung von Simplified Disaster Recovery	943
	Vorbereiten von Computern für die Verwendung mit Simplified Disaster Recovery	946
	Sicherstellen, dass Simplified Disaster Recovery für Backups aktiviert ist	950
	Verwendung der Notfallwiederherstellungs-Informationsdateien durch Simplified Disaster Recovery	952
	Festlegen oder Ändern des alternativen Speicherorts für die Notfallwiederherstellungs-Informationsdatei	954
	Ändern des Standardpfads für die Notfallwiederherstellungs-Informationsdateien	955
	Pfad zur Notfallwiederherstellung-Informationsdatei	956
	Erstellen eines SDR-Datenträger-Image	957
	Inhalt des Simplified Disaster Recovery-Datenträger-Image	980
	Benutzerszenarien, wenn ein Benutzer den Assistenten zum Erstellen eines SDR-Datenträgers startet	981
	Sich vorbereiten, um sich von einem Systemausfall durch die Anwendung von Simplified Disaster Recovery zu erholen	983
	Austauschen von Hardware während der Notfallwiederherstellung	985
	Vorbereiten der Wiederherstellung von IBM-Computern mit Simplified Disaster Recovery	986
	Wiederherstellen eines Computers mithilfe von Simplified Disaster Recovery	987

Wiederherstellungshinweise für die Anwendung von Simplified Disaster Recovery in Verbindung mit Speicherpools und Speicherplätzen	995
Hinweise zum Einsatz von Simplified Disaster Recovery mit Exchange, SQL, SharePoint, CAS, Hyper-V-Hosts und Deduplication Feature	999
Erweiterte Datenträgerkonfiguration in Verbindung mit dem Assistenten "Computer wiederherstellen"	1001
Manuelles Ausführen der Notfallwiederherstellung	1005
Durchführen einer manuellen Notfallwiederherstellung eines lokalen Backup Exec-Servers auf einem Windows-Computer	1006
Manuelles Ausführen der Notfallwiederherstellung eines Remote-Backup Exec-Servers oder Remote-Agent auf einem Windows-Computer	1011

Kapitel 22	Integration in Veritas™ Information Map	1017
	Info zu Veritas™ Information Map	1017
	Zusammenarbeit von Backup Exec und Veritas™ Information Map	1018
	Anforderungen für die Integration in Veritas™ Information Map	1018
	Integration von Backup Exec in Veritas™ Information Map	1019
	Unterstützte Datenquellen bei der Integration in Veritas™ Information Map	1022
	Best Practices für die Integration in Veritas™ Information Map	1022
	Tipps zur Fehlerbehebung bei der Integration in Veritas™ Information Map	1023
	Einschränkungen für die Integration in Veritas™ Information Map	1027

Anhang A	Backup Exec Agent for Windows	1028
	Infos zum Agent for Windows	1028
	Anforderungen für Agent for Windows	1029
	Beenden und Starten von Agent for Windows	1030
	Erstellen eines Vertrauensverhältnisses zwischen dem Backup Exec-Server und einem Remote-Computer	1031
	Info zu Backup Exec Remote Agent Utility for Windows	1031
	Starten von Backup Exec Agent Utility	1032
	Anzeigen des Aktivitätsstatus eines Remote-Computers in Backup Exec Agent Utility	1033
	Anzeigen des Aktivitätsstatus von Remote-Computern in der Taskleiste	1033

Automatisches Starten von Backup Exec Agent Utility auf dem Remote-Computer	1034
Festlegen des Aktualisierungsintervalls auf dem Remote-Computer	1034
Info zum Veröffentlichen von Agent for Windows auf den Backup Exec-Servern	1035
Hinzufügen von Backup Exec-Servern, auf denen Agent for Windows Informationen bereitstellen kann	1036
Bearbeiten von Informationen zum Backup Exec-Server, auf den Agent for Windows Informationen bereitstellt	1037
Entfernen von Backup Exec-Servern, auf denen Agent for Windows Informationen bereitstellen kann	1038
Konfigurieren des Datenbankzugriffs für Oracle-Vorgänge	1038
Entfernen eines Sicherheitszertifikats für einen Backup Exec-Server, der Vertrauensverhältnis mit Agent for Windows hat	1040
Verwenden des Befehlszeilen-Applet von Backup Exec Agent Utility	1041
Parameter für das Befehlszeilen-Applet von Backup Exec Agent Utility	1042

Anhang B	Backup Exec Deduplizierungsfunktion	1046
	Info zu Deduplication Feature	1047
	Deduplizierungsmethoden für Backup Exec Agents	1049
	Anforderungen für Deduplication Feature	1051
	Installieren von Deduplication Feature	1056
	Konvertieren einer älteren Version des Deduplizierungsspeichers in eine neuere Version	1056
	Konfigurieren eines OpenStorage-Geräts	1058
	Bearbeiten von Eigenschaften eines OpenStorage-Geräts	1061
	Angabe eines Backup Exec-Servers mit Näherung zu einem gemeinsam genutzten OpenStorage-Gerät	1063
	Erstellen oder Importieren des Deduplizierungsspeichers	1064
	Bearbeiten der Eigenschaften eines Deduplizierungsspeichergeräts	1067
	Ändern des Kennworts für das Login-Konto für Deduplizierungsspeicher	1072
	Wählen von Speichergeräten für die gemeinsame Nutzung über Direktzugriff	1073
	Bearbeiten von Servereigenschaften für den Direktzugriff	1074
	Ändern des Speicherorts für ein Deduplizierungsspeichergerät	1075

Gemeinsames Nutzen eines Deduplizierungsgeräts durch mehrere Backup Exec-Server	1077
Einsatz der clientseitigen Deduplizierung	1078
So werden Backup-Aufträge für die Deduplizierung eingerichtet	1079
Verwenden der optimierten Duplizierung, um deduplizierte Daten zwischen OpenStorage-Geräten oder Deduplizierungsspeichergeräten zu kopieren	1080
Kopieren deduplizierter Daten auf Bänder	1084
Verwendung der Deduplizierung mit Verschlüsselung	1084
Wiederherstellen eines Deduplizierungs-Plattenspeichergeräts oder von deduplizierten Daten	1085
Notfallwiederherstellung des Deduplizierungsspeichergeräts	1085
Notfallwiederherstellung von OpenStorage-Geräten	1087

Anhang C

Backup Exec Agent for VMware	1088
Agent for VMware	1089
Anforderungen für die Verwendung des Agent for VMware	1090
Einsatz des Agent for VMware unter Windows Server 2016 und höher	1091
Installieren von Agent for VMware	1092
Hinzufügen eines VMware vCenter-Servers oder ESX-/ESXi-Host zur Serverliste auf der Registerkarte "Backup- und Wiederherstellung"	1092
Anzeigen von Details zu VMware-Ressourcen	1093
Installieren von Agent for Windows auf virtuellen VMware-Computern	1094
Push-Installation von Agent for Windows auf virtuellen VMware-Computern	1096
Info zum Einrichten einer vertrauenswürdigen Verbindung zu einem vCenter/ESX(i)-Server	1097
Einrichten einer vertrauenswürdigen Verbindung zu einem vCenter/ESX(i)-Server	1098
Empfehlungen dazu, wann virtuelle Backups und wann Backups mit Agent genutzt werden sollten.	1098
Sichern von virtuellen VMware-Computern	1100
Festlegen von Backup-Standardoptionen für virtuelle Computer	1109
Automatisches Sichern neuer virtueller VMware-Computer mit Backup Exec während eines Backup-Auftrags	1115
Verwenden von Granular Recovery Technology (GRT) mit Agent for VMware	1115

So funktioniert die Katalogisierung mit virtuellen Backups über VMware	1120
Wiederherstellen virtueller VMware-Computer und VMDK-Dateien	1121
Info zur Sofortwiederherstellung eines virtuellen VMware-Computers	1131
Anforderungen an die Sofortwiederherstellung eines virtuellen VMware-Computers	1134
Hinweise zur Sofortwiederherstellung eines virtuellen VMware-Computers	1135
Best Practices bei der Sofortwiederherstellung eines virtuellen VMware-Computers	1136
Erstellen eines Auftrags für die Sofortwiederherstellung eines virtuellen VMware-Computers	1137
Entfernen eines sofort wiederhergestellten virtuellen VMware-Computers	1140
Beheben von Fehlern mit dem Agent for VMware	1143
Informationen zur Funktion "Wiederherstellung bereit" für virtuelle VMware-Computer	1143
Anforderungen zum Validieren eines virtuellen VMware-Computers für die Wiederherstellung	1147
Hinweise zur Validierung von virtuellen VMware-Computern für die Wiederherstellung	1148
Best Practices zum Validieren eines virtuellen VMware-Computers für die Wiederherstellung	1149
Erstellen eines Auftrags zum Validieren eines virtuellen Computers für die Wiederherstellung	1149

Anhang D	Backup Exec Agent for Microsoft Hyper-V	1153
	Agent for Microsoft Hyper-V	1154
	Anforderungen für die Verwendung des "Agent for Microsoft Hyper-V"	1156
	Installieren des "Agent for Microsoft Hyper-V"	1159
	Hinweise zum Einsatz des Agent for Hyper-V	1159
	Speicherplatzoptimierung mit Agent for Hyper-V	1162
	Hinzufügen eines Hyper-V-Hosts zur Serverliste auf der Registerkarte "Backup und Wiederherstellung"	1163
	Anzeigen von Details zu Hyper-V-Ressourcen	1164
	Installieren von Agent for Windows auf virtuellen Hyper-V-Computern	1165
	Push-Installation von Agent for Windows auf virtuellen Hyper-V-Computern	1166

Sichern von virtuellen Computern mit Microsoft Hyper-V	1167
Festlegen der Standard- Backup-Optionen für Hyper-V	1175
So schützt Backup Exec automatisch neue virtuelle Computer während eines Backup-Auftrags	1179
Verwenden von Granular Recovery Technology (GRT) mit Agent for Hyper-V	1180
Sichern und Wiederherstellen virtueller Hyper-V-Computer mit hoher Verfügbarkeit	1184
Informationen zu Backups von auf SMB-/Scale-out-Dateiservern gehosteten virtuellen Computern	1184
So funktioniert die Katalogisierung mit virtuellen Backups über Hyper-V	1185
Wiederherstellen von virtuellen Microsoft Hyper-V-Computern	1187
Info zur Sofortwiederherstellung eines virtuellen Hyper-V-Computers	1193
Anforderungen für die Sofortwiederherstellung eines virtuellen Hyper-V-Computers	1199
Hinweise zur Sofortwiederherstellung eines virtuellen Hyper-V-Computers	1200
Erstellen eines Auftrags für die Sofortwiederherstellung eines virtuellen Hyper-V-Computers	1201
Aufgaben nach der Sofortwiederherstellung	1203
Infos zum Entfernen eines sofort wiederhergestellten virtuellen Hyper-V-Computers	1203
Entfernen eines sofort wiederhergestellten virtuellen Hyper-V-Computers	1204
Best Practices bei der Sofortwiederherstellung eines virtuellen Hyper-V-Computers	1207
Informationen zur Funktion "Wiederherstellung bereit" für virtuelle Hyper-V-Computer	1207
Anforderungen zum Validieren eines virtuellen Hyper-V-Computers für die Wiederherstellung	1212
Hinweise zum Validieren eines virtuellen Hyper-V-Computers für die Wiederherstellung	1212
Best Practices beim Validieren eines virtuellen Hyper-V-Computers für die Wiederherstellung	1213
Erstellen eines Auftrags zum Validieren eines virtuellen Computers für die Wiederherstellung	1214
Fehlerbehebung bei Problemen mit Backup Exec Agent for Microsoft Hyper-V	1217

Anhang E	Backup Exec Agent for Microsoft SQL Server	
	1218
	Info zum Agent for Microsoft SQL Server	1218
	Voraussetzungen für die Verwendung des SQL Agent	1220
	Info zum Installieren des SQL Agent	1221
	Backup-Strategien für SQL	1221
	Hinzufügen von SQL-Servern zur Serverliste auf der Registerkarte "Backup und Wiederherstellung"	1223
	Konfigurieren von Backup Exec zum Ausführen einer Konsistenzprüfung vor jedem SQL-Backup	1224
	Verwendung der Snapshot-Technologie mit dem SQL Agent	1225
	Verwenden von Datenbank-Snapshots für SQL-Server	1226
	Sichern von SQL-Datenbanken und Transaktionsprotokollen	1228
	Festlegen der Standard-Backup-Optionen für SQL Server	1244
	SQL-Datenbanken und Transaktionsprotokolle wiederherstellen	1256
	Wiederherstellen der SQL-Master-Datenbank	1259
	Neustarten von SQL unter Verwendung von Datenbankkopien	1260
	Notfallwiederherstellung von SQL Server	1262
	Manuelle Wiederherstellung eines SQL Server	1264
Anhang F	Backup Exec Agent for Microsoft Exchange Server	1266
	Informationen zum Backup Exec Exchange Agent	1267
	Voraussetzungen für die Verwendung des Exchange Agents	1268
	Bewilligen von Berechtigungen auf dem Exchange Server, um Datenbank-Backups und -wiederherstellungen sowie Granular Recovery Technology-Vorgänge zu ermöglichen	1272
	Info zur Installation des Exchange Agent	1277
	Hinzufügen von Exchange-Servern und Datenbankverfügbarkeitsgruppe zur Serverliste auf der Registerkarte "Backup und Wiederherstellung"	1278
	So erstellen Sie bevorzugte Server-Konfigurationen für Microsoft Exchange Database Availability Groups (DAG).	1279
	Für Exchange empfohlene Konfigurationen	1281
	Voraussetzungen für den Zugriff auf Exchange-Postfächer	1283
	Backup-Strategien für Exchange	1284
	Wie Granular Recovery Technology mit dem Exchange-Informationsspeicher funktioniert	1287
	Snapshot-Backups und Backups auf einem anderen Host mit dem Exchange Agent	1288

Sichern von Exchange-Daten	1290
Festlegen von Standard-Backup-Optionen für Exchange Server	1302
Wiederherstellen von Exchange-Daten	1309
Notfallwiederherstellung für Exchange-Server	1316

Anhang G Backup Exec Agent for Microsoft SharePoint 1318

Info zum Microsoft SharePoint-Agent	1318
Installieren des Microsoft SharePoint-Agent	1319
Anforderungen an den Microsoft SharePoint-Agent	1319
Einsatz des Agent for Microsoft SharePoint mit SharePoint Server 2010/2013/2016 und SharePoint Foundation 2010/2013/2016	1320
Hinzufügen einer Microsoft SharePoint-Serverfarm zur Serverliste auf der Registerkarte "Backup- und Wiederherstellung"	1321
Sichern von Microsoft SharePoint-Daten	1322
Festlegen der Standard-Backup-Optionen für SharePoint	1326
Wiederherstellen von Microsoft SharePoint-Daten	1329
Deaktivieren oder Aktivieren der Verbindung zwischen einem Microsoft SharePoint-Webserver und Backup Exec	1332
Anzeigen oder Ändern der Eigenschaften von SharePoint-Farmen	1333
Notfallwiederherstellung von Microsoft SharePoint 2010/2013/2016-Daten	1334

Anhang H Backup Exec Agent for Oracle auf Windows- oder Linux-Servern 1340

Info zu Backup Exec Oracle Agent	1340
Installieren des Oracle Agents	1342
Konfigurieren des Oracle Agent auf Windows-Computern und -Linux-Servern	1342
Konfigurieren einer Oracle-Instanz auf Windows-Computern	1345
Anzeigen einer Oracle-Instanz auf Windows-Computern	1349
Bearbeiten einer Oracle-Instanz auf Windows-Computern	1350
Löschen einer Oracle-Instanz auf Windows-Computern	1350
Aktivieren des Datenbankzugriffs für Oracle-Vorgänge auf Windows-Computern	1351
Konfigurieren einer Oracle-Instanz auf Linux-Servern	1353
Anzeigen einer Oracle-Instanz auf Linux-Servern	1356
Bearbeiten einer Oracle-Instanz auf Linux-Servern	1356
Löschen einer Oracle-Instanz auf Linux-Servern	1357

Aktivieren des Datenbankzugriffs für Oracle-Vorgänge auf Linux-Servern	1358
Informationen zu Authentifizierungsinformationen auf dem Backup Exec-Server	1359
Einstellung von Authentifizierungs-Identifikationsdaten auf dem Backup Exec-Server für Oracle-Vorgänge	1360
Löschen eines Oracle-Servers aus der Liste der Authentifizierungsdaten des Backup Exec-Servers	1362
Info zur Änderung von Informationen der Oracle-Instanz	1362
Sichern von Oracle-Datenbanken	1362
Sichern von Oracle RAC-Datenbanken	1364
Informationen über die Durchführung eines von DBA gestarteten Backup-Auftrags für Oracle	1366
Backup-Optionen für Oracle	1367
Wiederherstellen von Oracle-Ressourcen	1368
DBA-initiierte Wiederherstellungen für Oracle	1371
Wiederherstellungsoptionen für Oracle	1372
Informationen zum Umleiten einer Wiederherstellung von Oracle-Daten	1372
Erweiterte Wiederherstellungsoptionen in Oracle	1373
Ausführen einer umgeleiteten Wiederherstellung einer Oracle 12c-Datenbank unter Verwendung von Backup Exec	1375
Anforderungen zum Wiederherstellen der vollständigen Oracle-Instanz und -Datenbank unter Verwendung des ursprünglichen Oracle-Servers	1379
Wiederherstellen der vollständigen Oracle-Instanz und -Datenbank unter Verwendung des ursprünglichen Oracle-Servers	1380
Anforderungen für die Wiederherstellung der vollständigen Oracle-Instanz oder -Datenbank auf einen anderen als den ursprünglichen Oracle-Server-Computer.	1381
Wiederherstellen der vollständigen Oracle-Instanz oder -Datenbank auf einem anderen als den ursprünglichen Oracle-Server	1381
Best Practices für Backup Exec Agent for Oracle auf Windows- und Linux-Servern	1383

Anhang I	Backup Exec Agent for Enterprise Vault	1387
	Info zu Agent for Enterprise Vault	1387
	Anforderungen für Enterprise Vault Agent	1392
	Installieren von Enterprise Vault Agent	1392
	Info zu Backup-Methoden für Enterprise Vault-Backup-Aufträge	1393
	Backup-Optionen für Enterprise Vault	1397

Info zum Sichern von Enterprise Vault-Komponenten	1397
Konsistenzprüfungen für Enterprise Vault-Datenbanken und Compliance and Discovery Accelerator-Datenbanken	1400
Wiederherstellen von Enterprise Vault	1400
Enterprise Vault-Wiederherstellungsoptionen	1402
Info zum Wiederherstellen einzelner Dateien und Ordner mit Enterprise Vault Agent	1406
Info zur automatischen Umleitung von Enterprise Vault-Komponenten unter einem Enterprise Vault-Server	1407
Umleiten einer Wiederherstellung für eine Enterprise Vault-Komponente	1408
Konfigurieren von Enterprise Vault für die Verwendung des Namens des neuen SQL-Servers mit der Verzeichnisdatenbank	1411
Best Practices für den Enterprise Vault Agent	1412
Info zu Backup Exec Migrator for Enterprise Vault	1413
Anforderungen für Backup Exec Migrator for Enterprise Vault	1413
Funktionsweise des Backup Exec Migrator	1414
Info zur Verwendung gestaffelter Migrationen mit Backup Exec und dem Backup Exec Migrator	1417
Info zu Backup Exec Migrator-Ereignissen	1418
Info zu Backup Exec Migrator-Protokollen	1418
So aktivieren Sie die Backup Exec Migrator-Protokollierung	1420
Info zum Löschen der von Backup Exec Migrator migrierten Dateien	1422
Konfigurieren von Backup Exec Migrator	1423
Info zum Anzeigen migrierter Enterprise Vault-Daten	1431
Info zum Abrufen migrierter Enterprise Vault-Daten	1432
Info über das Dienstprogramm zum Wiederherstellen von Partitionen	1433
Enterprise Vault-Login-Konto	1438
Optionen zu Enterprise Vault	1438

Anhang J

Backup Exec Agent for Microsoft Active Directory

.....	1439
Info zum Agent for Microsoft Active Directory	1439
Anforderungen für Agent for Microsoft Active Directory	1440
Info zum Sichern von Active Directory und ADAM/AD LDS	1441
Optionen für Active Directory und ADAM/AD LDS-Backup-Aufträge bearbeiten	1442
Optionen für Backup-Aufträge von Microsoft Active Directory	1444

Anhang K

Infos zum Wiederherstellen von einzelnen Active Directory- und ADAM/AD LDS-Objekten	1446
Backup Exec Central Admin Serverfunktion	1449
Infos zu Central Admin Server Feature	1450
Anforderungen zum Installieren von CAS	1452
Auswählen des Speicherorts für CAS-Speicher- und Mediendaten	1453
Installieren von Central Admin Server Feature	1455
Push-Installation eines verwalteten Backup Exec-Server vom zentralen Administrationsserver aus	1456
Optionen im Dialogfeld "Verwalteten Backup Exec-Server konfigurieren"	1461
Installieren eines verwalteten Backup Exec-Servers über eine Firewall	1463
Aktualisieren einer vorhandenen CAS-Installation	1466
Umwandlung eines Backup Exec-Servers in einen zentralen Administrationsserver	1468
Umwandlung eines Backup Exec-Servers in einen verwalteten Backup Exec-Server	1469
Löschen eines verwalteten Backup Exec-Servers aus einer CAS-Umgebung	1472
Umbenennen eines zentralen Administrationsservers	1473
Umbenennen eines verwalteten Backup Exec-Servers	1474
Reduzieren des Netzwerkverkehrs in CAS	1475
Mit CAS bereitgestellte, zentralisierte und replizierte Katalogspeicherorte	1476
Ändern der Einstellungen für einen verwalteten Backup Exec-Server	1479
Erreichen der CAS-Kommunikationsschwellenwerte	1491
Aktivieren bzw. Deaktivieren der Kommunikation zwischen dem verwalteten Backup Exec-Server und dem zentralen Administrationsserver	1492
Warnmeldungen und Benachrichtigungen in CAS	1493
Aktivieren verwalteter Backup Exec-Server für die Verwendung einer verfügbaren Netzwerkkarte	1494
Info zur Auftragsdelegierung in CAS	1495
Kopieren von Aufträgen statt Delegieren von Aufträgen in CAS	1495
Info zum Hinzufügen von Speichergeräten in einer CAS-Umgebung	1496

Funktionsweise von Data Lifecycle Management (DLM) in einer CAS-Umgebung	1496
Abrufen von Medienüberwachungsinformationen für einen verwalteten Backup Exec-Server	1497
Verwenden von Backup Exec-Server-Pools in CAS	1498
Auswählen eines Backup Exec-Server-Pools für Backups	1499
Erstellen von Backup Exec-Server-Pools	1500
Hinzufügen verwalteter Backup Exec-Server zu einem Backup Exec-Serverpool	1500
Löschen von Backup Exec-Server-Pools	1501
Entfernen eines verwalteten Backup Exec-Server aus einem Backup Exec-Server-Pool	1501
Funktionsweise der zentralisierten Wiederherstellung in CAS	1501
Funktionsweise der CAS-Wiederherstellung von Daten, die sich auf mehreren Speichergeräten befinden	1503
Info zum Wiederherstellen fehlgeschlagener Aufträge in CAS	1504
Anhalten oder Wiederaufnehmen eines verwalteten Backup Exec-Servers	1507
Beenden oder Starten von Backup Exec-Diensten für einen verwalteten Backup Exec-Server	1508
Anzeigen von verwalteten Backup Exec-Serveigenschaften	1508
Anzeigen der Einstellungen für einen zentralen Administrationsserver	1511
Notfallwiederherstellung in CAS	1513
Fehlerbehebung in CAS	1515
Ausführen von Backup Exec Utility für CAS-Vorgänge	1516
Deinstallieren von Backup Exec vom zentralen Administrationsserver	1517
Deinstallieren von Backup Exec von einem verwalteten Backup Exec-Server	1518

Anhang L

Backup Exec Advanced Disk-based Backupfunktion	1519
Info zum Einsatz von Advanced Disk-based Backup Feature	1519
So verwenden Sie synthetische Backups anstelle von wiederkehrenden vollständigen Backups	1520
Festlegen der Standard-Backup-Optionen für Advanced Disk Based Backup Feature	1522
Infos zur True Image-Wiederherstellung für synthetische Backups	1524
Verwenden von Offhost-Backups zur Verarbeitung von Remote-Computer-Backups auf dem Backup Exec-Server	1527

Konfigurieren von Offhost-Backup-Optionen für einen Backup-Auftrag	1530
Bewährte Methoden für Off-Host-Backup	1532
Fehlerbehebung bei Off-Host-Backups	1533
Off-Host-Backup-Probleme mit Hardwareanbietern	1537

Anhang M	Backup Exec NDMP-Funktion	1538
	Funktionen von NDMP Feature	1539
	Anforderungen für das Verwenden von NDMP Feature	1539
	Info zum Installieren von NDMP Feature	1540
	Hinzufügen von NDMP-Server zu Backup Exec	1540
	Gemeinsames Nutzen des Bandlaufwerks auf NDMP-Servern zwischen mehreren Backup Exec-Servern	1542
	NDMP-Backup-Optionen für NDMP-Server	1543
	Backup-Auswahlen für NDMP-Server	1547
	Verwenden von Mustern zum Ausschließen von Dateien und Verzeichnissen von einem NDMP-Server-Backup	1548
	Unterstützte Konfigurationen für das Duplizieren von Daten aus NDMP-Servern	1549
	Wiederherstellen und Umleiten von Wiederherstellungsdaten für NDMP-Server	1550
	Wiederherstellungsoptionen für NDMP-Server	1551
	Festlegen der Standard-Backup-Optionen für NDMP Feature	1554
	Anzeigen der Eigenschaften eines NDMP-Servers	1556
	NDMP-Servereigenschaften	1556
	Anzeigen von Speichereigenschaften für einen NDMP-Server	1557
	Speichereigenschaften für einen NDMP-Server	1557

Anhang N	Backup Exec Agent for Linux	1559
	Info zu Agent for Linux	1560
	Info zu geöffneten Dateien und Agent for Linux	1560
	Anforderungen für Agent for Linux	1560
	Installieren von Agent for Linux	1561
	Installation von Agent for Linux	1562
	Info zur Backup Exec-Operator-Gruppe (beoper) für den Agent for Linux	1565
	Info zum Festlegen des Vertrauens für einen standortfernen Linux-Computer in der Backup Exec-Liste von Servern	1566
	Festlegen von Vertrauen und Hinzufügen von standortfernen Linux-Computern zur Backup Exec-Liste von Servern	1567
	Hinzufügen zusätzlicher Backup Exec-Server, auf denen Agent for Linux Informationen bereitstellen kann	1567

Info zum Konfigurieren von Agent for Linux	1568
Ausschließen der Dateien und Verzeichnisse von allen Backup-Aufträgen für Linux-Computer	1569
Bearbeiten von Konfigurationsoptionen für Linux-Computer	1570
Konfigurationsoptionen für Linux-Computer	1570
Info zum Sichern eines Linux-Computers durch Verwendung des Agent for Linux	1578
Linux-Backup-Optionen	1579
Infos zum Sichern und Wiederherstellen von Novell Open Enterprise Server(OES)-Komponenten	1580
Info zum Wiederherstellen von Daten auf Linux-Computern	1582
Informationen zum Wiederherstellen von Novell OES-Komponenten	1582
Optionen für Wiederherstellungsaufträge für Linux-Computer	1582
Bearbeiten der Standardoptionen für Backup-Aufträge für Linux-Computer	1584
Standardoptionen für Backup-Aufträge für Linux-Computer	1584
Deinstallieren von Agent for Linux	1586
Manuelles Deinstallieren von Agent for Linux	1587
Beim manuellen Deinstallieren des Agent for Linux zu entfernende Laufzeitskripte	1588
Starten des Agent for Linux-Daemon	1589
Beenden des Agent for Linux-Daemon	1590
Fehlerbehebung für den Agent for Linux	1590

Anhang O

Backup Exec Remote Media Agent for Linux	1597
Info zu Remote Media Agent for Linux	1598
Funktionsweise von Remote Media Agent for Linux	1599
Anforderungen an Remote Media Agent for Linux	1600
Infos zu geöffneten Dateien und Remote Media Agent for Linux	1601
Info zum Installieren von Remote Media Agent for Linux	1601
Installieren von Remote Media Agent for Linux	1602
Deinstallieren von Remote Media Agent for Linux	1605
Starten des Remote Media Agent für Linux-Daemon	1607
Beenden des Remote Media Agent for Linux-Daemon	1607
Info zum Festlegen des Vertrauens für einen Remote Media Agent for Linux-Computer in der Backup Exec-Liste von Servern	1608
Festlegen von Vertrauen und Hinzufügen eines Remote Media Agent for Linux-Computer zur Backup Exec-Liste von Servern	1608

Hinzufügen zusätzlicher Backup Exec-Server, für die Remote Media Agent for Linux veröffentlichen kann	1609
Suchen der Dateien der simulierten Bandbibliothek	1609
Info zur Backup Exec-Operator-Gruppe (beoper) für Remote Media Agent for Linux	1610
Manuelles Erstellen der Backup Exec-Operatorengruppe (beoper) für Remote Media Agent for Linux	1611
Info zum Hinzufügen eines Linux-Servers als Remote Media Agent for Linux	1612
Hinzufügen eines Linux-Servers als Remote Media Agent for Linux	1612
Optionen für den Remote Media Agent for Linux	1612
Ändern des Ports für die Kommunikation zwischen Backup Exec-Server und Remote Media Agent for Linux	1614
Info zum Erstellen von Speichergerätepools für mit Remote Media Agent for Linux verbundene Geräte	1615
Bearbeiten der Eigenschaften von Remote Media Agent for Linux	1616
Eigenschaften von Remote Media Agent for Linux	1616
Löschen eines Remote Media Agent for Linux aus der Backup Exec-Liste von Servern	1617
Gemeinsames Nutzen eines Remote Media Agent for Linux von mehreren Backup Exec-Servern	1617
Info zum Speichern von Daten durch Verwendung des Remote Media Agent for Linux	1618
Info zum Wiederherstellen von Daten mit Remote Media Agent for Linux	1618
Tape Library Simulator Utility	1619
Erstellen einer simulierten Bandbibliothek	1620
Optionen für simulierte Bandbibliotheken	1621
Anzeigen der Eigenschaften von simulierten Bandbibliotheken	1621
Eigenschaften von simulierten Bandbibliotheken	1622
Löschen einer simulierten Bandbibliothek	1623
Verwalten simulierter Bandbibliotheken über die Befehlszeile	1624
Befehlszeilen-Switches für das Tape Library Simulator-Dienstprogramm	1625
Fehlerbehebung in Remote Media Agent for Linux	1625
Anhang P Eingabehilfen und Backup Exec	1628
Info zu Eingabehilfen und Backup Exec	1628
Informationen zu Tastaturkurzbefehlen in Backup Exec	1629
Tastaturkurzbefehle der Registerkarte "Startseite"	1630

Tastaturkurzbefehle für die Registerkarte "Backup und Wiederherstellung"	1631
Tastenkombinationen auf der Registerkarte "Auftragsüberwachung"	1640
Tastaturkurzbefehle der Registerkarte "Speicher"	1644
Tastaturkurzbefehle der Registerkarte "Berichte"	1653
Allgemeine Tastaturnavigation innerhalb der Backup Exec-Benutzeroberfläche	1654
Tastaturnavigation innerhalb der Dialogfelder in Backup Exec	1655
Listenfeldnavigation in Backup Exec	1656
Navigation in Dialogfeldern mit Registerkarten in Backup Exec	1656
Festlegen der Optionen zur Eingabehilfe	1657
Glossar	1658
Index	1665

Einführung in Backup Exec

In diesem Kapitel werden folgende Themen behandelt:

- [Info zu Backup Exec](#)
- [Funktionsweise von Backup Exec](#)

Info zu Backup Exec

Backup Exec ist eine leistungsstarke Datenverwaltungslösung für Windows® Server-Netzwerke. Das Client/Server-Design von Backup Exec ermöglicht schnelles, zuverlässiges Sichern und Wiederherstellen von Daten für alle Server, Anwendungen und Arbeitsstationen im Netzwerk.

Backup Exec ist in mehreren Konfigurationen für Netzwerke verschiedener Größen verfügbar. Darüber hinaus bieten die Agents und Optionen von Backup Exec Lösungen zum Skalieren Ihrer Backup Exec-Umgebung und zum Erweitern der Unterstützung verschiedener Plattformen und Funktionen.

Siehe "[Funktionsweise von Backup Exec](#)" auf Seite 40.

Funktionsweise von Backup Exec

Mithilfe der Backup Exec-Administratorkonsole können Sie Backup Exec-Aufgaben wie das Senden von Backups, Wiederherstellen von Daten, Konfigurieren des Speichers und Überwachen von Aufträgen steuern. Sie können die Administratorkonsole über den Backup Exec-Server (einen Windows-Server, auf dem Backup Exec installiert ist) oder einen Remote-Computer ausführen. Nachdem Backup-, Wiederherstellungs- oder andere Vorgänge erstellt wurden, verarbeitet

der Backup Exec-Server die Aufträge bzw. delegiert die Aufträge für die Verarbeitung an die Multi-Backup Exec-Serverumgebungen.

Backup Exec enthält folgende Funktionen:

- **Problemlose Planung von Backups**
Backup Exec-Administratoren können geplante Backups für Windows- und Linux-Computer im ganzen Netzwerk einrichten. Die flexible kalenderbasierte Verwaltung von Backup Exec ermöglicht eine mühelose Planung der Verarbeitung von Backups außerhalb der Spitzenlastzeiten.
- **Systemwiederherstellung abschließen**
Simplified Disaster Recovery von Backup Exec sorgt für Gewissheit bei der schnellen Wiederherstellung ganzer Systeme. Beim Konfigurieren eines Backups, erhalten Sie einen eindeutigen Hinweis, dass Sie die Daten ausgewählt haben, die notwendig sind, um ein Backup für Simplified Disaster Recovery durchzuführen. Nachdem Sie kritische Systemkomponenten eines Computers gesichert haben, verwenden Sie den "Assistent zum Erstellen eines SDR-Datenträgers", um ein vereinfachtes Disaster Recovery-Datenträger-Image zu erstellen. Sie können das Datenträger-Image verwenden, um eine Notfallwiederherstellung eines Deduplizierungsspeicherordners durchzuführen.
- **Umfassende Überwachung und intuitive Funktionsweise für alltägliche Aufgaben**
Mit der "Auftragsüberwachung" können Sie alle Backup-, Wiederherstellungs-, Installations- und Speicheraufträge an einem einzigen Ort überwachen und verwalten. Auf der Registerkarte "Startseite" werden Statistiken für Ihre gesamte Backup Exec-Umgebung angezeigt. Mithilfe der Ansicht "Server" können Sie den Backup-Status aller Computer in Ihrem Netzwerk überwachen. Interaktive Warnmeldungen zeigen die Situationen an, die Ihre Aufmerksamkeit erfordern. Backup-Ergebnisse können vom Auftragsverlauf eines Backups angezeigt werden. Der Auftragsverlauf enthält Statistiken, Fehler und andere Informationen zu dem Backup. Der Katalog von Backup Exec ist eine Datenbank mit allen gesicherten Daten. Backup Exec verwendet den Katalog, um die zur Wiederherstellung ausgewählten Elemente nachzuverfolgen.
Assistenten führen Sie durch die meisten Vorgänge von Backup Exec, einschließlich die Erstellung von Backup- und Wiederherstellungsaufträgen und der Konfiguration des Speichers.
- **Automatisches Data Lifecycle Management für plattenbasierte und Cloud-Speicher**
Mithilfe von Data Lifecycle Management löscht Backup Exec automatisch abgelaufene Backup-Sätze auf dem Festplattenspeicher, dem Festplattenkassettendatenträger, dem Deduplizierungsspeicher, Speichergruppen, Cloud-Speichern und virtuellen Datenträgern. Sie geben an, wie lange Backup-Daten aufbewahrt werden, wenn Sie einen Backup-Auftrag

erstellen, der an ein plattenbasierten Speichergerät geschickt wird. Wenn die Aufbewahrungszeit für Backup-Daten abläuft, löscht Data Lifecycle Management die Backup-Sätze und gibt Speicherkapazität für neue Backup-Sätze frei.

Siehe "[Löschen abgelaufener Backup-Sätze auf plattenbasiertem Speicher durch Data Lifecycle Management \(DLM\)](#)" auf Seite 393.

- Vereinfachte Geräte- und Medienverwaltung

Backup Exec verwendet die Funktion "Advanced Device and Media Management" (ADAMM), um Datenaufbewahrung auf Bändern zu verwalten. ADAMM kennzeichnet die auf Datenträgern gespeicherten Backup-Sätze entsprechend den festgelegten Regeln als abgelaufen.

Installation

In diesem Kapitel werden folgende Themen behandelt:

- [Info zum Installieren von und den Lizenzierungsoptionen für Backup Exec](#)
- [Backup Exec - Vorinstallations-Checkliste](#)
- [Ausführen der Umgebungsprüfung vor Installation oder Upgrade von Backup Exec](#)
- [Microsoft SQL Server Express Edition-Komponenten, die mit Backup Exec installiert worden sind](#)
- [Systemanforderungen für Backup Exec](#)
- [Installieren von Backup Exec mithilfe des Installationsassistenten](#)
- [Installieren zusätzlicher Agents und Funktionen auf dem lokalen Backup Exec-Server](#)
- [Installieren von Backup Exec auf Remote-Computern über die Push-Installation](#)
- [Methoden für die Installation von Agent for Windows](#)
- [Installieren von Remote Administrator](#)
- [Installieren von Backup Exec über die Befehlszeile \(Silent-Mode\)](#)
- [Info zum Installationsprotokoll](#)
- [Anzeigen des Installationsübersichtsberichts](#)
- [Reparieren von Backup Exec](#)
- [Aktualisieren von Backup Exec mit Veritas Update](#)
- [Anzeigen installierter Aktualisierungen](#)

- [Deinstallieren von Backup Exec](#)
- [Anzeigen von Lizenzinformationen](#)
- [Backup Exec-Lizenzvertragsinformationen](#)
- [Infos zum Aktualisieren von Backup Exec](#)
- [Aufgaben nach der Installation](#)
- [Deinstallieren von Backup Exec](#)
- [Deinstallieren von Backup Exec mit der Befehlszeile](#)
- [Deinstallieren der Backup Exec-Funktionen vom lokalen Backup Exec-Server](#)

Info zum Installieren von und den Lizenzierungsoptionen für Backup Exec

Der Backup Exec-Installationsassistent führt Sie durch den Prozess des Installierens von Backup Exec und seiner Agents und Optionen. Mithilfe des Installationsassistenten können Sie Backup Exec und seine Agents und Optionen auf einem lokalen Computer installieren oder Sie können sie über eine Push-Installation auf einem Remote-Computer installieren. Der Computer, auf dem Backup Exec installiert wird, wird als Backup Exec-Server bezeichnet. Sie können außerdem Remote Administrator installieren, eine Anwendung, die die Verwaltung des Backup Exec-Servers von einem Windows Remote-Server oder einer Arbeitsstation aus ermöglicht.

Hinweis: Sie können Backup Exec bzw. den Agent for Windows nicht auf einem Datenträger installieren, der für die Datenduplikation unter Windows, auf einem ReFS-Datenträger oder auf freigegebenen Clustervolumen aktiviert wurde.

Wenn Sie Backup Exec installieren, können Sie eine Lizenz auf zwei Arten eingeben:

Tabelle 2-1
Lizenzierungsoptionen

Element	Beschreibung
Manuelles Eingeben der Berechtigungs-IDs	<p>Sie können die Berechtigungs-IDs eingeben, die auf Ihrem Lizenzzertifikat aufgelistet sind. Diese bestehen aus einem Buchstaben und 10 Ziffern (z. B. A0123456789). Nach dem Eingeben der Berechtigungs-IDs stellt Backup Exec eine Verbindung zum Webdienst her und fordert den verknüpften Lizenzschlüssel an. Zum manuellen Eingeben der Berechtigungs-IDs ist eine Internetverbindung erforderlich.</p> <p>Hinweis: Lizenzen aus aus vorherigen Versionen von Backup Exec können die neueste Version von Backup Exec nicht aktivieren.</p>
Importieren von Lizenzen aus der Lizenzdatei	<p>Sie können Ihre Lizenzdateien (.slf) aus einer Netzwerkfreigabe oder einem lokalen Laufwerk importieren.</p> <p>Sie müssen Sie aus dem Licensing Portal abrufen. Auf der Website des Lizenzierungsportals finden Sie eine Datei mit allen registrierten Berechtigungs-IDs.</p> <p>Nach der Installation sind die SLF-Dateien im folgenden Speicherort zu finden:</p> <p>Windows 2008 und höher: C:\ProgramData\Veritas Shared\Licenses</p>
Eine 60-Tage-Testversion installieren	<p>Eine 60-Tage-Testversion ist für Backup Exec verfügbar. Wenn Sie während der Installation keine Berechtigungs-IDs oder Lizenzdateien eingeben, wird eine Testversion installiert.</p>

Nach der Installation von Backup Exec können Sie zusätzliche Agents und Funktionen installieren, wenn Sie die entsprechenden Lizenzen erworben haben. Weitere Informationen zum Hinzufügen von Agents und Funktionen finden Sie im Preisgestaltungs- und Lizenzierungshandbuch zu Backup Exec. Sie können Backup Exec oder Agent for Windows über eine Push-Installation auf Remote-Computern installieren.

Die Installation über eine Befehlszeile ist ebenfalls möglich. Die Installation über die Befehlszeile wird als Silent-Mode-Installation bezeichnet. Bei der Installation

im Silent-Mode wird das Programm "Setup.exe" auf den Backup Exec-Installationsmedien verwendet.

Backup Exec installiert während des Installationsprozesses möglicherweise die folgenden zusätzlichen Produkte:

- Microsoft Report Viewer 2010 SP1
- Microsoft .NET Framework 4.6
- Microsoft Visual C++ 2008 Service Pack 1 Redistributable Package MFC Security Update
- Microsoft Visual C++ 2010 Service Pack 1 Redistributable Package MFC Security Update
- Microsoft Visual C++ 2012 Redistributable Package
- Microsoft Visual C++ 2015 Redistributable Package
- Microsoft SQL Server 2014 Express mit SP2

Informationen zu den Best Practices zum Installieren von Backup Exec finden Sie unter *Best Practices für Backup Exec*.

Siehe ["Installieren von Backup Exec mithilfe des Installationsassistenten"](#) auf Seite 55.

Siehe ["Installieren zusätzlicher Agents und Funktionen auf dem lokalen Backup Exec-Server"](#) auf Seite 66.

Siehe ["Installieren von Backup Exec auf Remote-Computern über die Push-Installation"](#) auf Seite 68.

Siehe ["Installieren von Agent for Windows auf Remote-Computern über eine Push-Installation"](#) auf Seite 78.

Siehe ["Installieren von Backup Exec über die Befehlszeile \(Silent-Mode\)"](#) auf Seite 103.

Siehe ["Backup Exec - Vorinstallations-Checkliste"](#) auf Seite 46.

Backup Exec - Vorinstallations-Checkliste

Vor der Installation von Backup Exec sollten folgende Aufgaben ausgeführt werden:

- Führen Sie den Backup Exec Environment Check auf dem Computer aus, auf dem Sie Backup Exec installieren. Beim Environment Check wird der Computer analysiert, um sicherzustellen, dass der Installationsvorgang vollständig durchgeführt werden kann. Wenn Backup Exec Konfigurationsfehler findet, die während der Installation behoben werden können oder welche die Installation behindern, werden Warnungen angezeigt. Obwohl der Environment Check bei

der Installation automatisch durchgeführt wird, empfiehlt es sich in manchen Fällen, diesen manuell durchzuführen, bevor Sie Backup Exec installieren oder bevor Sie Daten mit Backup Exec sichern.

Siehe ["Ausführen der Umgebungsprüfung vor Installation oder Upgrade von Backup Exec"](#) auf Seite 48.

- Überprüfen Sie die Backup Exec-Hardwarekompatibilitätsliste, um sicherzustellen, dass die Version Ihrer Speicher-Hardware von Backup Exec unterstützt wird.
- Installieren Sie die Speichergeräte (Controller, Laufwerke, Wechsler) auf dem Backup Exec-Server. Weitere Informationen zur Installation entnehmen Sie der Dokumentation, die Ihrem Speichergerät beigelegt ist. Verwenden Sie zur Konfiguration des Controllers und der Speichergeräte geeignete Hardware-Einrichtungsfunktionen von Windows. Weitere Informationen hierzu finden Sie in der Dokumentation zu Microsoft Windows. Die unterstützten Speichertypen finden Sie in der Liste der mit Backup Exec kompatiblen Hardware.
- Überprüfen Sie die Windows-Sicherheitseinstellungen, um sicherzustellen, dass sie die korrekte Ausführung von Backup Exec-Dienstkontodaten nicht einschränken.
Siehe ["Ändern der Identifikationsdaten für ein Dienstkonto"](#) auf Seite 777.
- Stellen Sie sicher, dass Port 50104 für den Backup Exec Management Service verfügbar ist.
- Wenn das Laufwerk, auf dem Sie Backup Exec installieren möchten, verschlüsselt oder komprimiert ist und Sie eine standardmäßige SQL Express-Datenbank verwenden möchten, stellen Sie sicher, dass ein unverschlüsseltes und dekomprimiertes Laufwerk für die Installation von SQL Express vorhanden ist.
- Überprüfen Sie den Namen des Computers, auf dem Sie Backup Exec installieren möchten. Er sollte nur standardmäßige ANSI-Zeichen enthalten. Möglicherweise kommt es zu Fehlern, wenn Sie Backup Exec auf einem Computer installieren, dessen Name andere Zeichen als die standardmäßigen ANSI-Zeichen enthält.
- Wenn Sie Backup Exec unter einer nicht-englischen Version von Windows installieren möchten und alle der folgenden Bedingungen zutreffen, laden Sie die Setup-Datei für Microsoft SQL Server 2014 Express mit SP2 von der Microsoft-Website herunter, bevor Sie Backup Exec installieren:
 - Sie möchten eine lokale Backup Exec SQL Express-Instanz verwenden.
 - Der Computer, auf dem Backup Exec installiert werden soll, verfügt über nicht-englische SQL Server-Instanzen.

Ausführen der Umgebungsprüfung vor Installation oder Upgrade von Backup Exec

Backup Exec Environment Check ist ein Dienstprogramm, das auf einem Computer während der Installation automatisch ausgeführt wird und mit dem die folgenden Informationen angezeigt werden:

- Ob der Computer die Mindestanforderungen für die Installation erfüllt, z. B. in Bezug auf Betriebssystem, Speicherplatz, Arbeitsspeicher und ausreichende Login-Konto-Berechtigungen.
Siehe "[Systemanforderungen für Backup Exec](#)" auf Seite 51.
- Ob Software von Drittanbietern, die Backup Exec-Anschlüsse verwendet, ordnungsgemäß konfiguriert ist.
- Wenn Komponenten erforderlich sind und wenn diese mit Backup Exec kompatibel sind, werden Komponenten installiert.
- Ob frühere Versionen von Backup Exec und Backup -Optionen installiert sind.
- Ob Speichergeräte und zugehörige Treiber ordnungsgemäß installiert sind und vom Windows-Betriebssystem erkannt werden.
- Ob auf dem Datenträger mit dem Deduplizierungsspeicher weniger als 12 % freier Speicherplatz verfügbar ist.
- Ob die Deduplizierungsdienste gestartet wurden.
- Ob das Windows-Hotfix (Windows Update) nicht installiert wurde.

Folgende Ergebnisse werden für jedes Element aufgeführt:

Tabelle 2-2 Ergebnisse des Environment Check

Ergebnis	Beschreibung
Erfolgreich	Es bestehen keine Inkompatibilitäten, die die Installation von Backup Exec verhindern. Für Hardware zeigt dieses Ergebnis an, dass die Hardwarekonfiguration von Backup Exec erkannt wurde.
Warnung	Es besteht eine Inkompatibilität mit Backup Exec. Einige Probleme werden möglicherweise bei der Installation von Backup Exec behoben. Eine Warnung verhindert nicht die Installation von Backup Exec. Wenn die Progleme jedoch nicht bei der Installation behoben werden, schlagen die Aufträge möglicherweise fehl.
Fehlgeschlagen	Es besteht eine Inkompatibilität mit Backup Exec, die eine erfolgreiche Installation verhindert. Es müssen Maßnahmen durchgeführt werden, damit Backup Exec erfolgreich installiert werden kann.

Obwohl die Umgebungsprüfung bei der Installation automatisch durchgeführt wird, empfiehlt es sich in manchen Fällen, sie manuell durchzuführen, bevor Sie Backup Exec installieren oder bevor Sie Daten mit Backup Exec sichern.

So überprüfen Sie die Installationsumgebung vor der Installation:

- 1** Klicken Sie im Installationsmedienbrowser (Browser.exe) auf "Vor der Installation" und dann auf "Backup Exec".
- 2** Klicken Sie auf "Weiter".
- 3** Sie haben folgende Möglichkeiten:

So überprüfen Sie die Konfiguration auf dem lokalen Computer: Wählen Sie "Lokaler Environment Check".

So überprüfen Sie die Konfiguration auf einem Remote-Computer: Wählen Sie "Remoter Environment Check".

- 4** Klicken Sie auf "Weiter".
- 5** Wenn Sie "Remoter Environment Check" in Schritt 3 wählen, führen Sie einen der folgenden Schritte aus und klicken Sie dann auf "Weiter".:

So wählen Sie den Computernamen aus einer Liste: Gehen Sie wie folgt vor:

- Klicken Sie auf "Server aus Liste hinzufügen".
- Wählen Sie in der Liste den Computer und klicken Sie dann auf "Weiter".

So fügen Sie den Computernamen manuell hinzu: Gehen Sie wie folgt vor:

- Klicken Sie auf "Server manuell hinzufügen".
- Geben Sie im Feld Domäne den Namen der Domäne ein.
- Geben Sie im Feld "Computernamen" den Namen des Computers ein.
- Klicken Sie auf "OK".
- Geben Sie den Benutzernamen und das Kennwort für diesen Computer ein.
- Klicken Sie auf "OK".

So entfernen Sie einen Computernamen aus der Liste der Computer, auf denen der Environment Check ausgeführt wird: Gehen Sie wie folgt vor:

- Wählen Sie den Computer aus der Liste aus.
- Klicken Sie auf "Entfernen".

- 6 Überprüfen Sie die Ergebnisse der Umgebungsprüfung und aktivieren Sie "Ergebnisse speichern in", um diese zu speichern.

Klicken Sie zum Ändern des Speicherorts, an dem die Ergebnisse des Environment Check gespeichert werden sollen auf "Pfad ändern". Navigieren Sie dann zu einem neuen Speicherort.
- 7 Klicken Sie auf "Fertigstellen".

Microsoft SQL Server Express Edition-Komponenten, die mit Backup Exec installiert worden sind

Das Installationsprogramm von Backup Exec installiert Komponenten von Microsoft SQL Server 2014 Express mit SP2, die für die Ausführung von Backup Exec erforderlich sind.

Backup Exec fordert Sie auf, eine der folgenden Schritte durchzuführen:

- Installieren Sie die erforderlichen Microsoft SQL Server Express-Komponenten mit Backup Exec, und erstellen Sie eine standardmäßige Backup Exec-Instanz. Dies ist die empfohlene Aktion.

Hinweis: SQL Express kann auf einem Server installiert werden, der andere Instanzen von SQL Express oder vollständige Versionen von SQL ausführt.

- Wählen Sie eine Microsoft SQL Server 2008 R2 SP2-Instanz aus, die bereits im Netzwerk, in dem Backup Exec ausgeführt werden möchten, vorhanden ist.

Wenn Sie Backup Exec in einer bereits vorhandenen Instanz von SQL 2008 R2 SP2 installieren, vergewissern Sie sich, dass die Instanz installiert ist, bevor Sie die Installation fortsetzen.

Vorsicht: Backup Exec wird möglicherweise nicht ordnungsgemäß ausgeführt, wenn die Installation in einer bestehenden SQL Server-Instanz erfolgt, in der bei der Kollatierung zwischen Groß- und Kleinschreibung unterschieden wird. Daher wird empfohlen, Backup Exec nicht in SQL Server-Instanzen dieses Typs zu installieren.

Wenn Backup Exec in einer bereits vorhandenen Instanz installiert wird, ist die Funktion zur automatischen Wiederherstellung der Master-Datenbank nicht verfügbar. Zur Wiederherstellung der Master-Datenbank müssen Sie diese durch

die Kopie ersetzen, die Backup Exec bei dem Backup der Master-Datenbank automatisch erstellt und aktualisiert.

Wenn Backup Exec Updates anwendet, wird die SQL-Instanz gestoppt. Dadurch verlieren andere Datenbanken möglicherweise in der gleichen Instanz an Konnektivität. Wenn eine Remote-SQL-Instanz verwendet wird, stellen Sie sicher, dass Backup Exec eine gute Netzwerkkonnektivität mit der Instanz hat, um Fehler zu vermeiden. Es wird eine standardmäßige Instanz von SQL Express empfohlen.

Die Installation mehrerer Backup Exec-Datenbanken in einer einzigen SQL Server-Instanz ist nicht möglich.

Hinweis: Wenn Sie einen verwalteten Backup Exec-Server installieren, wird empfohlen, für die Installation der Backup Exec-Datenbank für diesen verwalteten Server eine Microsoft SQL Server 2008 R2 SP2-Instanz oder höher auszuwählen. Sie sollten jedoch nicht dieselbe SQL Server-Instanz auswählen, die vom zentralen Administrationsserver verwendet wird.

Siehe "[Systemanforderungen für Backup Exec](#)" auf Seite 51.

Systemanforderungen für Backup Exec

Um Backup Exec ausführen zu können, muss der Computer mindestens folgende Anforderungen erfüllen:

Tabelle 2-3 Mindestsystemanforderungen

Element	Anforderungen
Betriebssystem	<p>Die unterstützten Betriebssysteme, Plattformen und Anwendungen finden Sie in der Liste der mit Backup Exec kompatiblen Software.</p> <p>Hinweis: Backup Exec unterstützt die Installation von Backup Exec-Servern nur unter 64-Bit-Betriebssystemen.</p> <p>Sie können einen Backup Exec-Server nicht auf einem Computer installieren, auf dem die Installationsoption "Windows Server Core" von Windows Server 2008 oder höher ausgeführt wird. Sie können Backup Exec Agent for Windows nur auf Server Core-Computern installieren.</p> <p>Die Installation von SQL Express oder SQL Server auf einem Windows Server 2008-Computer, dessen Rolle als schreibgeschützter Domänencontroller (RODC) konfiguriert ist, ist nicht zulässig. Mit der Rolle "Schreibgeschützter Domänencontroller" können Sie keine lokalen Konten verwenden, die für SQL Express und SQL Server erforderlich sind. Wenn Sie Backup Exec auf einem RODC-Computer installieren, müssen Sie für die Backup Exec-Datenbank eine Remote-SQL-Instanz auswählen.</p> <p>Für Computer mit Windows Server 2012 und höher können Sie Backup Exec oder den Agent for Windows nicht auf einem Datenträger installieren, der für die Datendeduplikation unter Windows, auf einem ReFS-Datenträger oder auf freigegebenen Clustervolumes aktiviert wurde.</p>
Webbrowser	Internet Explorer 7.0 oder höher
Prozessor	Intel Pentium, Xeon, AMD oder kompatibel
Bildschirmauflösung	1024 x 768
SQL Server oder SQL Express	SQL Server 2014 Express mit SP2

Element	Anforderungen
Arbeitsspeicher	<p>Erforderlich: 1 GB RAM über den Betriebssystemanforderungen für den exklusiven Gebrauch durch Backup Exec.</p> <p>Empfohlen: 2 GB RAM (oder mehr, um eine bessere Leistung zu erzielen)</p> <p>Hinweis: Die Anforderungen an den Arbeitsspeicher sind abhängig von den auszuführenden Vorgängen, den installierten Funktionen und der Konfiguration des Computers.</p> <p>Für Central Admin Server Feature: 1 GB RAM erforderlich; 2 GB RAM empfohlen.</p> <p>Recovery Disk: mindestens 1 GB (dediziert) für die mehrsprachige Version.</p> <p>Empfehlungen für den virtuellen Speicher: 20 MB mehr als die für Windows empfohlene Gesamtgröße für die Auslagerungsdatei (für alle Datenträger). Anweisungen zum Anzeigen und Festlegen der Größe der Auslagerungsdatei finden Sie in der Microsoft Windows-Dokumentation.</p>
Sprache der Benutzeroberfläche	<p>Die Backup Exec-Benutzeroberfläche wird in dem Format angezeigt, das in den Regions- und Spracheinstellungen in der Systemsteuerung konfiguriert ist. Sie können die Backup Exec-Anzeigesprache ändern und so die Benutzeroberflächenelemente in einer anderen Sprache anzeigen.</p> <p>Wenn Backup Exec eine Sprache nicht unterstützt, wird die Benutzeroberfläche auf Englisch angezeigt. Die Benutzeroberfläche wird auch auf Englisch angezeigt, wenn das Menü- und die Dialogfeldoption auf eine andere Sprache als jene eingestellt ist, in der Sie die Benutzeroberfläche anzeigen möchten. Wenn Sie nicht eine der in Tabelle 2-4 aufgeführten unterstützten Sprachen verwenden, müssen Sie das Sprachpaket "Englisch" unter Windows installieren.</p>
Speicherplatzinstallation	<p>1,26 GB (typische Installation)</p> <p>1,91 GB (mit allen Funktionen)</p> <p>Hinweis: Die Anforderungen an den Speicherplatz hängen von den auszuführenden Vorgängen, den installierten Funktionen und der Systemkonfiguration ab. Die Backup Exec-Datenbank und die Backup Exec-Kataloge benötigen zusätzlichen Speicherplatz. Zusätzliche 525 MB sind für SQL Express erforderlich. Festplattenspeicher benötigen ebenfalls zusätzlichen Speicherplatz.</p>

Element	Anforderungen
Weitere Hardware	<p>Die folgende Hardware wird empfohlen:</p> <ul style="list-style-type: none"> ■ Netzwerkkarte oder eine virtuelle Netzwerkkarte ■ CD-/DVD-Laufwerk ■ Eine Maus
Speicher-Hardware	<p>Sie können Speichermedien-Laufwerke, Wechsler, Wechseldatenträger und nicht austauschbare Festplatten verwenden. Die unterstützten Speichertypen finden Sie in der Liste der mit Backup Exec kompatiblen Hardware.</p> <p>Weitere Informationen zum Hinzufügen von Laufwerken zu einer automatischen bzw. virtuellen Bandbibliothek finden Sie im Preisgestaltungs- und Lizenzierungshandbuch zu Backup Exec.</p>

Tabelle 2-4 Unterstützte Benutzeroberflächensprachen für Backup Exec

Sprache	Sprachcode
Chinesisch (Vereinfacht)	ZH
Chinesisch (Traditionell)	CH
Englisch	EN
Französisch	FR
Deutsch	DE
Italienisch	IT
Japanisch	JP
Koreanisch	KO
Spanisch	ES
Russisch	RU
Portugiesisch (Brasilien)	PT

Siehe ["Installieren von Backup Exec mithilfe des Installationsassistenten"](#) auf Seite 55.

Installieren von Backup Exec mithilfe des Installationsassistenten

Das Backup Exec-Installationsprogramm stellt zwei Methoden der Installation bereit: typisch und benutzerdefiniert. Eine Standardinstallation ist einfacher als eine benutzerdefinierte Installation und alle im Lieferumfang Ihrer Lizenz enthaltenen Agents und Funktionen werden installiert. Eine Standardinstallation ist i. d. R. für kleine, einfachere Umgebungen geeignet. Eine benutzerdefinierte Installation ist für große oder komplexe Umgebungen, wie zum Beispiel einen Remote-Backup Exec-Server oder eine Umgebung mit Enterprise Server Feature ausgelegt. In einer benutzerdefinierten Installation können Sie auswählen, welche in der Lizenz enthaltenen Funktionen und Agents installiert werden. Dies ist ideal für Benutzer, der steuern möchte, welche Agents und Funktionen installiert werden.

Bei einer Standardinstallation trifft Backup Exec die folgenden Entscheidungen für Sie, basierend auf üblichen Installationsszenarien:

- Backup Exec wird auf einem lokalen Backup Exec-Server installiert.
- SQL Express wird mit der Standardinstanz installiert.
- Alle in Ihrer Lizenz enthaltenen Agents und Funktionen werden installiert.
- Veritas Update wird automatisch ausgeführt.

Hinweis: Stellen Sie vor der Installation sicher, dass Ihre Lizenzen für die zu installierenden Backup Exec-Editionen verfügbar sind. Sie müssen eine Lizenz eingeben, um eine beliebige Edition von Backup Exec zu installieren, aber Sie können die Testversion ohne Lizenz installieren.

Wählen Sie entweder die Standard- oder die benutzerdefinierte Installation:

[Durchführen einer Standardinstallation](#)

[Ausführen einer benutzerdefinierten Installation](#)

Durchführen einer Standardinstallation

Folgen Sie diesen Schritten zum Ausführen einer Standardinstallation von Backup Exec. Bei einer Standardinstallation von Backup Exec werden alle in Ihrer Lizenz enthaltenen Funktionen installiert.

So führen Sie eine Standardinstallation von Backup Exec durch

- 1** Klicken Sie im Installationsmedien-Browser auf "Produkte installieren" und wählen Sie dann "Backup Exec" aus.

Wenn die erforderliche Version von Microsoft.NET Framework nicht bereits auf diesem Computer installiert ist, wird sie von Backup Exec installiert.

Das Backup Exec-Installationsprogramm nutzt jetzt Microsoft .NET Framework 4.6. Nicht alle Windows-Versionen unterstützen .NET Framework 4.6. Wenn das Backup Exec-Installationsprogramm ein Betriebssystem antrifft, das den Einsatz einer anderen Version des .NET Framework erfordert, blockiert Backup Exec die Installation und gibt eine Fehlermeldung aus, die Sie anweist, die erforderliche Version von .NET Framework zu installieren.

- 2** Lesen Sie im Fenster "Willkommen" die Lizenzvereinbarung, klicken Sie dann auf "Ich akzeptiere die Bedingungen der Lizenzvereinbarung" und anschließend auf "Weiter".

- 3** Aktivieren Sie im Bereich "Installationstyp" die Option "Standardinstallation" und klicken Sie dann auf "Weiter".

- 4** Backup Exec Environment Check wird automatisch ausgeführt.

- 5** Prüfen Sie die Ergebnisse der Umgebungsprüfung. Sie haben folgende Möglichkeiten:

- Wenn die Umgebungsprüfung keine Probleme ergibt, die eine erfolgreiche Installation von Backup Exec verhindern könnten, klicken Sie auf "Weiter".
- Wenn die Umgebungsprüfung Probleme ergibt, die eine erfolgreiche Installation von Backup Exec verhindern könnten, klicken Sie auf "Abbrechen". Beheben Sie die Probleme, bevor Sie erneut versuchen, Backup Exec zu installieren.

- 6** Wählen Sie im Bereich "Lizenzen hinzufügen" eine der folgenden Methoden zum Hinzufügen von Lizenzen.

Führen Sie zum manuellen Eingeben von Berechtigungs-IDs folgende Schritte in der angegebenen Reihenfolge aus:

- Geben Sie im Feld "Berechtigungs-ID eingeben" die entsprechende ID aus Ihrem Lizenzzertifikat ein.
- Klicken Sie auf "Zur Liste hinzufügen".
- Wiederholen Sie diesen Vorgang für jede Berechtigungs-ID.

Hinweis: Zum Validieren der Berechtigungs-IDs ist eine Internetverbindung erforderlich. Wenn keine Internetverbindung besteht, importieren Sie die Lizenzen aus der Lizenzdatei, die in Ihrem Lizenzzertifikat enthalten ist, oder installieren Sie eine Testversion.

Führen Sie zum Importieren der Lizenzen aus der Lizenzdatei folgende Schritte in der angegebenen Reihenfolge aus:

- Klicken Sie auf "Lizenzdatei importieren".
- Öffnen Sie den Ordner der Lizenzdateien, und wählen Sie dann die entsprechende Datei aus.

So installieren Sie eine Testversion: Geben Sie keine Berechtigungs-ID ein bzw. importieren Sie keine Lizenzdatei. Fahren Sie mit dem nächsten Schritt fort.

Nach dem Eingeben der Berechtigungs-IDs klicken Sie auf "Weiter".

- 7 Sie werden eventuell aufgefordert, Kontaktdaten für Lizenzvertrag-Berechtigungs-IDs einzugeben.
- 8 Wenn Sie Berechtigungs-IDs eingegeben haben, führen Sie einen der folgenden Schritte im Bereich "Lizenzen prüfen" aus.

Führen Sie zum Installieren einer lizenzierten Version von Backup Exec die folgenden Schritte in der angegebenen Reihenfolge aus:

- Wählen Sie im Feld "Eine auf dem Computer zu installierende Backup Exec-Version auswählen" die zu installierende Backup Exec-Lizenz aus.
- Aktivieren Sie die Kontrollkästchen für die zu installierenden Agents und Funktionen.
- Wählen Sie im Dropdown-Menü die Anzahl der Lizenzen aus, die Sie installieren möchten.

Wählen Sie zum Installieren einer Testversion von Backup Exec im Feld "Wählen Sie eine zu installierende Backup Exec-Editionslizenz aus" die Option "Test". Diese Option ist nur verfügbar, wenn eine Lizenz installiert ist. Ist keine Lizenz installiert, wird automatisch eine Testversion installiert, wenn Sie auf "Weiter" klicken.

Wenn der Vorgang im Bereich "Lizenzen prüfen" abgeschlossen ist, klicken Sie auf "Weiter".

- 9** Geben Sie im Bereich "Dienstkonto" einen Benutzernamen, ein Kennwort und eine Domäne für ein Administratorkonto ein, das die Backup Exec-Systemdienste verwenden können, und klicken Sie auf "Weiter".

Backup Exec kann nur ohne Kennwort auf einem unterstützten Windows-Server installiert werden, wenn Windows entsprechend konfiguriert ist. Wenn Sie dies trotzdem versuchen, wird die folgende Fehlermeldung angezeigt, wenn Backup Exec-Dienste erstellt werden: Der eingegebene Kontoname und/oder das Kennwort sind nicht korrekt. Geben Sie die Login-Informationen erneut ein, und versuchen Sie es erneut.

Sie können Windows jedoch so konfigurieren, dass leere Kennwörter verwendet werden können. Weitere Informationen dazu finden Sie in der Windows-Dokumentation.

- 10** Wenn Sie das Verzeichnis ändern möchten, in dem Backup Exec-Dateien installiert sind, klicken Sie auf "Ändern" und wählen Sie dann einen neuen Speicherort aus.

Wenn Sie das Verzeichnis zu einem neuen Speicherort ändern, stellen Sie sicher, dass Sie einen sicheren Speicherort auswählen, in dem Sie vertrauliche Daten wie zum Beispiel Kennwörter speichern können.

Werden während der Installation von Backup Exec Backup Exec-Datenbank(BEDB)-Dateien aus einer vorherigen Installation erkannt, können Sie entweder die neuen oder vorhandenen Datenbankdateien auswählen. Wenn Sie die neuen Datenbankdateien wählen, werden die vorhandenen in einen anderen Speicherort kopiert.

Wenn Sie jedoch die vorhandenen Datenbankdateien wählen, wird gewarnt, dass die Installation fehlschlagen kann, falls die vorhandenen Datenbankdateien aus einer anderen Version von Backup Exec als der stammen, die installiert wird.

Klicken Sie auf "Weiter".

- 11** Wenn das Dialogfeld "SQL Express Setup" geöffnet wird, führen Sie die folgenden Schritte durch, um den Speicherort der SQL-Installationsdatei zu suchen:
- Klicken Sie auf "Durchsuchen".
 - Wechseln Sie zu dem Speicherort, in den Sie die Setup-Datei für SQL Express 2008 R2 SP2 heruntergeladen haben.
 - Klicken Sie auf "OK".
 - Klicken Sie auf "Weiter".

12 Im Teilfenster "Remote-Computer" führen Sie einen der folgenden Schritte aus.

Führen Sie zum Installieren von Agent for Windows auf einem Remote-Computer folgende Schritte in der angegebenen Reihenfolge aus:

- Klicken Sie auf "Hinzufügen".
- Wählen Sie "Einzelcomputer hinzufügen" aus.
- Geben Sie den vollqualifizierten Namen des Remote-Computers ein oder klicken Sie auf "Remote-Computer durchsuchen", um den Remote-Computer zu lokalisieren.
- Geben Sie unter "Identifikationsdaten für Remote-Computer" die Identifikationsdaten ein, die Backup Exec zum Herstellen einer Verbindung mit den Remote-Servern verwenden kann.
Sie müssen Administrator-Identifikationsdaten verwenden.
- Klicken Sie auf "Weiter".
- Geben Sie im Feld "Zielordner" den Pfad ein, in dem Sie die Dateien installieren möchten.
- Klicken Sie auf "Weiter".
- Wenn alle Computer in der Liste validiert wurden und die Liste vollständig ist, klicken Sie auf "Weiter".

So installieren Sie Agent for Windows auf mehreren Computern unter Verwendung der gleichen Einstellungen: Führen Sie folgende Schritte in der angegebenen Reihenfolge aus:

- Klicken Sie auf "Hinzufügen".
- Wählen Sie "Mehrere Computer mit den gleichen Einstellungen hinzufügen" aus.
- Geben Sie den vollqualifizierten Namen des Remote-Computers ein oder klicken Sie auf "Durchsuchen", um den Remote-Computer zu lokalisieren.
- Klicken Sie auf "Zur Liste hinzufügen".
Geben Sie den vollqualifizierten Namen ein und klicken Sie dann für alle Remote-Computer, auf denen Sie die Push-Installation des Agent for Windows ausführen möchten, auf "Zur Liste hinzufügen".
- Geben Sie unter "Identifikationsdaten für Remote-Computer" die Identifikationsdaten ein, die Backup Exec zum Herstellen einer Verbindung mit den Remote-Servern verwenden kann.
Sie müssen Administrator-Identifikationsdaten verwenden.
- Klicken Sie auf "Weiter".

- Geben Sie im Feld "Zielordner" den Pfad ein, in dem Sie die Dateien installieren möchten.
- Klicken Sie auf "Weiter".
- Wenn alle Computer in der Liste validiert wurden und die Liste vollständig ist, klicken Sie auf "Weiter".

So fahren Sie fort, ohne den Agent for Windows über eine Push-Installation zu installieren. Klicken Sie auf "Weiter".

- 13** Wählen Sie im Bereich "Data Backup" einen Speicherort für eine Kopie der vorhandenen Backup Exec-Datenbank.

Sie können diese Kopie verwenden, wenn das Upgrade auf Backup Exec fehlschlägt.

Nachdem das Upgrade auf Backup Exec abgeschlossen ist, wird der Deduplizierungsspeicher auf eine neuere Version aktualisiert. Der Deduplizierungsspeicherordner bleibt offline, bis die Konvertierung abgeschlossen ist. Nachdem die Konvertierung abgeschlossen ist, und Dienste neu gestartet wurden, wird der Deduplizierungsspeicher online geschaltet.

Aufträge, deren Ziel Deduplizierungsspeicher sind, schlagen während der Konvertierung fehl. Auf anderen Speichergeräten geplante Aufträge werden weiterhin ausgeführt, während der Deduplizierungsspeicher konvertiert wird. Die geschätzte Zeit für die Konvertierung wird in Monaten, Tagen und Stunden angezeigt. Es wird empfohlen, dass Sie eine sekundäre Kopie der Deduplizierungsdaten vor dem Upgrade behalten. Sie können diese dann verwenden, falls die Konvertierung fehlschlägt.

Hinweis: Dieser Bereich wird nur angezeigt, wenn Sie Backup Exec aktualisieren.

- 14** Aktivieren Sie das Kontrollkästchen "Ich habe die Informationen gelesen und verstanden" und klicken Sie dann auf "Weiter".
- 15** Lesen Sie die Backup Exec-Installationsübersicht und klicken Sie dann auf "Installieren".
- 16** Wenn Sie den Agent for Windows auf Remote-Computern installiert haben, klicken Sie im Dialogfeld "Remote-Installation" auf "Weiter".

- 17** Wenn die Installation abgeschlossen ist, können Sie den Computer neu starten, die Readme-Datei anzeigen oder die Backup Exec-Verknüpfung auf dem Desktop entfernen.
- 18** Klicken Sie auf "Weiter" und anschließend auf "Fertigstellen", um den Assistenten zu schließen.

Wenn Sie das System neu starten, startet der Computer automatisch neu.

Beim Installieren wird das Installationsprotokoll "`BKUPINST20.htm`" im folgenden Ordner auf dem Computer erstellt, auf dem Backup Exec installiert wird.

Windows 2008 und höher: `%ProgramData%\Veritas\Backup Exec\Protokolle`

Siehe ["Info zum Installationsprotokoll"](#) auf Seite 113.

Ausführen einer benutzerdefinierte Installation

Folgen Sie diesen Schritten, um eine benutzerdefinierte Installation von Backup Exec auszuführen. Bei einer benutzerdefinierten Installation können Sie auswählen, welche Agents und Funktionen der eingegebenen Lizenzen installiert werden. Beachten Sie, dass Sie eine benutzerdefinierte Installation verwenden können, um weitere Agents und Funktionen zu installieren, die noch nicht in Ihrer Lizenz enthalten sind.

So führen Sie eine benutzerdefinierte Installation von Backup Exec durch

- 1** Klicken Sie im Installationsmedien-Browser auf "Produkte installieren" und wählen Sie dann "Backup Exec" aus.

Wenn die erforderliche Version von Microsoft.NET Framework nicht bereits auf diesem Computer installiert ist, wird sie von Backup Exec installiert.

Der Backup Exec-Installationsassistent nutzt jetzt Microsoft .NET Framework 4.6. Nicht alle Windows-Versionen unterstützen .NET Framework 4.6. Wenn der Installationsassistent ein Betriebssystem erkennt, das den Einsatz einer anderen Version des .NET Framework erfordert, blockiert Backup Exec die Installation und gibt eine Fehlermeldung aus, die Sie auffordert, die erforderliche Version von .NET Framework zu installieren.

- 2** Lesen Sie im Fenster "Willkommen" die Lizenzvereinbarung, klicken Sie dann auf "Ich akzeptiere die Bedingungen der Lizenzvereinbarung" und anschließend auf "Weiter".
- 3** Aktivieren Sie im Bereich "Installationstyp" die Option "Benutzerdefinierte Installation" und klicken Sie dann auf "Weiter".
- 4** Wählen Sie im Menü die Optionen "Lokale Installation" und "Backup Exec-Software und -Funktionen installieren". Klicken Sie auf "Weiter".
- 5** Backup Exec Environment Check wird automatisch ausgeführt.

- 6** Prüfen Sie die Ergebnisse der Umgebungsprüfung. Sie haben folgende Möglichkeiten:
- Wenn die Umgebungsprüfung keine Probleme ergibt, die eine erfolgreiche Installation von Backup Exec verhindern könnten, klicken Sie auf "Weiter".
 - Wenn die Umgebungsprüfung Probleme ergibt, die eine erfolgreiche Installation von Backup Exec verhindern könnten, klicken Sie auf "Abbrechen". Beheben Sie die Probleme, bevor Sie erneut versuchen, Backup Exec zu installieren.

- 7** Wählen Sie im Bereich "Lizenzen hinzufügen" eine der folgenden Methoden zum Eingeben von Lizenzen.

Führen Sie zum manuellen Eingeben von Berechtigungs-IDs folgende Schritte in der angegebenen Reihenfolge aus:

- Geben Sie im Feld "Berechtigungs-ID eingeben" die entsprechende ID aus Ihrem Lizenzzertifikat ein.
- Klicken Sie auf "Zur Liste hinzufügen".
- Wiederholen Sie diesen Vorgang für jede zu installierende Lizenz.
- Klicken Sie auf "Weiter", um die Berechtigungs-IDs zu validieren.

Hinweis: Zum Validieren der Berechtigungs-IDs ist eine Internetverbindung erforderlich. Wenn keine Internetverbindung besteht, importieren Sie die Lizenzen aus der Lizenzdatei oder installieren Sie eine Testversion.

Führen Sie zum Importieren der Lizenzen aus der Lizenzdatei folgende Schritte in der angegebenen Reihenfolge aus:

- Klicken Sie auf "Lizenzdatei importieren".
- Öffnen Sie den Ordner der Lizenzdateien, und wählen Sie dann die entsprechende Datei aus.

So installieren Sie eine Testversion: Geben Sie keine Berechtigungs-ID ein bzw. importieren Sie keine Lizenzdatei. Fahren Sie mit dem nächsten Schritt fort.

Nach dem Eingeben der Berechtigungs-IDs klicken Sie auf "Weiter".

- 8** Wenn Sie Berechtigungs-IDs eingegeben haben, führen Sie einen der folgenden Schritte im Bereich "Lizenzen prüfen" aus.

Führen Sie zum Installieren einer lizenzierten Version von Backup Exec die folgenden Schritte in der angegebenen Reihenfolge aus:

- Wählen Sie im Feld "Eine auf dem Computer zu installierende Backup Exec-Version auswählen" die zu installierende Backup Exec-Lizenz aus.

- Aktivieren Sie die Kontrollkästchen für die zu installierenden Agents und Funktionen.
- Wählen Sie im Dropdown-Menü die Anzahl der Lizenzen aus, die Sie installieren möchten.
- Wenn Sie keine Auswahl treffen, wählt Backup Exec standardmäßig die Lizenz mit dem größten Funktionssatz.

Wählen Sie zum Installieren einer Testversion von Backup Exec im Feld "Wählen Sie eine zu installierende Backup Exec-Editionslizenz aus" die Option "Test". Diese Option ist nur verfügbar, wenn eine Lizenz installiert ist. Ist keine Lizenz installiert, wird automatisch eine Testversion installiert, wenn Sie auf "Weiter" klicken.

Im Bereich "Lizenzen prüfen" können Sie auch die Kapazität für jeden Berechtigungs-ID anzeigen und anpassen.

Wenn der Vorgang im Bereich "Lizenzen prüfen" abgeschlossen ist, klicken Sie auf "Weiter".

- 9 Im Bereich "Funktionen konfigurieren" werden unter "Wählen Sie die zu installierenden Funktionen" alle in den Lizenzen, für die Sie Berechtigungs-IDs eingegeben haben, enthaltenen Funktionen und Agents angezeigt. Aktivieren Sie das Kontrollkästchen neben den zu installierenden Funktionen und Agents. Sie können die Auswahl von Agents und Funktionen aufheben, um zu verhindern, dass sie jetzt installiert werden. Funktionen und Agents sind nach Edition und basierend auf den eingegebenen Lizenzen sortiert. Beachten Sie, dass eine Testversion Funktionen für Backup Exec Bronze, Silber und Gold Edition auf dieser Seite anzeigt.

Agents und Funktionen, für die Sie keine Lizenz eingegeben haben, werden angezeigt, sind aber nicht verfügbar. Wenn Sie zuerst eine Testlizenz und später eine Lizenz mit weniger Agents oder Funktionen installieren, werden die entsprechenden Agents und Funktionen entfernt.

Wenn Sie das Konfigurieren von Agents und Funktionen abgeschlossen haben, klicken Sie auf "Weiter".

- 10 Wenn Sie zusätzliche Sprachen für Backup Exec installieren möchten, wählen Sie im Bereich "Sprachen wählen" und klicken Sie dann auf "Weiter".

- 11** Überprüfen Sie im Bereich "Ziel" die Speicherplatzanforderungen für die zum Installieren ausgewählten Elemente. Wenn Sie den Installationsordner für Backup Exec ändern möchten, klicken Sie auf "Ändern" und wählen Sie einen Ordner aus oder erstellen Sie einen neuen. Es wird empfohlen, keinen Bereitstellungspunkt als Zielordner auszuwählen, da Backup Exec beim Löschen des Bereitstellungspunkts deinstalliert wird.

Erkennt das Installationsprogramm Backup Exec-Datenbank(BEDB)-Dateien aus einer vorherigen Installation, können Sie entweder die neuen oder vorhandenen Datenbankdateien verwenden. Wenn Sie die neuen Datenbankdateien wählen, werden die vorhandenen in einen anderen Speicherort kopiert.

Wenn Sie jedoch die vorhandenen Datenbankdateien wählen, wird gewarnt, dass die Installation fehlschlagen kann, falls die vorhandenen Datenbankdateien aus einer anderen Version von Backup Exec als der stammen, die installiert wird.

Wenn Sie die Zielinformationen geprüft haben, klicken Sie auf "Weiter".

- 12** Geben Sie im Bereich "Dienstkonto" einen Benutzernamen, ein Kennwort und eine Domäne für ein Administratorkonto ein, das die Backup Exec-Systemdienste verwenden können, und klicken Sie auf "Weiter".

Backup Exec kann nur ohne Kennwort auf einem unterstützten Windows-Server installiert werden, wenn Windows entsprechend konfiguriert ist. Wenn Sie dies trotzdem versuchen, wird die folgende Fehlermeldung angezeigt, wenn Backup Exec-Dienste erstellt werden:

Der eingegebene Kontoname und/oder das Kennwort sind nicht korrekt. Geben Sie die Login-Informationen erneut ein, und versuchen Sie es erneut.

Sie können Windows jedoch so konfigurieren, dass leere Kennwörter verwendet werden können. Weitere Informationen dazu finden Sie in der Windows-Dokumentation.

- 13** Führen Sie im Fenster "SQL Server auswählen" eine der folgenden Aktionen aus, um einen Speicherort für die Backup Exec-Datenbank auszuwählen.

Hinweis: Das Fenster "SQL Server auswählen" wird für Aktualisierungen nicht angezeigt. Der Speicherort der Datenbank kann während des Aktualisierungsvorgangs nicht geändert werden. Um den Speicherort der Datenbank nach dem Aktualisierungsvorgang zu ändern, verwenden Sie BE Utility.

Zum Erstellen einer lokalen Backup Exec SQL Express-Instanz führen Sie folgende Schritte in der angegebenen Reihenfolge aus:

- Klicken Sie auf "Erstellen einer lokalen Backup Exec SQL Express-Instanz zum Speichern der Backup Exec-Datenbank".
- Um den Speicherort für die Backup Exec-SQL Express-Instanz zu ändern, klicken Sie auf "Durchsuchen".
- Wählen Sie den Speicherort und klicken anschließend auf "OK".

So verwenden Sie eine vorhandene SQL Server 2008 R2 SP2-Instanz führen Sie folgende Schritte in der angegebenen Reihenfolge aus:

- Klicken Sie auf "Vorhandene Instanz von SQL Server 2008 R2 mit Service Pack 2 oder höher verwenden".
- Wählen Sie die Instanz aus.
- Beachten Sie, wenn Backup Exec in einer bereits vorhandenen Instanz installiert wird, ist die Funktion zur automatischen Wiederherstellung der Master-Datenbank nicht verfügbar. Zur Wiederherstellung der Master-Datenbank ersetzen Sie diese durch die Kopie, die Backup Exec beim Backup der Master-Datenbank automatisch erstellt und aktualisiert. Weitere Informationen: Siehe ["Microsoft SQL Server Express Edition-Komponenten, die mit Backup Exec installiert worden sind"](#) auf Seite 50.

Wenn Sie fertig sind, klicken Sie auf "Weiter".

- 14** Backup Exec versucht jetzt, eine Verbindung zur Instanz herzustellen.
- 15** Wenn das Dialogfeld "SQL Express Setup" geöffnet wird, führen Sie die folgenden Schritte durch, um den Speicherort der SQL-Installationsdatei zu suchen:
 - Klicken Sie auf "Durchsuchen".
 - Wechseln Sie zu dem Speicherort, in den Sie die Setup-Datei für SQL Express 2008 R2 SP2 heruntergeladen haben.
 - Klicken Sie auf "OK".
 - Klicken Sie auf "Weiter".
- 16** Wenn Sie dazu aufgefordert werden, wählen Sie aus, wie Gerätetreiber für mit dem Server verbundene Bandspeichergeräte vom Gerätetreiber-Installationsprogramm installiert werden sollen, und klicken Sie dann auf "Weiter".

Es wird empfohlen, dass Sie die Option "Gerätetreiber für alle Bandgeräte verwenden" aktivieren.

17 Wenn Sie aufgefordert werden, geben Sie die Informationen ein oder wählen Sie Einstellungen für die zusätzlichen zu installierenden Funktionen und klicken Sie anschließend jeweils auf "Weiter".

18 Lesen Sie die Backup Exec-Installationsübersicht und klicken Sie dann auf "Installieren".

Der vollständige Installationsvorgang kann mehrere Minuten dauern. Es kann sein, dass der Verlauf dabei mehrere Minuten lang nicht aktualisiert wird.

19 Wenn die Installation abgeschlossen ist, können Sie den Computer neu starten, die Readme-Datei anzeigen oder die Backup Exec-Verknüpfung auf dem Desktop entfernen.

20 Klicken Sie auf "Weiter" und anschließend auf "Fertigstellen", um den Assistenten zu schließen.

Wenn Sie das System neu starten, startet der Computer automatisch neu.

Installieren zusätzlicher Agents und Funktionen auf dem lokalen Backup Exec-Server

Sie können Agenten und Funktionen installieren, wenn Sie Backup Exec installieren. Wenn Sie jedoch Backup Exec bereits installiert haben und zusätzliche Agents oder Funktionen installieren möchten, lesen Sie die Dokumentation zu diesen Funktionen, um sicherzustellen, dass der Computer aller Mindestanforderungen erfüllt. Außerdem benötigen Sie eine gültige Lizenz für die zu installierenden Agents und Funktionen. Die Backup Exec-Dienste werden während der Installation von zusätzlichen Funktionen möglicherweise angehalten. Wenn zu diesem Zeitpunkt noch aktive Aufträge ausgeführt werden, erhalten Sie die Aufforderung, diese anzuhalten oder die Fertigstellung der Aufträge abzuwarten.

Hinweis: Ist Central Admin Server Feature installiert und Sie möchten weitere Funktionen auf einem verwalteten Backup Exec-Server installieren, können Sie den verwalteten Backup Exec-Server anhalten. Wenn ein verwalteter Backup Exec-Server angehalten wurde, leitet der Administrationsserver keine Aufträge an ihn weiter. Wenn die Installation abgeschlossen ist, setzen Sie den verwalteten Backup Exec-Server wieder in Betrieb.

Siehe ["Anhalten oder Wiederaufnehmen eines verwalteten Backup Exec-Servers"](#) auf Seite 1507.

So installieren Sie zusätzliche Backup Exec-Funktionen auf dem lokalen Backup Exec-Server

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und dann auf "Installation und Lizenzierung" und "Funktionen und Lizenzen auf diesem Backup Exec-Server installieren".

Sie werden möglicherweise aufgefordert, die Installationsmedien einzufügen.

- 2 Sie haben folgende Möglichkeiten:

So geben Sie
Seriennummern manuell ein

Hinweis: Zum Validieren der Seriennummern ist eine Internetverbindung erforderlich. Wenn keine Internetverbindung besteht, importieren Sie die Lizenzen aus der Lizenzdatei oder installieren Sie eine Testversion.

Gehen Sie dazu in folgender Reihenfolge vor:

- Geben Sie im Feld "Seriennummer eingeben" die entsprechende Seriennummer aus Ihrem Lizenzzertifikat ein.
- Klicken Sie auf "Zur Liste hinzufügen".
- Wiederholen Sie den Vorgang für jede Seriennummer.

So importieren Sie Lizenzen
aus der Lizenzdatei

Gehen Sie dazu in folgender Reihenfolge vor:

- Klicken Sie auf "Lizenzdatei importieren".
- Öffnen Sie den Ordner der Lizenzdateien, und wählen Sie dann die entsprechende Datei aus.

So installieren Sie eine
Testversion

Geben Sie keine Seriennummer ein oder importieren Sie eine Lizenzdatei. Gehen Sie zu Schritt 5.

- 3 Klicken Sie auf "Weiter".

Sie werden aufgefordert, Kontaktdaten für Lizenzvertragsseriennummern einzugeben.

- 4 Wenn Sie Produktaktivierungs-Seriennummern eingegeben haben, werden im Bereich "Lizenzen prüfen" die Editionen angezeigt, für die Sie Lizenzen eingegeben haben. Sie können auch das Feld "Zugeordnete Kapazität" für jede Edition bearbeiten, um anzugeben, welchen Anteil der verfügbaren Kapazität jede Edition nutzen kann.

Wählen Sie zum Installieren einer Testversion von Backup Exec im Feld "Wählen Sie eine zu installierende Backup Exec-Editionslizenz aus" die Option "Test". Diese Option ist nur verfügbar, wenn eine Lizenz installiert ist. Ist keine Lizenz installiert, wird automatisch eine Testversion installiert, wenn Sie auf "Weiter" klicken.

- 5 Klicken Sie auf "Weiter".
- 6 Gehen Sie wie folgt vor:
 - Aktivieren Sie die Kontrollkästchen für die zusätzlichen zu installierenden Funktionen.
 - Deaktivieren Sie die Kontrollkästchen für die Funktionen, die Sie entfernen möchten.
- 7 Klicken Sie auf "Weiter".
- 8 Wenn Sie dazu aufgefordert werden, geben Sie Informationen ein, oder wählen Sie die Einstellungen für zusätzliche Funktionen, die installiert werden sollen. Klicken Sie nach jeder Auswahl auf "Weiter".
- 9 Lesen Sie die Backup Exec-Installationsübersicht und klicken Sie dann auf "Installieren".

Die Backup Exec-Dienste werden während der Installation von zusätzlichen Funktionen angehalten. Wenn zu diesem Zeitpunkt noch aktive Aufträge ausgeführt werden, erhalten Sie die Aufforderung, diese anzuhalten oder die Fertigstellung der Aufträge abzuwarten.

Die Dienste werden erneut gestartet, wenn die Installation abgeschlossen ist.
- 10 Klicken Sie auf "Fertigstellen".

Installieren von Backup Exec auf Remote-Computern über die Push-Installation

In den folgenden Fällen ist eine Push-Installation von Backup Exec nicht möglich:

- Push-Installation aus einem 64-Bit-Betriebssystem auf ein 32-Bit-Betriebssystem
- Push-Installation aus einem 32-Bit-Betriebssystem auf ein 32-Bit- oder 64-Bit-Betriebssystem

Wenn Sie Backup Exec über Terminaldienste installieren und sich die Installationsmedien auf einem gemeinsam genutzten Laufwerk befinden (Netzwerkfreigabe), müssen Sie einen UNC-Pfad verwenden. Die Installation über zugeordnete Laufwerke wird nicht unterstützt.

Sie können mehrere Server-Installationen einrichten. Backup Exec verarbeitet bis zu fünf Remote-Computer-Installationen gleichzeitig.

Hinweis: Backup Exec installiert die erforderliche Version von Microsoft .NET Framework, wenn diese nicht bereits auf dem Computer installiert ist, auf dem Backup Exec über eine Push-Installation installiert werden soll. Das Backup Exec-Installationsprogramm nutzt jetzt Microsoft .NET Framework 4.6. Nicht alle Windows-Versionen unterstützen .NET Framework 4.6. Wenn das Backup Exec-Installationsprogramm ein Betriebssystem antrifft, das den Einsatz einer anderen Version des .NET Framework erfordert, blockiert Backup Exec die Installation und gibt eine Fehlermeldung aus, die Sie anweist, die erforderliche Version von .NET Framework zu installieren.

Vor der Installation von Backup Exec auf Remote-Computern sollten Sie die besonderen Hinweise lesen.

Tabelle 2-5 Besondere Hinweise zur Installation von Backup Exec-Optionen auf Remote-Computern

Element	Hinweis
Windows Server 2008 und höher	<p>Für eine Push-Installation von Backup Exec auf einem Computer mit Windows Server 2008 und höher müssen Sie in der Ausnahmenliste der Windows-Firewall auf dem Zielcomputer die folgenden Elemente aktivieren:</p> <ul style="list-style-type: none">■ Datei- und Druckerfreigabe■ Windows-Verwaltungsinstrumentation (WMI) <p>Weitere Informationen dazu finden Sie in der Dokumentation zu Microsoft Windows.</p> <p>Sie können Backup Exec nicht auf Datenträgern installieren, auf denen unter Windows die Datendeduplizierung aktiviert wurde, bzw. auf ReFS-Datenträgern oder freigegebenen Clustervolumes.</p>
Symantec Endpoint Protection (SEP) 11.0 oder höher	<p>Um Backup Exec mit einer Push-Installation auf einem Computer mit Symantec Endpoint Protection (SEP), Version 11.0 oder höher, zu installieren, müssen Sie SEP für die gemeinsame Nutzung von Dateien und Druckern konfigurieren. Die Datei- und Druckerfreigabefunktion ist standardmäßig deaktiviert.</p>

Hinweis: Sie können auch das Microsoft-Dienstprogramm "Software" verwenden, um Backup Exec auf einem Remote-Computer zu installieren. In Ihrer Microsoft-Dokumentation finden Sie weitere Informationen.

Beim Installieren wird das Installationsprotokoll `BKUPINST20.htm` im folgenden Ordner auf dem Computer erstellt, auf dem Backup Exec installiert wird.

Windows 2008 und höher: `%ProgramData%\Veritas\Backup Exec\Protokolle`

So installieren Sie Backup Exec über die Push-Installation auf Remote-Computern

1 Sie haben folgende Möglichkeiten:

So installieren Sie Backup Exec über eine Push-Installation von den Installationsmedien auf Remote-Computern

Gehen Sie dazu nach folgender Reihenfolge vor:

- Klicken Sie im Installationsmedien-Browser auf "Produkte installieren" und wählen Sie dann "Backup Exec" aus.
- Klicken Sie im Begrüßungsbildschirm auf "Weiter".
- Wählen Sie "Ich nehme die Bedingungen der Lizenzvereinbarung an" aus, und klicken Sie anschließend auf "Weiter".
- Klicken Sie auf "Benutzerdefinierte Installation".
- Deaktivieren Sie "Lokale Installation" und aktivieren Sie "Remote-Installation".
- Klicken Sie auf "Weiter".

So installieren Sie Backup Exec über eine Push-Installation vom Backup Exec-Server auf den Remote-Computern

Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Installation und Lizenzierung" und dann "Agents und Backup Exec-Server auf anderen Servern installieren".

2 Im Teilfenster "Remote-Computer" führen Sie einen der folgenden Schritte aus:

So installieren Sie Backup Exec auf einem Remote-Computer

Gehen Sie dazu in folgender Reihenfolge vor:

- Klicken Sie auf "Hinzufügen".
- Wählen Sie "Einzelcomputer hinzufügen" aus.
- Wählen Sie "Backup Exec" und klicken dann auf "Weiter".
- Geben Sie den vollqualifizierten Namen des Remote-Computers ein oder klicken Sie auf "Remote-Computer durchsuchen", um den Remote-Computer zu lokalisieren.

So installieren Sie Backup Exec auf mehreren Computern unter Verwendung der gleichen Einstellungen

Gehen Sie dazu in folgender Reihenfolge vor:

- Klicken Sie auf "Hinzufügen".
- Wählen Sie "Mehrere Computer mit den gleichen Einstellungen hinzufügen" aus.
- Wählen Sie "Backup Exec" und klicken dann auf "Weiter".
- Geben Sie den vollqualifizierten Namen des Remote-Computers ein oder klicken Sie auf "Durchsuchen", um den Remote-Computer zu lokalisieren.
- Klicken Sie auf "Zur Liste hinzufügen". Geben Sie den vollständig qualifizierten Namen ein und klicken Sie dann für alle Remote-Computer, auf denen Sie die Push-Installation der Funktionen ausführen möchten, auf "Zur Liste hinzufügen".

- 3 Geben Sie unter "Identifikationsdaten für Remote-Computer" die Identifikationsdaten ein, die Backup Exec zum Herstellen einer Verbindung mit den Remote-Servern verwenden kann.

Sie müssen Administrator-Identifikationsdaten verwenden.

- 4 Klicken Sie auf "Weiter".
- 5 Wählen Sie eine der folgenden Methoden aus, um Lizenzen einzugeben:

So geben Sie
 Seriennummern
 aus Ihrem
 Lizenzzertifikat ein

Hinweis: Zum
 Validieren der
 Seriennummern ist
 eine
 Internetverbindung
 erforderlich. Wenn
 keine
 Internetverbindung
 besteht, importieren
 Sie die Lizenzen
 aus der Lizenzdatei
 oder installieren Sie
 eine Testversion.

Gehen Sie dazu in folgender Reihenfolge vor:

- Geben Sie im Feld "Seriennummer eingeben" die entsprechende Seriennummer aus Ihrem Lizenzzertifikat ein.
- Klicken Sie auf "Zur Liste hinzufügen".
- Wiederholen Sie diesen Vorgang für alle zu installierenden Funktionen und Agents.
- Klicken Sie auf "Weiter", um die Seriennummern zu validieren.

So importieren Sie
 Lizenzen aus einer
 Lizenzdatei

Gehen Sie dazu in folgender Reihenfolge vor:

- Klicken Sie auf "Lizenzdatei importieren".
- Öffnen Sie den Ordner der Lizenzdateien, und wählen Sie dann die entsprechende Datei aus.

So installieren Sie
 eine Testversion

Geben Sie keine Seriennummer ein oder importieren Sie eine Lizenzdatei. Gehen Sie zu Schritt [8](#).

6 Klicken Sie auf "Weiter".

Sie werden aufgefordert, Kontaktdaten für Lizenzvertragsseriennummern einzugeben.

7 Wenn Sie im Bereich "Lizenzen überprüfen" die Seriennummern zur Produktaktivierung eingegeben haben, führen Sie eine der folgenden Aktionen aus:

So installieren Sie eine lizenzierte Version von Backup Exec

Gehen Sie dazu in folgender Reihenfolge vor:

- Wählen Sie im Feld "Eine auf dem Computer zu installierende Backup Exec-Version auswählen" die zu installierende Backup Exec-Lizenz aus.
- Aktivieren Sie die Kontrollkästchen für die zu installierenden Agents und Funktionen.
- Wählen Sie im Dropdown-Menü die Anzahl der Lizenzen aus, die Sie installieren möchten.

So installieren Sie eine Testversion

Wählen Sie im Feld "Eine auf dem Computer zu installierende Backup Exec-Version auswählen" die Option "Test".

8 Klicken Sie auf "Weiter".

9 Wählen Sie im Fenster "Funktionen konfigurieren" alle zusätzlich zu installierenden Funktionen aus.

Sie können beispielsweise zusätzliche Standardfunktionen oder Agents und Funktionen auswählen, die für eine Testinstallation verfügbar sind.

Hinweis: Wenn Sie die Installation von Backup Exec aus einem Server auf einen anderen durchführen, zeigt die Funktionszuordnung im Dialogfeld "Funktionen konfigurieren" den Server an, von dem aus die Push-Installation gestartet wurde, nicht den Server, auf dem das Produkt installiert wird.

10 Geben Sie im Feld "Zielordner" den Pfad ein, in dem Sie Backup Exec installieren möchten.

11 Klicken Sie auf "Weiter".

12 Vervollständigen Sie die Optionen für die Dienstkonto-Identifikationsdaten wie folgt:

Benutzername	<p>Geben Sie den Benutzernamen für ein Administratorkonto ein, das die Backup Exec-Dienste verwenden können.</p> <p>Wenn der Remote-Computer Mitglied einer Domäne ist, verwenden Sie das Konto eines Domänenadministrators oder ein gleichwertiges Konto, das Mitglied der Domänenadministratorgruppe ist.</p> <p>Wenn der Remote-Computer Mitglied einer Arbeitsgruppe ist, verwenden Sie die Kontodaten eines Administrators oder eines gleichwertigen Kontos, das Mitglied der Administratorgruppe auf diesem Computer ist.</p>
Kennwort	Geben Sie das Kennwort für ein Administratorkonto ein, das die Backup Exec-Dienste verwenden können.
Domäne	<p>Wenn der Computer einer Domäne zugeordnet ist, wählen Sie die Domäne des Computers.</p> <p>Ist der Computer einer Arbeitsgruppe zugeordnet, wählen Sie den Computernamen aus.</p>

13 Klicken Sie auf "Weiter".

14 Führen Sie einen der folgenden Schritt aus, um einen Speicherort auszuwählen, in dem die Backup Exec-Datenbank gespeichert werden soll. Klicken Sie anschließend auf "Weiter".

Zum Erstellen einer lokalen Backup Exec SQL Express-Instanz	<p>Gehen Sie dazu in folgender Reihenfolge vor:</p> <ul style="list-style-type: none"> ■ Klicken Sie auf "Erstellen einer lokalen Backup Exec SQL Express-Instanz zum Speichern der Backup Exec-Datenbank". ■ Zum Ändern des Datenbankspeicherorts geben Sie im Feld "Zielordner" das gewünschte Verzeichnis ein.
---	---

So verwenden Sie eine vorhandene SQL Server 2008 R2 SP2-Instanz

Gehen Sie dazu in folgender Reihenfolge vor:

- Klicken Sie auf "Vorhandene Instanz von SQL Server 2008 R2 mit Service Pack 2 oder höher verwenden".
- Wählen Sie die Instanz aus.

Wenn Backup Exec in einer bereits vorhandenen Instanz installiert wird, ist die Funktion zur automatischen Wiederherstellung der Master-Datenbank nicht verfügbar. Zur Wiederherstellung der Master-Datenbank müssen Sie diese durch die Kopie ersetzen, die Backup Exec bei dem Backup der Master-Datenbank automatisch erstellt und aktualisiert.

Siehe ["Microsoft SQL Server Express Edition-Komponenten, die mit Backup Exec installiert worden sind"](#) auf Seite 50.

Backup Exec versucht, eine Verbindung zu der Instanz herzustellen.

Dieser Schritt wird während der Upgrades übersprungen.

- 15** Klicken Sie auf "Weiter".
- 16** Nehmen Sie eine Auswahl für Bandgerätetreiber vor und klicken Sie dann auf "Weiter".

Hinweis: Sie müssen keine Bandgerätetreiber installieren, wenn Backup Exec unter Windows Server 2012 oder höher ausgeführt wird. Kernelmodustreiber und tapeinst.exe werden nicht mehr installiert, wenn Backup Exec unter Windows Server 2012 oder höher ausgeführt wird.

Siehe ["Installieren von Bandgerätetreibern "](#) auf Seite 449.

- 17** Klicken Sie auf "Weiter".
- 18** Wenn Sie dazu aufgefordert werden, geben Sie Informationen ein oder wählen Einstellungen für weitere Funktionen und klicken Sie danach jeweils auf "Weiter" bzw. "OK".
- 19** Wenn die Remote-Computer von Backup Exec validiert wurden, können Sie die Liste wie folgt ändern:

So fügen Sie einen Remote-Computer manuell hinzu

Klicken Sie auf "Hinzufügen" und dann auf "Einzelcomputer hinzufügen".

So fügen Sie mehrere Remote-Computer manuell hinzu	Klicken Sie auf "Hinzufügen" und dann auf "Mehrere Computer mit den gleichen Einstellungen hinzufügen".
So fügen Sie mehrere Remote-Computer durch das Importieren einer vorhandenen Liste der Computer hinzu	<p>Klicken Sie auf "Importieren und exportieren", und wählen Sie dann eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> ■ Wählen Sie "Aus Datei importieren", um Backup Exec zum Hinzufügen der Namen der Remote-Computer aus einer ausgewählten Liste zu aktivieren. ■ Wählen Sie "Auf diesem Backup Exec-Server veröffentlichte Server importieren", damit Backup Exec die Namen aller Remote-Computer hinzufügen kann, die für die Veröffentlichung auf diesem Backup Exec-Server eingerichtet sind. <p>Sie müssen Remote-Computer-Identifikationsdaten für die Liste der Remote-Computer eingeben.</p>
So ändern Sie das Produkt, das Sie zum Installieren oder Ändern anderer Installationseigenschaften ausgewählt haben	Wählen Sie den Remote-Computer aus, den Sie ändern möchten, und klicken Sie dann auf "Bearbeiten".
So löschen Sie einen Remote-Computer aus der Liste	Wählen Sie den Remote-Computer aus, den Sie löschen möchten, und klicken Sie dann auf "Löschen".
So sichern Sie die Liste der Remote-Computer und der verbundenen Remote-Computer-Identifikationsdaten	<p>Überprüfen Sie, dass "Serverliste für zukünftige Remote-Installationssitzungen speichern" markiert ist.</p> <p>Diese Option ermöglicht es, dass die Namen und Identifikationsdaten aller Remote-Computer automatisch hinzugefügt werden, wenn Sie das nächste Mal Backup Exec oder Funktionen auf diesen Remote-Computern installieren.</p>

So speichern Sie die Liste der Remote-Computer in einer XML-Datei

Klicken Sie auf "Importieren und exportieren" und klicken Sie dann auf "In Datei exportieren".

Sie können den Speicherort auswählen, an dem die Datei "Push_Export.xml" gespeichert werden soll. Diese Option ist nützlich, wenn Sie dieselbe Liste für mehrere Backup Exec-Server benutzen möchten. Wenn Sie die Liste importieren, müssen Sie die Remote-Computer-Identifikationsdaten erneut eingeben.

So beheben Sie die Fehler, die während der Validierung gefunden wurden

Klicken Sie mit der rechten Maustaste auf den Namen des Computers und klicken Sie dann auf "Fehler beheben".

So aktivieren Sie Backup Exec, um einen ungültigen Remote-Computer erneut zu validieren

Klicken Sie mit der rechten Maustaste auf den Namen des Computers, und klicken Sie dann auf Validierung erneut vornehmen.

20 Wenn alle Computer in der Liste validiert wurden und die Liste vollständig ist, klicken Sie auf "Weiter".

21 Lesen Sie die Backup Exec-Installationsübersicht und klicken Sie dann auf "Installieren".

Siehe ["Info zum Installationsprotokoll"](#) auf Seite 113.

22 Klicken Sie auf "Weiter" und anschließend auf "Fertigstellen", um den Assistenten zu schließen.

Wenn Sie den Remote-Computer noch nicht neu gestartet haben, müssen Sie den Neustart jetzt durchführen, damit die Konfigurationseinstellungen wirksam werden.

Methoden für die Installation von Agent for Windows

Sie können Agent for Windows je nach Ihrer Umgebung mithilfe der folgenden Methoden installieren:

- Über eine Push-Installation von Agent for Windows auf einem oder mehreren Remote-Computern vom Backup Exec-Server aus.

Siehe ["Installieren von Agent for Windows auf Remote-Computern über eine Push-Installation"](#) auf Seite 78.

- Fügen Sie den Remote-Computer der Liste von Servern hinzu und installieren Sie den Agent for Windows auf dem Remote-Computer.
Siehe ["Hinzufügen von zu sichernden Servern zur Serverliste auf der Registerkarte "Backup und Wiederherstellung"](#) auf Seite 167.
- Zentrale Verwaltung der Installation von Agent for Windows auf Computern im Netzwerk mithilfe eines Microsoft Active Directory-Netzwerks
Siehe ["Installation von Agent for Windows in einem Active Directory-Netzwerk"](#) auf Seite 87.
- Verwenden Sie eine Eingabeaufforderung.
Siehe ["Installieren von Agent for Windows auf einem Remote-Computer über eine Eingabeaufforderung"](#) auf Seite 92.
- Nutzen Sie Befehlsskriptdateien.
Siehe ["Installieren von Agent for Windows mithilfe eines Befehlsskripts"](#) auf Seite 95.

Installieren von Agent for Windows auf Remote-Computern über eine Push-Installation

Sie können den Agent for Windows auf Remote-Computern von einem Backup Exec-Server über eine Push-Installation installieren. Push-Installationen sind zeitsparend, da es für die Installation nicht erforderlich ist, am Zielcomputer vor Ort anwesend zu sein. Sie können den Agent for Windows auf einer unbegrenzten Anzahl von Remote-Computern über eine Push-Installation installieren. Backup Exec kann bis zu fünf aktive Push-Installationen auf einmal verarbeiten.

Prüfen Sie vor der Installation von Agent for Windows auf Remote-Computern die folgenden Besonderheiten.

Tabelle 2-6 Besonderheiten bei der Installation von Agent for Windows

Element	Hinweis
ForceGuest-Konfiguration	<p>Die Push-Installation von Agent for Windows ist nicht möglich, wenn der Remote-Computer für ForceGuest konfiguriert ist und sich nicht in einer Domäne befindet. ForceGuest ist eine Betriebssystemkonfiguration, die Zugriffsrechte von Benutzern, die sich mit diesem System verbinden, auf die Zugriffsebene "Gast" beschränkt. Verwenden Sie stattdessen die Installationsmedien oder das Netzwerk, um Agent for Windows auf dem Windows-Computer zu installieren. Sie können ForceGuest auch deaktivieren. Weitere Informationen hierzu finden Sie in der Dokumentation zu Microsoft Windows.</p> <p>Siehe "Installieren von Backup Exec über die Befehlszeile (Silent-Mode)" auf Seite 103.</p>
Server Core-Option von Windows Server 2008/2012 und höher	<p>Backup Exec installiert eine Befehlszeilenversion von Agent for Windows auf den Computern, auf denen die Installationsoption "Server Core" von Windows Server 2008/2012 und höher ausgeführt wird. Das Backup Exec Agent Utility-Befehlszeilen-Applet wird mit Agent for Windows installiert. Mit diesem Applet können Sie Backup Exec-Vorgänge auf dem Remote-Computer überwachen.</p> <p>Siehe "Parameter für das Befehlszeilen-Applet von Backup Exec Agent Utility" auf Seite 1042.</p>
Windows-Datendeduplikation, ReFS-Datenträger und freigegebene Clustervolumes	<p>Sie können Agent for Windows nicht auf einem Datenträger installieren, der für die Datendeduplikation unter Windows, auf einem ReFS-Datenträger oder auf freigegebenen Clustervolumes aktiviert wurde.</p>

Element	Hinweis
Windows Vista/2008 oder höher	<p>Für die Push-Installation der Backup Exec-Funktionen auf einem Computer mit Windows Vista/Server 2008 oder höher müssen Sie in der Ausnahmenliste der Windows-Firewall des Zielcomputers bestimmte Elemente aktivieren. Diese sind:</p> <ul style="list-style-type: none"> ■ Datei- und Druckerfreigabe ■ Windows-Verwaltungsinstrumentation (WMI) <p>Weitere Informationen dazu finden Sie in der Dokumentation zu Microsoft Windows.</p> <p>Für die Push-Installation auf einem Computer mit dem unterstützten Backup Exec-Server muss sich der Zielcomputer in einer Domäne befinden.</p> <p>Weitere Informationen dazu finden Sie in der Microsoft Knowledge Base.</p>
Symantec Endpoint Protection 11.0 oder höher	<p>Um Funktionen mit einer Push-Installation auf einem Computer mit Symantec Endpoint Protection (SEP) Version 11.0 oder höher zu installieren, müssen Sie SEP für die Datei- und Druckerfreigabe konfigurieren. Die gemeinsame Nutzung von Dateien und Druckern ist standardmäßig deaktiviert.</p>
Vertrauen Sie dem Backup Exec-Server und dem Remote-Computer.	<p>Wenn Sie eine Verbindung vom Backup Exec-Server zu einem Remote-Computer herstellen, müssen Sie eine Vertrauensstellung zwischen dem Backup Exec-Server und dem Remote-Computer herstellen, um eine sichere Verbindung herzustellen. Um die Vertrauensstellung herzustellen, müssen Sie den Remote-Computer auf der Registerkarte "Backup und Wiederherstellung" der Liste von Servern hinzufügen.</p> <p>Siehe "Serverliste auf der Registerkarte 'Backup und Wiederherstellung'" auf Seite 166.</p>

Bei der Installation wird auf dem Computer, auf dem Backup Exec installiert wird, ein Installationsprotokoll namens `BKUPINST20.htm` erstellt und auf dem Remote-Computer das Protokoll "RAWSinst20.htm".

Siehe ["Info zum Installationsprotokoll"](#) auf Seite 113.

Wenn bei der Installation von Agent for Windows mithilfe dieses Verfahrens Probleme auftreten, können Sie Agent for Windows auch manuell installieren.

Siehe ["Installieren von Agent for Windows auf einem Remote-Computer über eine Eingabeaufforderung"](#) auf Seite 92.

So installieren Sie Agent for Windows über eine Push-Installation auf Remote-Computern

1 Sie haben folgende Möglichkeiten:

- | | |
|---|---|
| <p>So installieren Sie Agent for Windows über eine Push-Installation von den Installationsmedien auf Remote-Computern</p> | <p>Gehen Sie dazu nach folgender Reihenfolge vor:</p> <ul style="list-style-type: none"> ■ Klicken Sie im Installationsmedien-Browser auf "Installation" und dann auf "Backup Exec". ■ Aktivieren Sie auf der Startseite die Option "Ich nehme die Bedingungen der Lizenzvereinbarung an" aus, und klicken Sie auf "Weiter". ■ Klicken Sie auf "Benutzerdefinierte Installation". ■ Deaktivieren Sie "Lokale Installation" und aktivieren Sie "Remote-Installation". ■ Klicken Sie auf "Weiter". |
|---|---|

<p>So installieren Sie Agent for Windows über eine Push-Installation vom Backup Exec-Server aus auf Remote-Computern</p>	<p>Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Installation und Lizenzierung" und dann "Agents und Backup Exec-Server auf anderen Servern installieren".</p>
--	--

2 Sie haben folgende Möglichkeiten:

So installieren Sie Agent for Windows auf einem Remote-Computer

Gehen Sie dazu nach folgender Reihenfolge vor:

- Klicken Sie im Fenster "Remote-Computer" auf "Hinzufügen".
- Wählen Sie "Einzelcomputer hinzufügen" aus.
- Wählen Sie "Agent for Windows" und klicken dann auf "Weiter".
- Geben Sie den vollqualifizierten Namen des Remote-Computers ein oder klicken Sie auf "Remote-Computer durchsuchen", um den Remote-Computer zu lokalisieren.

So installieren Sie Agent for Windows auf mehreren Computern unter Verwendung der gleichen Einstellungen

Gehen Sie dazu nach folgender Reihenfolge vor:

- Klicken Sie im Fenster "Remote-Computer" auf "Hinzufügen".
- Wählen Sie "Mehrere Computer mit den gleichen Einstellungen hinzufügen" aus.
- Wählen Sie "Agent for Windows" und klicken dann auf "Weiter".
- Geben Sie den vollqualifizierten Namen des Remote-Computers ein oder klicken Sie auf "Durchsuchen", um den Remote-Computer zu lokalisieren.
- Klicken Sie auf "Zur Liste hinzufügen". Geben Sie den vollständig qualifizierten Namen ein und klicken Sie dann für alle Remote-Computer, auf denen Sie die Push-Installation der Funktionen ausführen möchten, auf "Zur Liste hinzufügen".

- 3 Geben Sie unter "Identifikationsdaten für Remote-Computer" die Identifikationsdaten ein, die Backup Exec zum Herstellen einer Verbindung mit den Remote-Servern verwenden kann.

Sie müssen Administrator-Identifikationsdaten verwenden.

- 4 Klicken Sie auf "Weiter".
- 5 Geben Sie im Feld "Zielordner" den Pfad ein, in dem Sie die Dateien installieren möchten.
- 6 Klicken Sie auf "Weiter".

7 Wenn die Remote-Computer von Backup Exec validiert wurden, können Sie die Liste wie folgt ändern:

So fügen Sie einen Remote-Computer manuell hinzu	Klicken Sie auf "Hinzufügen" und dann auf "Einzelcomputer hinzufügen".
--	--

So fügen Sie mehrere Remote-Computer manuell hinzu	Klicken Sie auf "Hinzufügen" und dann auf "Mehrere Computer mit den gleichen Einstellungen hinzufügen".
--	---

So fügen Sie mehrere Remote-Computer durch das Importieren einer vorhandenen Liste der Computer hinzu	<p>Klicken Sie auf "Importieren und exportieren", und wählen Sie dann eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> ■ Wählen Sie "Aus Datei importieren", um Backup Exec zum Hinzufügen der Namen der Remote-Computer aus einer ausgewählten Liste zu aktivieren. ■ Wählen Sie "Auf diesem Backup Exec-Server veröffentlichte Server importieren", damit Backup Exec die Namen aller Remote-Computer hinzufügen kann, die für die Veröffentlichung auf diesem Backup Exec-Server eingerichtet sind.
---	---

Sie müssen Remote-Computer-Identifikationsdaten für die Liste der Remote-Computer eingeben.

So ändern Sie das Produkt, das Sie zum Installieren oder Ändern anderer Installationseigenschaften ausgewählt haben	Wählen Sie den Remote-Computer aus, den Sie ändern möchten, und klicken Sie dann auf "Bearbeiten".
---	--

So löschen Sie einen Remote-Computer aus der Liste	Wählen Sie den Remote-Computer aus, den Sie löschen möchten, und klicken Sie dann auf "Löschen".
--	--

So sichern Sie die Liste der Remote-Computer und der verbundenen Remote-Computer-Identifikationsdaten	<p>Überprüfen Sie, dass "Serverliste für zukünftige Remote-Installationssitzungen speichern" markiert ist.</p> <p>Ist diese Option aktiviert, können die Namen aller Remote-Computer und ihrer Identifikationsdaten automatisch hinzugefügt werden, wenn Sie Backup Exec oder Funktionen auf diesen Remote-Computern installieren möchten.</p>
---	--

So speichern Sie die Liste der Remote-Computer in einer XML-Datei

Klicken Sie auf "Importieren und exportieren" und klicken Sie dann auf "In Datei exportieren".

Sie können den Speicherort auswählen, um die XML-Datei zu speichern. Diese Option ist nützlich, wenn Sie dieselbe Liste für mehrere Backup Exec-Server benutzen möchten. Wenn Sie die Liste importieren, müssen Sie die Remote-Computer-Identifikationsdaten erneut eingeben.

So beheben Sie die Fehler, die während der Validierung gefunden wurden

Klicken Sie mit der rechten Maustaste auf den Namen des Computers, und klicken Sie dann auf Fehler beheben.

So aktivieren Sie Backup Exec, um einen ungültigen Remote-Computer erneut zu validieren

Klicken Sie mit der rechten Maustaste auf den Namen des Computers, und klicken Sie dann auf Validierung erneut vornehmen.

- 8** Wenn alle Computer in der Liste validiert wurden und die Liste vollständig ist, klicken Sie auf "Weiter".
- 9** Lesen Sie die Backup Exec-Installationszusammenfassung und klicken Sie dann auf "Installieren".

Siehe ["Info zum Installationsprotokoll"](#) auf Seite 113.

- 10** Klicken Sie auf "Weiter" und anschließend auf "Fertigstellen", um den Assistenten zu schließen.

Wenn Sie den Remote-Computer noch nicht neu gestartet haben, müssen Sie den Neustart jetzt durchführen, damit die Konfigurationseinstellungen wirksam werden.

Updates für den Agent for Windows auf Remote-Computern installieren

Wenn ein Backup Exec-Server mit Patches aktualisiert wird, wird eine Warnmeldung generiert, um Sie darauf hinzuweisen, dass der Agent for Windows auf Remote-Computern mit den gleichen Patches aktualisiert werden muss. Darüber hinaus gibt die Eigenschaft "Entsprechen die Updates auf diesem Server den Updates, die auf dem Backup-Server installiert sind?" in den Eigenschaften des Remote-Computers an, ob der Remote-Computer an den Backup Exec-Server angeglichen wurde. Über die Backup Exec-Konsole können Sie die

Remote-Computer sofort, zu einem geplanten Zeitpunkt oder zu einem sich wiederholenden Zeitpunkt aktualisieren. Sie können eine Gruppe von Remote-Computern auch gleichzeitig aktualisieren.

Siehe ["Aktualisieren von Backup Exec mit Veritas Update"](#) auf Seite 115.

So installieren Sie Updates für den Agent for Windows

- 1** Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" mit der rechten Maustaste auf den Remote-Computer oder die Gruppe, die aktualisiert werden muss.
- 2** Wählen Sie "Aktualisieren".

3 Wählen Sie im Dialogfeld "Updates installieren" die gewünschte Option für den Zeitpunkt des Updates.

Wiederkehrend	Wählen Sie diese Option, um einen wiederkehrenden Zeitplan für den Auftrag zu erstellen.
Wiederholungsmuster	Soll der Auftrag nach einem Zeitplan wiederholt werden, konfigurieren Sie die Häufigkeit. Sie können den Auftrag stündlich, täglich, wöchentlich, monatlich oder jährlich ausführen.
Gestartet am	Geben Sie das Datum ein, an dem der Zeitplan wirksam werden soll.
Kalender	Zeigen Sie alle geplanten Aufträge im Kalender an, um Zeitplankonflikte zu suchen.
Den geplanten Auftrag für X Stunden beibehalten, bevor er neu geplant wird	Spezifizieren Sie die maximale Dauer nach der eingeplanten Startzeit, nach der Backup Exec den Auftrag als verpasst ansehen neu planen soll.
Abbrechen des Auftrags, falls er X Stunden nach der ursprünglich festgelegten Startzeit noch immer ausgeführt wird	Geben Sie den Zeitraum nach der geplanten Startzeit des Auftrags an, nach dessen Ablauf der Auftrag abgebrochen wird, wenn er noch ausgeführt wird.
Jetzt ohne regelmäßigen Zeitplan ausführen	Wählen Sie diese Option, um den Auftrag sofort auszuführen, ohne weitere Instanzen zu planen.
Ausführen am	Wählen Sie ein bestimmtes Datum für die Ausführung des Auftrags, ohne weitere Instanzen zu planen.
Computer automatisch neu starten, nachdem die Updates für Backup Exec Agent for Windows installiert wurden und wenn ein Neustart erforderlich ist	Wählen Sie diese Option, damit Backup Exec den Remote-Computer automatisch neu starten kann, wenn erforderlich.

4 Klicken Sie auf "OK".

Installation von Agent for Windows in einem Active Directory-Netzwerk

Sie können die Installation von Backup Exec Agent for Windows auf den Computern in einem Active Directory-Netzwerk zentral verwalten. Sie können die Installation einmal konfigurieren und dann ein Gruppenrichtlinienobjekt verwenden, um diese Installation Computern einer Organisationseinheit zuzuordnen. Die Funktionen werden automatisch installiert, wenn ein Computer der Organisationseinheit gestartet wird.

Hinweis: Überprüfen Sie die Bereitstellungspläne Ihrer Organisation, bevor Sie ein Rollout von Backup Exec Agent for Windows auf den Client-Computern implementieren. Sie sollten außerdem die Dokumentation zum Gruppenrichtlinien-Desktopmanagement und Active Directory durchlesen.

Tabelle 2-7 Installieren von Agent for Windows in einem Active Directory-Netzwerk

Aktion	Beschreibung
<p>Erstellen Sie eine Umformung für Agent for Windows.</p> <p>Siehe „Erstellen einer Umformung“ auf Seite 89.</p>	<p>Eine Umwandlung enthält die Änderungen, die Sie zum Windows-Installateuropaket für das Mittel für Windows, wenn ein Computer beginnt, wie den Installationspfad vornehmen möchten.</p> <p>Voraussetzungen für die Erstellung einer Umformung:</p> <ul style="list-style-type: none"> ■ Auf dem betreffenden Computer muss Microsoft Windows 2008 oder höher installiert sein. ■ Auf Windows Server 2008-Computern, auf denen Sie den Agent for Windows installieren möchten, muss .NET Framework 2.0 SP2 ausgeführt werden. ■ Agent for Windows kann nur auf Computern mit MSXML 6.0 installiert werden. ■ Die Computer, auf denen Sie den Agent for Windows installieren möchten, müssen Microsoft Visual C++ Runtime 8.0/9.0/10.0/11.0 ausführen. Sie können ein Gruppenrichtlinienobjekt konfigurieren, um alle Ablaufkomponenten von Microsofts Visual C++ bereitzustellen oder sie auf jedem Agent for Windows-Computer manuell zu installieren. Weitere Informationen über das Konfigurieren eines Gruppenrichtlinienobjekts erhalten Sie in Ihrer Microsoft Windows-Dokumentation. ■ Es werden nur Computerzuweisungen unterstützt. Benutzerzuweisungen werden nicht unterstützt.
<p>Erstellen Sie einen Verteilungspunkt (eine Freigabe), der die Quelldatei des zu installierenden Agent for Windows enthält.</p> <p>Siehe „Erstellen eines Software-Verteilungspunkts (Freigabe)“ auf Seite 90.</p>	<p>Sie müssen die Umformung, die Sie erstellen, und das Verzeichnis von Backup Exec RAWS32 oder RAWSX64 auf den Verteilungspunkt kopieren.</p>

Aktion	Beschreibung
<p>Konfigurieren Sie schließlich ein Gruppenrichtlinienobjekt, um die Umformung und das RAWXS32- bzw. RAWXS64-Verzeichnis im Verteilungspunkt Computern einer Active Directory-Organisationseinheit zuzuordnen.</p> <p>Siehe „Konfigurieren eines Gruppenrichtlinienobjekts“ auf Seite 90.</p>	<p>Die Software wird automatisch installiert, sobald die Computer der Organisationseinheit gestartet werden.</p>

Erstellen einer Umformung

Erstellen einer Umformung

- Sie haben folgende Möglichkeiten:
 - Klicken Sie im Installationsmedienbrowser von Backup Exec auf "Produkte installieren" und dann auf "Agent for Windows".
 - Öffnen Sie auf einem Backup Exec-Server, auf dem Backup Exec installiert ist, den Ordner "<Backup Exec-Installationspfad>\Backup Exec\Agents\RAWS32 or RAWXS64" und doppelklicken Sie auf "Setup.exe".
- Klicken Sie im Begrüßungsbildschirm auf "Weiter".
- Klicken Sie im Fenster "Installationsart" auf "Umformung erstellen, um Active Directory für die Installation des Agent for Windows zu verwenden" und anschließend auf "Weiter".
- Geben Sie im Fenster "Installationsoptionen" den Pfad, an dem Sie die Dateien installieren möchten, in den Bereich "Zielordner" ein.
- Klicken Sie auf "Weiter".
- Geben Sie einen Dateinamen und einen Pfad an, unter dem die Umformung erstellt werden soll, und klicken Sie auf "Weiter".

Wählen Sie für die Umformung einen beschreibenden Dateinamen. Zum Beispiel könnte der Name der Funktionen in der Umformung und das Betriebssystem enthalten, auf die for Umformung angewendet werden soll (z. B. "AgentStandardPfadKeineBekanntgabe").
- Um die Umformung zu erstellen, klicken Sie auf "Installieren".
- Nach erfolgter Erstellung der Umformung richten Sie einen Verteilungspunkt für die Quelldateien ein.

Erstellen eines Software-Verteilungspunkts (Freigabe)

Um Agent for Windows in einem Active Directory-Netzwerk zu installieren, müssen Sie nach Erstellung der Umformung einen Software-Verteilungspunkt erstellen.

Tabelle 2-8 So erstellen Sie einen Software-Verteilungspunkt (Freigabe)

Schritt	Beschreibung
Schritt 1	Erstellen Sie einen freigegebenen Ordner, und richten Sie die Berechtigungen so ein, dass Clientcomputer, auf denen die Installation erfolgen soll, Zugriff auf den gemeinsamen Ordner haben.
Schritt 2	<p>Kopieren Sie die folgenden Verzeichnisse vom Backup Exec-Server in den freigegebenen Ordner:</p> <ul style="list-style-type: none"> ■ RAWS32 oder RAWSX64 ■ MSXML ■ VCRdist ■ DotNetFx <p>Standardmäßig befinden sich diese Ordner in "<Backup Exec-Installationspfad>\Backup Exec\Agents".</p>
Schritt 3	Kopieren Sie die Umformung vom Pfad, unter dem sie erstellt wurde, in das RAWS32- bzw. RAWSX64-Verzeichnis im freigegebenen Ordner.
Schritt 4	Konfigurieren Sie ein Gruppenrichtlinienobjekt zum Verteilen der Quelldateien.

Konfigurieren eines Gruppenrichtlinienobjekts

Um Agent for Windows in einem Active Directory-Netzwerk zu installieren, müssen Sie ein Gruppenrichtlinienobjekt konfigurieren, nachdem Sie einen Software-Verteilungspunkt und eine Umformung erstellt haben.

So konfigurieren Sie ein Gruppenrichtlinienobjekt für die Installation der Software

- 1** Klicken Sie im Active Directory-Snap-In zur Verwaltung von einzelnen Benutzern und Benutzergruppen auf "Eigenschaften" und erstellen Sie ein neues Gruppenrichtlinienobjekt oder bearbeiten Sie ein bereits bestehendes.

Weitere Informationen zur Erstellung eines Gruppenrichtlinienobjekts finden Sie in der Dokumentation zu Microsoft Windows.
- 2** Erweitern Sie unter "Computerkonfiguration" den Knoten "Softwareeinstellungen".
- 3** Klicken Sie mit der rechten Maustaste auf "Software-Installation" und wählen Sie "Neu" und anschließend "Paket".
- 4** Suchen Sie im Dialogfeld "Datei öffnen" den Software-Verteilungspunkt, indem Sie den UNC-Namen (Universal Naming Convention) verwenden, beispielsweise \\Servername\Freigabename. Wählen Sie die Paketdatei und klicken Sie dann auf "Öffnen".
- 5** Wählen Sie die Paketdatei "Veritas Backup Exec Agent for Windows.msi" aus und klicken Sie auf "Öffnen".
- 6** Wenn Sie dazu aufgefordert werden, wenden Sie die erweiterbare Option an.
- 7** Nachdem Active Directory das MSI-Paket geprüft hat, müssen Sie auf der Registerkarte "Allgemeine Eigenschaften" sicherstellen, dass die richtige Version der Funktionen installiert wird.
- 8** Richten Sie auf der Registerkarte "Bereitstellung von Software" die Konfiguration für Ihre Umgebung ein.

Stellen Sie sicher, dass die Option "Diese 32-Bit-x86-Anwendung für WIN64-Computer verfügbar machen" nicht aktiviert ist.

Falls Sie den Agent for Windows deinstallieren möchten, wenn der Computer aus der Organisationseinheit genommen wird, wählen Sie die Option "Anwendung deinstallieren, wenn sie außerhalb des Verwaltungsbereichs liegt".
- 9** Klicken Sie auf der Registerkarte "Änderungen" auf "Hinzufügen", suchen Sie die Freigabe, und wählen Sie die von Ihnen erstellte Umformung aus.
- 10** Wählen Sie "Öffnen", nehmen Sie alle notwendigen Änderungen vor, und klicken Sie anschließend auf "OK".

11 Schließen Sie alle Dialogfelder.

Wenn ein Computer in der von Ihnen angegebenen Organisationseinheit gestartet wird, wird die Umformung verarbeitet und die angegebenen Funktionen werden installiert.

12 Zeigen Sie das Installationsprotokoll an, das auf den Zielcomputern erstellt wird, um die Installation von Agents for Windows zu überprüfen.

Installieren von Agent for Windows auf einem Remote-Computer über eine Eingabeaufforderung

Sie können Agent for Windows mithilfe einer Eingabeaufforderung installieren.

Der Installationsprozess erstellt ein Installationsprotokoll namens "RAWSinst20.htm".

Siehe "[Info zum Installationsprotokoll](#)" auf Seite 113.

So verwenden Sie eine Eingabeaufforderung für die Installation von Agent for Windows auf einem Remote-Computer

- 1 Ordnen Sie auf einem Remote-Computer dem Agent-Verzeichnis einen Laufwerksbuchstaben zu. Standardmäßig befindet sich das Agent-Verzeichnis unter folgendem Pfad:

<Backup Exec-Installationsordner>\Backup Exec\Agents

oder Sie können die folgenden Ordner auf dem gleichen lokalen Verzeichnis kopieren:

So installieren Sie auf einem 32-Bit-Computer

Ordner "RAWS32", "MSXML", "VCRedist" und "DotNetFx"

So installieren Sie auf einem 64-Bit-Computer

Ordner "RAWSX64", "MSXML", "VCRedist", und "DotNetFx"

- 2 Öffnen Sie ein Befehlszeilenfenster und geben Sie den in Schritt 1 zugeordneten Laufwerksbuchstaben sowie den folgenden Pfad ein:

So installieren Sie auf einem 32-Bit-Computer

`\RAWS32`

So installieren Sie auf einem 64-Bit-Computer

`\RAWSX64`

3 Sie haben folgende Möglichkeiten:

So installieren Sie Agent for Windows auf einem 32-Bit-Computer ohne Veröffentlichung

Führen Sie folgenden Befehl aus:
`setup.exe /RANT32: /S:
/DISADVRT:`

So installieren Sie Agent for Windows auf einem 32-Bit-Computer mit aktivierter Veröffentlichung

Führen Sie folgenden Befehl aus:
`setup.exe /RANT32: /S: /ADVRT:
Backup Exec-Servername 1 Backup
Exec-Servername 2`

So installieren Sie Agent for Windows auf einem 32-Bit-Computer und starten den Computer automatisch neu

Führen Sie folgenden Befehl aus:
`setup.exe/RANT32: /S: /BOOT:`

So installieren Sie Agent for Windows auf einem 64-Bit-Computer ohne Veröffentlichung

Führen Sie folgenden Befehl aus:
`setup.exe /RAWSX64: /S:
/DISADVRT:`

So installieren Sie Agent for Windows auf einem 64-Bit-Computer mit aktivierter Veröffentlichung

Führen Sie folgenden Befehl aus:
`setup.exe /RAWSX64: /S: /ADVRT:
Backup Exec-Server 1 Backup
Exec-Server 2`

So installieren Sie Agent for Windows auf einem 64-Bit-Computer und starten den Computer automatisch neu

Führen Sie folgenden Befehl aus:
`setup.exe /RAWSX64 /S: /BOOT:`

Agent for Windows wird auf dem Remote-Computer im folgenden Verzeichnis installiert:

Wenn Sie Agent for Windows auf einem 32-Bit-Computer installiert haben:

`<Backup
Exec-Installationsordner>\Backup
Exec\RAWS32`

Wenn Sie Agent for Windows auf einem 64-Bit-Computer installiert haben:

`<Backup
Exec-Installationsordner>\Backup
Exec\RAWSx64`

Deinstallieren von Agent for Windows von einem Remote-Computer über eine Eingabeaufforderung

Sie können Agent for Windows über eine Eingabeaufforderung deinstallieren.

So deinstallieren Sie Agent for Windows von einem Remote-Computer über eine Eingabeaufforderung

- 1 Ordnen Sie auf dem Remote-Computer dem Agent for Windows-Verzeichnis einen Laufwerksbuchstaben zu, wobei Sie den folgenden Pfad verwenden:

So deinstallieren Sie Agent for Windows von einem 32-Bit-Computer

```
<Backup
Exec-Installationsordner>\Backup
Exec\Agents\RAWS32
```

So deinstallieren Sie Agent for Windows von einem 64-Bit-Computer:

```
<Backup
Exec-Installationsordner>\Backup
Exec\Agents\RAWSX64
```

- 2 Öffnen Sie eine Eingabeaufforderung, und geben Sie dann den in Schritt 1 zugeordneten Laufwerksbuchstaben ein.
- 3 Führen Sie folgenden Befehl aus:

So deinstallieren Sie Agent for Windows von einem 32-Bit-Computer

```
setup.exe /RANT32: /S: /U:
```

Mit dem Parameter /S: wird der Vorgang im Silent-Mode und ohne die Vorteile einer Benutzeroberfläche ausgeführt. Der Parameter /U: bezeichnet einen Deinstallationsvorgang.

So deinstallieren Sie Agent for Windows von einem 64-Bit-Computer:

```
setup.exe /RAWSX64: /S: /U:
```

Siehe ["Installieren von Agent for Windows auf einem Remote-Computer über eine Eingabeaufforderung"](#) auf Seite 92.

Installieren von Agent for Windows mithilfe eines Befehlsskripts

Sie können Agent for Windows mithilfe von Befehlsskriptdateien installieren. Die Befehlsskriptdateien sind im Backup Exec-Installationsverzeichnis enthalten.

Der Installationsprozess erstellt ein Installationsprotokoll namens "RAWSinst20.htm".

Siehe ["Info zum Installationsprotokoll"](#) auf Seite 113.

So installieren Sie Agent for Windows mithilfe eines Befehlsskripts

- 1** Weisen Sie dem Agent-Verzeichnis auf einem Backup Exec-Server einen Laufwerksbuchstaben zu. Standardmäßig befindet sich das Agent-Verzeichnis unter folgendem Pfad:

<Backup Exec-Installationsordner>\Backup Exec\Agents

- 2** Sie haben folgende Möglichkeiten:

So installieren Sie Agent for Windows auf einem 32-Bit-Computer	Doppelklicken Sie im Verzeichnis RAW32 auf "setupaa".
---	---

So installieren Sie Agent for Windows auf einem 64-Bit-Computer	Doppelklicken Sie im Verzeichnis RAW64 auf "setupaa64".
---	---

Deinstallieren von Agent for Windows mithilfe eines Befehlsskripts

Eine Befehlsskriptdatei für die Deinstallation von Agent for Windows ist verfügbar.

So deinstallieren Sie Agent for Windows mithilfe eines Befehlsskripts

- 1** Weisen Sie dem Agent-Verzeichnis auf einem Backup Exec-Server einen Laufwerksbuchstaben zu. Standardmäßig befindet sich das Agent-Verzeichnis im folgenden Pfad:

<Backup Exec-Installationsordner>\Backup Exec\Agents

- 2** Sie haben folgende Möglichkeiten:

So deinstallieren Sie Agent for Windows von einem 32-Bit-Computer	Doppelklicken Sie im Verzeichnis "RAW32" auf "Uninstallaafo".
---	---

So deinstallieren Sie Agent for Windows von einem 64-Bit-Computer	Doppelklicken Sie im Verzeichnis "RAW64" auf "Uninstallaafo64".
---	---

- 3** Starten Sie den Computer neu.

Siehe ["Installieren von Agent for Windows mithilfe eines Befehlsskripts"](#) auf Seite 95.

Installieren von Remote Administrator

Der Remote Administrator dient zur Verwaltung des Backup Exec-Servers von einem Windows-Server oder einer Windows-Workstation an einem Remote-Standort. Um den Remote Administrator zu unterstützen, müssen die Backup

Exec-Systemdienste auf dem Backup Exec-Server ausgeführt werden, den Sie verwalten möchten.

Hinweis: Backup Exec unterstützt Remote Administrator unter 32-Bit-Betriebssystemen nicht.

Sie können Remote Administrator nicht verwenden, um die Server zu verwalten, auf denen eine andere Version von Backup Exec installiert ist. Der Einsatz verschiedener Versionen von Remote Administrator zum Verwalten verschiedener Versionen von Backup Exec ist jedoch möglich.

So installieren Sie den Remote Administrator

- 1** Klicken Sie im Installationsmedien-Browser auf "Produkte installieren".
- 2** Klicken Sie auf "Backup Exec".
- 3** Aktivieren Sie auf der Startseite die Option "Ich nehme die Bedingungen der Lizenzvereinbarung an" aus und klicken Sie auf "Weiter".
- 4** Aktivieren Sie im Teilfenster "Installationstyp" die Option "Benutzerdefinierte Installation" und klicken Sie dann auf "Weiter".
- 5** Aktivieren Sie die Option "Lokale Installation" und klicken Sie dann auf "Nur remote Administratorkonsole installieren".
- 6** Klicken Sie auf "Weiter".
- 7** Führen Sie im Fenster "Ziel" einen der folgenden Schritte aus:
 - Überprüfen Sie die Speicherplatzanforderungen für die Installation.
 - Um den Speicherort zu ändern, in dem die Dateien installiert werden, klicken Sie auf Ändern. So können Sie ein anderes Verzeichnis für die Installation auswählen.
- 8** Klicken Sie auf "Weiter".
- 9** Überprüfen Sie die Backup Exec-Installationszusammenfassung und klicken Sie dann auf "Installieren".
- 10** Klicken Sie auf "Weiter" und anschließend auf "Fertigstellen", um den Assistenten zu schließen.

Siehe ["Ausführen des Remote Administrator"](#) auf Seite 100.

Installieren von Remote Administrator über die Befehlszeile

Sie können auch die Silent-Mode-Installation verwenden, um den Remote Administrator zu installieren. Optionen für Remote Administrator werden mit dem Gebrauch von weiteren Befehlsparametern festgelegt.

Hinweis: Backup Exec unterstützt Remote Administrator unter 32-Bit-Betriebssystemen nicht.

Sie können Remote Administrator nicht verwenden, um die Server zu verwalten, auf denen eine andere Version von Backup Exec installiert ist. Der Einsatz verschiedener Versionen von Remote Administrator zum Verwalten verschiedener Versionen von Backup Exec ist jedoch möglich.

So installieren Sie Remote Administrator über die Befehlszeile:

- 1 Öffnen Sie eine Windows-Eingabeaufforderung.
- 2 Wechseln Sie zum Laufwerk, das das Backup Exec-Installationsmedium enthält.
- 3 Wechseln Sie zum folgenden Verzeichnis:

```
\be\winnt\install\bex64
```

- 4 Geben Sie `setup /TS:` und die entsprechenden Switches ein. Beispiel:

```
setup /RA: /S:
```

Die Befehlszeilenparameter für die Installation von Remote Administrator im Silent-Mode werden in der folgenden Tabelle beschrieben.

Beachten Sie die folgenden allgemeinen Regeln für den Einsatz von Parametern:

- Ersetzen Sie kursiv dargestellte Werte durch die auf Ihre Umgebung zutreffenden Werte, z. B. *Kennwort* durch Ihr Kennwort.
- Schließen Sie den Wert in Anführungszeichen ein, wenn er Leerzeichen enthält, z. B. "<Backup Exec-Installationspfad>\Backup Exec".

Tabelle 2-9 Befehlszeilenparameter für die Installation des Remote Administrators im Silent-Mode

Parameter	Zusätzliche Parameter	Beschreibung
/RA:		Installiert Remote Administrator unter Verwendung der Optionen, die mit den zusätzlichen Switches angegeben wurden.
	/DEST:" <i>Laufwerk:\Pfad</i> "	Legt den Pfad fest, in dem der Remote Administrator installiert wird. Andernfalls wird der Standardpfad <i><Backup Exec-Installationsmode>Bakup Exec</i> genutzt.
	/DOCS:	Installiert die Online-Dokumentation.
	/NOINSTALL:	Hier können Sie alle Installationsoptionen auswählen, ohne Backup Exec tatsächlich zu installieren. Diese Option kann mit dem Switch "/CPF:" verwendet werden.

Parameter	Zusätzliche Parameter	Beschreibung
	<i>/CPF:"Pfad\Dateiname.cpf"</i>	Erstellt eine Datei, die alle eingegebenen Installationsparameter enthält. Beachten Sie, dass die XML-Datei nicht verschlüsselt ist, d. h. Parameter, wie z. B. das Kennwort, werden unverschlüsselt angezeigt.
-?		Hilfe zum Einsatz der Befehlszeile.

Siehe ["Installieren von Backup Exec über die Befehlszeile \(Silent-Mode\)"](#) auf Seite 103.

Ausführen des Remote Administrator

Der Remote Administrator dient zur Verwaltung des Backup Exec-Servers von einem Windows-Server oder einer Windows-Workstation an einem Remote-Standort. Um den Remote Administrator zu unterstützen, müssen die Backup Exec-Systemdienste auf dem Backup Exec-Server ausgeführt werden.

Sie werden möglicherweise aufgefordert, einen Benutzernamen und ein Kennwort einzugeben, um eine Netzwerkfreigabe zu durchsuchen, und zwar auch dann, wenn Sie im remoten Administratorsystem unter einem Konto eingeloggt sind, das für diese Freigaben gültig ist. Geben Sie einen domänenqualifizierten Benutzernamen und ein domänenqualifiziertes Kennwort ein, wenn Sie dazu aufgefordert werden (z. B. Domäne1\Hans).

Wenn Sie sich bei unterschiedlichen Arbeitsgruppen einloggen, können Sie bei den Eingaben der Login-Daten für die Arbeitsgruppenkonten die Eingabezeile für die Arbeitsgruppe leer lassen und lediglich eine Benutzer-ID angeben.

Hinweis: Backup Exec unterstützt Remote Administrator unter 32-Bit-Betriebssystemen nicht. Sie können Remote Administrator nicht verwenden, um die Server zu verwalten, auf denen eine andere Version von Backup Exec installiert ist. Der Einsatz verschiedener Versionen von Remote Administrator zum Verwalten verschiedener Versionen von Backup Exec ist jedoch möglich.

Siehe "[Installieren von Remote Administrator](#)" auf Seite 96.

So führen Sie Remote Administrator aus

- 1** Klicken Sie auf "Starten".
- 2** Zeigen Sie auf "Programme", und klicken Sie dann auf "Backup Exec".

Wenn Sie eine Verbindung von einem Backup Exec-Server zu einer Remote-Administratorkonsole herstellen, klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Mit Backup Exec-Server verbinden".

3 Wählen Sie die entsprechenden Optionen aus.

Dienste verwalten	Wählen Sie diese Option zum Aufrufen des Backup Exec-Dienstmanagers, um Dienste anzuhalten und zu starten oder um Identifikationsdaten für das Ausführen der Dienste festzulegen.
Servername	<p>Geben Sie den Namen des Backup Exec-Servers ein. Sie können den Namen aus der Liste auswählen oder den Namen des Servers eingeben, wenn Sie Remote Administrator von einem Backup Exec-Server aus ausführen.</p> <p>Jeder Server in der Domäne, auf dem Backup Exec installiert wurde, wird automatisch im Listenfeld angezeigt.</p>
Benutzername	<p>Geben Sie einen Administrator-Benutzernamen für den Server an, mit dem Sie eine Verbindung herstellen möchten. Geben Sie den Benutzernamen im Format "Domäne\Benutzername" an.</p> <p>Das Einloggen bei der Remote-Administratorkonsole über einen Benutzernamen ohne Kennwort ist unter Windows Server 2008 und Vista nicht möglich. Dazu müssen Sie Windows so konfigurieren, dass leere Kennwörter zugelassen werden. Andernfalls wird die Fehlermeldung "Fehler beim Login: Einschränkung des Benutzerkontos" angezeigt. Weitere Informationen dazu finden Sie in der Windows-Dokumentation.</p>
Kennwort	Geben Sie das Kennwort für den Benutzer ein.
Domäne	Geben Sie die Domäne an, welcher der Benutzer angehört. Geben Sie den Namen der Domäne ein, die in der Option "Benutzername" verwendet wurde.

Der Status der lokalen Dienste wird am unteren Rand dieses Dialogfelds angezeigt. Wenn Sie eine Verbindung zu diesem Server herstellen möchten

und diese fehlschlägt, wird in diesem Dialogfeld der Status des Dienstes für den Server angezeigt, zu dem Sie eine Verbindung herstellen wollten.

4 Klicken Sie auf "OK".

Wenn Sie die Funktion "Konsole sperren" verwendet haben, um die Backup Exec-Konsole zu sperren, müssen Sie Identifikationsdaten zur Verbindung mit dem Backup Exec-Server eingeben.

Siehe ["Sperren und Freigeben der Backup Exec-Konsole"](#) auf Seite 134.

Installieren von Backup Exec über die Befehlszeile (Silent-Mode)

Die Installation von Backup Exec über die Befehlszeile wird als Silent-Mode-Installation bezeichnet. Bei dieser Installationsmethode werden das Programm "setup.exe" auf dem Backup Exec-Installationsmedium, eine Reihe von Befehls-Switches und der Switch "/S:" verwendet.

Voraussetzungen für die Befehlszeileninstallation:

- Backup Exec-Installationsmedium.
- Administratorrechte auf dem Computer, auf dem Backup Exec installiert, konfiguriert oder von dem das Produkt deinstalliert werden soll

Beim Installieren wird das Installationsprotokoll `BKUPINST20.htm` auf dem Computer erstellt, auf dem Backup Exec installiert wird.

Siehe ["Info zum Installationsprotokoll"](#) auf Seite 113.

So installieren Sie Backup Exec über die Befehlszeile (Silent-Mode)

- 1** Öffnen Sie eine Windows-Eingabeaufforderung.
- 2** Wechseln Sie zum Laufwerk, das das Backup Exec-Installationsmedium enthält.
- 3** Wechseln Sie zum folgenden Verzeichnis:

```
\be\winnt\install\bex64
```

4 Geben Sie `setup /TS:` und die entsprechenden Switches ein. Beispiel:

```
setup /TS: /USER:<user> /DOM:Domane /PASS:Kennwort
/SLF: "C:\Pfad\slf.slf", "C:\Pfad\slf2.slf" /S:
```

Siehe ["Befehlszeilen-Switches für die Installation von Backup Exec im Silent-Mode"](#) auf Seite 104.

Wenn Sie die Befehlszeilen-Switches ohne den Switch `/S:` verwenden, wird das Installationsprogramm für Backup Exec mit den Befehlszeilenparametern als Standardwerten für die Installationsoptionen gestartet. Wenn `/S:` etwa im oben genannten Beispiel ausgelassen wurde, werden beim Start des Installationsprogramms für Backup Exec der Benutzername, die Domäne, das Kennwort und die Lizenz verwendet, die in den Installationsdialogfeldern angezeigt werden.

5 Drücken Sie die Eingabetaste.

Befehlszeilen-Switches für die Installation von Backup Exec im Silent-Mode

Die Befehlszeilenparameter für die Backup Exec-Installation im Silent-Mode werden in der folgenden Tabelle beschrieben.

Im Folgenden sehen Sie allgemeine Regeln für die Anwendung dieser Parameter:

- Ersetzen Sie kursiv dargestellte Werte durch die auf Ihre Umgebung zutreffenden Werte. Beispiel: Ersetzen Sie einen Benutzernamen mit *user*.
- Schließen Sie den Wert in Anführungszeichen ein, wenn er Leerzeichen enthält, beispielsweise "Wöchentliches Backup".

Siehe ["Installieren von Backup Exec über die Befehlszeile \(Silent-Mode\)"](#) auf Seite 103.

Tabelle 2-10 Befehlszeilen-Switches für die Installation von Backup Exec im Silent-Mode

Parameter	Zusätzliche Parameter	Beschreibung
/TS:		Installiert Backup Exec unter Verwendung der Optionen, die mit den zusätzlichen Switches angegeben wurden. Erforderlich: /USER:"Benutzer" /DOM:"dm" /PASS:"kw".

Parameter	Zusätzliche Parameter	Beschreibung
	/USER: " <i>Benutzer</i> " /DOM: " <i>dm</i> " /PASS: " <i>kw</i> "	<p>Erforderlich. Legt einen vorhandenen Benutzer, eine Domäne und ein Kennwort für das Backup Exec-Systemdienstkonto fest. Bei der Installation im Silent-Mode wird kein Benutzer angelegt.</p> <p>Hinweis: Wenn bei der Verwendung von "/PASS:" Anführungszeichen als Bestandteil des Kennworts benötigt werden, müssen Sie diese in folgendem Format eingeben: \". Wenn z. B. das Kennwort Kenn"wort lautet, geben Sie /PASS:kenn\"wort ein. Wenn die Zeichen \" Teil des Kennwortes sind, muss jedem Zeichen ein \ vorausgehen. Wenn z. B. das Kennwort Kenn\"wort lautet, geben Sie /PASS:kenn\\\"wort ein.</p>
	/DEST:" <i>Laufwerk</i> :\ <i>Pfad</i> "	<p>Der lokale Pfad, in dem Backup Exec installiert ist. Andernfalls wird der Standardpfad <i><Backup Exec-Installationsordner>\Backup Exec</i> genutzt.</p>
	/DOCS:	Installiert die Online-Dokumentation.

Parameter	Zusätzliche Parameter	Beschreibung
	/BELANG: <i>Sprache</i>	<p>Installiert die Backup Exec-Sprachressourcendateien.</p> <p>Geben Sie mit den Backup Exec-Sprachparametern eine oder mehrere der folgenden Parameter an, um anzugeben, welche Sprachdateien Sie installieren möchten:</p> <ul style="list-style-type: none"> ■ EN installiert Englisch. ■ DE installiert Deutsch. ■ ES installiert Spanisch. ■ FR installiert Französisch. ■ IT installiert Italienisch. ■ PT installiert Portugiesisch. ■ RU installiert Russisch. ■ JP installiert Japanisch. ■ KO installiert Koreanisch. ■ ZH installiert Chinesisch (vereinfacht). ■ CH installiert Chinesisch (traditionell). <p>Das folgende Beispiel zeigt an, wie der Parameter "/BELANG" verwendet werden kann, um Englisch, Deutsch und Spanisch zu installieren:</p> <p>/BELANG: "EN DE ES"</p>
	/NOINSTALL:	<p>Ermöglicht Ihnen, alle Installationsoptionen auszuwählen, ohne die Backup Exec-Software tatsächlich zu installieren. Diese Option kann mit dem Switch "/CPF:" verwendet werden.</p>
	/CPF:" <i>Pfad\Dateiname.cpf</i> "	<p>Erstellt eine Datei, die alle eingegebenen Installationsparameter enthält. Beachten Sie, dass die Datei nicht verschlüsselt wird, sodass Parameter sichtbar sind.</p>

Parameter	Zusätzliche Parameter	Beschreibung
	/SLF: <i>slf-Datei</i>	<p>Legt eine oder mehrere Lizenzen fest, die für die Installation von Backup Exec und zusätzlicher Funktionen verwendet werden sollen. Für die Installation von Remote Administrator sind keine Lizenzen erforderlich. Sie können maximal 99 Lizenzen angeben. Fehlt die Angabe von Lizenzen, wird eine Backup Exec-Testversion installiert.</p> <p>Die folgenden Beispiele zeigen, wie der Switch "/SLF" verwendet werden kann:</p> <p><i>/SLF:"C:\path\slf1.slf"</i></p> <p><i>/SLF:"C:\path\slf1.slf","C:\path\slf2.slf","C:\path\ slf3.slf"</i></p> <p>Hinweis: Wenn Sie eine Lizenz für eine Funktion oder einen Agent installieren, müssen Sie auch einen Parameter eingeben, der die Funktion bzw. den Agent angibt. Die Parameter, die eine Funktion oder einen Agent angeben, sind in dieser Tabelle enthalten.</p>
	/DISABLETELEMETRY:	Deaktiviert die Option, Backup Exec-Nutzungsdaten per Internet zu senden.
	/BOOT:	Initiiert automatisch einen Neustart des Computers während einer Installation im Hintergrund oder einer Deinstallation.

Parameter	Zusätzliche Parameter	Beschreibung
	/TD:NEW, ALL oder NONE	<p>Hinweis: Keine der zusätzlichen /TD-Schalter werden für Windows Server 2012 oder höher unterstützt.</p> <p>/TD:NEW installiert Bandlaufwerke nur für Laufwerke, die keine Treiber geladen haben.</p> <p>/TD:ALL installiert Bandtreiber für alle Laufwerke.</p> <p>/TD:NONE installiert keine Bandgerätetreiber.</p> <p>Hinweis: Um die Bandtreiber unter Windows Server 2008 R2 zu installieren, müssen Sie die Signierungsrichtlinie für Windows-Treiber auf "Ignorieren" festlegen. Bei Windows Server 2008 schlägt die Treiberinstallation jedoch fehl, wenn für die Signierungsrichtlinie "Ignorieren" festgelegt ist. Sie können die Treiber stattdessen mithilfe des Installationsprogramms für Gerätetreiber (tapeinst.exe) installieren. Weitere Informationen zu Signierungsrichtlinien finden Sie in der Microsoft Windows-Dokumentation.</p>
	/DBSERVER:"Server\Instanz"	Installiert die Backup Exec-Datenbank auf dem angegebenen SQL-Server.
	/BACKUPDATA:	Gibt an, wenn eine Kopie der aktuellen Backup Exec-Datenbank während eines Upgrade von Backup Exec gespeichert wird.

Parameter	Zusätzliche Parameter	Beschreibung
	/BACKUPDIR:	<p>Gibt den Speicherort an, an dem die Backup Exec-Datenbank während eines Upgrade von Backup Exec gespeichert wird. Der Ordner, den Sie auswählen, muss leer sein. Eine Kopie Ihrer aktuellen Backup Exec-Datenbank wird an dem Speicherort abgelegt, den Sie angeben und wird verwendet, wenn das Upgrade ausfällt.</p> <p>Hinweis: Dieser Parameter wird ignoriert, wenn der entsprechende Parameter "/BACKUPDATA:" nicht angegeben wird.</p>
	/DBINSTPATH: <i>"SQL Express-Zielverzeichnis"</i>	Installiert die Standardinstanz von SQL Express im dafür bestimmten Ordner.
	/ADVRT: <i>"Backup Exec-Server"</i>	Installiert Agent for Windows und ermöglicht die Veröffentlichung.
	/DISADVRT:	Installiert Agent for Windows ohne Bekanntgabe.
	/SQLXSETUP: <i>"SQL Express Install Package"</i>	Gibt den Speicherort des sprachspezifischen Installationspakets für Microsoft SQL Server 2014 Express mit SP2 an.
	/LOADER:	Installiert Library Expansion Feature. Diese Funktion wird nicht für Windows Server 2012 oder höher unterstützt.
	/NFR:	Installiert die nicht für den Weiterverkauf bestimmte Version. Um diese Version zu installieren, müssen Sie eine Lizenz für die nicht für den Weiterverkauf bestimmte Version eingeben.
	/TRIAL:	Installiert die Testversion.
	/APPLICATIONS:	Installiert Agent for Databases and Applications.
	/VRAY	Installiert die V-Ray Edition. Sie müssen eine V-Ray-Lizenz eingeben, um diese Version zu installieren.

Parameter	Zusätzliche Parameter	Beschreibung
	/CAPACITY	Installiert die Capacity Edition. Sie müssen eine Capacity-Lizenz eingeben, um diese Version zu installieren.
	/CAPACITYLITE	Installiert Capacity Edition Lite. Sie müssen eine Lizenz für Capacity Editions Lite eingeben, um diese Edition zu installieren
	/VIRT:	Installiert Agent for VMware and Hyper-V.
	/ENTSERVER:	<p>Installiert Enterprise Server Feature.</p> <p>Für den Enterprise Server Feature-Switch müssen Sie außerdem mindesten einen der folgenden Switches verwenden, um anzugeben, welche Funktion installiert werden soll.</p> <ul style="list-style-type: none"> ■ /CASO: Installiert Central Admin Server Feature. ■ /ADBO: Installiert Advanced Disk Based Backup Feature.
	/ADBO:	<p>Installiert Advanced Disk Based Backup Feature.</p> <p>Mit diesem Switch müssen Sie /ENTSERVER: verwenden.</p>
	/CASO:	<p>Installiert Central Admin Server Feature.</p> <p>Mit diesem Switch müssen Sie /ENTSERVER: verwenden.</p>
	/MMS:"CAS-Servername"	Erstellt einen verwalteten Backup Exec-Server zur Verwendung mit Central Admin Server Feature.

Parameter	Zusätzliche Parameter	Beschreibung
	/CASOPVLLOCAL: <1 oder 0>	<p>/CASOPVLLOCAL:1 zeigt an, dass Geräte- und Mediendaten lokal auf dem verwalteten Server gespeichert werden. Verwenden Sie diesen Parameter mit "/MMS:".</p> <p>/CASOPVLLOCAL:0 zeigt an, dass Geräte- und Mediendaten auf dem Administrationsserver gespeichert werden. Verwenden Sie diesen Parameter mit "/MMS:".</p>
	/ACCESSCATALOGSANDRESTORE:	<p>Aktiviert uneingeschränkten Zugriff auf Kataloge und Backup-Sätze zur Wiederherstellung.</p> <p>Dieser Switch wird mit dem Switch "/MMS:<CAS-Servername>" verwendet und ersetzt den Switch "/SSO:<Name des primären Servers>".</p>
	/NTA:	Installiert Agent for Windows.
	/NDMP:	Installiert NDMP Feature.
	/RALS:	Installiert Agent for Linux.
	/DEDUPE:	Installiert Deduplication Feature.
	/VTL:	Installiert Virtual Tape Library Unlimited Drive Feature.
	/RMAL:	Installiert Remote Media Agent for Linux.
	/COPYCONFIG:	Installiert die Funktion "Serverkonfigurationen kopieren".
-?		Hilfe zum Einsatz der Befehlszeile.

Installationsparameterdateien erstellen und einsetzen

Wenn Sie die Befehlszeilen-Switches ohne den Switch "/S:" verwenden, wird das Installationsprogramm für Backup Exec mit den Befehlszeilenparametern als Standardwerten für die Installationsoptionen gestartet. Geben Sie beispielsweise Folgendes ein:

```
SETUP /TS: /USER:Benutzer /DOM:Domäne /PASS:Kennwort
/SLF: "C:\Pfad\slf1.slf"
```

Das Installationsprogramm von Backup Exec wird gestartet. Der Bildschirm, in dem Sie die Login-Daten und die Lizenz eingeben können, wird angezeigt. Er enthält die Informationen, die Sie in der Befehlszeile angegeben haben.

Sie können außerdem den Befehl /CPF: verwenden, um eine Parameterdatei zu erstellen, die alle angegebenen Befehlszeilenoptionen enthält. Diese Parameterdatei kann dazu verwendet werden, Optionen für die Installation von Backup Exec oder Remote Administrator bereitzustellen. Beachten Sie, dass die XML-Datei nicht verschlüsselt ist, d. h. Parameter, wie z. B. das Kennwort, werden unverschlüsselt angezeigt.

So erstellen Sie Installationsparameterdateien:

- 1 Öffnen Sie eine Windows-Eingabeaufforderung.
- 2 Wechseln Sie zum Laufwerk, das das Backup Exec-Installationsmedium enthält.
- 3 Wechseln Sie zum folgenden Verzeichnis:

```
BE\WINNT\INSTALL\Bex64
```

- 4 Geben Sie `setup /TS:` und die entsprechenden Switches, einschließlich `"/CPF:"` und den vollständigen Pfad der Parameterdatei, an. Geben Sie beispielsweise Folgendes ein:

```
setup /TS: /USER:Benutzer /DOM:Domäne
/PASS:Kennwort/SLF: "C:\Pfadname\slf1.slf" /CPF: "A:\Dateiname" /S:
```

Backup Exec wird auf Ihrem Server installiert. Außerdem wird eine Parameterdatei, die den Benutzernamen, die Domäne, das Kennwort und die Lizenz enthält, auf einem Wechseldatenträger gespeichert. Sie können diese Parameterdatei zur Installation auf einem anderen Computer verwenden.

So verwenden Sie Installationsparameterdateien

- 1 Öffnen Sie eine Windows-Eingabeaufforderung.
- 2 Wechseln Sie zum Laufwerk, das das Backup Exec-Installationsmedium enthält.
- 3 Wechseln Sie zum folgenden Verzeichnis:

```
BE\WINNT\INSTALL\Bex64
```

- 4 Geben Sie Folgendes ein: `SETUP /PARAMS:"A:\Dateiname" /S:`
- 5 Wenn Sie einen Parameter überschreiben möchten, müssen Sie einen neuen Parameter festlegen. Um beispielsweise das Kennwort zu ändern, geben Sie Folgendes ein: `SETUP /PARAMS:"A:\Dateiname" /PASS:neues Kennwort/S:`

Info zum Installationsprotokoll

Backup Exec erstellt die Installationsprotokolldatei `BKUPINST20.htm`, wenn Backup Exec und Patches installiert werden. Diese Protokolldatei kann Ihnen dabei helfen, Installationsprobleme zu lösen. Die Protokolldatei enthält TechNotes für die am häufigsten auftretenden Fehler. Wenn Sie Agent for Windows installieren, wird auch die Protokolldatei "RAWSinst20.htm" erstellt.

Der Text der Protokolldatei liegt zudem in den folgenden Farben vor, damit Warnungen und Fehler leichter identifiziert werden können:

Tabelle 2-11 Installationsprotokollfarben

Farbe	Entsprechung
Schwarz	Normaler Betrieb
Orange	Warnmeldungen
Rot	Fehlermeldungen

Die Datei `BKUPINST20.htm` befindet sich am folgenden Speicherort:

Windows 2008 und höher: %ProgramData%\Veritas\Backup Exec\Protokolle

Hinweis: Der Ordner "ProgramData" ist möglicherweise ausgeblendet. Anweisungen zum Anzeigen ausgeblendeter Ordner finden Sie in der Microsoft Windows-Dokumentation.

Anzeigen des Installationsübersichtsberichts

Backup Exec erstellt einen Installationsübersichtsbericht, der die von Ihnen während der Installation ausgewählten Konfigurationseinstellungen enthält. Der Installationsübersichtsbericht wird mit dem Produktnamen und den Berechtigungs-IDs aktualisiert, wenn Sie zusätzliche Agents oder Funktionen installieren. Er wird auch dann aktualisiert, wenn Sie Agents oder Funktionen aus Backup Exec entfernen.

Der Installationsübersichtsbericht wird im folgenden Speicherort abgelegt:

Windows 2008 und höher: %ProgramData%\Veritas\Backup Exec\Protokolle\InstallSummary\<Computername>.htm

Der Installationsübersichtsbericht kann jederzeit über die Backup Exec-Administratorconsole oder die Registerkarte "Startseite" angezeigt werden, nachdem die Installation abgeschlossen ist.

So zeigen Sie den Installationsübersichtsbericht an

- ◆ Sie haben folgende Möglichkeiten:

Anzeigen der Installationsübersichtsbericht über die Administratorkonsole	Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Installation und Lizenzierung" und dann "Installationsübersichtsbericht".
Anzeigen der Installationsübersichtsbericht über die Registerkarte "Startseite"	Klicken Sie auf der Registerkarte "Startseite" unter "Installation und Upgrades" auf "Installationsübersichtsbericht".

Reparieren von Backup Exec

Wenn Sie feststellen, dass Backup Exec-Dateien oder Registrierungsschlüssel auf dem lokalen Backup Exec-Server fehlen oder beschädigt sind, führen Sie die Funktion "Reparieren" aus. Das Programm hält alle Backup Exec-Dienste an, installiert beschädigte Dateien und Registrierungsschlüssel erneut, installiert Bandgeräte neu (unabhängige Laufwerke und Wechsler) und startet anschließend die Dienste wieder. Die Datenbank wird nicht erneut installiert.

Alle Änderungen, die an Backup Exec-Programmdateien und -Registrierungsschlüsseln vorgenommen werden, werden auf die ursprünglichen Einstellungen zurückgesetzt.

So reparieren Sie Backup Exec

- 1** Schließen Sie die Backup Exec-Anwendung.
- 2** Wählen Sie in der Windows-Systemsteuerung die Option zum Deinstallieren eines Programms.
- 3** Wählen Sie "Backup Exec" und klicken Sie auf "Ändern".
- 4** Aktivieren Sie die Optionen "Lokale Installation" und "Reparieren" und klicken Sie auf "Weiter".

Stellen Sie sicher, dass die Option "Remote-Installation" nicht ausgewählt ist.

- 5** Wenn Sie aufgefordert werden, Identifikationsdaten für das Backup Exec-Dienstkonto einzugeben, geben Sie die richtigen Identifikationsdaten ein und klicken Sie auf "Weiter".
- 6** Wählen Sie die Option "Installieren".
 Sie werden möglicherweise aufgefordert, die Installationsmedien einzufügen.
- 7** Klicken Sie auf "Fertigstellen".

Aktualisieren von Backup Exec mit Veritas Update

Veritas Update stellt Updates für Backup Exec bereit und wird automatisch mit Backup Exec installiert.

Veritas Update kann manuell ausgeführt oder so konfiguriert werden, dass es automatisch jeden Tag zu einem bestimmten Zeitpunkt ausgeführt wird. Es kann auch konfiguriert werden, dass Updates automatisch heruntergeladen werden und eine Meldung ausgelöst wird, wenn der Download abgeschlossen ist, oder dass Updates erkannt werden und eine Meldung ausgelöst wird, anstatt die Updates herunterzuladen. Veritas Update ist in Backup Exec integriert, und der Zugriff darauf ist nur von Backup Exec aus möglich. Wenn Sie die Option zum automatischen Update aktivieren, können Sie Veritas Update so konfigurieren, dass es den Veritas-Webserver in geplanten Abständen überprüft. Wenn von Veritas Update Dateien installiert werden, dann wird die Installationsprotokolldatei `BKUPINST20.htm` entsprechend aktualisiert.

Wenn Sie Veritas Update über die Remote-Administratorkonsole (RAC) ausführen, beachten Sie die folgenden Verhaltensweisen:

- Veritas Update lädt Updates herunter und installiert Sie nur für den lokalen Server, auf dem RAC installiert ist, nicht dem Remote-Medienserver, auf den RAC verweist.
- Warnmeldungen von Veritas gelten für den Remote-Medienserver.
- Wenn Sie über die RAC-Schnittstelle "Installierte Updates" aufrufen, sehen Sie nur die Updates, die auf dem Remote-Medienserver installiert sind, nicht die auf dem lokalen RAC-Server.
- Um Updates anzuzeigen, die auf dem lokalen RAC-Server installiert sind, verwenden Sie die Windows-Systemsteuerung "Programme und Funktionen".
- Wenn Sie jedoch während der Verwendung der Remote-Administratorkonsole die Einstellungen für Veritas Update ändern, werden diese Einstellungen auf dem Remote-Server geändert.

Informationen zu den Best Practices zum Einsatz von Veritas Update finden Sie unter *Best Practices für Backup Exec*.

Hinweis: Beim Installieren und Aktualisieren werden die Backup Exec-Dienste unabhängig von der Anzahl der zu installierenden Updates nur einmal während der Veritas Update-Sitzung angehalten und gestartet. Alle ausgewählten Patches werden in der entsprechenden Reihenfolge installiert.

Planen automatischer Backup Exec-Updates mit Veritas Update

Sie können Veritas Update so konfigurieren, dass jeden Tag zu einer bestimmten Zeit auf Updates geprüft wird. Standardmäßig prüft Veritas Update jeden Tag um 22:00 Uhr auf Updates.

Zum geplanten Zeitpunkt stellt Veritas Update automatisch eine Verbindung zur passenden Website her und stellt fest, ob Ihre Dateien aktualisiert werden müssen. Sie können Veritas Update so konfigurieren, dass entweder Updates automatisch heruntergeladen und eine Meldung ausgelöst wird, wenn der Download abgeschlossen ist, oder dass verfügbare Downloads erkannt werden und eine Meldung ausgelöst und dann gewartet wird, bis Sie den Download bestätigen.

Backup Exec sendet die folgenden Veritas Update-Warnmeldungen:

Tabelle 2-12 Warnmeldungen von Veritas Update

Backup Exec sendet diese Warnmeldung	Wenn
Informationsmeldungen von Veritas Update	Ein Update wurde installiert.
Warnungen von Veritas Update	Ein Update ist erfolgreich installiert. Sie müssen jedoch den Computer neu starten.
Fehlermeldungen von Veritas Update	Ein Update konnte nicht installiert werden.

So planen Sie das automatische Herunterladen von Updates mit Veritas Update

- Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Backup Exec-Einstellungen".
- Klicken Sie im linken Teilfenster auf "Veritas Update".
- Wählen Sie "Täglich nach Updates suchen".
- Geben Sie eine neue Uhrzeit im Feld "Um:" ein, um die Tageszeit festzulegen, zu der Veritas Update ausgeführt wird. Standardmäßig ist dieses Feld auf 22:00 Uhr eingestellt.
- Wählen Sie eine der folgenden Optionen aus, um festzulegen, was Veritas Update tun soll, wenn verfügbare Updates erkannt werden:
 - Wenn Sie die Option "Meldung senden, wenn Updates verfügbar sind, aber Updates nicht heruntergeladen oder installieren" aktivieren, sendet Veritas Update eine Meldung, wenn verfügbare Updates erkannt wurden, diese Updates werden jedoch nicht heruntergeladen oder installiert.
 - Wenn Sie die Option "Updates zuerst heruntergeladen und dann eine Warnmeldung senden" aktivieren, werden alle verfügbaren Updates von

Veritas Update heruntergeladen. Anschließend wird gemeldet, dass die Updates installiert werden können.

- 6 Klicken Sie auf "OK", um das Fenster "Einstellungen" zu schließen, oder "Klicken Sie hier, um Veritas Update auszuführen", um Veritas Update zu starten.

Manuelles Ausführen von Veritas Update

Wenn Sie Veritas Update starten, wird automatisch nach verfügbaren Updates gesucht. Diese werden dann angezeigt.

So laden Sie Updates mit Veritas Update herunter und führen Sie aus

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Installation und Lizenzierung" und dann "Veritas Update". Daraufhin prüft Veritas Update auf verfügbare Updates und zeigt diese an.
- 2 Aktivieren Sie die Kontrollkästchen neben den Updates, die Sie installieren möchten.
- 3 Klicken Sie auf "Installieren".
- 4 Klicken Sie im Dialogfeld "Patch-Vorgang starten" auf "Ja", um den Installationsvorgang fortzusetzen, oder auf "Nein", um den Vorgang abubrechen.
- 5 Wenn Sie auf die Option "Ja" im Dialogfeld "Patch-Vorgang starten" geklickt haben, wird das Update von Veritas Update heruntergeladen und das Update-Installationsprogramm gestartet. Folgen Sie den Installationsanweisungen im Update, um die Installation abzuschließen.

Siehe ["Anzeigen installierter Aktualisierungen"](#) auf Seite 117.

Siehe ["Updates für den Agent for Windows auf Remote-Computern installieren"](#) auf Seite 84.

Anzeigen installierter Aktualisierungen

Sie können die Updates anzeigen, die auf einem Backup Exec-Server installiert sind. Hierfür müssen Sie mit Administratorrechten angemeldet sein. Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Installation und Lizenzierung" und dann "Installierte Updates".

Wenn ein Feature Pack vor einem anderen Feature Packs installiert wird, wird das frühere Feature Pack nicht mehr angezeigt, da es im späteren enthalten ist.

Ein Hotfix, der nach der Veröffentlichung des Feature Packs angeboten wird, wird mit dem früheren Feature Pack angezeigt.

Tabelle 2-13 Optionen für installierte Updates

Element	Beschreibung
Installierte Updates	Listet die auf einem Backup Exec-Server installierten Hotfixes und Service Packs auf.
Klicken Sie hier, um Veritas Update auszuführen	Ermöglicht das Ausführen von Veritas Update zum Installieren von Hotfixes und Service Packs.
Klicken Sie hier, um verfügbare Updates anzuzeigen.	Zeigt die Hotfixes und Service Packs an, die als Download verfügbar sind.

Deinstallieren von Backup Exec

Zum Deinstallieren von bereits installierten Hotfixes oder Feature Packs müssen Sie "Programme und Funktionen" in der Windows-Systemsteuerung verwenden.

Gehen Sie zum Deinstallieren von Hotfixes oder Feature Packs folgendermaßen vor:

- 1 Öffnen Sie das Windows-Startmenü.
- 2 Geben Sie "Programme und Funktionen" ein, um nach "Programme und Funktionen" in der Systemsteuerung zu suchen. Wählen Sie die entsprechende Systemsteuerungsfunktion aus, wenn sie in den Suchergebnissen angezeigt wird.
- 3 Klicken Sie im linken Teilfenster von "Programme und Funktionen" in der Systemsteuerung auf "Installierte Updates anzeigen".
- 4 Scrollen Sie zum Eintrag "Backup Exec (TM)". Hier sind alle bereits installierten Hotfixes und Feature Packs aufgelistet.
- 5 Wählen Sie ein Hotfix oder Feature Pack aus und klicken Sie auf "Deinstallieren", um mit die Deinstallation zu beginnen.

Anzeigen von Lizenzinformationen

Sie können Informationen zu den auf einem Backup Exec-Server lizenzierten und installierten Agents und Funktionen anzeigen.

Sie können auch Ihre Kapazitätsnutzung und Berechtigung mit einem Veritas Smart Meter verfolgen. Gehen Sie zur Veritas Smart Meter-Seite, um die Gesamtdatenmenge zu sehen, die gesichert wurde. Stellen Sie sicher, dass die Telemetrie in Backup Exec aktiviert ist, um die Kapazitätsnutzung in Veritas Smart

Meter anzuzeigen. Backup Exec sendet Telemetrie-Daten in regelmäßigen Abständen. Die Daten, die Sie in Smart Meter sehen, zeigen möglicherweise nicht die aktuellen Daten an, da Backup Exec die Telemetrie regelmäßig aktualisiert.

<https://taas.veritas.com/>

So zeigen Sie Lizenzinformationen an:

- ◆ Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Installation und Lizenzierung" und dann "Lizenzinformationen".

Backup Exec-Lizenzvertragsinformationen

Nachdem Sie Lizenzverträge für Backup Exec erworben oder importiert haben, wird die -Lizenzierungsportal-Website automatisch mit Ihren Lizenzvertragsinformationen aktualisiert.

Die verknüpfte Berechtigung enthält folgende Informationen:

- Lizenzierungsinformationen für das erworbene Produkt.
- Aktivierungsinformationen
- Lizenzinformationen, wenn ein Vertrag erworben wurde.

Backup Exec nutzt die Vertragsablaufsinformationen, um automatisch Backup Exec-Warnmeldungen festzulegen, die Sie erinnern, die Lizenzverträge zu verlängern, bevor sie ablaufen. Erinnerungsmeldungen werden in Intervallen von 30, 60 und 90 Tagen festgelegt, basierend auf dem Ablaufdatum des Lizenzvertrags. Wenn Sie den Lizenzvertrag nicht verlängern, wird eine Warnmeldung gesendet, wenn der Lizenzvertrag abläuft.

Der Bereich "Informationen-Lizenzierung" in der Backup Exec-Konsole zeigt die Anzahl der Tage bis zum Ablauf des Vertrags der aktuell installierten Lizenz.

So zeigen Sie Backup Exec-Lizenzvertragsinformationen an

- ◆ Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Installation und Lizenzierung" und dann "Lizenzvertragsinformationen".

Siehe "[Aktualisieren von abgelaufenen Wartungsverträgen](#)" auf Seite 119.

Aktualisieren von abgelaufenen Wartungsverträgen

Wenn Ihre Wartungsverträge ablaufen, führen Sie folgende Schritte aus, um die Verträge zu aktualisieren.

Hinweis: Sie können den Remote-Administrator auf einem Remote-Windows-Server oder einer Remote-Windows-Arbeitsstation nicht verwenden, um Wartungsverträge zu aktualisieren.

Tabelle 2-14 So aktualisieren Sie abgelaufene Wartungsverträge

Schritt	Zusätzliche Information
Erwerben Sie neue Lizenzverträge.	Wenden Sie sich an den Händler.
Rufen Sie eine aktualisierte Lizenzdatei ab	Aktualisieren Sie Ihre derzeitigen Berechtigungen mit einem neuen Datum und einer neuen Dienstvertragsnummer.
Starten Sie den Installationsassistenten von der Backup Exec-Administratorkonsole.	Verwenden Sie die Option "Funktionen und Lizenzen auf diesem Backup Exec-Server installieren" des Menüs "Installation und Lizenzierung", auf das Sie über die Backup Exec-Schaltfläche zugreifen können.
Verwenden Sie den Installationsassistenten, um die neuen Berechtigungs-IDs hinzuzufügen, und entfernen Sie dann die abgelaufenen Berechtigungs-IDs.	Nachdem Sie die abgelaufenen Berechtigungs-IDs in der Liste ausgewählt haben, verwenden Sie die Option "Entfernen".

Siehe ["Backup Exec-Lizenzvertragsinformationen"](#) auf Seite 119.

Verwalten von Lizenzvertragskundennummern

In Backup Exec haben Sie die Möglichkeit, alle Ihre Lizenzvertragskundennummern zu speichern.

Sie müssen diese Nummern angeben, wenn Sie sich mit dem technischen Support in Verbindung setzen.

So verwalten Sie Lizenzvertragskundennummern

- Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Installation und Lizenzierung" und dann "Kundennummern des Lizenzvertrags".
- Sie haben folgende Möglichkeiten:
 - Um eine neue Kundennummer hinzuzufügen, klicken Sie auf "Neu" und geben Sie dann Ihre Kundennummer und alle etwaigen dazugehörigen Informationen ein.
Sie finden Ihre Kundennummer im Feld "Entitlement Owner" (Eigentümer) auf dem Zertifikat.

- Um eine Kundennummer zu entfernen, wählen Sie die Nummer in der Liste aus und klicken Sie dann auf "Löschen".
- 3 Klicken Sie auf "Schließen".

Infos zum Aktualisieren von Backup Exec

Zum Aktualisieren von Backup Exec aus älteren Versionen auf Backup Exec Update 1 (20.1) oder höher müssen Sie eine gültige Lizenz angeben. Sie können vorhandene Lizenzen nicht zum Aktualisieren auf die neueste Version verwenden, auch dann nicht, wenn Sie einen gültigen Wartungsvertrag haben. Sie müssen die vorherige Version von Backup Exec vor dem Aktualisieren nicht deinstallieren. Die neueste Version wird über die vorherigen Version installiert. Verschiedene Versionen von Backup Exec dürfen nicht auf demselben Computer installiert sein.

Hinweis: Backup Exec unterstützt die Installation von Backup Exec-Servern nur unter 64-Bit-Betriebssystemen. Jedoch können Sie den Agent for Windows unter 32-Bit-Betriebssystemen installieren.

Die meisten Einstellungen und alle Kataloge und alle Datenverzeichnisse aus den vorherigen Versionen von Backup Exec werden beibehalten, es sei denn, Sie entfernen sie. Diese Version von Backup Exec kann Daten aus jeder vorherigen Version von Backup Exec oder von Backup Exec für NetWare lesen und wiederherstellen, ausgenommen Fälle, bei denen die Einstellung eines Produkts beschlossen wurde.

Wenn Sie aus einer vorherigen Version aktualisiert, konvertiert Backup Exec automatisch die vorhandenen Definitionen, Konfigurationen und Aufträge auf die aktuelle Version. Dabei werden eventuell einige Aufträge kombiniert oder verschoben. Nach Abschluss der Migration zeigt Backup Exec den Migrationsbericht an, den Sie prüfen und bestätigen müssen, bevor Backup Exec die Aktualisierung fortsetzt. In diesem Bericht können Sie sehen, wie Ihre Aufträge migriert wurden.

Siehe ["Verwenden des Migrationsberichts, um zu bestimmen, wie sich vorhandene Aufträge nach einem Upgrade von einer früheren Version von Backup Exec geändert haben"](#) auf Seite 125.

Backup Exec bietet Abwärtskompatibilität wie folgt:

- Backup Exec kann mit Backup Exec 2014 Remote Agent for Windows Systems und höher kommunizieren.
- Backup Exec unterstützt parallele Installationen der Remote-Administratorkonsole für Backup Exec 15 und höher. Beispielsweise können Sie eine

Remote-Administratorkonsole für Backup Exec 15, Backup Exec 16 und die aktuelle Version verwenden.

Die Version des über Remote-Zugriff verwalteten Backup Exec-Servers muss mit der Version der Remote-Administratorkonsole übereinstimmen. So müssen Sie beispielsweise für einen Backup Exec 16-Server eine Remote-Administratorkonsole Version 16 oder eine ihrer Feature Pack-Versionen verwenden.

- Der Backup Exec Central Admin Server Feature-Server kann für rollende Upgrades mit Backup Exec 16 Feature Pack 2 kommunizieren.

Führen Sie vor dem Upgrade von Backup Exec folgende Schritte aus:

- Löschen Sie nicht mehr benötigte Auftragsverläufe und Kataloge, um das Zeitfenster für das Upgrade zu verkürzen.
- Führen Sie einen Datenbankwartungsauftrag aus.
- Überprüfen Sie, ob alle verfügbaren Updates für Ihre aktuelle Version von Backup Exec installiert sind.
- Suchen Sie Ihre Lizenzinformationen heraus, und überprüfen Sie, ob Ihre Lizenzen aktuell sind. Bei Upgrades müssen Sie die Lizenzinformationen für Backup Exec eingeben.

Sie können die Konfiguration Ihrer Backup Exec-Server oder des Datenbankspeicherorts nicht während des Upgrade-Vorgangs ändern. So können Sie z. B. einen Administrationsserver nicht in einen verwalteten Server ändern. Wenn Sie die Konfiguration Ihrer Backup Exec-Server ändern möchten, tun Sie dies vor oder nach der Aktualisierung auf die aktuelle Version. Um den Speicherort der Datenbank nach dem Aktualisierungsvorgang zu ändern, verwenden Sie BEUtility.

Hinweis: Wenn Sie eine ältere Version von Backup Exec aktualisieren, die eine nicht englische Windows-Version nutzt, müssen Sie die Setup-Datei für SQL Server 2014 Express mit SP2 für die entsprechende Sprache von der Microsoft-Website herunterladen.

Siehe ["Installieren von Backup Exec mithilfe des Installationsassistenten"](#) auf Seite 55.

Transport Layer Security (TLS) 1.2 protocol

Backup Exec verwendet das Transport Layer Security (TLS) 1.2 Protokoll für die sichere Kommunikation mit Backup Exec Remote Agents nur dann, wenn TLS 1.0 abgelaufen ist.

Wenn Backup Exec Remote Agents entdeckt, die in einer früheren Version als Backup Exec 15 FP1 ausgeführt werden und die TLS 1.2 in Ihrer Umgebung auf Basis der von Ihnen während des Patch- oder Upgrade-Vorgangs vorgenommenen Einstellungen nicht unterstützen, ist es möglich, dass das Backup und Wiederherstellen von Servern fehlschlägt.

Wir empfehlen, die Remote Agents unmittelbar nach dem Upgrade des Backup Exec Servers zu aktualisieren, damit eine sichere Kommunikation gewährleistet ist.

- **Szenario 1: Wenn Sie den Backup Exec von einer niedrigeren Version als Backup Exec 15 FP1 aktualisieren:**
 Wenn Sie Backup Exec aktualisieren, wird das Teilfenster "TLS-Protokoll" angezeigt. Aktivieren Sie das Kontrollkästchen "Fallback auf TLS v1.0 erlauben", wenn Sie die Remote Agents nicht sofort aktualisieren können. Diese Einstellung ermöglicht es Backup Exec, weiterhin TLS 1.0 für die Kommunikation mit älteren Remote Agents zu verwenden, sodass diese Agents gesichert und wiederhergestellt werden können. Wenn Sie dieses Kontrollkästchen nicht aktivieren, schlagen Aufträge für die Server bis zur Aktualisierung der Remote Agents fehl.
- **Szenario 2: Wenn Sie für Backup Exec einen Patch installieren und mit einem Remote Agent mit einer niedrigeren Version als Backup Exec 15 FP1 arbeiten:**
 Wenn Sie einen Patch für Backup Exec installieren, erscheint ein Dialogfeld. Klicken Sie auf "Nein", wenn Sie die Remote Agents nicht sofort aktualisieren können. Backup Exec verwendet weiterhin TLS 1.0 für die Kommunikation mit älteren Remote Agents, sodass Backups und Wiederherstellungen auch weiterhin funktionieren. Klicken Sie auf "Ja", wenn Sie TLS 1.2. verwenden. Aufträge für die Server schlagen so lange fehl, bis die Remote Agents aktualisiert werden.

Sowohl für das Upgrade- als auch für das Patch-Installationsszenario gilt Folgendes: Wenn Sie für ältere Remote Agents nicht auf TLS 1.0 zurückgreifen, schlagen die Backup- und Wiederherstellungsaufträge solange fehl, bis die Remote Agents aktualisiert werden.

Während der Installation des Patch oder eines Upgrade, wird der Registrierungswert auf 1 gesetzt, wenn Sie TLS 1.0. zulassen.

Registrierungspfad: HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Backup Exec For Windows\Backup Exec\Engine\Backup

ValueName: AllowTLSFallback

Value type: DWORD (32-Bit)

Wenn Sie die Backup Exec Remote-Agents aktualisiert haben, können Sie den Registrierungswert so einstellen, dass immer TLS 1.2. verwendet wird.

Wenn Sie TLS 1.2. verwenden wollen, setzen Sie ValueName: AllowTLSFallback auf 0.

Wenn Sie weiterhin TLS 1.0. verwenden, zeigt der Backup Exec-Medienserver jede Woche eine Warnmeldung an. Sollten Sie nicht wollen, dass Backup Exec die Warnmeldung anzeigt, dann aktualisieren Sie die älteren Agents auf die neueste Version von Backup Exec. Sie können die Warnmeldung auch deaktivieren, indem Sie den folgenden Registrierungsschlüssel bearbeiten.

Registrierungspfad: HKEY_LOCAL_MACHINE\Software\Symantec\Backup Exec For Windows\Backup Exec\Server

ValueName = SupressTLSAlert

Value type: DWORD (32-Bit)

Wenn Sie den Wert auf 1 setzen, sind die wöchentlichen Warnmeldungen deaktiviert.

Upgrade-Checkliste für Backup Exec

Führen Sie vor dem Upgrade aus einer vorherigen Version von Backup Exec auf die aktuelle Version die folgenden Schritte durch:

- Stellen Sie sicher, dass Ihre Backups auf dem neuesten Stand sind. Es wird empfohlen, immer ein vollständiges Backup auszuführen, bevor und nachdem Sie Anwendungen bzw. das Betriebssystem auf Backup-Quellen aktualisieren.
- Deaktivieren Sie Ihre Antivirensoftware.
- Prüfen Sie in der Liste der mit Backup Exec kompatiblen Software (SCL) und Hardware (HCL), ob die zu sichernden Anwendungen und Ihre Speichergeräte unterstützt werden.
- Laden Sie alle verfügbaren Upgrades und Hotfixes für die Version von Backup Exec herunter, die Sie installieren möchten.
- Planen Sie das Upgrade für einen Zeitpunkt, zu dem Systemausfälle die Benutzer nicht stören würden.
- Stellen Sie sicher, dass Ihre Berechtigungs-IDs bzw. Lizenzdateien verfügbar sind. Sie müssen während des Aktualisierens neue Lizenzinformationen zu Backup Exec eingeben.
Aktualisierte Informationen zur Lizenzierung finden Sie im *Backup Exec-Lizenzierungshandbuch*
- Lesen Sie die folgenden Themen im *Administratorhandbuch zu Backup Exec* :
 - *Systemanforderungen für Backup Exec*
Siehe "[Systemanforderungen für Backup Exec](#)" auf Seite 51.

- *Löschen abgelaufener Backup-Sätze auf plattenbasiertem Speicher durch Data Lifecycle Management (DLM)*
 Siehe "[Löschen abgelaufener Backup-Sätze auf plattenbasiertem Speicher durch Data Lifecycle Management \(DLM\)](#)" auf Seite 393.
- *Info zum Aktualisieren von früheren Backup Exec-Versionen*
 Siehe "[Infos zum Aktualisieren von Backup Exec](#)" auf Seite 121.
- Lesen Sie das Dokument *Best Practices für die Installation von Backup Exec* in der Backup Exec-Supportdatenbank.

Verwenden des Migrationsberichts, um zu bestimmen, wie sich vorhandene Aufträge nach einem Upgrade von einer früheren Version von Backup Exec geändert haben

Wenn Sie ein Upgrade auf Backup Exec durchführen, werden Ihre vorhandenen Definitionen, Konfigurationen und Aufträge automatisch in die aktuelle Version konvertiert. Wenn die Aufträge migriert werden, werden möglicherweise einige kombiniert oder verschoben. Nach Abschluss der Migration zeigt Backup Exec den Migrationsbericht an, damit Sie ihn prüfen und akzeptieren können. In diesem Bericht können Sie sehen, wie Ihre Aufträge migriert wurden. Die Informationen im Migrationsbericht können nicht neu erstellt werden, nachdem das Upgrade abgeschlossen ist.

Es wird empfohlen, den Migrationsbericht sorgfältig zu überprüfen, um festzustellen, wie Ihre vorhandenen Aufträge geändert wurden und wie Sie eventuell Aufträge manuell anpassen müssen. Sie können den Migrationsbericht jederzeit über die Backup Exec-Administratorkonsole oder die Registerkarte "Startseite" aufrufen, nachdem die Migration abgeschlossen ist.

Der Migrationsbericht ist unter folgenden Pfad gespeichert:

<Backup Exec-Installationsordner>\Backup
 Exec\Data\MigrationReportFiles\Data-Migration-Report.html.

Hinweis: Um den Migrationsbericht anzusehen, muss Javascript in Ihrem Webbrowser aktiviert sein. Wenn auf dem Server, auf dem Sie Backup Exec installiert haben, keinen Browser mit JavaScript aktiviert ist, können Sie den Migrationsbericht auf einen anderen Server mit JavaScript kopieren.

So zeigen Sie den Migrationsbericht an

- ◆ Sie haben folgende Möglichkeiten:

So zeigen Sie den Migrationsbericht über die Administratorkonsole an Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Installation und Lizenzierung" und dann "Migrationsbericht".

So zeigen Sie den Migrationsbericht über die Registerkarte "Startseite" an Klicken Sie auf der Registerkarte "Startseite" unter "Installation und Upgrades" auf "Migrationsbericht".

Siehe ["Konfigurieren der Registerkarte "Startseite""](#) auf Seite 139.

Aufgaben nach der Installation

Führen Sie für optimale Ergebnisse nach der Installation von Backup Exec folgende Schritte durch:

- Erstellen Sie Datenträgerspeicher, damit Backup Exec den Lebenszyklus Ihrer Backup-Daten automatisch verwalten kann.
 Siehe ["Konfigurieren von Festplattenspeicher"](#) auf Seite 372.
- Überprüfen Sie, ob die Speichergeräte ordnungsgemäß angeschlossen und korrekt konfiguriert sind.
- Entscheiden Sie sich, welche Typen von Speichergeräten Sie für Ihre Backup-Aufträge verwenden möchten. Bei der Vorbereitung der Backup Exec-Umgebung können Sie Speichergeräte konfigurieren.
- Informieren Sie sich darüber, wie Backup Exec Überschreibschutz für Ihre Bandmedien bereitstellt.
 Siehe ["Medienüberschreibschutzstufen für Bandmedien"](#) auf Seite 487.
- Informieren Sie sich über den Standardmediensatz für Bandmedien und dessen verwöchigen Überschreibschutz.
 Siehe ["Standard-Mediensätze"](#) auf Seite 473.
- Machen Sie sich mit Data Lifecycle Management vertraut.
 Siehe ["Löschen abgelaufener Backup-Sätze auf plattenbasiertem Speicher durch Data Lifecycle Management \(DLM\)"](#) auf Seite 393.
- Informieren Sie sich über das Erstellen von neuen Mediensätzen mit verschiedenen Aufbewahrungszeiträumen.
 Siehe ["Erstellen von Mediensätzen für Bänder"](#) auf Seite 480.

- Bestimmen Sie, welche Anmeldeinformationen für Ihr Backup Exec-Login-Konto beim Durchsuchen und bei der Backup-Auswahl zu verwenden sind. Sie können ein bereits vorhandenes Backup Exec-Login-Konto verwenden oder ein neues Konto erstellen.
 Siehe ["Backup Exec-Login-Konten"](#) auf Seite 762.
- Konfigurieren einer sicheren Verbindung zur Backup Exec-Datenbank
 Siehe ["Konfigurieren der Verschlüsselung für die Verbindung zur Backup Exec-Datenbank"](#) auf Seite 702.

Deinstallieren von Backup Exec

Verwenden Sie die Windows-Systemeinstellung "Software", um Backup Exec von einem Computer zu entfernen. Weitere Informationen zur Funktion "Software" finden Sie in Ihrer Microsoft-Dokumentation.

Bei der Deinstallation von Backup Exec werden auch Bandtreiber entfernt. Falls Sie Backup Exec erneut installieren und die Bandtreiber verwenden möchten, müssen Sie diese erneut installieren.

So deinstallieren Sie Backup Exec

- 1 Schließen Sie Backup Exec.
- 2 Wählen Sie in der Windows-Systemsteuerung die Option zum Deinstallieren eines Programms.
- 3 Wählen Sie "Backup Exec™" und klicken Sie auf "Deinstallieren".
- 4 Wenn Sie dazu aufgefordert werden, zu bestätigen, dass Sie Backup Exec von Ihrem Computer deinstallieren möchten, klicken Sie auf "Ja".
- 5 Wählen Sie, ob nur die Programmdateien von Backup Exec oder Backup Exec und alle seine verbundenen Dateien entfernt werden sollen.
- 6 Klicken Sie auf "Weiter".

Bei Fehlschlagen des Deinstallationsprogramms klicken Sie auf die Schaltfläche "Installationsprotokolldatei anzeigen", um weitere Informationen zu erhalten.

- 7 Starten Sie den Computer neu, wenn Sie dazu aufgefordert werden.

Siehe ["Deinstallieren der Backup Exec-Funktionen vom lokalen Backup Exec-Server"](#) auf Seite 128.

Deinstallieren von Backup Exec mit der Befehlszeile

Wenn Backup Exec bereits installiert wurde, können Sie "setup.exe" für die Deinstallation der Backup Exec-Programmdateien und -daten verwenden.

So deinstallieren Sie Backup Exec über die Befehlszeile:

- 1 Öffnen Sie eine Windows-Eingabeaufforderung.
- 2 Wechseln Sie zum Laufwerk, das das Backup Exec-Installationsmedium enthält.
- 3 Wechseln Sie zum folgenden Verzeichnis:

```
\be\winnt\install\bex64
```

- 4 Um die Backup Exec-Programmdateien zu entfernen, die gesamten Backup Exec-Daten jedoch zu behalten, geben Sie Folgendes ein:

```
SETUP /UNINSTALL:
```

Um sowohl die Backup Exec-Programmdateien als auch die Backup Exec-Daten zu entfernen, geben Sie Folgendes ein:

```
SETUP /REMOVEALL:
```

Siehe ["Installieren von Backup Exec über die Befehlszeile \(Silent-Mode\)"](#) auf Seite 103.

Deinstallieren der Backup Exec-Funktionen vom lokalen Backup Exec-Server

Der Installationsassistent entfernt Backup Exec-Funktionen vom lokalen Backup Exec-Server. Alle zugehörigen Dateien, Registrierungsschlüssel und Konfigurationen werden entfernt.

Hinweis: Lizenzdateien verbleiben auf dem Server, nachdem Funktionen deinstalliert wurden. Löschen Sie die Lizenzdateien nicht, während Backup Exec installiert ist. Durch das Löschen der Lizenzdateien wird die Testversion aktiviert.

So deinstallieren Sie Backup Exec-Funktionen vom lokalen Backup Exec-Server

- 1** Klicken Sie auf die Backup Exec-Schaltfläche und dann auf "Installation und Lizenzierung" und "Funktionen und Lizenzen auf diesem Backup Exec-Server installieren".
- 2** Klicken Sie im Bereich "Lizenzen hinzufügen" auf "Weiter".
- 3** Heben Sie im Fenster "Funktionen konfigurieren" die Auswahl der Agents oder Funktionen auf, die Sie deinstallieren möchten, und klicken Sie dann auf "Weiter".
- 4** Deaktivieren Sie das Kontrollkästchen für die Sprache, die Sie entfernen möchten.
- 5** Klicken Sie im Bereich "Sprachen auswählen" auf "Weiter".
- 6** Wenn Sie aufgefordert werden, Identifikationsdaten für das Backup Exec-Dienstkonto einzugeben, geben Sie die richtigen Identifikationsdaten ein und klicken Sie auf "Weiter".
- 7** Lesen Sie die Installationsübersicht und klicken Sie auf "Installieren", um den Vorgang zu starten.
- 8** Klicken Sie auf "Fertigstellen", sobald der Installationsassistent abgeschlossen ist.

Siehe ["Deinstallieren von Backup Exec"](#) auf Seite 127.

Erste Schritte

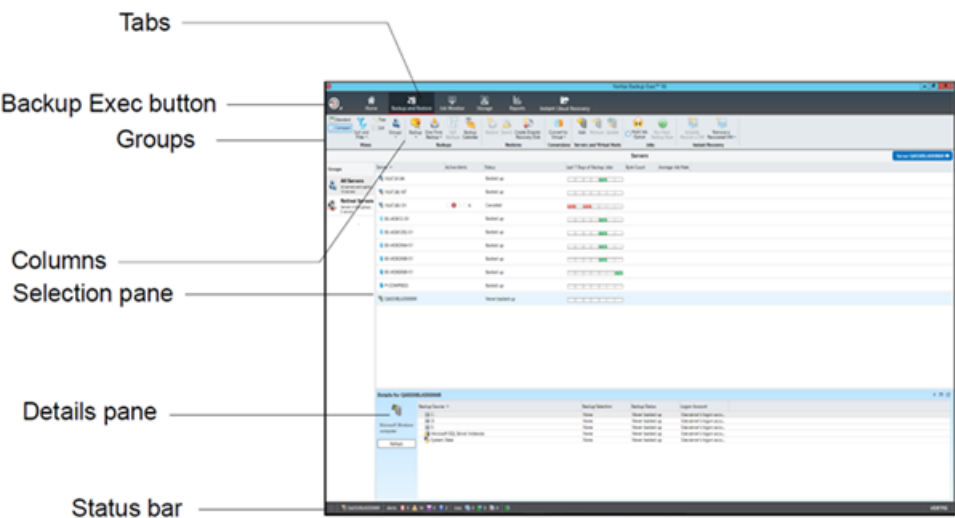
In diesem Kapitel werden folgende Themen behandelt:

- [Info zur Backup Exec-Administratorkonsole](#)
- [Herstellen einer Verbindung mit Veritas SaaS-Backup](#)
- [Anzeigen der Versionshinweise für Backup Exec](#)
- [Sperren und Freigeben der Backup Exec-Konsole](#)
- [Sortieren, Filtern und Kopieren von Informationen in der Backup Exec-Administratorkonsole](#)
- [Anpassen von Ansichten in der Backup Exec-Administratorkonsole](#)
- [Konfigurieren der Registerkarte "Startseite"](#)
- [Konfigurieren des RSS Reader](#)
- [Erstellen eines Plans für die Notfallwiederherstellung \(DPP\)](#)
- [Erste Schritte mit Backups](#)

Info zur Backup Exec-Administratorkonsole

Verwenden Sie die Backup Exec-Administratorkonsole, um Backups auszuführen, Daten wieder herzustellen, Aufträge zu überwachen, den Speicher zu konfigurieren und Berichte auszuführen.

Abbildung 3-1 Backup Exec-Administratorkonsole



Der Bildschirm der Administratorkonsole enthält die folgenden Elemente:

Tabelle 3-1 Komponenten der Administratorkonsole

Element	Beschreibung
Schaltfläche "Backup Exec"	Die Backup Exec-Schaltfläche wird links oben in der Administratorkonsole angezeigt. Um die Optionen in der Backup Exec-Schaltfläche anzuzeigen, klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie den Menünamen, aus und wählen Sie dann eine Option aus. Sie können Backup Exec-Vorgänge durch Klicken auf Optionen in einem Menü starten.

Element	Beschreibung
Registerkarten	<p>Mit den Registerkarten am oberen Bildschirm können Sie in Backup Exec navigieren.</p> <p>Sie können auf die folgenden Ansichten von der Navigationsleiste zugreifen:</p> <ul style="list-style-type: none"> ■ Startseite. Verwenden Sie diese Ansicht, um schnell auf die Backup Exec-Funktionen zuzugreifen, die Sie häufig verwenden. Passen Sie die Haupt-Ansicht an, indem Sie Elemente hinzufügen oder löschen. ■ Backup und Wiederherstellung. Erstellen Sie ein Backup oder einen Wiederherstellungsauftrag. ■ Auftragsüberwachung. Überwachen Sie und verwalten Sie Backup-, Wiederherstellungs-, Installations- und Speichervorgangsaufträge. ■ Speicher. Konfigurieren Sie Speicher, führen Sie Speichervorgänge aus und verwalten Sie Medien. ■ Berichte. Verwenden Sie diese Ansicht, um Berichte über den Backup Exec-Server, dessen Vorgänge und Verwendung von Geräten und Medien anzuzeigen, zu drucken, zu speichern, zu planen und zu erstellen. Sie haben ferner die Möglichkeit, Berichte in Backup Exec in den Formaten "PDF" und "HTML" anzuzeigen, sowie in den folgenden Formaten zu speichern und zu drucken: PDF, XML, HTML, XLS (Microsoft Excel) und CSV (Comma Separated Value). ■ Sofortwiederherstellung in der Cloud. Verwalten Sie die Notfallwiederherstellung mithilfe von Azure Site Recovery. Sie können den Replikationszustand von virtuellen Computern überwachen und die Replikation von virtuellen Hyper-V- und VMware-Computern aktivieren, deren Hosts mit Azure Site Recovery konfiguriert sind.
Gruppen	<p>Gruppen werden auf den Registerkarten in der Administratorkonsole angezeigt und enthalten die Befehle, die Aktionen wie zum Beispiel das Erstellen eines neuen Backup-Auftrags oder Konfigurieren von Speicher auslösen. Die Elemente in den Gruppen sind dynamisch und ändern sich entsprechend der Auswahl. Einige Optionen sind erst dann verfügbar, wenn Sie im Konsolenbildschirm ein Element ausgewählt oder eine vorausgesetzte Aufgabe durchgeführt haben.</p>

Element	Beschreibung
Spalten	<p>Passen Sie Spalten an, indem Sie eine der folgenden Aktionen ausführen:</p> <ul style="list-style-type: none"> ■ Ziehen und legen Sie Spalten ab, um ihren Speicherort zu ändern. ■ Klicken Sie mit der rechten Maustaste auf eine Spaltenüberschrift, um die Spalten anzuzeigenden Spalten auszuwählen oder um die Spalten zu sortieren und zu filtern. ■ Klicken Sie auf die Spalteüberschrift, um die Reihenfolge der Spalten zu ändern. <p>Beispielsweise werden Berichte in der Standardeinstellung in alphabetischer Reihenfolge angezeigt. Klicken Sie zum Umkehren der Reihenfolge in der Ansicht "Berichte" auf die Spaltenüberschrift "Name".</p>
Auswahlfenster	<p>Im Auswahlfenster wählen Sie die zu bearbeitenden Elemente, z. B. Server, die gesichert oder wiederhergestellt werden sollen.</p>
Teilfenster "Details"	<p>Weitere Details werden für den Server angezeigt, den Sie in der Liste mit den Servern ausgewählt haben. Im Teilfenster "Details" werden die Ressourcen für den ausgewählten Server und der Auswahl-, Backup-Status sowie Login-Kontoinformationen für jede Ressource angezeigt.</p> <p>Wenn Sie einen Hyper-V- oder VMware-Host in der Liste mit den Servern auswählen, sind die folgenden Details im Teilfenster "Details" enthalten:</p> <ul style="list-style-type: none"> ■ Die letzten 7 Tage für Backup-Aufträge ■ Das Datum des letzten Backups ■ Das Datum des nächsten geplanten Backups <p>Sie können auch Daten wiederherstellen und die Liste der virtuellen Gastcomputer von diesem Teilfenster aus filtern.</p>
Statusleiste	<p>Die Statusleiste wird an der Unterseite der Administratorkonsole angezeigt und liefert Informationen über den Backup Exec-Server, laufende und geplante Aufträge, Warnmeldungen und laufende Dienste.</p>
Aktualisieren	<p>Klicken Sie auf "F5", um die Benutzeroberfläche auf der Administratorkonsole zu aktualisieren.</p>

Herstellen einer Verbindung mit Veritas SaaS-Backup

Bei Veritas SaaS-Backup handelt es sich um eine gehostete Cloud-zu-Cloud-Backup-Lösung, die Schutz von Daten für Office 365 und andere SaaS-Workloads bietet.

Eine kostenlose Testversion von Veritas SaaS-Backup ist für Backup Exec-Benutzer verfügbar.

<https://www.veritas.com/form/trialware/saas-backup>

Eine Verbindung mit Veritas SaaS-Backup herstellen

- ◆ Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie Veritas SaaS-Backup.

Die Seite "Veritas SaaS-Backup" wird angezeigt.

[https://www.VERITAS.com/Product/Backup-and-Recovery/ SaaS-Backup?
Om_camp_id = Us_vrc_be_web_saas Backup_customers](https://www.VERITAS.com/Product/Backup-and-Recovery/SaaS-Backup?Om_camp_id=Us_vrc_be_web_saas_Backup_customers)

Anzeigen der Versionshinweise für Backup Exec

Sie können Informationen über die Version von Backup Exec, die Sie installiert haben, anzeigen.

So zeigen Sie die Versionshinweise für Backup Exec an

- 1 Klicken Sie auf die Schaltfläche "Backup Exec" und wählen Sie dann "Hilfe und Dokumentation" aus und klicken Sie dann auf "Informationen zu Backup Exec".
- 2 Klicken Sie auf "OK".

Sperren und Freigeben der Backup Exec-Konsole

Um die Backup Exec-Sitzung zu sperren, an der Sie gerade arbeiten, und die Backup Exec-Konsole vor unbefugtem Zugriff zu schützen, können Sie die Funktion "Konsole sperren" verwenden.

Sie können diese Funktion nur aktivieren, wenn das Kontrollkästchen "Backup Exec-Konsole schützen" in den Einstellungen für "Netzwerk und Sicherheit" aktiviert ist. Die Option "Konsole sperren" ist jetzt aktiviert.

Wenn Sie das Kontrollkästchen "Backup Exec-Konsole schützen" nicht aktivieren, ist die Option "Konsole sperren" nicht verfügbar.

Siehe ["Netzwerk- und Sicherheitsoptionen für Backup Exec ändern"](#) auf Seite 713.

Nachdem Sie die Benutzeroberfläche von Backup Exec gesperrt haben, müssen Sie das Kennwort eingeben, um eine Verbindung zur Backup Exec-Konsole herzustellen. Sie können dann nur Aufgaben in Backup Exec ausführen, wenn Sie die Backup Exec-Konsole freigeben.

Backup Exec enthält andere Dienstprogramme, die über die Konsole gestartet werden können und über eine eigene Benutzeroberflächen verfügen. Wenn beliebige dieser Dienstprogramme beim Sperren der Konsole geöffnet sind, können Sie sie weiterhin verwenden. Beispiele: Quick Assist, Installationsoptionen und Lizenzen, Hilfe, Backup Exec Services, Installations-Agents, Erstellen von Notfallwiederherstellungsdatenträgern usw.

Wenn Sie bei einem parallelen Upgrade eine niedrigere Version von MMS und eine aktualisierte Version von CAS haben und eine Verbindung zu MMS aus CAS herstellen, ist diese Funktion zwar verfügbar, kann aber nicht aktiviert werden (abgeblendet).

So sperren Sie die Backup Exec-Konsole bzw. geben sie frei

- 1** Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie "Konfiguration und Einstellungen > Backup Exec-Einstellungen > Netzwerk und Sicherheit".
- 2** Aktivieren Sie das Kontrollkästchen "Backup Exec-Konsole schützen".

Hinweis: Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

- 3** Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konsole sperren".

Das Dialogfeld "Mit Backup Exec-Server verbinden" wird angezeigt. Der Servername und der Benutzername sind deaktiviert.

- 4** Geben Sie das Kennwort für den Benutzernamen an, den Sie zum Einloggen bei der Backup Exec-Konsole verwendet haben.
- 5** Klicken Sie auf "Verbinden".

Der Zustand der Aufgaben, bevor die Backup Exec-Konsole gesperrt wurde, wird fortgesetzt. Sie können Backup Exec jetzt wieder verwenden.

Sortieren, Filtern und Kopieren von Informationen in der Backup Exec-Administratorkonsole

Sie können die auf den Registerkarten "Backup und Wiederherstellung", "Auftragsüberwachung" und "Speicher" angezeigten Informationen anpassen.

Sie können beliebige oder alle folgenden Aktionen durchführen:

- Wählen einer von Backup Exec bereitgestellten Standardkonfiguration, z. B. "Server mit aktiven Aufträgen" oder "Fehlgeschlagene Aufträge"
- Angeben einer Sortierreihenfolge für die Spalten, die in den Ansichten angezeigt werden.
- Angeben der Werte, die Sie zum Filtern der von Backup Exec angezeigten Informationen verwenden möchten
- Angeben der Spalten, die angezeigt werden sollen, und Festlegen ihrer Reihenfolge
- Erstellen und speichern einer Konfiguration zur späteren Wiederverwendung
- Kopieren der in der Liste aufgeführten Elemente in die Zwischenablage und Einfügen in eine beliebige Anwendung, die die Kopier- und Einfügefunktion des Betriebssystems unterstützt

So sortieren, filtern und kopieren Sie Informationen in der Backup Exec-Administratorkonsole

1 Sie haben folgende Möglichkeiten:

So passen Sie eine Ansicht der Computer in der Liste von Servern an	Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" in der Gruppe "Ansichten" auf "Sortieren und filtern".
---	---

So passen Sie eine Ansicht der Speichergeräte an	Klicken Sie auf der Registerkarte "Speicher" unter "Ansichten" auf "Liste" und dann auf "Sortieren und filtern".
--	--

2 Führen Sie einen der folgenden Schritte aus:

So wählen Sie eine Standardkonfiguration wie z. B. "Server mit gescheiterten Backups" oder eine zuvor von Ihnen erstellte und gespeicherte Konfiguration	Klicken Sie auf "Konfigurationen" und wählen Sie eine Konfiguration aus.
--	--

So geben Sie eine aufsteigende oder absteigende Sortierreihenfolge für die Spalten an	Klicken Sie auf "Sortieren", wählen Sie die gewünschten Optionen aus und klicken Sie dann auf "OK".
---	---

So geben Sie eine oder mehrere Spalten zum Filtern nach bestimmten Werten an	Klicken Sie auf "Filter", wählen Sie die gewünschten Optionen aus und klicken Sie dann auf "OK".
--	--

So geben Sie die anzuzeigenden Spalten und ihre Reihenfolge an	Klicken Sie auf "Spalten", wählen Sie die gewünschten Optionen aus und klicken Sie dann auf "OK".
--	---

So erstellen und speichern Sie eine Konfiguration	Klicken Sie auf "Speichern", wählen Sie die gewünschten Optionen aus und klicken Sie dann auf "OK".
---	---

So bearbeiten Sie eine konfigurierte Ansicht

1 Sie haben folgende Möglichkeiten:

So bearbeiten Sie eine Konfiguration über die Registerkarte "Backup und Wiederherstellung"	Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" in der Gruppe "Ansichten" auf "Sortieren und filtern".
--	---

So bearbeiten Sie eine Konfiguration über die Registerkarte "Speicher"	Klicken Sie auf der Registerkarte "Speicher" in der Gruppe "Ansichten" auf "Sortieren und filtern".
--	---

2 Klicken Sie auf "Konfigurationen".

3 Wählen Sie die zu bearbeitende Konfiguration aus und klicken Sie dann auf das Bleistiftsymbol.

So löschen Sie eine konfigurierte Ansicht

1 Sie haben folgende Möglichkeiten:

So löschen Sie eine Konfiguration über die Registerkarte "Backup und Wiederherstellung"	Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" in der Gruppe "Ansichten" auf "Sortieren und filtern".
---	---

So löschen Sie eine Konfiguration über die Registerkarte "Speicher"	Klicken Sie auf der Registerkarte "Speicher" in der Gruppe "Ansichten" auf "Sortieren und filtern".
---	---

2 Klicken Sie auf "Konfigurationen".

3 Wählen Sie die zu löschende Konfiguration aus und klicken Sie dann auf das Löschesymbol.

So kopieren Sie Informationen in der Backup Exec-Administratorkonsole

1 Klicken Sie auf allen Registerkarten außer der Registerkarte "Startseite" mit der rechten Maustaste auf ein Element in der Listenansicht.

2 Klicken Sie auf "Kopieren".

3 Öffnen Sie eine beliebige Anwendung, die Kopieren und Einfügen unterstützt, und fügen Sie die Informationen ein.

Anpassen von Ansichten in der Backup Exec-Administratorkonsole

Sie können die auf den Registerkarten "Backup und Wiederherstellung", "Auftragsüberwachung" und "Speicher" angezeigten Informationen anpassen.

Tabelle 3-2 Ansichten in der Backup Exec-Administratorkonsole

Anzeigen	Beschreibung
Standard	Zeigt die Informationen in einer Ansicht mit einer Beschreibung an.
Kompakt	Zeigt die Informationen in einer Platz sparenden Ansicht an.
Struktur	Zeigt die Felder in einer hierarchischen Struktur an. Diese Ansicht ist für die Serverliste auf der Registerkarte "Backup und Wiederherstellung" deaktiviert.
Liste	Zeigt die Elemente in einer Liste an, die Sie nach Spalten sortieren können. Diese Ansicht ist für die Serverliste auf der Registerkarte "Backup und Wiederherstellung" deaktiviert.

So passen Sie Ansichten über die Backup Exec-Administratorkonsole an

- ◆ Klicken Sie auf der Registerkarte "Backup und Wiederherstellung", "Auftragsüberwachung", "Speicher" oder "Sofortwiederherstellung in der Cloud" in der Gruppe "Ansichten" auf "Standard", "Kompakt", "Struktur" oder "Liste".

Hinweis: Die Ansichten "Struktur" und "Liste" sind für die Liste von Servern auf der Registerkarte "Backup und Wiederherstellung" deaktiviert.

Konfigurieren der Registerkarte "Startseite"

Sie können die Registerkarte "Startseite" anpassen, indem Sie die Elemente auswählen, die Sie anzeigen möchten. Sie können Elemente mit der Drag & Drop-Funktion zu einem anderen Speicherort auf der Registerkarte "Startseite" verschieben, oder Sie können ein einzelnes Element maximieren. Die Elemente auf der Registerkarte "Startseite" umfassen Backup Exec-Daten und Links zu Funktionen, die Sie häufig verwenden.

So konfigurieren Sie die Registerkarte "Startseite"

- 1
- Klicken Sie auf der Registerkarte "Startseite" in der Gruppe "Layout" auf das Layout für die anzuzeigenden Elemente.
- 2
- In den Gruppen "Systemzustand" und "Support" wählen Sie das Kontrollkästchen für die Elemente aus, die Sie angezeigt werden sollen.
- 3
- Zeigen Sie in der Gruppe "Sofortwiederherstellung in der Cloud" den DR-Zustand (Notfallwiederherstellung) und die Failover-Bereitschaft für einen in Azure konfigurierten Recovery Services-Tresor an.
- 4
- Passen Sie die Registerkarte "Startseite" weiter an, indem Sie die Elemente in die gewünschte Spalte ziehen und wie gewünscht positionieren.

Sie können das "Layout" konfigurieren und Elemente in den Gruppen "Systemzustand" und "Support" ausblenden oder anzeigen.

Wiederherstellen des Standardlayouts der Registerkarte "Startseite"

Die Standardkonfiguration der Registerkarte "Startseite" kann jederzeit wiederhergestellt werden.

So stellen Sie die Standardkonfiguration für die Registerkarte "Startseite" wieder her

- ◆
- Klicken Sie auf der Registerkarte "Startseite" in der Gruppe "Layout" auf "Registerkarte 'Startseite' zurücksetzen".

Gruppe "Layout"

Sie können eine der folgenden Layoutkonfigurationen auswählen, um die Elemente auf der Registerkarte "Startseite" anzuzeigen.

Tabelle 3-3 Elemente für das Layout der Registerkarte "Startseite"

Element	Beschreibung
Eine Spalte	Zeigt die Elemente der Registerkarte "Startseite" in einer Spalte an.
"Zwei Spalten"	Zeigt die Elemente der Registerkarte "Startseite" in zwei Spalten an.
Schmal/Breit	Zeigt die Elemente der Registerkarte "Startseite" in zwei Spalten mit einem schmalen und einem breiten Bereich an.
Drei Spalten	Zeigt die Elemente der Registerkarte "Startseite" in drei Spalten an.

Element	Beschreibung
Registerkarte 'Startseite' zurücksetzen	Stellt die Standardkonfiguration für die Inhalte der Registerkarte "Startseite" wieder her.

Gruppe "Systemzustand"

Die Elemente in der Gruppe "Systemzustand" geben einen Überblick über Warnmeldungen, Backup-Aufträge, Backup-Größen, Speicherstatus und Simplified Disaster Recovery. Sie können die folgenden Elemente auswählen, um sie auf der Registerkarte "Startseite" von Backup Exec anzuzeigen.

Tabelle 3-4 Systemzustand Gruppenelemente

Element	Beschreibung
Aktive Meldungen	<p>Hier können Sie alle Warnmeldungen anzeigen, auf die noch nicht reagiert wurde. Sie können die Warnmeldungen filtern, um bestimmte Typen von Warnmeldungen, die Quelle der Warnmeldungen und den Zeitraum anzuzeigen, in dem Warnmeldungen aufgetreten sind.</p> <p>Sie können alle folgenden Typen von Warnmeldungen anzeigen:</p> <ul style="list-style-type: none"> ■ Fehler ■ Warnung ■ Bedienereingriff erforderlich ■ Informationen
Warnmeldungsverlauf	Hier können Sie die Eigenschaften und Reaktionen für Warnmeldungen anzeigen.
Backup-Status	Stellt eine Übersicht des Backup-Auftragsstatus für die gesicherten Server bzw. die zum Sichern verfügbaren Server bereit.
Backup-Größe	Zeigt eine Übersicht der Menge der gesicherten Daten an. Sie können die Anzahl der Tage anpassen, für die Sie Informationen über die Backup-Größe anzeigen. Sie können außerdem den Typ von Backups, die angezeigt werden, auswählen.

Element	Beschreibung
Speicherstatus	<p>Stellt eine Übersicht des Speicherplatzes im Speicher bereit. Die Speicherinformationen umfassen die gesamte Kapazität, die den Speicherplatz anzeigt, der für die verschiedenen Typen von Daten verwendet wird.</p>
Simplified Disaster Recovery	<p>Stellt einen Status zur Verfügung, ob das Datenträger-Image der Simplified Disaster Recovery erstellt worden ist.</p> <p>Wenn das Datenträger-Image der Simplified Disaster Recovery nicht erstellt worden ist, können Sie den Link "SDR-Datenträger erstellen" klicken, um einen Assistenten zu starten, der Sie durch den Prozess führt.</p> <p>Siehe "Info zu Simplified Disaster Recovery" auf Seite 941.</p>
Datenbankverschlüsselungscode	<p>Gibt an, ob der Datenbankverschlüsselungscode exportiert wurde.</p> <p>Wenn Sie den Datenbankverschlüsselungscode nicht exportiert haben, sollten Sie dies tun, um sicherzustellen, dass Sie später auf die Backup Exec-Datenbank zugreifen können. Sie müssen den Datenbankverschlüsselungscode z. B. für die Notfallwiederherstellung und Migrierung zur Verfügung zu stellen.</p> <p>Siehe "Exportieren des Backup Exec-Datenbankverschlüsselungscode" auf Seite 698.</p>
Sichern virtueller Computer	<p>Listet die Anzahl virtueller Computern auf, die mit den Backup-Methoden "Virtuelle Backups" und "Backups mit Agent" gesichert werden.</p> <p>Die Informationen werden aktualisiert, wenn ein Backup-Auftrag erstellt, gelöscht oder bearbeitet wird. Sie werden auch aktualisiert, wenn die Benutzeroberfläche aktualisiert oder neu gestartet wird.</p>

Element	Beschreibung
Status der Sofortwiederherstellung in der Cloud	

Element	Beschreibung
	<p>Hier können Sie den Azure-Schutz, die Failover-Bereitschaft und den DR-Zustand prüfen.</p> <ul style="list-style-type: none"> ■ Schutz <p>Das Kreisdiagramm zeigt den Schutzstatus der konfigurierten virtuellen Computer im Recovery Services-Tresor in Azure an. Es wird die Anzahl der geschützten und nicht geschützten virtuellen Computer angezeigt. Geschützte virtuelle Computer können einen der folgenden Status haben:</p> <ul style="list-style-type: none"> ■ Geschützter ■ Nicht geschützt ■ Failover-Bereitschaft <p>Dieses Kreisdiagramm zeigt an, ob die virtuellen Computer zum Failover bereit sind.</p> <p>Die Failover-Bereitschaft wird nur für virtuelle Computer eines Recovery Services-Tresors in Azure angezeigt, die geschützt werden. Geschützte virtuelle Computer können einen der folgenden Status haben:</p> <ul style="list-style-type: none"> ■ Test empfohlen : Das Test-Failover war nicht erfolgreich, nachdem der virtuelle Computer geschützt wurde. Test-Failover empfohlen. ■ Erfolgreich durchgeführt : Mindestens ein erfolgreiches Test-Failover. ■ Nicht anwendbar : Der virtuelle Computer ist nicht für ein Test-Failover geeignet. ■ DR-Zustand (Zustand der Notfallwiederherstellung) <p>Dieses Kreisdiagramm zeigt den Status der Notfallwiederherstellung der virtuellen Computer an.</p> <p>Der DR-Zustand wird nur für virtuelle Computer eines Recovery Services-Tresors in Azure angezeigt, die geschützt werden. Geschützte virtuelle Computer können einen der folgenden</p>

Element	Beschreibung
	<p>Status haben:</p> <ul style="list-style-type: none"> ■ Kritisch : Es wurde mindestens ein kritische Replikationsfehler erkannt. Diese Fehler geben an, dass die Replikation hängengeblieben oder langsamer ist als die Datenänderungsrate für diese virtuellen Computer. ■ Warnung : Mindestens eine Warnung wurde ausgegeben, die die Replikation beeinträchtigen kann, oder darauf hinweist, dass die Replikation dieser virtuellen Computer sehr lange dauert. ■ Fehlerfrei : Die Replikation dieser virtuellen Computer wird gerade ausgeführt und es wurden keine Fehler oder Warnungen erkannt. ■ Nicht anwendbar : Virtuelle Computer sind nicht im Replikationsmodus. Beispiel: Virtuelle Computer mit Failover. <p>Siehe "Info zur Sofortwiederherstellung in der Cloud" auf Seite 852.</p>

Gruppe "Support"

Die Elemente in der Gruppe "Support" stellen technischen Support, Dokumentation, Lizenzierung und Wartungsverträge sowie die RSS Reader-Ressourcen bereit. Sie können die folgenden Elemente auswählen, um sie auf der Registerkarte "Startseite" von Backup Exec anzuzeigen.

Tabelle 3-5 "Support" Gruppenelemente

Element	Beschreibung
Technischer Support	<p>Stellt die folgenden Supportoptionen zur Verfügung, die Ihnen helfen, Produktfunktionen und Funktionalität zu verstehen oder Fehler zu beheben:</p> <ul style="list-style-type: none"> ■ Backup Exec Tech Center ■ Technischer Support für Backup Exec ■ Optimale Verfahren ■ Verwendung von MySupport zum Verwalten neuer oder vorhandener Supportfälle ■ Remote-Support ■ Registrieren, um Benachrichtigungen zu erhalten ■ Backup Exec-Updates abrufen
Dokumentation	<p>Stellt die folgenden Supportoptionen zur Verfügung, die Ihnen helfen, Produktfunktionen und Funktionalität zu verstehen oder Fehler zu beheben:</p> <ul style="list-style-type: none"> ■ Readme-Datei anzeigen ■ Administratorhandbuch (PDF) anzeigen ■ Anhang zum Administratorhandbuch (PDF) anzeigen
Lizenzierungsinformationen	<p>Stellt die folgenden Lizenzierungs- und Wartungsoptionen zur Verfügung, um Sie bei der Verwaltung von Wartungsverträgen und -lizenzen zu unterstützen:</p> <ul style="list-style-type: none"> ■ Lizenzinformationen anzeigen ■ Wartungsvertragsinformationen anzeigen
RSS Reader	<p>Lässt Sie Backup Exec- und RSS-Feeds anzeigen und hinzuzufügen.</p>

Element	Beschreibung
Installation und Upgrades	<p>Stellt die folgenden Berichte zur Verfügung:</p> <ul style="list-style-type: none"> ■ Migrationsbericht ■ Installationsübersichtsbericht <p>Dieses Element wird nur dann angezeigt, wenn Sie Backup Exec auf eine neuere Version aktualisieren.</p> <p>Siehe "Verwenden des Migrationsberichts, um zu bestimmen, wie sich vorhandene Aufträge nach einem Upgrade von einer früheren Version von Backup Exec geändert haben" auf Seite 125.</p> <p>Siehe "Anzeigen des Installationsübersichtsberichts" auf Seite 113.</p>

Konfigurieren des RSS Reader

Sie können den RSS Reader anpassen und festlegen, welche Standard-Backup Exec-Feeds angezeigt werden. Sie können zusätzliche RSS-Feeds von Backup Exec hinzufügen oder entfernen.

Der RSS Reader sortiert Artikel nach Datum und Uhrzeit. Es wird zwar nur der letzte Eintrag eines Artikels im RSS-Feed angezeigt, aber Sie können auch den ganzen Artikel aufrufen.

Der RSS Reader aktualisiert die RSS-Feeds alle 15 Minuten, wenn das Element auf der Registerkarte "Startseite" geöffnet ist. Ist ein RSS-Feed nicht im Reader geöffnet, wird er nicht aktualisiert.

So zeigen Sie einen Artikel im RSS Reader an

- 1 Aktivieren Sie auf der Registerkarte "Startseite" unter "Support" das Kontrollkästchen "RSS Reader".
- 2 Klicken Sie im RSS Reader auf Pfeil neben dem RSS-Feed, der den Artikel enthält.
- 3 Klicken Sie auf den Link für den gewünschten Artikel.

Der RSS Reader öffnet einen Ausschnitt des Artikels in einem neuen Fenster.

- 4 Klicken Sie auf "Zu vollständigem Artikel wechseln", um den gesamten Artikel in Internet Explorer anzuzeigen.

So passen Sie die RSS-Feeds im RSS Reader an

- 1 Aktivieren Sie auf der Registerkarte "Startseite" unter "Support" das Kontrollkästchen "RSS Reader".
- 2 Klicken Sie im RSS Reader auf das Bleistiftsymbol, um einen RSS-Feed hinzuzufügen.
- 3 Geben Sie folgende Daten an:

URL	Gibt den Speicherort des RSS-Feeds an, der dem RSS Reader hinzugefügt werden soll.
Name	Gibt den Namen des RSS-Feeds an, der dem RSS Reader hinzugefügt werden soll.
Klicken Sie hier, um weitere RSS-Feeds anzuzeigen	Zeigt eine Liste von RSS-Feeds an, die dem RSS Reader hinzugefügt werden können.

- 4 Klicken Sie auf "OK".

So entfernen Sie einen RSS-Feed aus dem RSS Reader

- 1 Aktivieren Sie auf der Registerkarte unter "Support" das Kontrollkästchen "RSS Reader".
- 2 Sie haben folgende Möglichkeiten:

So entfernen Sie einen Standard-Backup Exec-RSS-Feed	Deaktivieren Sie das Kontrollkästchen neben dem Backup Exec-RSS-Feed.
So entfernen Sie einen RSS-Feed, den Sie dem RSS Reader hinzugefügt haben	Klicken Sie neben dem Namen des RSS-Feeds auf das rote "X".

Erstellen eines Plans für die Notfallwiederherstellung (DPP)

Ziel der Notfallvorbereitung ist es, durch die Umsetzung von Strategien und Vorgehensweisen den Schaden und den Verlust von Dateien im Falle eines Notfalls so gering wie möglich zu halten.

Für die Notfallwiederherstellung gibt es grundsätzlich folgende Methoden:

- Automatisierte Notfallwiederherstellung. Mit Simplified Disaster Recovery (SDR) von Backup Exec wird die Notfallwiederherstellung für Windows-Computer automatisiert.
- Manuelle Notfallwiederherstellung – Sie können lokale und standortferne Windows-Computer manuell wiederherstellen.

Mit dem Plan für die Notfallwiederherstellung (DPP) soll so schnell wie möglich wieder der betriebsfähige Zustand hergestellt werden. Backup Exec ist eine entscheidende Komponente der DPP. Der Plan für die Notfallwiederherstellung (DPP), den Sie unter Einbeziehung von Backup Exec erstellen, sollte auf Ihre Netzwerkumgebung abgestimmt sein.

Weitere Informationen zum Ausführen einer manuellen Notfallwiederherstellung finden Sie in den folgenden Abschnitten:

Siehe ["Durchführen einer manuellen Notfallwiederherstellung eines lokalen Backup Exec-Servers auf einem Windows-Computer"](#) auf Seite 1006.

Siehe ["Manuelles Ausführen der Notfallwiederherstellung eines Remote-Backup Exec-Servers oder Remote-Agent auf einem Windows-Computer"](#) auf Seite 1011.

Obleich Umgebungen sich in der Regel unterscheiden, sollten Sie die folgenden Elemente bei der Konzeption des Plans berücksichtigen.

Tabelle 3-6 Hauptelemente eines Plans für die Notfallwiederherstellung

Element	Beschreibung
Schutz der Hardware	Die Hardwaregeräte im Netzwerk (CPUs, Laufwerke, Videogeräte) können durch verschiedene Arten von Systemausfällen beschädigt werden. Zum Schutz von Hardware werden heutzutage vor allem unterbrechungsfreie Stromversorgungen (Uninterruptible Power Supplies, UPS), Überspannungsschutzgeräte und Sicherheitsüberwachungsgeräte eingesetzt. Haben Sie diese Maßnahmen nicht bereits ergriffen, sollte deren Einrichtung auf jeden Fall in Erwägung gezogen werden. Diese Investition macht sich bei einem Systemausfall mehr als bezahlt.

Element	Beschreibung
Die Fähigkeit, den Firmenbetrieb auch während eines Systemausfalls aufrecht zu erhalten	Vergewissern Sie sich, dass in Ihrem Unternehmen Vorsichtsmaßnahmen für den Fall einer Unterbrechung der Funktionsfähigkeit des Netzwerkes existieren. Zum Beispiel klingeln Telefone in einer Verkaufsabteilung auch während eines Serverausfalls weiter. Aufträge und Bestellungen müssen daher bis zur Wiederherstellung des Servers handschriftlich entgegengenommen werden. Jede Abteilung sollte Strategien für solche Notfälle entwickeln. Auf diese Weise können die Geschäftsabwicklungen ungehindert weiterlaufen, bis der Server wieder betriebsfähig ist.
Eine solide Backup-Strategie	Von entscheidender Bedeutung für die schnelle Wiederherstellung des Dateiservers ist die Einrichtung einer gut durchdachten Backup-Strategie mit einem leistungsfähigen Medienrotationsschema.
Externe und duplizierte Backups.	Es ist unerlässlich, dass Sie die gesicherten Daten regelmäßig an eine externe Aufbewahrungseinrichtung senden. Wenn Sie Festplatten als Speichermedium verwenden, sollten Sie in einem zusätzlichen Schritt die Backups auf anderen Speichern duplizieren. Damit wird sichergestellt, dass bei Ausfall Ihrer Speichereinrichtung keines Ihrer Backups tatsächlich vernichtet wird. Es sollte auch in Betracht gezogen werden, Daten abhängig von ihrer Wichtigkeit in verschiedene externe Aufbewahrungseinrichtungen auszulagern.
Effektive Verwaltung der Notfallwiederherstellung	Eine Person oder eine Gruppe sollte die im Plan enthaltenen Maßnahmen für die Notfallvorbereitung Ihrer Firma ständig überwachen. Diese Person oder Gruppe sollte Schutzmaßnahmen für die Hardwaregeräte installieren und anschließend regelmäßig warten, alle Abteilungen sollten für den Fall eines zeitweisen Serverausfalls über eine Strategie verfügen, und es sollten regelmäßig Backups vorgenommen und im Rahmen eines Rotationsplans an externe Stellen ausgelagert werden. Dokumentieren Sie Ihren Plan für die Notfallwiederherstellung für Referenzzwecke.

Siehe ["Erste Schritte mit Backups"](#) auf Seite 151.

Erste Schritte mit Backups

Nach der Installation von Backup Exec können Sie einen Backup-Auftrag ausführen. Die folgende Tabelle beschreibt die empfohlene Vorgehensweise für die ersten Schritte.

Tabelle 3-7 Erste Schritte mit Backups

Schritt	Beschreibung
1. Konfigurieren des Speichers	<p>Sie müssen ein Speichergerät konfigurieren, bevor Sie Backup-Aufträge ausführen können.</p> <p>Wenn noch keine Speichergeräte wie Bandlaufwerke oder Wechsler konfiguriert sind, können Sie den Assistenten "Speicher konfigurieren" zum Einrichten von Speichergeräten in Backup Exec verwenden. Ein Assistent führt Sie durch die Konfiguration aller von Backup Exec unterstützten Speicher.</p> <p>Klicken Sie zum Starten des Assistenten auf der Registerkarte "Speicher" in der Gruppe "Konfigurieren" auf "Speicher konfigurieren". Der Assistent führt Sie durch die verbleibenden Schritte des Vorgangs.</p> <p>Siehe "Verwenden des Assistenten "Speicher konfigurieren" auf Seite 523.</p>
2. Konfigurieren von Backup Exec-Login-Konten	<p>Sie können das standardmäßige Backup Exec-Login-Konto verwenden, d. h. das System-Login-Konto für den Backup Exec-Server.</p> <p>Backup Exec verwendet standardmäßig das System-Login-Konto für die meisten Backups. Das System-Login-Konto enthält die Anmeldedaten des Backup Exec-Dienstkontos. Wenn das Dienstkonto keine Zugriffsrechte auf die von Ihnen ausgewählten Daten für das Backup hat, können Sie den "Assistenten für das Login-Konto" verwenden. Verwenden Sie diesen Assistenten, um zusätzliche Login-Konten zu erstellen, die die notwendigen Anmeldedaten für den Zugriff auf diese Daten enthalten.</p> <p>Klicken Sie zum Starten des "Assistenten für das Login-Konto" auf die Backup Exec-Schaltfläche. Wählen Sie "Konfiguration und Einstellungen" > "Login-Konten" > "Assistent für das Login-Konto".</p> <p>Siehe "Backup Exec-Login-Konten" auf Seite 762.</p>

Schritt	Beschreibung
3. Ausführen eines Backup-Auftrags	<p>Sie können einen beliebigen Computer sichern, auf dem der entsprechende Backup Exec Agent (z. B. Agent for Windows) installiert ist.</p> <p>Wenn Sie auf einem Computer noch keinen Backup Exec Agent installiert haben, können Sie dies nun nachholen. Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" unter "Server" auf "Hinzufügen" und nehmen Sie dann die entsprechende Auswahl vor. Der Assistent führt Sie durch die verbleibenden Schritte des Vorgangs.</p> <p>Wählen Sie zum Starten eines Backup-Auftrags auf der Registerkarte "Backup und Wiederherstellung" den zu sichernden Computer aus und klicken Sie dann in der Gruppe "Backups" auf "Backup". Klicken Sie auf ein Menüelement wie z. B. "Backup-to-Disk". Sie können auf "Bearbeiten" klicken, um Standardwerte zu ändern, oder Sie können auf "OK" klicken, um alle Standardwerte zu akzeptieren, sodass Backup Exec den Auftrag planen kann.</p> <p>Siehe "Sichern von Daten" auf Seite 174.</p>
4. Erstellen des Simplified Disaster Recovery-Datenträger-Image	<p>Backup Exec wählt standardmäßig alle Daten auf einem Computer für das Backup aus, einschließlich der kritischen Systemkomponenten, die Sie zum Durchführen einer vollständigen Systemwiederherstellung mithilfe von SDR benötigen. SDR-Backups sind Backups, bei denen alle kritischen Systemkomponenten für das Backup ausgewählt werden. SDR-Backups sind erforderlich, damit Backup Exec einen Computer neu erstellen und mithilfe SDR in einem funktionsfähigen Zustand wiederherstellen kann.</p> <p>Siehe "Sicherstellen, dass Simplified Disaster Recovery für Backups aktiviert ist" auf Seite 950.</p> <p>Nach dem Ausführen von SDR-Backups für alle zu schützenden Computer sollten Sie ein Simplified Disaster Recovery-Datenträger-Image (SDR) erstellen.</p> <p>Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" unter "Wiederherstellungen" auf "SDR-Datenträger erstellen". Der Assistent führt Sie durch die verbleibenden Schritte des Vorgangs.</p> <p>Siehe "Erstellen eines SDR-Datenträger-Image" auf Seite 957.</p>

Backups

In diesem Kapitel werden folgende Themen behandelt:

- Vorbereitung für Ihr erstes Backup mit Backup Exec
- Verbessern von Backups in Backup Exec
- Fehlerbehebung bei der Backup-Leistung
- Erforderliche Benutzerrechte für Backup-Aufträge
- Serverliste auf der Registerkarte "Backup und Wiederherstellung"
- Hinzufügen von zu sichernden Servern zur Serverliste auf der Registerkarte "Backup und Wiederherstellung"
- Entfernen eines Servers aus der Serverliste auf der Registerkarte "Backup und Wiederherstellung"
- Erstellen einer Servergruppe
- Ein- bzw. Ausblenden von Servergruppen auf der Registerkarte "Backup und Wiederherstellung"
- Hinzufügen von Servern zu einer Servergruppe
- Entfernen von Servern aus einer Servergruppe
- Bearbeiten einer Servergruppe
- Verschieben von Servern in die Gruppe "Ausrangierte Server"
- Verschieben von ausrangierten Servern in die Gruppe "Alle Server"
- Entfernen von Servergruppen aus Backup Exec
- Sichern von Daten

- Info zum Auswählen von zu sichernden Daten
- Ändern der Reihenfolge, in der Backup-Quellen gesichert werden
- Ausschließen von Dateien von Backups
- Einschließen spezifischer Dateien mit der Backup-Auswahl eines Backup-Auftrags
- Info zum Sichern von wichtigen Systemkomponenten
- Shadow Copy-Dateisystemkomponenten von Backup Exec
- Backup-Methoden in Backup Exec
- Konfigurieren von Backup-Methoden für Backup-Aufträge
- Ermittlung des Backup-Status von Dateien in Backup Exec
- Konfigurieren von Backup Exec, um Dateien nach einem Backup automatisch zu löschen
- Konfigurieren erweiterter Optionen für Backup-Aufträge
- Ausführen des nächsten geplanten Backup-Auftrags vor seiner geplanten Zeit
- Bearbeiten von Backup-Definitionen
- Prüfung der Identifikationsdaten für Backup-Quellen
- Ersetzen der Identifikationsdaten für eine Backup-Quelle
- Erstellen neuer Identifikationsdaten für eine Backup-Quelle
- Löschen ausrangierter oder nicht genutzter Backup-Quellen aus dem Teilfenster "Identifikationsdaten"
- Wie die Joborganisation in Backup Exec arbeitet
- Einschließlich ein spezifisches Datum im Zeitplan für einen Backup-Auftrag
- Durchführung von Backup-Aufträgen zu einem bestimmten Datum verhindern
- Anzeigen aller geplanten Backup-Aufträge im Kalender
- Hinzufügen einer Stufe zu einer Backup-Definition
- Bearbeiten von Stufen
- Manuelles Duplizieren von Backup-Sätzen bzw. Auftragsverläufen
- Manuelle Ausführung von Probelaufaufträgen

- [Gesicherte Daten manuell überprüfen](#)
- [Kopieren von Daten von einer virtuellen Bandbibliothek auf ein physisches Bandgerät mit DirectCopy](#)

Vorbereitung für Ihr erstes Backup mit Backup Exec

Bevor Sie Daten sichern, sollten Sie eine Backup-Strategie entwickeln, die die Backup-Methode, die Häufigkeit und die Datenaufbewahrungsmethoden umfasst, die für Ihre Organisation angebracht sind. Eine Backup-Strategie ist die Sammlung von Verfahren, die Sie zum Sichern Ihrer Umgebung implementieren. Sie haben möglicherweise verschiedene Strategien für verschiedene Bereiche des Unternehmens.

Sie müssen möglicherweise auch Ihre Backup-Umgebung analysieren, um die folgenden Fragen zu beantworten:

- Wie viele Daten müssen gesichert werden?
- Wie lange dauert das Backup?
- Wie viel Speicher ist erforderlich?

Sollte die Leistung von Backup- oder Wiederherstellungsaufträgen beeinträchtigt sein, folgen Sie den Schritten zur Fehlerbehebung in den folgenden Abschnitten.

Siehe ["Verbessern von Backups in Backup Exec"](#) auf Seite 156.

Siehe ["Fehlerbehebung bei der Backup-Leistung"](#) auf Seite 160.

Bevor Sie einen Backup-Auftrag ausführen, sollten Sie sich vergewissern, dass Sie über die entsprechenden Benutzerrechte verfügen.

Siehe ["Erforderliche Benutzerrechte für Backup-Aufträge"](#) auf Seite 165.

Sie müssen Speicher konfigurieren, bevor Sie Backup-Aufträge erstellen. Sie können Backup Exec so einrichten, dass bestimmte Speichergeräte oder logische Gruppierungen von Geräten verwendet werden, z. B. Speicherpools.

Mit den folgenden Aufgaben können Sie Speicherhardware und Medien auf optimale und effektive Weise verwalten:

- Erstellen von plattenbasiertem Speicher, damit Backup Exec die Aufbewahrung der Backup-Daten automatisch verwalten kann
 Siehe ["Konfigurieren von Festplattenspeicher"](#) auf Seite 372.
- Einrichten von Speichergerätepools, um die Auslastung durch Aufträge gleichmäßig zu verteilen
 Siehe ["Erstellen von Speichergerätepools"](#) auf Seite 512.

- Erstellen von Mediensätzen, um die Datenaufbewahrung für Bandkassettenmedien zu verwalten
 Siehe "[Standard-Mediansätze](#)" auf Seite 473.
- Konfigurieren von Deduplizierungsdatenenträgerspeicher, um Speicher und Netzwerkbandbreite zu optimieren
 Siehe "[Info zu Deduplication Feature](#)" auf Seite 1047.

Verbessern von Backups in Backup Exec

Backups werden in einer Gruppe von Systemen ausgeführt. Nehmen wir an, diese Systeme sind Rohrleitungen mit unterschiedlichem Querschnitt, vom Ausgangsdatenenträger bis zum Backup-Ziel. Ist eine dieser Leitungen eingeschränkt, kommt es zu Engpässen, die den gesamten Backup-Vorgang verlangsamen. Die Schritte zur Fehlerbehebung in diesem Abschnitt helfen Ihnen bei der Identifizierung von Engpässen in Backup- oder Wiederherstellungsvorgängen.

Folgende Variablen könnten sich auf die Backup- oder Wiederherstellungsleistung auswirken:

Element	Beschreibung
Hardware	<p>Folgende Hardwarevariablen könnten sich auf die Leistung auswirken:</p> <ul style="list-style-type: none"> ■ Die Geschwindigkeit des Festplattencontrollers ■ Nicht ordnungsgemäße Verkabelung oder Terminierung ■ Fehler, die von der Festplatte, dem Bandlaufwerk, dem Festplattencontroller oder dem SCSI-Bus verursacht werden <p>Bestätigen Sie, dass der Controller auf die Bandlaufwerke abgestimmt ist. Ist dies nicht der Fall, kann es zu unerwarteten Leistungseinschränkungen kommen.</p> <p>Bestätigen Sie, dass die SCSI-BIOS-Einstellungen wie folgt eingerichtet sind:</p> <ul style="list-style-type: none"> ■ Die Option "Initiate Wide Negotiation" muss auf "Yes" festgelegt sein, wenn das Bandgerät über eine Wide-SCSI-Kabelverbindung (68 Pins) angeschlossen ist. ■ Die Bandlaufwerke sind nicht an einen SCSI-Raid-Controller angeschlossen

Element	Beschreibung
System	Kapazität und Geschwindigkeit des Medienservers, auf dem das Backup durchgeführt wird, und der zu sichernde Remote-Computer haben starken Einfluss auf die Leistung. Die Systemaktivität während des Backups beeinflusst ebenfalls die Leistung. Das Backup fragmentierter Festplatten dauert länger. Stark fragmentierte Festplatten verringern nicht nur die Geschwindigkeit, mit der die Daten auf das Band geschrieben werden, sondern beeinträchtigen auch die Systemleistung insgesamt. Das Sichern fragmentierter Dateien dauert länger, da sich die einzelnen Datensegmente an unterschiedlichen Stellen auf der Festplatte befinden. Diese Fragmentierung erhöht die Zugriffszeit. Defragmentieren Sie die Festplatten daher regelmäßig.
Arbeitsspeicher	Die Größe des verfügbaren Arbeitsspeichers beeinflusst die Geschwindigkeit von Backups. Zu wenig Arbeitsspeicher, falsche Einstellungen für Auslagerungsdateien und zu wenig Speicherplatz auf der Festplatte können zu einer übermäßigen Auslagerung und verringerten Leistung führen. Stellen Sie sicher, dass alle Anwendungen und Prozesse den beim Start zugewiesenen Arbeitsspeicher nach dem Beenden wieder freigeben. Ist dies nicht der Fall, kommt es zu Speicherverlusten.
Dateitypen	Eine durchschnittliche Datei wird mit einem Verhältnis von 2:1 komprimiert, wenn die Hardware-Komprimierung genutzt wird. Das Komprimierungsverhältnis kann je nach Typ der zu sichernden Dateien variieren. Wenn keine Komprimierung verwendet wird, läuft das Bandgerät mit der angegebenen Geschwindigkeit. Durchschnittliche Komprimierungsverhältnissen können die Backup-Geschwindigkeit verdoppeln. Grafik- und Bilddateien sind bereits vollständig auf der Festplatte komprimiert. Die Hardware-Komprimierung wird vom Bandgerät und nicht von der Backup-Software durchgeführt.
Komprimierung	Bei einer erfolgreichen Komprimierung kann sich die Datenübertragungsrate des Bandlaufwerks bis auf das Doppelte der ursprünglichen Rate erhöhen. Die Komprimierung kann je nach den Eingabedaten stark variieren. Bilddateien aus einem Grafikprogramm können mit einem Verhältnis von 4,5:1 oder mehr komprimiert werden, Binärdateien vielleicht nur mit 1,5:1. Daten, die bereits komprimiert oder verschlüsselt sind, wachsen eventuell um bis zu fünf Prozent erweitert werden, wenn Sie eine weitere Komprimierung anwenden. Dieser Wachstum kann den Datendurchsatz des Laufwerks verringern.

Element	Beschreibung
Dateien	Die Gesamtzahl von Dateien auf einem Datenträger und die relative Größe der einzelnen Dateien haben Einfluss auf die Leistung. Das Sichern von Datenträgern, die weniger aber größere Dateien enthalten, ist schneller. Der Vorgang ist langsamer, wenn der Datenträger zahlreiche kleine Dateien enthält. Eine große Anzahl von Dateien, die sich im gleichen Ordner befinden, können effizienter als Dateien an mehreren Speicherorten gesichert werden.
Blockgröße	Höhere Blockgrößen verbessern die Komprimierungsrate. Dadurch erhöhen sich der Datendurchsatz des Laufwerks und die Kapazität des Bands. Stellen Sie sicher, dass Block- und Puffergröße ordnungsgemäß eingestellt sind. Datendurchsatz erhöht sich im Verhältnis zur erzielten Komprimierung, bis der maximale Durchsatz erreicht ist. Erhöhen Sie die Blockgröße nicht über die Standardeinstellung.

Element

Beschreibung

Netzwerk

Die physische Verbindung zu einem Remote-Datenträger begrenzt die Backup-Geschwindigkeit für diesen Datenträger. Die Geschwindigkeit, mit der die Festplatten eines Remote-Servers gesichert werden können, hängt von folgenden Faktoren ab:

- Hersteller und Modell der Netzwerkkarten
- Konfiguration von Modus/Rahmentyp des Adapters
- Verbindungs-Hardware
- Windows-Einstellungen
- Standort der Laufwerke Die lokalen Festplatten auf dem Medienserver können normalerweise mit einer höheren Geschwindigkeit gesichert werden als Remote-Server über ein Netzwerk.

Eine gängige Ursache für langsame Netzwerk-Backups ist die Konfiguration des Netzwerks. Funktionen wie Vollduplex und automatische Erkennung werden möglicherweise nicht vollständig in allen Umgebungen unterstützt. Legen Sie zum Verbessern des Durchsatzes die Geschwindigkeit auf 100 MB und die serverseitige Duplex-Einstellung auf "Halb/Voll" fest. Ermitteln Sie, an welchem Ethernet-Port des Switch der Server angeschlossen ist, und legen Sie die Einstellung "SWITCH PORT" auf "100 MB" und Duplex auf "Halb/Voll" fest. Führen Sie diesen Vorgang für den Switch-Port des Backup-Servers und aller zu sichernden Computer durch.

Hinweis: Wenn anstatt des Switch ein Hub verwendet wird, wird Vollduplex möglicherweise nicht unterstützt. Weitere Informationen zu Gerätefunktionen erhalten Sie beim Hersteller.

Hinweis: Die Einstellungen auf Switch und Netzwerkkarte müssen übereinstimmen. Beispiel: Ist der Switch-Port auf "100 MB" und "Halbduplex" eingestellt, müssen dieselben Einstellungen auf der Netzwerkkarte festgelegt sein.

Wenn ein Vollduplex-Backup-Auftrag langsamer als ein Halbduplex-Backup-Auftrag ist, wird Vollduplex möglicherweise nicht für die vorliegende Kombination aus Netzwerkkarte, Treiber und Switch unterstützt. Wenden Sie sich an den Hersteller der Netzwerkkarte und des Switches, um aktuelle Treiber, Firmware oder andere Supportdokumentation zu erhalten.

Der Netzwerkkartentreiber kann eine häufige Ursache für langsamen Datendurchsatz sein. Dieser Treiber kann durch ein Service Pack des Betriebssystems überschrieben werden. Wenn ein Service Pack angewendet und der Treiber überschrieben wurde, installieren Sie den OEM-Treiber erneut.

Element	Beschreibung
Debugging	Ist Debugging aktiviert, kann sich dies auch auf die Systemleistung auswirken. Debugging, das über das Applet "Services" ausgeführt wird, ist ein vorübergehender Vorgang. Starten Sie die Dienste bzw. den Computer neu, um das Debugging zu beenden. Ein über die Windows-Registrierung konfiguriertes Debugging wird ständig ausgeführt. Wenn Sie die Dienste im Debug-Modus belassen, wachsen die Protokolle ständig. Deaktivieren Sie daher zum Verbessern der Leistung den Debug-Modus, wenn das Problem behoben wurde, löschen Sie die älteren Debug-Dateien, oder komprimieren Sie den Protokollordner.
Backup Exec-Datenbank	Ist die Backup Exec-Datenbank (BEDB) auf einer vorhandenen SQL-Instanz installiert, die von anderen Anwendungen genutzt wird, kann dies auch die Leistung beeinträchtigen. Dies ist besonders in einer Umgebung mit Central Administration Server (CAS) wichtig. Andere Anwendungen können Probleme verursachen, wenn sie alle verfügbaren Ressourcen innerhalb der Instanz nutzen.

Fehlerbehebung bei der Backup-Leistung

Sie haben mehrere Möglichkeiten zum Identifizieren der Ursachen von Leistungsproblemen in Backup Exec-Aufträgen. Dieser Abschnitt enthält Vorschläge zur Fehlerbehebung für die folgenden Auftragstypen:

- Lokales Backup auf Festplatte
- Remote-Backup auf Festplatte
- Lokales Backup auf Band
- Remote-Backup auf Band

Lokales Backup auf Festplatte

1. Legen Sie eine Basis fest. Überprüfen Sie vorherige Aufträge auf der Registerkarte "Auftragsüberwachung" im Bereich "Auftragsverlauf". Notieren Sie sich sowohl die Geschwindigkeit der vorherigen Aufträge als auch die Gesamtdauer dieser Backups. Prüfen Sie, wie lange das Ausführen diese Aufträge gedauert hat, nicht den Datendurchsatz. Wenn aktuelle Aufträge länger dauern als vorherige oder nicht den Erwartungen in Bezug auf Geschwindigkeit entsprechen, setzen Sie die Fehlerbehebung fort.
2. Grenzen Sie das Problem ein. Wenn der Backup-Auftrag mehrere Laufwerke oder Agents enthält, teilen Sie ihn in entsprechende separate Aufträge auf.

Sie können dann die Leistung jedes Laufwerks oder Agent separat überprüfen. Klicken Sie zum Aufteilen des Backup-Auftrags auf die Schaltfläche "Backup Exec", wählen Sie das Laufwerk "C\$", planen Sie den Auftrag und klicken Sie auf "Senden". Wenn die Leistung nur für einen bestimmten Auftrag niedrig ist, setzen Sie die Fehlerbehebung nur diesen Auftrag fort.

3. Wenn ein bestimmter Auftrag weiterhin eine geringe Leistung aufweist, teilen Sie ihn erneut auf, um zu ermitteln, welcher Teil der Daten die Leistung am stärksten beeinflusst.

Ein Datenabschnitt mit vielen kleinen Dateien und Ordnern wirkt sich negativ auf die Leistung aus. Dies ist normal.

Prüfen Sie, ob die Daten an einen anderen Speicherort umgeleitet werden. Einige Dateisysteme ermöglichen, dass Daten über eine Remote-Verbindung in einem Ordner bereitgestellt werden. Die Dateien in diesen Ordnen können sich auf Remote-Servern befinden, was die Backup-Leistung beeinträchtigen kann.

4. Testen Sie den Backup-to-Disk (B2D)-Durchsatz. Verwenden Sie Windows, um mindestens 2 GB Daten im Backup-Auftrag auf die B2D-Festplatte zu kopieren. Vergleichen Sie die Leistung dieses Vorgangs mit der Leistung des Backups. Ist die Leistung beider Vorgänge vergleichbar, befindet sich der Leistungsengpass wahrscheinlich in dem Festplattensubsystem, in dem sich die B2D-Ordner befinden. Verschieben Sie die B2D-Ordner in ein schnelleres Festplattensubsystem oder setzen Sie die Fehlerbehebung fort.
5. Testen Sie den Systemdurchsatz. Wenn der Auftrag auf Dateien und nicht auf einer Exchange-, SQL- oder einer anderen Datenbank basiert, erstellen Sie ein ähnliches Backup in NTBackup (Windows-Backup) und führen Sie ein Backup-to-Disk durch. Vergleichen Sie die Leistung des NTBackup-Auftrags mit der des Backup Exec-Auftrags.

Wenn Sie eine Exchange-, SQL- oder andere Datenbank sichern müssen, erstellen Sie einen Backup-to-Disk-Auftrag in Backup Exec, der 2 GB an Daten an den Speicherort dieses Datenbank-Agent sichert. Führen Sie den gleichen Test mit NTBackup durch. Vergleichen Sie die Leistung der beiden Backups. Wenn die Leistung ähnlich ist, wird Backup Exec bei Systemkapazität ausgeführt.

Remote-Backup auf Datenträger

1. Legen Sie eine Basis fest. Überprüfen Sie vorherige Aufträge auf der Registerkarte "Auftragsüberwachung" im Bereich "Auftragsverlauf". Notieren Sie sich sowohl die Geschwindigkeit der vorherigen Aufträge als auch die Gesamtdauer dieser Backups. Prüfen Sie, wie lange das Ausführen diese Aufträge gedauert hat, nicht den Datendurchsatz. Wenn aktuelle Aufträge

länger dauern als vorherige oder nicht den Erwartungen in Bezug auf Geschwindigkeit entsprechen, setzen Sie die Fehlerbehebung fort.

2. Grenzen Sie das Problem ein. Wenn der Backup-Auftrag mehrere Laufwerke oder Agents enthält, teilen Sie ihn in entsprechende separate Aufträge auf. Sie können dann die Leistung jedes Laufwerks oder Agent separat überprüfen. Klicken Sie zum Aufteilen des Backup-Auftrags auf die Schaltfläche "Backup Exec", wählen Sie das Laufwerk "C\$", planen Sie den Auftrag und klicken Sie auf "Senden". Wenn die Leistung nur für einen bestimmten Auftrag niedrig ist, setzen Sie die Fehlerbehebung nur diesen Auftrag fort.
3. Wenn ein bestimmter Auftrag weiterhin eine geringe Leistung aufweist, teilen Sie ihn erneut auf, um zu ermitteln, welcher Teil der Daten die Leistung am stärksten beeinflusst. Ein Datenabschnitt mit vielen kleinen Dateien und Ordnern wirkt sich negativ auf die Leistung aus. Dies ist normal.

Prüfen Sie, ob die Daten an einen anderen Speicherort umgeleitet werden. Einige Dateisysteme ermöglichen, dass Daten über eine Remote-Verbindung in einem Ordner bereitgestellt werden. Die Dateien in diesen Ordnern können sich auf Remote-Servern befinden, was die Backup-Leistung beeinträchtigen kann.

4. Testen Sie den Netzwerkdurchsatz. Kopieren Sie zwischen 500 MB und 1 GB an Daten aus dem Backup-Server auf den Remote-Server. Notieren Sie sich, wie lange das Kopieren dauert. Erstellen Sie zum Ausführen dieses Kopiervorgangs einen Pfad zu einem anderen Server. Geben Sie in der Windows-Eingabeaufforderung folgenden Befehl ein `<\\Name des Remote-Servers\c$>`. Wenn das Laufwerk angezeigt wird, kopieren Sie die Daten.

Verwenden Sie das gleiche Verfahren, um Daten aus dem Remote-Server auf den Backup-Server zu kopieren, und notieren Sie sich, wie lange der Vorgang dauert.

Vergleichen Sie die Geschwindigkeit dieser beiden Netzwerktests mit der Leistung von Backup Exec. Wenn die Leistung von Backup Exec geringer als die des Dateikopiertests ist, ist das Netzwerk wahrscheinlich nicht der Engpass.

In diesem Fall sollten Sie den gleichen Test auf einem anderen Remote-Server oder zwischen zwei anderen Servern ausführen. So können Sie bestimmen, ob die Leistungsprobleme vom Netzwerk allgemein oder einem bestimmten Server im Netzwerk verursacht werden. Wenn Sie keine Netzwerkprobleme erkennen, fahren Sie mit dem nächsten Schritt fort.

5. Testen Sie den Systemdurchsatz. Sichern Sie den Remote-Server mit NTBackup (Windows-Backup). Wenn der Remote-Server in NTBackup nicht sichtbar ist, erstellen Sie ein zugeordnetes Laufwerk auf dem Serverlaufwerk und versuchen Sie, mindestens 2 GB zu sichern. Vergleichen Sie die

NTBackup- und die Backup Exec-Protokolle und notieren Sie sich die Leistungsunterschiede.

Lokales Backup auf Band

1. Legen Sie eine Basis fest. Überprüfen Sie vorherige Aufträge auf der Registerkarte "Auftragsüberwachung" im Bereich "Auftragsverlauf". Notieren Sie sich sowohl die Geschwindigkeit der vorherigen Aufträge als auch die Gesamtdauer dieser Backups. Prüfen Sie, wie lange das Ausführen dieser Aufträge gedauert hat, nicht den Datendurchsatz. Wenn aktuelle Aufträge länger dauern als vorherige oder nicht den Erwartungen in Bezug auf Geschwindigkeit entsprechen, setzen Sie die Fehlerbehebung fort.
2. Löschen Sie alle temporären Hardwarefehler. Schalten Sie Server, Bandlaufwerk oder Bandbibliothek aus und wieder ein. Schalten Sie zuerst den Backup-Server und dann das Bandlaufwerk bzw. die Bibliothek aus. Warten Sie ein paar Sekunden und schalten Sie Bandlaufwerk bzw. Bandbibliothek wieder ein. Wenn das Bandlaufwerk bzw. die Bandbibliothek bereit ist, schalten Sie den Server ein. Führen Sie den Backup-Auftrag erneut aus und prüfen Sie die Leistung. Besteht das Leistungsproblem weiterhin, setzen Sie die Fehlerbehebung fort.
3. Prüfen Sie das SCSI-Subsystem. Die geringe Leistung kann von der Festplatte, dem Bandlaufwerk, dem Festplattencontroller, dem SCSI-Bus oder unsachgemäßer Verkabelung oder Terminierung verursacht werden. Stellen Sie sicher, dass Folgendes zutrifft:
 - Der Controller ist auf die Bandlaufwerke abgestimmt.
 - Die SCSI-BIOS-Einstellungen sind ordnungsgemäß festgelegt.
 - Die Option "Initiate Wide Negotiation" muss auf "Yes" festgelegt sein, wenn das Bandgerät über eine Wide-SCSI-Kabelverbindung (68 Pins) angeschlossen ist.
 - Die Bandlaufwerke sind nicht an einen SCSI-Raid-Controller angeschlossen.

Die Verifizierung zeigt den Zustand des SCSI-Subsystems an. Da die Verifizierung nur Daten liest und Vorgänge im Speicher auf dem Medienserver ausführt, begrenzt die Geschwindigkeit des SCSI-Subsystems die Leistung der Verifizierung. Sie können die Leistung des Vorgangs anhand der Protokolle für die Aufträge, die eine Verifizierung enthalten. Ist die Verifizierung langsam, befindet sich der Engpass wahrscheinlich im SCSI-Subsystem.

4. Teilen Sie den Auftrag in kleinere Aufträge auf, zu ermitteln, welche Agents oder Funktionen die Leistung beeinträchtigen könnten. Zeigt einer der kleineren Aufträge Leistungsprobleme, führen Sie die Fehlerbehebung für diesen Auftrag durch.

5. Wenn Sie ein bestimmter Auftrag immer noch eine verringerte Leistung anzeigt, teilen Sie den Auftrag erneut auf, um zu bestimmen, ob sich ein bestimmter Teil der Daten negativ auf die Leistung auswirkt. Ein Datenabschnitt mit vielen kleinen Dateien und Ordnern wirkt sich negativ auf die Leistung aus. Dies ist normal.

Prüfen Sie, ob die Daten an einen anderen Speicherort umgeleitet werden. Einige Dateisysteme ermöglichen, dass Daten über eine Remote-Verbindung in einem Ordner bereitgestellt werden. Die Dateien in diesen Ordnern können sich auf Remote-Servern befinden, was die Backup-Leistung beeinträchtigen kann.

6. Testen Sie den Systemdurchsatz. Sichern Sie den Remote-Server mit NTBackup (Windows-Backup). Wenn der Remote-Server in NTBackup nicht sichtbar ist, erstellen Sie ein zugeordnetes Laufwerk auf dem Serverlaufwerk und versuchen Sie, mindestens 2 GB zu sichern. Vergleichen Sie die NTBackup- und die Backup Exec-Protokolle und notieren Sie sich die Leistungsunterschiede.
7. Eine erfolgreiche Komprimierung kann die Datenübertragungsrate des Bandlaufwerks fast verdoppeln. Die Komprimierung kann je nach den Eingabedaten stark variieren. Bilddateien können mit einem Verhältnis von 4,5:1 oder mehr komprimiert werden. Binärdateien dagegen können nur mit 1,5:1 komprimiert werden. Daten, die bereits komprimiert oder verschlüsselt sind, wachsen eventuell um bis zu fünf Prozent erweitert werden, wenn Sie eine weitere Komprimierung anwenden. Diese Erweiterung kann den Datendurchsatz des Laufwerks verringern.

Hat die Hardware- oder Software-Komprimierung nicht die gewünschte Wirkung, wählen Sie die andere Methode. Bearbeiten Sie dazu die Backup-Auftragseigenschaften: Wählen Sie in den "Einstellungen" unter "Allgemein" in der Dropdown-Liste "Komprimierungstyp" eine andere Option.

Remote-Backup auf Band

1. Die Fehlerbehebung ist mit der für "Lokales Backup auf Band" (siehe oben) identisch. Sie können auch die folgenden Schritte durchführen.
2. Testen Sie den Netzwerkdurchsatz. Kopieren Sie zwischen 500 MB und 1 GB an Daten aus dem Backup-Server auf den Remote-Server und notieren Sie sich die Dauer. Erstellen Sie dazu einen Pfad zu einem anderen Server. Geben Sie in der Windows-Eingabeaufforderung folgenden Befehl ein: `<\\Name des Remote-Servers\c$>` . Wenn das Laufwerk angezeigt wird, kopieren Sie die Daten.

Verwenden Sie das gleiche Verfahren, um Daten aus dem Remote-Server auf den Backup-Server zu kopieren, und notieren Sie sich, wie lange der Vorgang dauert.

Vergleichen Sie die Geschwindigkeit dieser beiden Netzwerktests mit der Leistung von Backup Exec. Wenn die Leistung von Backup Exec geringer als die des Dateikopiertests ist, ist das Netzwerk wahrscheinlich nicht der Engpass.

In diesem Fall sollten Sie den gleichen Test auf einem anderen Remote-Server oder zwischen zwei anderen Servern ausführen. So können Sie bestimmen, ob die Leistungsprobleme vom Netzwerk allgemein oder einem bestimmten Server im Netzwerk verursacht werden. Wenn Sie keine Netzwerkprobleme erkennen, fahren Sie mit dem nächsten Schritt fort.

3. Testen Sie den Systemdurchsatz. Sichern Sie den Remote-Server mit NTBackup (Windows-Backup). Wenn der Remote-Server in NTBackup nicht sichtbar ist, erstellen Sie ein zugeordnetes Laufwerk auf dem Serverlaufwerk und versuchen Sie, mindestens 2 GB zu sichern. Vergleichen Sie die NTBackup- und die Backup Exec-Protokolle und notieren Sie sich die Leistungsunterschiede.

Hinweis: Wenn keine Remote-Backups mit NTBackup möglich sind, führen Sie NTBackup lokal auf dem Remote-Server aus und führen Sie dort einen lokalen Backup-Auftrag aus. Verwenden Sie Backup Exec, um dieselben Daten auf der Festplatte zu sichern, und vergleichen Sie die Leistung der beiden Backups. In den meisten Fällen sind Backup Exec-Aufträge auf Festplatte schneller als auf Band.

Erforderliche Benutzerrechte für Backup-Aufträge

Um Backup-Vorgänge durchzuführen, sind die folgenden Windows-Benutzerrechte für das Dienstkonto und Backup Exec-Login-Konten erforderlich:

- Fungieren als Teil des Betriebssystems.
- Sichern von Dateien und Verzeichnissen.
- Wiederherstellen von Dateien und Verzeichnissen.
- Verwalten von Überwachungs- und Sicherheitsprotokoll.
- Login als Chargenjob (nur für Windows Vista und höher).

Weitere Informationen zu Benutzerrechte für Windows-Betriebssysteme finden Sie in Ihrer Microsoft-Dokumentation.

Siehe ["Ändern der Identifikationsdaten für ein Dienstkonto"](#) auf Seite 777.

Siehe ["Backup Exec-Login-Konten"](#) auf Seite 762.

Serverliste auf der Registerkarte "Backup und Wiederherstellung"

Sie können eine Liste von Servern auf der Registerkarte "Backup und Wiederherstellung" anzeigen. Die Liste enthält Server, die von Backup Exec während eines Upgrade erkannt wurden, Server, die Sie manuell hinzufügen und solche, die Backup Exec während einer Katalogisierung erkennt. Server müssen der Liste hinzugefügt sein, damit Sie sie für Backup-Aufträge auswählen können.

Sie können auch die Serveraktivität und den Auftragsstatus von der Serverliste aus überwachen. Standardmäßig zeigt Backup Exec die Warnmeldungen eines Servers, Backup-Status und einen Kalender der letzten sieben Tage von Backup-Aufträgen an. Es werden außerdem Datum und Uhrzeit der vorherigen und anstehenden geplanten Backups angezeigt. Sie können die Spalten dieser Liste anpassen, um zusätzliche Informationen anzuzeigen.

Sie können die folgenden Details auswählen, die Sie zu jedem Server in der Liste anzeigen möchten:

- Server
- Servertyp
- Version des Servers
- Backup Exec-Version
- Datenquellentypen
- Backup-Auswahlen
- Aktive Warnmeldungen
- Status
- "Letzte 7 Tage" für Backup-Aufträge
- Letztes Backup
- Nächstes Backup
- Prozent abgeschlossen
- Verstrichene Zeit
- Byte-Anzahl
- Durchschnittliche Auftragsrate

- Beschreibung

Auf Windows-Servern muss Agent for Windows installiert sein, bevor Sie sie der Liste von Servern hinzufügen können. Wenn Sie Windows-Server zu Backup Exec hinzufügen, haben Sie die Möglichkeit, Agent for Windows standortfern auf ihnen zu installieren.

Wenn Sie einen Server nicht mehr mit Backup Exec überwachen oder sichern möchten, können Sie ihn aus der Serverliste löschen.

Siehe ["Hinzufügen von zu sichernden Servern zur Serverliste auf der Registerkarte "Backup und Wiederherstellung""](#) auf Seite 167.

Siehe ["Entfernen eines Servers aus der Serverliste auf der Registerkarte "Backup und Wiederherstellung""](#) auf Seite 168.

Hinzufügen von zu sichernden Servern zur Serverliste auf der Registerkarte "Backup und Wiederherstellung"

Bevor Sie eine Backup-Definition erstellen können, müssen Sie die zu schützenden Server auswählen, die Sie der Serverliste auf der Registerkarte "Backup und Wiederherstellung" hinzufügen möchten. Sie können Server während der Push-Installation hinzufügen, oder Sie können folgendes Verfahren durchführen, um Server zu einem beliebigen Zeitpunkt hinzuzufügen.

So fügen Sie der Serverliste Server hinzu

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" unter "Server und virtuelle Hosts" auf "Hinzufügen".
- 2 Führen Sie diese Schritte aus, um der Serverliste einen oder mehrere Server hinzuzufügen.

Hinweis: Wenn Backup Exec unter Verwendung der Option "Daten für das Backup erkennen" Server gefunden hat, werden sie im Dialogfeld "Durchsuchen" unter der Überschrift "Server ohne Agent for Windows" angezeigt.

Siehe ["Hinzufügen gefundener Server zur Liste von Servern in Backup Exec"](#) auf Seite 710.

Siehe ["Serverliste auf der Registerkarte "Backup und Wiederherstellung""](#) auf Seite 166.

Entfernen eines Servers aus der Serverliste auf der Registerkarte "Backup und Wiederherstellung"

Wenn Sie einen Server nicht mehr mit Backup Exec überwachen oder sichern möchten, können Sie ihn aus der Serverliste löschen. Sie können Daten von Servern nicht mehr sichern oder wiederherstellen, nachdem Sie sie aus der Liste von Servern löschen.

Hinweis: Wenn Sie einen Server aus der Liste entfernen, auf dem geplante Aufträge ausstehen, werden diese gelöscht. Die Aufträge werden nicht wie geplant ausgeführt. Entfernen Sie einen Server nicht aus der Serverliste, wenn Sie diesen Server noch sichern möchten.

Sie sollten diesen Vorgang nicht verwenden, um einen verwalteten Backup Exec-Server aus einer CAS-Umgebung zu löschen. Sie sollten verwaltete Backup Exec-Server unter Verwendung der Registerkarte "Speicher" löschen.

Siehe ["Entfernen eines verwalteten Backup Exec-Server aus einem Backup Exec-Server-Pool"](#) auf Seite 1501.

So entfernen Sie Server aus der Liste von Servern

- 1 Klicken Sie auf der Registerkarte Backup und Wiederherstellung mit der rechten Maustaste auf den Server den Sie aus der Serverliste löschen möchten.
- 2 Klicken Sie auf Entfernen.
- 3 Klicken Sie auf Ja, um zu bestätigen, dass die den Server wirklich von der Serverliste löschen möchten.

Siehe ["Serverliste auf der Registerkarte "Backup und Wiederherstellung"](#) auf Seite 166.

Erstellen einer Servergruppe

Servergruppen sind eine Möglichkeit, Serverinformationen in der Liste von Servern zu organisieren und anzuzeigen. Sie können Servergruppen anhand beliebiger Kriterien erstellen. Es könnte sich z. B. anbieten, Server mit einem bestimmten Typ von Daten oder Server an einem bestimmten Standort in einer Gruppe zusammenzufassen. Wenn Sie dann Servergruppen anzeigen, werden nur die ausgewählten Servergruppen in der Liste der Servern auf der Registerkarte "Backup und Wiederherstellung" angezeigt. Durch das Anzeigen von Servergruppen können

Sie schnell den Status aller Server in der Gruppe auf einen Blick überwachen. Sie können auch eine gesamte Servergruppe sichern.

Siehe ["Sichern von Daten"](#) auf Seite 174.

Backup Exec verfügt über zwei vorkonfigurierte Servergruppen. Die Servergruppe "Alle Server" enthält alle Server. Die Gruppe "Ausrangierte Server" ist für Server gedacht, die Sie nicht mehr mit Backup Exec überwachen. Server werden nicht mehr in der Gruppe "Alle Server" angezeigt, wenn Sie sie in die Gruppe "Ausrangierte Server" verschieben.

So erstellen Sie eine Servergruppe

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" unter "Ansichten" auf "Gruppen".
- 2 Klicken Sie auf "Hinzufügen".
- 3 Geben Sie im Feld "Gruppenname" einen Namen für die Servergruppe ein. Sie sollten die Servergruppe z. B. nach dem Typ der Server in der Gruppe oder den Speicherort der Server benennen.
- 4 Im Feld "Beschreibung" geben Sie eine Beschreibung für die Servergruppe ein.
- 5 (Optional) Sie haben folgende Möglichkeiten, die die Server in Ihrer Umgebung zu filtern, um die hinzuzufügenden Server zu suchen:

So filtern Sie Server nach Typ	Wählen Sie im Feld "Sertyp" den zu suchenden Sertyp aus.
--------------------------------	--

So filtern Sie Server nach Datentyp	Wählen Sie im Feld "Datenertyp" die Daten aus, die sich auf dem zu suchenden Server befinden.
-------------------------------------	---

So filtern Sie Server nach Name	Geben Sie den Namen des Servers ganz oder teilweise im Feld "Name enthält" ein.
---------------------------------	---

- 6 Im Gruppenfeld "Server" wählen Sie die Server aus, die Sie der Servergruppe hinzufügen möchten und klicken Sie auf "OK".

Siehe ["Ein- bzw. Ausblenden von Servergruppen auf der Registerkarte "Backup und Wiederherstellung"](#) auf Seite 170.

Siehe ["Hinzufügen von Servern zu einer Servergruppe"](#) auf Seite 170.

Siehe ["Entfernen von Servern aus einer Servergruppe"](#) auf Seite 171.

Siehe ["Bearbeiten einer Servergruppe"](#) auf Seite 171.

Siehe ["Verschieben von Servern in die Gruppe "Ausrangierte Server"](#) auf Seite 172.

Siehe ["Entfernen von Servergruppen aus Backup Exec"](#) auf Seite 173.

Ein- bzw. Ausblenden von Servergruppen auf der Registerkarte "Backup und Wiederherstellung"

Sie zeigen Servergruppen im Teilfenster "Gruppen" an. Wenn Sie Backup Exec installieren, ist das Teilfenster "Gruppen" standardmäßig aktiviert. Wenn Sie keine Servergruppen verwenden, können Sie das Teilfenster "Gruppen" ausblenden. Doppelklicken Sie auf eine Servergruppe im Teilfenster "Gruppen", um ausführliche Information über die Aufträge der Servergruppe, den Auftragsverlauf und alle aktiven Warnmeldungen anzuzeigen.

So zeigen Sie Servergruppen auf der Registerkarte "Backup und Wiederherstellung" an

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" unter "Ansichten" auf "Gruppen".
 - 2 Aktivieren Sie die Option "Servergruppen anzeigen".
- Mithilfe der Option "Servergruppen anzeigen" können Sie das Teilfenster "Gruppen" links neben der Serverliste ein- bzw. ausblenden.

Siehe ["Erstellen einer Servergruppe"](#) auf Seite 168.

Hinzufügen von Servern zu einer Servergruppe

Sie können Server einer vorhandenen Servergruppe hinzufügen.

So fügen Sie der Servergruppe Server hinzu

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" im Teilfenster "Gruppen" mit der rechten Maustaste auf die Gruppe, der Sie einen Server hinzufügen möchten.
- 2 Wählen Sie "Bearbeiten".
- 3 Wählen Sie im Gruppenfeld "Server" die Server aus, die Sie der Servergruppe hinzufügen möchten.

Anhand der folgenden Felder können Sie die Liste der Server filtern, damit Sie den Server finden können, den Sie hinzufügen möchten.

- Servertyp
- Datentyp
- Name enthält

- 4 Klicken Sie auf "OK".

Siehe ["Erstellen einer Servergruppe"](#) auf Seite 168.

Entfernen von Servern aus einer Servergruppe

Sie können Server aus einer vorhandenen Servergruppe entfernen.

So entfernen Sie Server aus einer Servergruppe

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" im Teilfenster "Gruppen" mit der rechten Maustaste auf die Gruppe, aus der Sie einen Server entfernen möchten.
- 2 Wählen Sie "Bearbeiten".
- 3 Heben Sie im Gruppenfeld "Server" die Auswahl der Server auf, die Sie aus der Servergruppe entfernen möchten.

Anhand der folgenden Felder können Sie die Liste der Server filtern, damit Sie den Server finden können, den Sie entfernen möchten.

- Servertyp
- Datentyp
- Name enthält

- 4 Klicken Sie auf "OK".

Siehe ["Erstellen einer Servergruppe"](#) auf Seite 168.

Bearbeiten einer Servergruppe

Sie können eine vorhandene Servergruppe bearbeiten, indem Sie den Namen oder die Beschreibung der Gruppe ändern.

So bearbeiten Sie eine Servergruppe

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" unter "Gruppen" mit der rechten Maustaste auf die Gruppe, die Sie bearbeiten möchten.
- 2 Wählen Sie "Bearbeiten".
- 3 Sie haben folgende Möglichkeiten:

So ändern Sie den Namen der Servergruppe

Geben Sie im Feld "Gruppenname" den neuen Namen für die Servergruppe ein.

So ändern Sie die Beschreibung der Servergruppe

Im Feld "Beschreibung" geben Sie die neue Beschreibung für die Servergruppe ein.

- 4 Klicken Sie auf "OK".

Siehe ["Erstellen einer Servergruppe"](#) auf Seite 168.

Verschieben von Servern in die Gruppe "Ausrangierte Server"

Sie können auch Server von Backup Exec ausrangieren, indem Sie sie in die Gruppe "Ausrangierte Server" verschieben. Die Gruppe "Ausrangierte Server" ist für Server gedacht, die Sie nicht mehr mit Backup Exec überwachen. Sie können alle Informationen über ausrangierte Server auf der Registerkarte "Backup und Wiederherstellung" ansehen, indem Sie auf die Gruppe "Ausrangierte Server" klicken. Ausrangierte Server werden jedoch nicht mehr in der Gruppe "Alle Server" angezeigt, gemeinsam mit den Servern, die Sie regelmäßig sichern und überwachen. Es ist möglicherweise nützlich, Server auszurangieren, wenn Sie Backup Exec benutzen, um viele Server zu überwachen.

Sie können keine neuen Backup-Aufträge für Server erstellen, die sich in der Gruppe "Ausrangierte Server" befinden. Jedoch werden alle geplanten Backup-Aufträge noch auf ausrangierten Servern ausgeführt. Sie können Daten von ausrangierten Servern wiederherstellen.

Wenn Sie einen ausrangierten Server später wieder in die Gruppe "Alle Server" verschieben möchten, können Sie auf den entsprechenden Server klicken und ihn aus der Gruppe "Ausrangierte Server" in die Gruppe "Alle Server" verschieben.

So rangieren Sie Server aus den Servergruppen aus

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" unter "Gruppen" mit der rechten Maustaste auf "Ausrangierte Server".
- 2 Klicken Sie auf "Bearbeiten".
- 3 (Optional) Sie haben folgende Möglichkeiten, die die Server in Ihrer Umgebung zu filtern, um die auszurangierenden Server zu suchen:

So filtern Sie Server nach Typ	Wählen Sie im Feld "Servertyp" den zu suchenden Servertyp aus.
--------------------------------	--

So filtern Sie Server nach Datentyp	Wählen Sie im Feld "Datenertyp" die Daten aus, die sich auf dem zu suchenden Server befinden.
-------------------------------------	---

So filtern Sie Server nach Name	Geben Sie den Namen des Servers ganz oder teilweise im Feld "Name enthält" ein.
---------------------------------	---

- 4 Wählen Sie im Gruppenfeld "Server" die Server aus, die Sie ausrangieren möchten, und klicken Sie dann auf "OK".

Siehe ["Erstellen einer Servergruppe"](#) auf Seite 168.

Verschieben von ausrangierten Servern in die Gruppe "Alle Server"

Sie können auch Server von Backup Exec ausrangieren, indem Sie sie in die Gruppe "Ausrangierte Server" verschieben. Die Gruppe "Ausrangierte Server" ist für Server gedacht, die Sie nicht mehr mit Backup Exec überwachen.

Siehe ["Verschieben von Servern in die Gruppe "Ausrangierte Server" auf Seite 172.](#)

Soll ein ausrangierter Server wieder überwacht werden, können Sie ihn erneut aktivieren. Verschieben Sie ihn dazu aus der Gruppe "Ausrangierte Server" in die Gruppe "Alle Server".

So aktivieren Sie ausrangierte Server erneut

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" unter "Gruppen" auf "Ausrangierte Server".
- 2 Wählen Sie im Teilfenster "Server" den gewünschten Server aus.
- 3 Ziehen Sie den Server in das Teilfenster "Gruppen" und die Gruppe "Alle Server".

Siehe ["Erstellen einer Servergruppe"](#) auf Seite 168.

Entfernen von Servergruppen aus Backup Exec

Wenn Sie eine Servergruppe nicht mehr verwenden möchten, können Sie sie aus Backup Exec entfernen. Das Löschen einer Servergruppe wirkt sich nicht auf die Server in der Gruppe aus. Es entfernt nur die Zuordnung zwischen den Servern und Ihrer Fähigkeit, diese in der Gruppe zu erkennen. Sie können Server nach wie vor sichern und überwachen, nachdem Sie die Servergruppe entfernt haben, zu der sie gehören. Sie können weder die Servergruppe "Alle Server" noch die Servergruppe "Ausrangierte Server" entfernen.

So entfernen Sie Servergruppen

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" unter "Gruppen" mit der rechten Maustaste auf die Servergruppe, die Sie löschen möchten.
- 2 Klicken Sie auf "Entfernen".
- 3 Bestätigen Sie, dass Sie die Servergruppe entfernen möchten.

Siehe ["Erstellen einer Servergruppe"](#) auf Seite 168.

Sichern von Daten

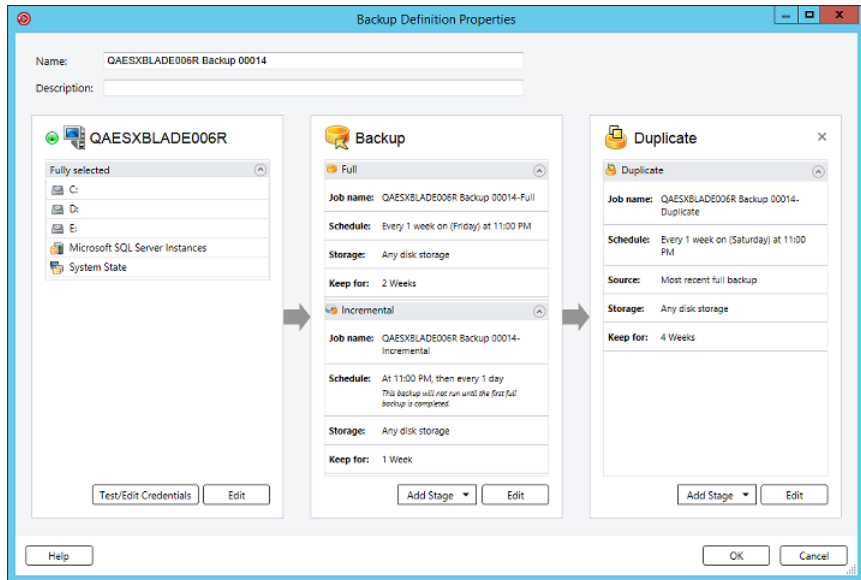
Wenn Sie Daten sichern möchten, erstellen Sie einen Container, der "Backup-Definition" genannt wird.

Backup-Definitionen enthält die Backup-Auswahl, Auftragsvorlagen und Stufen.

Tabelle 4-1 Backup-Definitionsinhalte

Element	Beschreibung
Backup-Auswahl	Die Backup-Auswahl enthält alle Server, Datenträger und Daten, die Sie zum Sichern ausgewählt haben.
Auftragsvorlagen	<p>Auftragsvorlagen sind die Sammlung von Einstellungen, die Backup Exec verwendet, um Aufträge zu erstellen. Die Einstellungen für Backup-Aufträge können beispielsweise Planungsoptionen, Optionen für Speichergeräte oder Backup-Methoden für ausgewählte Datentypen umfassen. Wenn Sie ein Backup ausführen möchten, kombiniert Backup Exec die Auftragsvorlage mit der Backup-Auswahl, um einen Backup-Auftrag zu erstellen, der dann entsprechend der von ihnen angegebenen Optionen ausgeführt wird.</p> <p>Backup-Definitionen enthalten immer eine Auftragsvorlage, die die vollständige Backup-Methode verwendet, aber wiederkehrende Aufträge können auch Auftragsvorlagen für inkrementelle, datenspezifische oder differenzielle Backups enthalten.</p> <p>Siehe "Backup-Methoden in Backup Exec" auf Seite 205.</p>
Stufen	Stufen sind optionale Aufgaben, die Sie mit Backup-Aufträgen ausführen können. Backup-Definitionen können eine oder mehrere Stufen enthalten. Sie können Stufen erstellen, die die Backup-Daten kopieren oder virtuelle Computer mit den Backup-Daten erstellen.

Abbildung 4-1 Backup-Definition (mit Backup-Auswahl, vollständigen und inkrementellen Auftragsvorlagen und einer duplizierten Stufe)



Backup Exec bietet Ihnen viele Möglichkeiten für das Erstellen von Backup-Aufträgen, um Ihre Daten zu schützen, u. a.:

- Erstellen Sie eine wiederkehrende Backup-Definition, um den vollen oder teilweisen Inhalt eines einzelnen Servers oder mehrerer Server zu sichern. Wenn Sie auswählen, Daten von mehreren Servern oder Anwendungen zu sichern, können Sie separate Backup-Definitionen für jeden Server oder jede Anwendung erstellen. Außerdem können Sie eine Backup-Definition erstellen, die alle Server und Anwendungen umfasst. Wenn Sie separate Backup-Definitionen erstellen, ist es einfacher, Probleme zu identifizieren, wenn Backup-Aufträge ausfallen. Auch wenn ein Problem mit einem Server entsteht, der ein Backup-Ausfall verursacht, können die anderen Backups noch erfolgreich abschließen. Wenn Sie Backup-Definition erstellen, die alle Server und Anwendungen umfasst, kostet es weniger Arbeit, den Status des Auftrags zu überwachen. Sie können eine Standardmethode für das Sichern von mehreren Servern im Dialogfeld "Backups" der Backup Exec-Einstellungen auswählen. Siehe ["Konfigurieren der Standardeinstellungen zum Sichern mehrerer Server oder Anwendungen"](#) auf Seite 693.

Hinweis: Sie können mehrere Server nicht mit einem synthetischen Backup-Auftrag oder einer Konvertierung zum virtuellen Auftrag sichern.

- Erstellen Sie einen Backup-Auftrag, sodass er nur einmal ausgeführt wird. Ein einmaliges Backup wird nur einmal ohne wiederkehrende Instanzen ausgeführt. Mithilfe eines einmaligen Backups können Sie z. B. den Grundzustand eines Servers festhalten, bevor Sie ein Upgrade durchführen oder neue Software installieren. Nachdem mit Backup Exec ein einmaliges Backup erstellt wurde, wird der Auftrag gelöscht und nicht zusammen mit den wiederkehrenden Aufträgen gespeichert. Informationen zu einem einmaligen Backup nach Abschluss des Auftrags können Sie im Auftragsverlauf anzeigen lassen.

Warnung: Data Lifecycle Management löscht alle abgelaufenen Backup-Sätze, die von einem einmaligen Backup-Auftrag erstellt wurden. DLM bewahrt den letzten Backup-Satz nicht mehr auf, nachdem der Aufbewahrungszeitraum abgelaufen ist, wenn der Backup-Satz aus einem einmaligen Backup stammt. Um zu verhindern, dass die Backup-Sätze automatisch gelöscht werden, können Sie spezifische Backup-Sätze manuell aufbewahren oder das Ablaufdatum ändern.

Siehe ["Löschen abgelaufener Backup-Sätze auf plattenbasiertem Speicher durch Data Lifecycle Management \(DLM\)"](#) auf Seite 393.

- Erstellen Sie eine neue Backup-Definition unter Verwendung von Einstellungen einer der vorhandenen Backup-Definition.
Wenn Sie eine Backup-Definition erstellen möchten, die einer vorhandenen Backup-Definition ähnlich ist, können Sie die Einstellungen der vorhandenen Definition in eine neue Definition übernehmen. Backup-Methoden, Auftragseinstellungen und Stufen werden in eine neue Backup-Definition für den oder die für das Backup ausgewählten Server kopiert. Sie müssen lediglich die Backup-Auswahl festlegen. Sie können bei Bedarf jede beliebige Auftragseinstellung ändern.
- Erstellen Sie eine Servergruppe aus ähnlichen Computern und sichern Sie die gesamte Gruppe auf einmal.
Servergruppen sind eine Möglichkeit, Serverinformationen in der Liste von Servern zu organisieren und anzuzeigen. Sie können Servergruppen anhand beliebiger Kriterien erstellen. Es könnte sich z. B. anbieten, Server mit einem bestimmten Typ von Daten oder Server an einem bestimmten Standort in einer Gruppe zusammenzufassen.

Sie können vorhandene Backup-Definitionen auch bearbeiten, um ihre Zeitpläne, die Backup-Auswahl oder andere Einstellungen zu ändern.

Um Remote-Computer zu schützen, müssen Sie den Agent for Windows auf dem Remote-Computer installieren. Der Agent for Windows ist ein Systemdienst, der

auf Windows-Servern und -Arbeitsstationen ausgeführt wird. Er ermöglicht ein effizientes Backup, da Aufgaben, die bei anderen Backup-Technologien intensive Netzwerkinteraktionen erfordern, hier lokal vorgenommen werden.

Informationen zu den Best Practices zum Einsatz von Backup-Aufträgen finden Sie unter *Best Practices für Backup Exec*.

Siehe ["Methoden für die Installation von Agent for Windows"](#) auf Seite 77.

So sichern Sie Daten

1 Wählen Sie eine der folgenden Methoden aus, um Daten zu sichern:

So erstellen Sie wiederkehrende Backup-Aufträge

Führen Sie die folgenden Schritte durch:

- Wählen Sie auf der Registerkarte "Backup und Wiederherstellung" den oder die zu sichernden Server oder die Servergruppe.
- Klicken Sie mit der rechten Maustaste auf den/die Server oder die Servergruppe.
- Wählen Sie im Menü "Backup" die Backup-Option, die Sie verwenden möchten.

So erstellen Sie ein einmaliges Backup

Führen Sie die folgenden Schritte durch:

- Wählen Sie auf der Registerkarte "Backup und Wiederherstellung" den oder die zu sichernden Server oder die Servergruppe.
- Klicken Sie in der Gruppe "Backup" auf "Einmaliges Backup".
- Wählen Sie die Backup-Option aus, die Sie verwenden möchten.

So erstellen Sie eine neue Backup-Definition unter Verwendung der Einstellungen von einer vorhandenen Backup-Definition

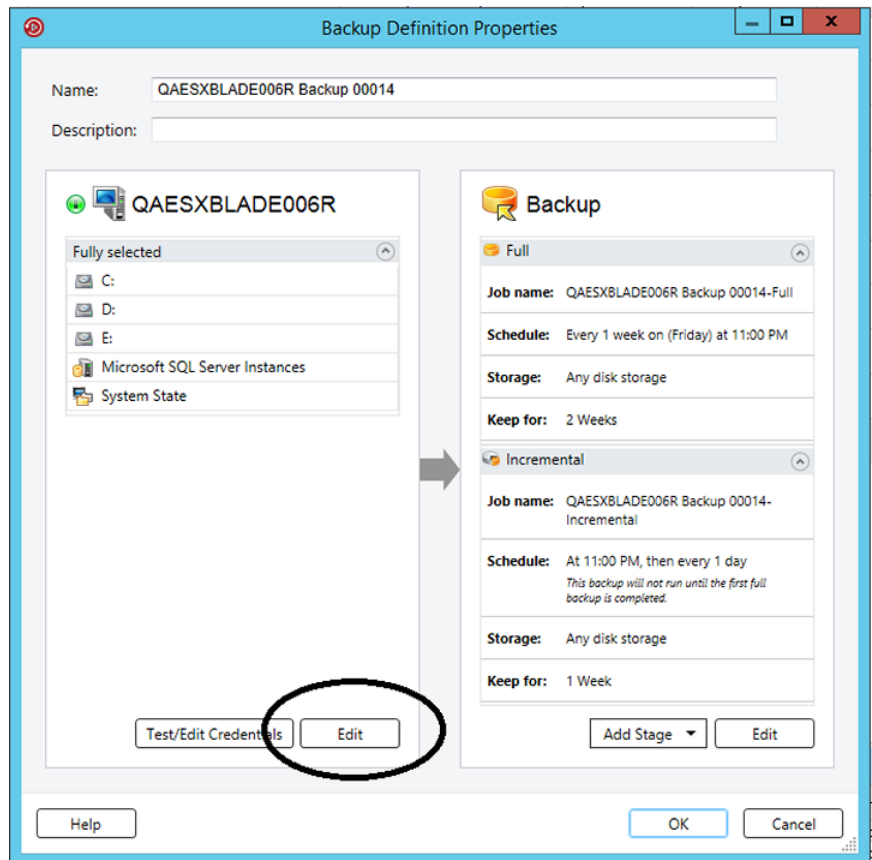
Führen Sie die folgenden Schritte durch:

- Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" mit der rechten Maustaste auf den oder die zu sichernden Server.
Sie können die Einstellungen einer Backup-Definition nicht wiederverwenden, um einen Backup-Auftrag für eine Servergruppe zu erstellen.
- Wählen Sie im Menü "Backup" die Option "Neues Backup mit den Einstellungen eines vorhandenen Backups erstellen".
- Wählen Sie im Dialogfeld "Backup-Auftrag-Auswahl" die Backup-Definition aus, die die Einstellungen enthält, die Sie kopieren möchten.
- Klicken Sie auf "OK".

So erstellen Sie eine Backup-Definition für eine Servergruppe

Führen Sie die folgenden Schritte durch:

- Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" unter "Gruppen" mit der rechten Maustaste auf die Servergruppe, die Sie sichern möchten.
 - Wählen Sie im Menü "Backup" die Backup-Option, die Sie verwenden möchten.
- 2 Geben Sie im Feld "Name" einen Namen für die Backup-Definition ein.
 - 3 Geben Sie im Feld "Beschreibung" eine Beschreibung für die Backup-Definition ein.
 - 4 Klicken Sie im Dialogfeld "Auswahl" auf "Bearbeiten".



- 5 So fügen Sie der Backup-Definition zusätzliche Server hinzu
 - Klicken Sie auf "Hinzufügen".
 - Wählen Sie den Server oder die Server aus, die Sie der Backup-Definition hinzufügen möchten.
 - Klicken Sie auf "OK".

- 6 Wählen Sie die Daten aus, die Sie sichern möchten.

Server werden standardmäßig in ihrer Gesamtheit ausgewählt. Wenn Sie nicht den gesamten Server sichern möchten, doppelklicken Sie auf den Servernamen, um den gesamten Inhalt anzuzeigen. Wählen Sie die Kontrollkästchen für jedes Element aus, das Sie sichern möchten.

Hinweis: Das Aufheben der Auswahl für die kritischen Systemkomponenten eines Servers führt zu der Erstellung von Backup-Sätzen, die für einige Wiederherstellungsszenarien nicht verwendet werden können.

Siehe ["Info zum Sichern von wichtigen Systemkomponenten"](#) auf Seite 200.

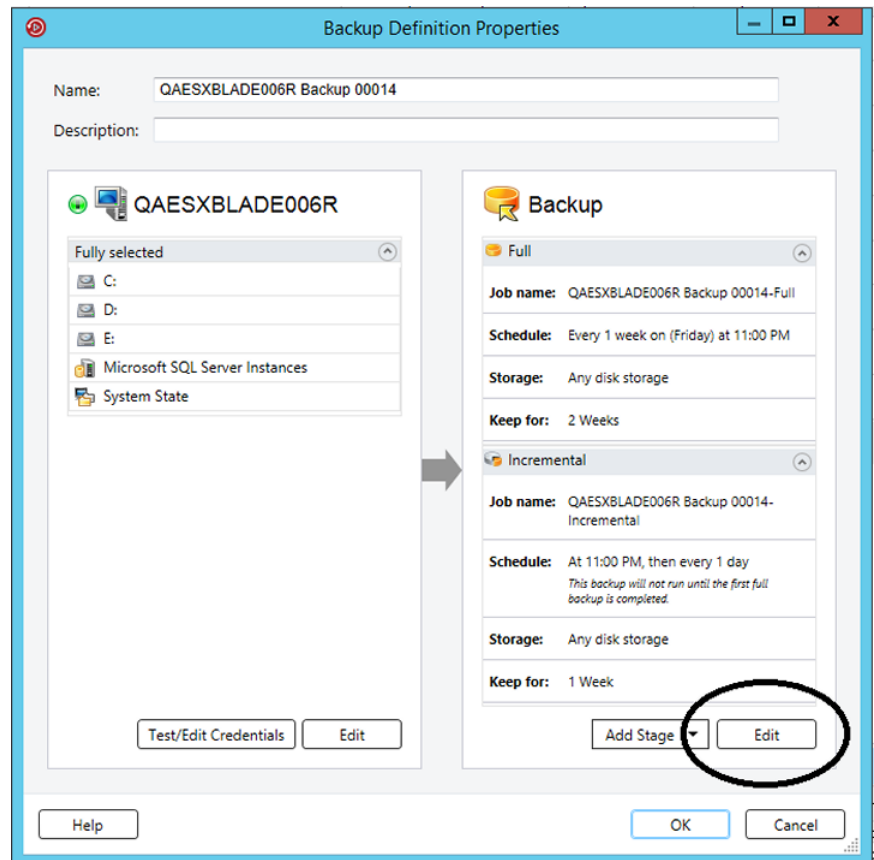
- 7 Um die Sicherung bestimmter Datenträger oder virtueller Rechner vorzuziehen, wählen Sie das gewünschte Element und klicken Sie auf "Als geschäftskritisch kennzeichnen".

Siehe ["Info zum Auswählen von zu sichernden Daten"](#) auf Seite 186.

- 8 Klicken Sie auf "OK".

- 9 Klicken Sie im Dialogfeld "Backup" auf "Bearbeiten".

Hinweis: Wenn Sie die Backup-Einstellungen von einer vorhandenen Backup-Definition kopiert haben, oder wenn Sie die bestehenden oder die Standardeinstellungen nicht ändern möchten, können Sie mit Schritt 13 fortfahren.



- 10 Klicken Sie im linken Teilfenster auf "Planen" und wählen Sie dann aus, wann Sie den Backup-Auftrag oder die Aufträge ausführen möchten.
- 11 Klicken Sie im linken Teilfenster auf "Speicher" und wählen Sie dann das Speichergerät aus, das Sie für den Backup-Auftrag oder die Aufträge verwenden möchten.

- 12** Wählen Sie im linken Teilfenster alle Zusatzfunktionen aus, die auf den Backup-Auftrag oder die Aufträge angewendet werden sollen.

Alle restlichen Optionen im linken Teilfenster sind optional. Die Optionen variieren abhängig davon, was Sie zum Sichern ausgewählt haben.

Beispielsweise können Sie Benachrichtigungen einrichten, damit Benutzer E-Mails oder SMS bezüglich dieser Backup-Definition erhalten können.

Netzwerk	<p>Wählen Sie diese Option aus, um die Netzwerkschnittstelle festzulegen, über die Backup Exec auf standortferne Computer zugreift.</p> <p>Siehe "Konfigurieren erweiterter Optionen für Backup-Aufträge" auf Seite 223.</p>
Benachrichtigung	<p>Wählen Sie diese Option aus, um die Konfiguration von Backup Exec zur Benachrichtigung bestimmter Empfänger nach Abschluss des Backup-Auftrags zu ermöglichen.</p> <p>Für jeden Backup-Auftrag und jede Phase können verschiedene Benachrichtigungsempfänger konfiguriert werden. Backup Exec kann Empfänger per E-Mail oder SMS benachrichtigen.</p> <p>Siehe "Benachrichtigungsoptionen für Aufträge" auf Seite 357.</p>
Probelauf	<p>Wählen Sie diese Option aus, um einen Testauftrag zu konfigurieren, der automatisch Speicherkapazität, Identifikationsdaten und Medienintegrität prüft.</p> <p>Der Testauftrag hilft Ihnen beim Feststellen von Problemen, die den Backup-Auftrag möglicherweise davon abhalten, den Auftrag erfolgreich abzuschließen.</p> <p>Siehe "Konfigurieren automatischer Testlaufaufträge für Backup-Aufträge" auf Seite 653.</p>
Überprüfen	<p>Wählen Sie diese Option aus, um einen Auftrag zu erstellen, der nach Abschluss des Auftrags automatisch überprüft, ob alle Daten erfolgreich gesichert wurden.</p> <p>Ein Überprüfungsauftrag unterstützt Sie beim Festlegen, ob die verwendeten Medien defekt sind.</p> <p>Siehe "Konfigurieren der automatischen Prüfung von Aufträgen" auf Seite 655.</p>

Instant GRT	<p>Wählen Sie diese Option aus, um den Vorgang Instant GRT oder Vollständige Katalogisierung für einen GRT-fähigen Auftrag zu konfigurieren. Sie können die vollständige Katalogisierung sofort nach Abschluss des Backup-Auftrags ausführen, für einen späteren Zeitpunkt planen oder im Rahmen des Backup-Auftrags ein Instant GRT durchführen.</p> <p>Siehe "Konfigurieren der Optionen für Instant GRT und Vollständige Katalogisierung zum Verbessern der Backup-Leistung von GRT-Aufträgen" auf Seite 656.</p>
Advanced Open File	<p>Wählen Sie diese Option aus, um die Snapshot-Einstellungen zu konfigurieren, die Backup Exec zum Durchführen eines Backup-Auftrags anwendet. Mit der Snapshot-Technologie kann Backup Exec alle Dateien erfassen, die geöffnet sind, wenn ein Backup ausgeführt wird.</p> <p>Sie können auch die Auftragswiederaufnahme aktivieren, mit der Sie unterbrochene Backup-Aufträge fortsetzen können.</p> <p>Siehe "Konfigurieren von Advanced Open File-Optionen für Backup-Aufträge" auf Seite 664.</p> <p>Siehe "Konfigurieren der Auftragswiederaufnahme" auf Seite 667.</p>
Advanced Disk-based Backup	<p>Wählen Sie diese Option aus, um die eine Off-Host-Backup-Verarbeitung für den Backup-Auftrag zu konfigurieren.</p> <p>Siehe "Konfigurieren von Offhost-Backup-Optionen für einen Backup-Auftrag" auf Seite 1530.</p>
Befehle vor/nach dem Auftrag	<p>Wählen Sie diese Option aus, um Befehle zu konfigurieren, die vor dem Beginn oder nach dem Abschluss von Backup-Aufträgen ausgeführt werden sollen.</p> <p>Siehe "Konfigurieren von Befehlen vor oder nach Backup-Aufträgen" auf Seite 670.</p>
Dateien und Ordner	<p>Wählen Sie diese Option aus, um die Verarbeitung von Dateisystemattributen, wie zum Beispiel von Abzweigungen und symbolischen Links, zu konfigurieren.</p> <p>Siehe "Konfigurieren von Datei- und Ordneroptionen für Backup-Aufträge" auf Seite 676.</p>

Enterprise Vault	<p>Wählen Sie diese Option aus, um Enterprise Vault-Optionen zu konfigurieren.</p> <p>Siehe "Backup-Optionen für Enterprise Vault" auf Seite 1397.</p>
Linux und Macintosh	<p>Hiermit konfigurieren Sie Optionen für Linux- oder Macintosh-Computer, die in den Backup-Auftrag integriert sind.</p> <p>Siehe "Linux-Backup-Optionen" auf Seite 1579.</p>
Microsoft Active Directory	<p>Wählen Sie diese Option aus, um Optionen für alle Microsoft Active Directory-Daten zu konfigurieren, die im Backup-Auftrag integriert sind.</p> <p>Siehe "Optionen für Backup-Aufträge von Microsoft Active Directory" auf Seite 1444.</p>
Microsoft Exchange	<p>Wählen Sie diese Option aus, um Optionen für alle Microsoft Exchange-Daten zu konfigurieren, die im Backup-Auftrag integriert sind.</p> <p>Siehe "Sichern von Exchange-Daten" auf Seite 1290.</p>
Virtuelle Computer	<p>Wählen Sie diese Option aus, um Optionen für alle virtuellen Computer zu konfigurieren, die im Backup-Auftrag integriert sind.</p> <p>Siehe "Sichern von virtuellen Computern mit Microsoft Hyper-V" auf Seite 1167.</p> <p>Siehe "Sichern von virtuellen VMware-Computern" auf Seite 1100.</p>
Microsoft SharePoint	<p>Wählen Sie diese Option aus, um Optionen für alle SharePoint-Daten zu konfigurieren, die im Backup-Auftrag integriert sind.</p> <p>Siehe "Sichern von Microsoft SharePoint-Daten" auf Seite 1322.</p>
Microsoft SQL	<p>Wählen Sie diese Option aus, um Optionen für alle SQL-Daten zu konfigurieren, die im Backup-Auftrag integriert sind.</p> <p>Siehe "Sichern von SQL-Datenbanken und Transaktionsprotokollen" auf Seite 1228.</p>

NDMP	<p>Wählen Sie diese Option aus, um Optionen für alle NDMP-Daten zu konfigurieren, die im Backup-Auftrag integriert sind.</p> <p>Siehe "NDMP-Backup-Optionen für NDMP-Server" auf Seite 1543.</p>
Oracle	<p>Wählen Sie diese Option aus, um Optionen für alle Oracle-Daten zu konfigurieren, die im Backup-Auftrag integriert sind.</p> <p>Siehe "Backup-Optionen für Oracle" auf Seite 1367.</p>
Ausschlüsse	<p>Wählen Sie diese Option aus, um bestimmte Dateien oder bestimmte Dateitypen aus Backups ein- oder auszuschließen.</p> <p>Siehe "Ausschließen von Dateien von Backups" auf Seite 195.</p>

- 13** Wenn Sie mit der Konfiguration der Backup-Definition fertig sind, klicken Sie auf "OK".
- 14** (Optional) Sie können dieser Backup-Definition Stufen hinzufügen, um die Daten zu kopieren oder virtuelle Computer mit den Backup-Daten zu erstellen.

Hinweis: Sie können einem einmaligen Backup keine Stufe hinzufügen.

Siehe ["Hinzufügen einer Stufe zu einer Backup-Definition"](#) auf Seite 244.

- 15** Klicken Sie auf "OK", um die Einstellungen der Backup-Definition zu speichern.

Die Backup-Aufträge und Stufen werden zur ausgewählten Zeit ausgeführt.

Siehe ["Erstellen einer Servergruppe"](#) auf Seite 168.

Siehe ["Bearbeiten von Backup-Definitionen"](#) auf Seite 226.

Siehe ["Info zum Auswählen von zu sichernden Daten"](#) auf Seite 186.

Siehe ["Ändern der Reihenfolge, in der Backup-Quellen gesichert werden"](#) auf Seite 192.

Infos zum Sichern von Datenträgern, für die unter Windows die Deduplizierung aktiviert ist

In Windows Server 2012 wurde die native Dateisystemdeduplizierung eingeführt. Wenn ein Windows-Datenträger Daten dedupliziert, gelten die deduplizierten Daten

als optimiert. Daten im ursprünglichen, nicht deduplizierten Format gelten als nicht optimiert.

Backup Exec unterstützt das Sichern von Datenträgern, auf denen die Windows-Deduplizierung aktiviert ist. Wenn Sie optimierte Daten sichern, sichert Backup Exec sie im ursprünglichen, nicht optimierten Format. Stellen Sie sicher, dass Sie genügend Speicherplatz haben, um die nicht-optimierten Daten auf dem Backup-Ziel zu sichern, bevor Sie den Backup-Auftrag ausführen. Die optimierten Dateien werden nicht auf der Backup-Quelle selbst bearbeitet.

Wenn Sie die gesicherten Daten wiederherstellen, stellt Backup Exec die Dateien als nicht-optimiert wieder her. Stellen Sie sicher, dass Sie genügend Speicherplatz haben, um die nicht-optimierten Daten wiederherzustellen. Sie freien Speicherplatz auf dem Datenträger schaffen, auf dem Sie die Dateien wiederherstellen möchten. Führen Sie den Windows Garbage Collector aus, um den Speicherplatz auf dem Datenträger zu optimieren, bevor Sie die Wiederherstellung vornehmen.

Sichern und Wiederherstellen von Dateien der virtuellen Festplatte (VHD) von Microsoft in Backup Exec

Microsoft Windows 2008 R2 ermöglicht es Benutzern, native VHD-Dateien zu erstellen. Eine VHD-Datei ist eine virtuelle Festplatte, die in einer einzelnen Datei enthalten ist. Weitere Informationen zu VHD-Dateien finden Sie in der Windows-Dokumentation.

Mit Backup Exec können Sie native VHD-Dateien sichern und wiederherstellen. Ist eine native VHD-Datei nicht bereitgestellt, können Sie sie zusammen mit dem Datenträger, auf dem sich befindet, sichern und wiederherstellen.

Ist eine native VHD-Datei mit einem Laufwerksbuchstaben oder einem leeren Ordnerpfad bereitgestellt, wird die Datei beim Sichern übersprungen. Bereitgestellte VHD-Dateien können nicht in eine Backup-Auswahl aufgenommen werden. Wählen Sie zum Sichern der Daten in einer bereitgestellten VHD-Datei den dazugehörigen Bereitstellungspunkt in der Backup-Auswahl aus.

Siehe "[Sichern von Daten](#)" auf Seite 174.

Sie können auch einen Wiederherstellungsauftrag auf eine native VHD umleiten, wenn Sie Windows Server 2008 R2 oder höher verwenden. Wenn Sie einen Wiederherstellungsauftrag auf eine native VHD umleiten, erstellt Backup Exec eine VHD-Datei, die dynamisch wächst, sobald Sie Daten in ihr speichern. Die Datei wächst, bis sie eine Größe von 2040 GB erreicht. Dies ist die maximale Größe für eine native VHD-Datei. Sie können eine VHD-Datei mit Daten aus allen umgeleiteten Backup-Sätzen oder für jeden Backup-Satz eine separate VHD-Datei erstellen.

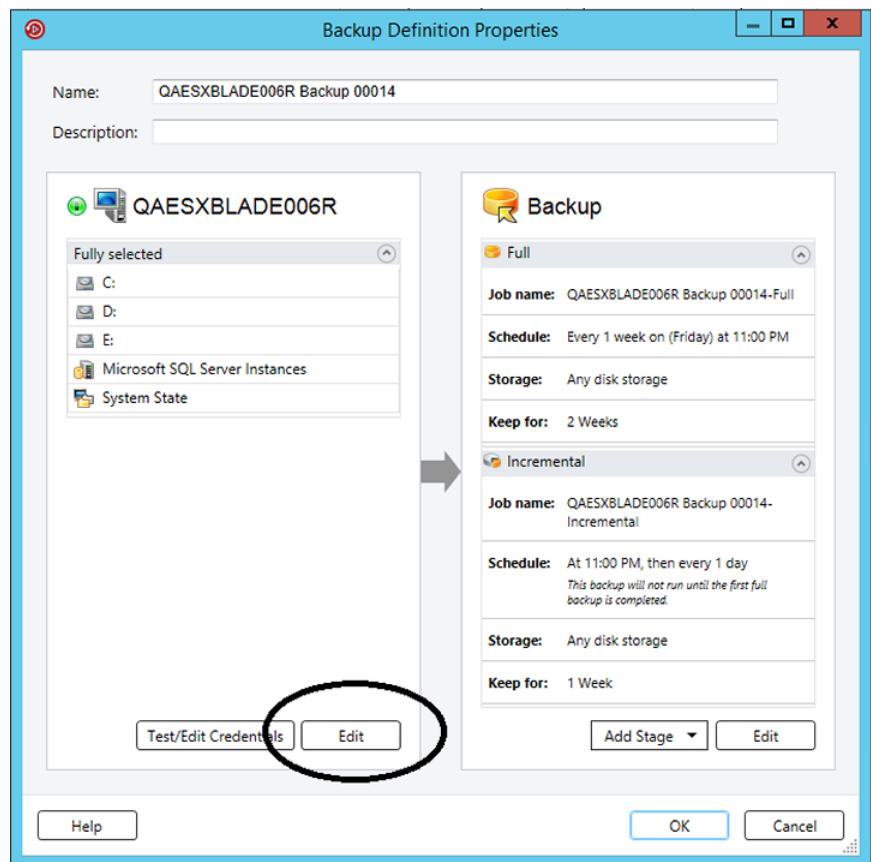
Backup Exec Agent for Hyper-V ist mit Microsoft-VHDX-Dateien kompatibel:

Siehe ["Hinweise zum Einsatz des Agent for Hyper-V"](#) auf Seite 1159.

Info zum Auswählen von zu sichernden Daten

Wenn Sie einen Server sichern, schließt Backup Exec standardmäßig alle Daten auf dem Server in die Backup-Auswahl ein. Wenn Sie die Backup-Auswahl ändern möchten, können Sie auf "Bearbeiten" im Feld "Auswahl" im Dialogfeld "Eigenschaften der Backup-Definition" klicken.

Abbildung 4-2 Auswahlfelder im Dialogfeld "Eigenschaften der Backup-Definition"



Siehe ["Sichern von Daten"](#) auf Seite 174.

Anstatt alle Daten auf einem Server zu sichern, können Sie Laufwerke, Ordner, Dateien, Systemstatus, Netzwerkfreigaben oder Datenbanken auf der Registerkarte "Durchsuchen" auswählen.

Um die Ansicht für ein Element zu erweitern oder auszublenden, klicken Sie auf den Pfeil neben dem Element oder doppelklicken Sie auf den Namen des Elements. Um den Inhalt eines Elements anzuzeigen, doppelklicken Sie auf das Elementsymbol. Der Inhalt des Elements wird in dem Rahmen rechts in der Ansicht "Backup-Auswahl" angezeigt. Durch Klicken auf angezeigte Ordner und Unterordner in beiden Fensterbereichen können Sie verschiedene Dateiebenen aufrufen.

Windows Server bietet die Option an, Datenträger mit der BitLocker-Funktion zu verschlüsseln. Backup Exec unterstützt das Backup und die Wiederherstellung von Datenträgern, für die der BitLocker aktiviert ist. Dies erfolgt entweder durch das manuelle Entsperren der Zieldatenträger oder durch Verwenden der Auto-Unlock-Funktion von Microsoft. Weitere Informationen finden Sie in der Dokumentation von Microsoft

Wenn Sie die Remote-Auswahl durchsuchen, erfordert Backup Exec ein gültiges Login-Konto, um die Computerinhalte zu erweitern. Wenn das Standard-Login-Konto keinen Zugriff auf eine Remote-Auswahl ermöglicht, fordert Backup Exec Sie auf, ein anderes vorhandenes Login-Konto auszuwählen. Sie können auch ein neues Login-Konto erstellen, das auf die Auswahl zugreifen kann.

Siehe ["Prüfung der Identifikationsdaten für Backup-Quellen"](#) auf Seite 234.

Siehe ["Ersetzen der Identifikationsdaten für eine Backup-Quelle"](#) auf Seite 235.

Siehe ["Erstellen neuer Identifikationsdaten für eine Backup-Quelle"](#) auf Seite 236.

Um Daten im Backup einzuschließen, aktivieren Sie das Kontrollkästchen neben dem Laufwerk oder Verzeichnis, das Sie sichern möchten.

Dieses Thema enthält folgende Informationen:

[Ressourcen als geschäftskritisch kennzeichnen](#)

[Bestimmte Dateien oder Unterverzeichnisse ein- und ausschließen](#)

[Mehrere Server oder Anwendungen auswählen](#)

[Wichtige Systemkomponenten auswählen](#)

[Verwenden vollständig qualifizierter Domännennamen in der Backup-Auswahl](#)

Ressourcen als geschäftskritisch kennzeichnen

Mithilfe der Option "Als geschäftskritisch kennzeichnen" können Sie die für Sie wichtigsten Ressourcen auswählen. Backup Exec sichert die als geschäftskritisch gekennzeichneten Ressourcen im Backup-Fenster vor den nicht als geschäftskritisch gekennzeichneten Ressourcen. Wenn Sie eine Ressource als geschäftskritisch

kennzeichnen, werden die entsprechenden untergeordneten Ressourcen auch als geschäftskritisch gekennzeichnet. Wenn Sie ein Element als geschäftskritische Ressource kennzeichnen, ändert Backup Exec das entsprechende Symbol in der Backup-Satz-Ansicht und im Assistenten für Wiederherstellungsaufträge.

Die Option "Als geschäftskritisch kennzeichnen" steht für die folgenden Ressourcen zur Verfügung:

- Windows-Datenträger und UNIX-Stammvolumen
- Exchange-Datenbanken
- SQL-Instanzen
- Virtuelle Computer - Ordner
- Virtuelle Computer
- SharePoint-Ressourcen
- Oracle-Instanzen

Hinweis: Die Option "Als geschäftskritisch kennzeichnen" ist bei einer teilweisen Auswahl deaktiviert. Außerdem steht sie Enterprise Vault-Ressourcen wie Compliance Accelerator und Discovery Accelerator nicht zur Verfügung.

Die Kennzeichnung als geschäftskritische Ressource gilt nur für den jeweils vorliegenden Auftrag. Es ist keine globale Einstellung. Wenn Sie die Ressource eines Servers als geschäftskritisch kennzeichnen und noch weitere Ressourcen von demselben Server auswählen, wird die Backuppriorität für die geschäftskritische Ressource nur bei diesem Server in Bezug auf die anderen Ressourcen berechnet. Bei Aufträgen, die sich auf mehrere Server beziehen, werden geschäftskritische Ressourcen in absteigender Reihenfolge der Serverpriorität gesichert.

Auch kritische Systemressourcen können als geschäftskritisch gekennzeichnet werden. Wenn keine kritischen Systemressourcen ausgewählt werden, werden die als geschäftskritisch gekennzeichneten Ressourcen innerhalb desselben Backup-Auftrags vor den kritischen Systemressourcen gesichert. Das beste Vorgehensweise für kritische Systemressourcen ist jedoch die Durchführung eines separaten Backup-Auftrags. Hinweis: Wenn Sie geschäftskritische Ressourcen und kritische Systemressourcen in demselben Backup-Auftrag sichern, wird der Systemstatus immer als letztes gesichert, unabhängig davon, ob es sich um eine als geschäftskritisch gekennzeichnete Ressource handelt.

Nach der Kennzeichnung von Elementen als geschäftskritische Ressourcen können Sie die Backup-Reihenfolge mithilfe der Pfeilschaltflächen auf der Registerkarte "Auswahldetails" ändern. Eine nicht als geschäftskritisch gekennzeichnete Ressource kann jedoch nicht vor eine als geschäftskritisch gekennzeichnete verschoben werden. Beispiel: Wenn Sie Laufwerk C als geschäftskritische

Ressource kennzeichnen, Laufwerk E jedoch nicht, können Sie Laufwerk E nicht vor Laufwerk C verschieben.

Siehe ["Ändern der Reihenfolge, in der Backup-Quellen gesichert werden"](#) auf Seite 192.

Hinweis: Bei rollenden Upgrades wird die Kennzeichnung als geschäftskritisch erst dann auf an verwaltete Backup Exec-Server delegierte Aufträge angewendet, wenn für die verwalteten Server ein Upgrade auf die neueste Version von Backup Exec durchgeführt wird.

Bestimmte Dateien oder Unterverzeichnisse ein- und ausschließen

Auf der Registerkarte "Auswahldetails" können Sie Dateien für Backups ein- oder ausschließen, indem sie Dateiattribute angeben. Ausnahmen gelten für alle Aufträge in einer Backup-Definition.

Auf der Registerkarte "Auswahldetails" haben Sie folgende Möglichkeiten:

- Unterverzeichnisse mit einschließen oder ausschließen. Beispielsweise können Sie beschließen, einen übergeordneten Ordner zu sichern, ohne die Ordner zu sichern, die in diesem liegen.
- Nur geänderte Dateien mit einschließen. Beispielsweise können Sie nur die Dateien sichern, die sich seit dem letzten Backup-Auftrag geändert haben.
- Nur schreibgeschützte Dateien einschließen.
- Schließen Sie Dateien nach Dateinameattributen ein oder aus. Sie können z. B. nur Dateien mit der Erweiterung ".txt" auswählen oder Dateien mit der Erweiterung ".exe" vom Backup ausschließen. Wenn Sie Dateien anhand eines nicht existierenden Attributs ausschließen, werden alle Dateien des betreffenden Typs ausgeschlossen. Ausschlüsse basierend auf einem SQL-Datenbankdatum führen z. B. dazu, dass alle SQL-Elemente ausgeschlossen werden, da SQL-Datenbanken kein Datumsattribut aufweisen.
- Wählen Sie nur Dateien aus einem bestimmten Datumsbereich. Sie können z. B. alle Dateien auswählen, die im Dezember erstellt oder geändert wurden.
- Geben Sie die Dateien an, auf die in einer angegebenen Anzahl von Tagen nicht zugegriffen wurde. Beispielsweise können Sie die Dateien im Ordner "Eigene Dateien" auswählen, auf die seit 30 Tage nicht mehr zugegriffen wurde. Führen Sie dann ein vollständiges Backup aus, und wählen Sie die Methode zum Sichern und Löschen der Dateien aus.

Siehe ["Ausschließen von Dateien von Backups"](#) auf Seite 195.

Siehe ["Einschließen spezifischer Dateien mit der Backup-Auswahl eines Backup-Auftrags"](#) auf Seite 198.

Mehrere Server oder Anwendungen auswählen

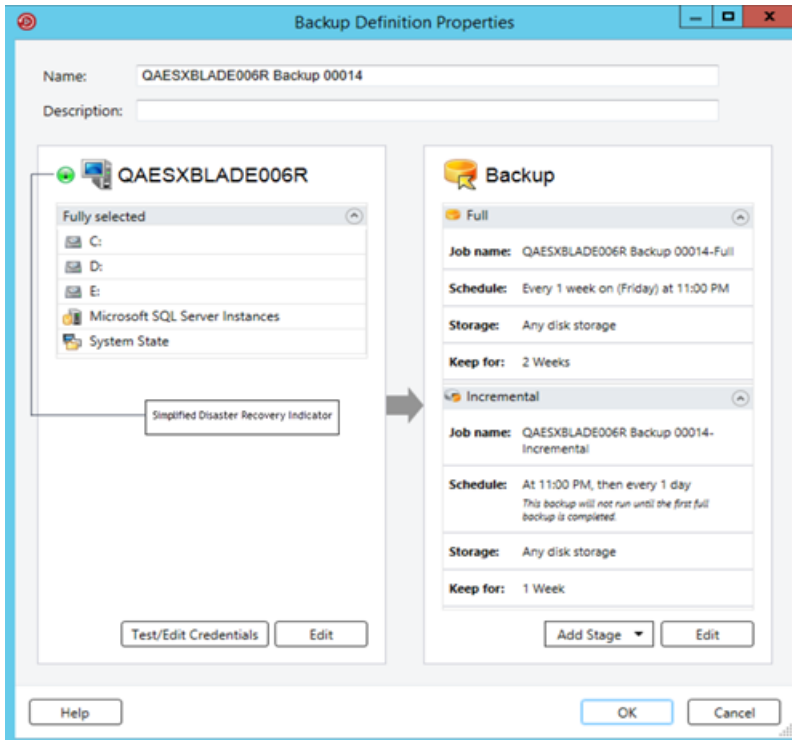
Wenn Sie auswählen, Daten von mehreren Servern oder Anwendungen zu sichern, können Sie separate Backup-Definitionen für jeden Server oder jede Anwendung erstellen. Außerdem können Sie eine Backup-Definition erstellen, die alle Server und Anwendungen umfasst. Wenn Sie separate Backup-Definitionen erstellen, ist es einfacher, Probleme zu identifizieren, wenn Backup-Aufträge ausfallen. Auch wenn ein Problem mit einem Server entsteht, der ein Backup-Ausfall verursacht, können die anderen Backups noch erfolgreich abschließen. Wenn Sie eine Backup-Definition erstellen, die alle Server und Anwendungen umfasst, ist es weniger arbeitsintensiv, den Status des Auftrags zu überwachen. Sie können eine Standard- Methode für das Sichern von mehreren Servern im Dialogfeld "Backups" der Backup Exec-Einstellungen auswählen.

Siehe ["Konfigurieren der Standardeinstellungen zum Sichern mehrerer Server oder Anwendungen"](#) auf Seite 693.

Wichtige Systemkomponenten auswählen

Wenn alle wichtigen Systemkomponenten in Ihren ausgewählten Backup-Aufträgen eingeschlossen sind, sehen Sie auf der "Simplified Disaster Recovery" -Anzeige im Auswahlteifenster die Meldung "EIN". Wenn Sie eine oder mehrere wichtige Systemkomponentendateien abwählen, sehen Sie auf der Anzeige die Meldung "AUS".

Abbildung 4-3 Im Dialogfeld "Eigenschaften der Backup-Definition" ist die Simplified Disaster Recovery aktiviert.



Siehe ["Info zum Sichern von wichtigen Systemkomponenten"](#) auf Seite 200.

Wenn Sie die Auswahl kritischer Systemkomponenten aufheben, kann dies dazu führen, dass Ihre Backup-Daten in bestimmten Wiederherstellungsszenarien nicht verwendet werden können.

Sie müssen alle wichtigen Systemkomponenten in die Backup-Auswahl einschließen, wenn Sie beabsichtigen, eines der folgenden Wiederherstellungsszenarien zu verwenden:

- Simplified Disaster Recovery
- Konvertierung in virtuelle Computer
- Vollständige Online-Wiederherstellung eines Windows-Computers

Verwenden vollständig qualifizierter Domänennamen in der Backup-Auswahl

Überall in Backup Exec, wo ein Computernamen eingegeben werden kann, können Sie auch den vollständig qualifizierten Domänennamen eingeben. Zudem kann Backup Exec beim Auflisten von Computernamen vollständig qualifizierte Domänennamen anzeigen.

Für voll qualifizierte Domänennamen gelten folgende Regeln:

- Die maximale Anzahl von Zeichen für jede Bezeichnung (der Text zwischen Punkten) ist 63.
- Die maximale Gesamtzahl von Zeichen in dem voll qualifizierten Namen ist 254, einschließlich der Punkte, aber ausschließlich der \\-Zeichen.
- Folgende Zeichen sind für den Namen unzulässig: * | < > ?

Es wird nicht empfohlen, sowohl vollständig qualifizierte Domänennamen als auch nicht-qualifizierte Domänennamen zu verwenden. Es wird empfohlen, dass Sie den vollständig qualifizierten Domänennamen eingeben.

Wenn Sie z. B. einen Computer mit dem Namen Test_Computer verwenden, gibt es zwei Möglichkeiten. Eine Auswahl trägt die Bezeichnung Test_Computer. Der voll qualifizierte Name in der Auswahl lautet Test_Computer.domäne.unternehmen.com. In diesem Fall behandelt Backup Exec jede Auswahl als eigenen Computer, obwohl beide den gleichen Computer bezeichnen. Bei allen Backup-Aufträgen, in denen der Kurzname des Computers verwendet wird, enthält der Katalog den Kurznamen. Bei allen Backup-Aufträgen, in denen der vollständig qualifizierte Name verwendet wird, enthält der Katalog den vollständig qualifizierten Namen.

Siehe ["Ändern der Reihenfolge, in der Backup-Quellen gesichert werden"](#) auf Seite 192.

Ändern der Reihenfolge, in der Backup-Quellen gesichert werden

Nachdem Sie die Auswahlen für einen Backup-Auftrag vorgenommen haben, können Sie Backup Exec so konfigurieren, dass die Auswahlen in einer bestimmten Reihenfolge verarbeitet werden. Sie können beispielsweise Backup-Aufträge erstellen, in denen Ihre wichtigsten Backup-Quellen zuerst gesichert werden.

Sie müssen eine Backup-Quelle auswählen, um die Quelle oder beliebige untergeordnete neu zu sortieren. Wenn eine Backup-Quelle dynamisch im Backup enthalten ist, können Sie die Reihenfolge, in der untergeordnete gesichert werden, nicht angeben. Immer wenn Sie eine Backup-Quelle ein- oder ausschließen, wird

ein Eintrag in den Details der Backup-Auswahl erstellt. Sie können die Reihenfolge beliebiger Einträge auf der Registerkarte "Auswahldetails" ändern.

Es gibt einige Beschränkungen hinsichtlich des Änderns der Reihenfolge von Backup-Quellen.

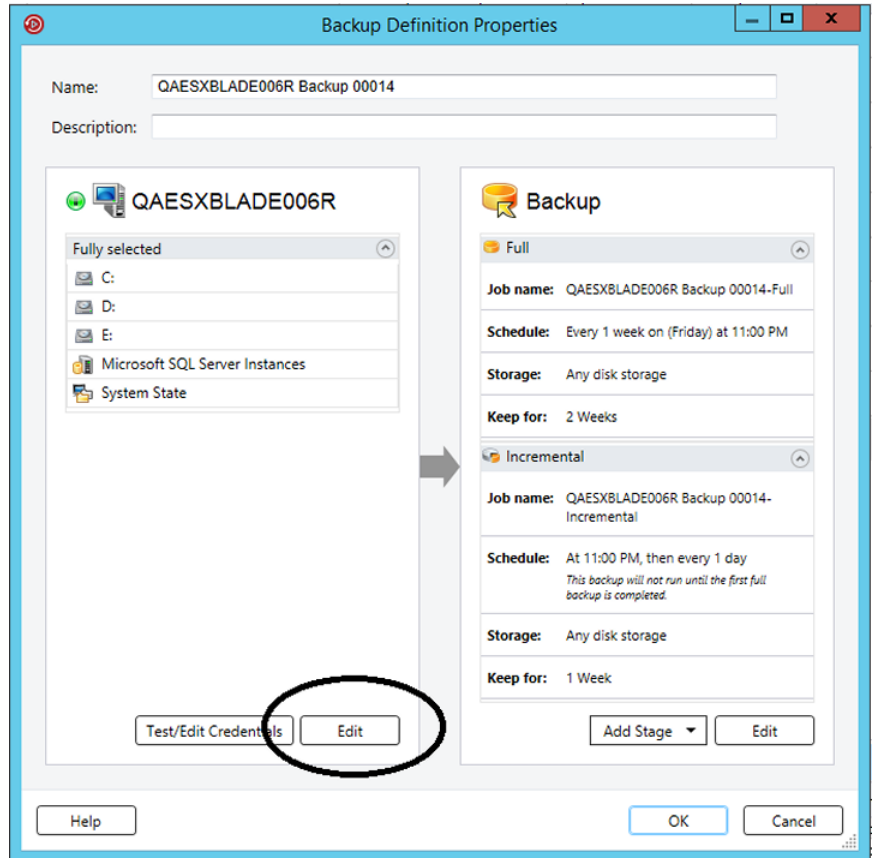
- Backup-Quellen, die sich auf Verzweigungen der Struktur befinden, müssen gemeinsam gesichert werden. Verzweigungen sind Container für Backup-Quellen in der Struktur. Einzelne Anwendungen werden in der Backup Exec-Struktur als Verzweigungen angezeigt. Wenn Sie einen Server haben, der SharePoint-, SQL- und Exchange-Daten enthält, wird jede Anwendung als Verzweigung angezeigt. Sie können die Backup-Reihenfolge einzelner Elemente in einer Verzweigung ändern, aber nicht von Elementen über mehrere Verzweigungen hinweg.

Beispiel: Wenn Sie einen Datenträger und eine SQL-Datenbank sichern möchten, müssen Sie die SQL-Instanzen nacheinander sichern. Sie können die Reihenfolge ändern, in der die SQL-Instanzen gesichert werden. Sie können jedoch eine SQL-Instanz sichern und dann den Datenträger, bevor Sie die anderen SQL-Instanzen sichern.

- Alle Daten, die sich in einer spezifischen Backup-Quelle befindet, werden als nur ein Element behandelt. Sie können die Reihenfolge ändern, in der die Backup-Quellen gesichert werden. Sie können auch die Reihenfolge ändern, in der die Daten in einer Backup-Quelle gesichert werden. Die Reihenfolge der Daten über mehrere Backup-Quellen hinweg kann jedoch nicht geändert werden. Beispiel: Wenn Sie zwei Datenträger sichern, können Sie auswählen, welcher Datenträger zuerst gesichert werden soll. Sie können auch die Reihenfolge auswählen, in der die Daten auf den einzelnen Datenträgern gesichert werden. Sie können jedoch erst Daten auf einem anderen Datenträger sichern, wenn alle Daten auf dem ersten Datenträger gesichert wurden.
- Die Reihenfolge bestimmter Systemressourcen kann nicht geändert werden. Beispiel: Shadow Copy-Komponenten und Systemstatus-Backup-Quellen müssen immer zuletzt gesichert werden.

So ändern Sie die Reihenfolge, in der Backup-Quellen unterstützt werden

- 1 Erstellen oder bearbeiten Sie eine Backup-Definition.
- 2 Klicken Sie im Dialogfeld "Auswahl" auf "Bearbeiten".



- 3 Sie haben folgende Möglichkeiten:

So ordnen Sie die Server in einer Backup-Definition mit mehreren Servern neu

Verwenden Sie im linken Teilfenster des Dialogfelds "Backup-Auswahl" die Pfeile nach oben und unten, um die Reihenfolge der Server oder der Anwendungen zu konfigurieren.

Backup Exec sichert die Server oder die Anwendungen am Anfang der Liste zuerst.

So ordnen Sie die Backup-Quellen innerhalb eines Servers neu

Gehen Sie wie folgt vor:

- Wählen Sie im linken Teilfenster des Dialogfelds "Backup-Auswahl" den Server aus, der die Ressourcen enthält, die Sie neuordnen möchten.
- Klicken Sie anschließend im rechten Teilfenster des Dialogfelds "Backup-Auswahl" auf die Registerkarte "Auswahldetails".
- Um die Backup-Quellen neuuzuordnen, wenn ein ganzer Server ausgewählt ist, müssen Sie die einzelnen Auswahlen, die Sie neuordnen möchten, einfügen:
 - Klicken Sie auf "Einfügen" und wählen Sie "Auswahl einfügen".
 - Wählen Sie die Backup-Quelle aus, die Sie neuordnen möchten, und klicken Sie auf "OK".

Wiederholen Sie diesen Schritt für jede Backup-Quelle, die Sie neuordnen möchten.

- Verwenden Sie im rechten Teilfenster des Dialogfelds "Backup-Auswahl" die Pfeile nach oben und unten, um die Reihenfolge der Server oder der Anwendungen zu konfigurieren.
 Backup Exec sichert die Backup-Quellen am Anfang der Liste zuerst.
- Klicken Sie auf "OK".

4 Klicken Sie auf "OK".

Siehe ["Sichern von Daten"](#) auf Seite 174.

Siehe ["Info zum Auswählen von zu sichernden Daten"](#) auf Seite 186.

Ausschließen von Dateien von Backups

Sie können bestimmte Dateien oder Typen von Dateien von den Backups ausschließen, wenn Sie sicherstellen möchten, dass sie nicht gesichert werden. Beispielsweise werden Sie vielleicht keine MP3-Dateien, schreibgeschützten Dateien oder Dateien aus bestimmten Verzeichnissen sichern wollen.

Sie können Dateien auf drei Arten von Backups ausschließen:

- **Ausschließen von Dateien von Backup-Aufträgen**
 Wenn Sie Dateien von den einzelnen Backup-Aufträgen ausschließen, treffen diese Ausschlüsse nicht auf die anderen Backup-Aufträge in der zugehörigen Backup-Definition zu. Die Ausschlüsse auf der Auftragsebene betreffen auch

Ihre anderen Backup-Definitionen nicht. Der Ausschluss trifft nur auf den jeweiligen Backup-Auftrag zu. Sie können einen Ausschluss auf Auftragsebene nicht auf das gesamte Backup anwenden.

- **Ausschließen von Dateien von Backup-Definitionen**
Wenn Sie Dateien von Backup-Aufträgen ausschließen, treffen diese Ausschlüsse nicht auf die anderen Backup-Definition zu. Die Ausnahmen treffen nur auf Aufträge in dieser Backup-Definition zu.
- **Globales Ausschließen von Dateien von allen Backups**
Wenn Sie Dateien global von allen Backups ausschließen, treffen diese Ausschlüsse auf alle Ihre Backup-Definitionen zu. Backup Exec überspringt automatisch alle globalen Ausschlüsse, wenn Sie Backup-Aufträge ausführen.

So schließen Sie Dateien von Backup-Definitionen aus

1 Sie haben folgende Möglichkeiten:

So schließen Sie Dateien von Backup-Aufträgen aus Führen Sie die folgenden Schritte durch:

- Erstellen oder bearbeiten Sie eine Definition.
- Klicken Sie im Dialogfeld "Backup" auf "Bearbeiten".
- Wählen Sie im linken Teilfenster "Ausschlüsse".
- Klicken Sie auf "Einfügen".

So schließen Sie Dateien von einer Backup-Definition aus Führen Sie die folgenden Schritte durch:

- Erstellen oder bearbeiten Sie eine Backup-Definition.
- Klicken Sie im Dialogfeld "Auswahl" auf "Bearbeiten".
- Klicken Sie auf der Registerkarte "Auswahldetails" auf "Einfügen" und wählen Sie dann "Ausschlüsse auf Backup-Ebene hinzufügen" aus.

So schließen Sie Dateien
global von allen Backups aus

Führen Sie die folgenden Schritte durch:

- Klicken Sie auf die Backup Exec-Schaltfläche.
- Wählen Sie "Konfiguration und Einstellungen" und anschließend "Auftragsstandardeinstellungen".
- Klicken Sie auf "Auswahl ausschließen".
- Klicken Sie auf "Einfügen".

2 Füllen Sie nach Bedarf die folgenden Felder aus, um die Dateien zu festzulegen, die Sie ausschließen möchten:

Ressourcenname

Geben Sie den Namen des Datenträgers oder Laufwerks, den bzw. das Sie von den Backups ausschließen möchten.

Pfad

Geben Sie den Pfad des Ordners und/oder des Unterordners ein, der die Dateien enthält, die Sie ausschließen möchten. Sie können Platzhalterzeichen verwenden. Verwenden Sie ein Fragezeichen (?) als Platzhalter für ein einzelnes Zeichen. Verwenden Sie zwei Sternchen (**) als Platzhalter für eine beliebige Anzahl von Zeichen.

Name

Geben Sie den Namen einer bestimmten Datei ein, die Sie vom Backup ausschließen möchten. Sie können Platzhalterzeichen verwenden. Verwenden Sie ein Fragezeichen (?) als Platzhalter für ein einzelnes Zeichen. Verwenden Sie zwei Sternchen (**) als Platzhalter für eine beliebige Anzahl von Zeichen.

Beispiel: Um alle Dateien mit der Dateierweiterung EXE auszuschließen, geben Sie "***.exe" ein.

3 Konfigurieren Sie nach Bedarf die folgenden Optionen:

Auf Unterverzeichnisse anwenden	Wählen Sie diese Option aus, um den Inhalt aller Unterordner auszuschließen, wenn Sie ein Verzeichnis auswählen.
Nur geänderte Dateien	Wählen Sie diese Option aus, um nur die Dateien im angegebenen Verzeichnis auszuschließen.
Nur schreibgeschützte Dateien	Wählen Sie diese Option, um nur schreibgeschützte Dateien im angegebenen Verzeichnis auszuschließen.
Dateien mit	Wählen Sie diese Option, um die Dateien auszuschließen, die während eines bestimmten Zeitraums erstellt oder geändert wurden. Sie müssen das Start- und Enddatum für den Zeitraum, für den Sie Dateien ausschließen möchten, auswählen.
Dateien ohne Zugriff in den letzten x Tagen	Wählen Sie diese Option, um alle Dateien auszuschließen, auf die nicht in einer bestimmten Anzahl von Tagen zugegriffen wurde. Sie müssen die Anzahl von Tagen eingeben.

4 Klicken Sie auf "OK".

Siehe ["Info zum Auswählen von zu sichernden Daten "](#) auf Seite 186.

Siehe ["Einschließen spezifischer Dateien mit der Backup-Auswahl eines Backup-Auftrags"](#) auf Seite 198.

Einschließen spezifischer Dateien mit der Backup-Auswahl eines Backup-Auftrags

Wenn Sie eine Backup-Definition erstellen, erstellen Sie auch eine Backup-Auswahlliste. Die Backup-Auswahl enthält die zu sichernden Dateien und Daten. Sie können zusätzliche spezifische Dateien oder Backup-Quellen mit einer weiteren Backup-Auswahl einschließen. Wenn Sie Dateien mit einer Backup-Auswahl einschließen, können Sie bestimmte Bedingungen auswählen, die erfüllt werden müssen, damit die Datei eingeschlossen werden kann. Beispiel: Es sollen schreibgeschützte Dateien, die sich in einem spezifischen Verzeichnis befinden, eingeschlossen werden. Wenn Sie eine Datei mit der Backup-Auswahl eines Backup-Auftrags einschließen, sichert Backup Exec die reguläre Backup-Auswahl und schließt die spezifisch ausgewählten Dateien ein.

So schließen Sie spezifische Dateien mit der Backup-Auswahl eines Backup-Auftrags ein

- 1 Erstellen oder bearbeiten Sie eine Backup-Definition.
- 2 Klicken Sie im Dialogfeld "Auswahl" auf "Bearbeiten".
- 3 Klicken Sie auf der Registerkarte "Auswahldetails" auf "Einfügen" und wählen Sie dann "Auswahl einfügen".
- 4 Füllen Sie nach Bedarf die folgenden Felder aus, um die Dateien festzulegen, die Sie einschließen möchten:

Ressourcenname	Tragen Sie den Namen des zu sichernden Datenträgers bzw. Laufwerks ein.
Pfad	Geben Sie den Pfad des Ordners und/oder des Unterordners ein, der die Dateien enthält, die Sie einschließen möchten. Sie können Platzhalterzeichen verwenden. Verwenden Sie ein Fragezeichen (?) als Platzhalter für ein einzelnes Zeichen. Verwenden Sie zwei Sternchen (**) als Platzhalter für eine beliebige Anzahl von Zeichen.
Name	<p>Geben Sie den Namen einer bestimmten Datei ein, die Sie in das Backup einschließen möchten. Sie können Platzhalterzeichen verwenden. Verwenden Sie ein Fragezeichen (?) als Platzhalter für ein einzelnes Zeichen. Verwenden Sie zwei Sternchen (**) als Platzhalter für eine beliebige Anzahl von Zeichen.</p> <p>Beispiel: Um alle Dateien mit der Dateierweiterung ".exe" einzuschließen, geben Sie "***.exe" ein.</p>

5 Konfigurieren Sie nach Bedarf die folgenden Optionen:

Auf Unterverzeichnisse anwenden	Wählen Sie diese Option, um den Inhalt aller Unterordner einzuschließen, wenn Sie ein Verzeichnis auswählen.
Nur geänderte Dateien	Wählen Sie diese Option, um nur die Dateien im angegebenen Verzeichnis einzuschließen.
Nur schreibgeschützte Dateien	Wählen Sie diese Option, um nur schreibgeschützte Dateien im angegebenen Verzeichnis einzuschließen.
Dateien mit	Wählen Sie diese Option, um die Dateien einzuschließen, die während eines bestimmten Zeitraums erstellt oder geändert wurden. Sie müssen das Start- und Enddatum für den Zeitraum, für den Sie Dateien ausschließen möchten, auswählen.
Dateien ohne Zugriff in den letzten x Tagen	Wählen Sie diese Option, um alle Dateien einzuschließen, auf die nicht in einer bestimmten Anzahl von Tagen zugegriffen wurde. Sie müssen die Anzahl von Tagen eingeben.
Als geschäftskritisch kennzeichnen	Wählen Sie diese Option, wenn die Sicherung der ausgewählten Ressource vor den anderen, nicht als geschäftskritisch gekennzeichneten Ressourcen erfolgen soll.

6 Klicken Sie auf "OK".

Siehe ["Info zum Auswählen von zu sichernden Daten "](#) auf Seite 186.

Siehe ["Ausschließen von Dateien von Backups"](#) auf Seite 195.

Info zum Sichern von wichtigen Systemkomponenten

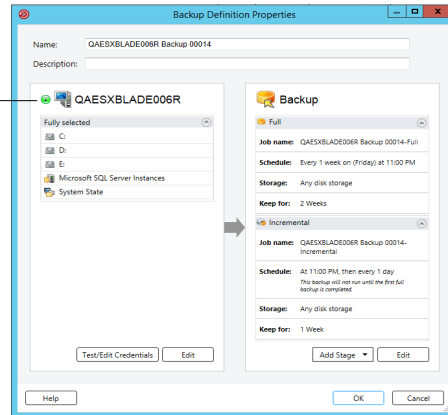
Backup Exec ist so konfiguriert, dass die für eine vollständige Systemwiederherstellung erforderlichen kritischen Systemkomponenten automatisch gesichert werden. Durch die Sicherung kritischer Systemkomponenten wird sichergestellt, dass Sie bei einem Systemausfall zur Wiederherstellung Ihrer Computer in der Lage sind.

Wenn alle wichtigen Systemkomponenten in Ihren ausgewählten Backup-Aufträgen eingeschlossen sind, sehen Sie auf der "Simplified Disaster Recovery" -Anzeige im Auswahlteifenster die Meldung "EIN". Wenn Sie eine oder mehrere wichtige

Systemkomponentendateien abwählen, sehen Sie auf der Anzeige die Meldung "AUS".

Abbildung 4-4 Im Dialogfeld "Eigenschaften der Backup-Definition" ist die Simplified Disaster Recovery aktiviert.

Simplified Disaster Recovery-
Anzeige



Sie müssen alle wichtigen Systemkomponenten in die Backup-Auswahl einschließen, wenn Sie beabsichtigen, eines der folgenden Wiederherstellungsszenarien zu verwenden:

- Simplified Disaster Recovery
Siehe ["Info zu Simplified Disaster Recovery"](#) auf Seite 941.
- Konvertierung in virtuelle Computer
Siehe ["Funktionsweise der Konvertierung eines physischen Computers in einen virtuellen in Backup Exec"](#) auf Seite 581.
- Abschließen der Online-Wiederherstellung eines Microsoft Windows-Computers
Siehe ["Vollständige Online-Wiederherstellung eines Microsoft Windows-Computers"](#) auf Seite 267.

Einige Wiederherstellungsszenarien sind nur für bestimmte Datentypen und Backup Exec-Agents verfügbar. Zusätzlich müssen Sie eine bestimmte Backup-Methode für einige Datentypen auswählen, wenn Sie beabsichtigen, eine physisch-virtuelle oder Backup-virtuelle Konvertierung zu verwenden.

Tabelle 4-2 Wiederherstellungsszenarien nach Datentyp

Name des Dateisystems oder Agent	Betriebssystem und Anwendungen sind installiert und funktionieren	Vollständige Offsite-Wiederherstellung kann durchgeführt werden	Physische/virtuelle Konvertierung kann durchgeführt werden	Backup-virtuelle Konvertierung kann durchgeführt werden	Simplified Disaster Recovery kann durchgeführt werden
Active Directory	Ja	Ja	Ja	Ja	Ja
Active Directory Lightweight	Ja	Nein	Nein	Nein	Nein
CSV	Ja	Ja	Nein	Nein	Ja
EFI	Ja	Ja	Nein	Nein	Ja
Enterprise Vault	Ja	Nein	Nein	Nein	Nein
Exchange Agent	Ja	Nein	Ja, bei einem inkrementellen oder differenziellen Backup muss die Backup-Methode "Blockebene" verwendet werden.	Ja, bei einem inkrementellen oder differenziellen Backup muss die Backup-Methode "Blockebene" verwendet werden.	Nein
FAT	Ja	Ja	Ja	Ja	Ja
Hyper-V-Agent	Ja	Nein	Nein	Nein	Nein
NTFS	Ja	Ja	Ja	Ja	Ja
Oracle RMAN Windows Agent	Ja	Nein	Nein	Nein	Nein
ReFS	Ja	Ja	Nein	Nein	Ja
Shadow Copy-Komponenten	Ja	Ja	Ja	Ja	Ja

Name des Dateisystems oder Agent	Betriebssystem und Anwendungen sind installiert und funktionieren	Vollständige Systemwiederherstellung kann durchgeführt werden	Physische/virtuelle Konvertierung kann durchgeführt werden	Backup-virtuelle Konvertierung kann durchgeführt werden	Simplified Disaster Recovery kann durchgeführt werden
SharePoint Agent	Ja	Nein	Nein	Nein	Nein
SQL Agent	Ja	Nein	Ja, bei einem inkrementellen oder differenziellen Backup muss die Backup-Methode "Blockebene" verwendet werden.	Ja, bei einem inkrementellen oder differenziellen Backup muss die Backup-Methode "Blockebene" verwendet werden.	Nein
Systemstatus	Ja	Ja	Ja	Ja	Ja
Desktop-PC	Ja	Ja	Nein	Nein	Ja
VMware Agent	Ja	Nein	Nein	Nein	Nein
Windows-Duplex	Ja	Ja	Nein	Nein	Ja

Sie können kritische Systemkomponenten nicht einzeln als Backup-Auswahl auswählen. Sie müssen den gesamten Server auswählen, um sicherzustellen, dass alle kritischen Systemkomponenten im Backup eingeschlossen werden. Wenn Sie das Sichern eines Servers auswählen, schließt Backup Exec alle Systemgeräte und Anwendungs-Agents des Servers ein. Backup Exec erkennt und schützt dynamisch alle kritischen und nicht-kritischen Systemgeräte und Anwendungsagenten.

Sie können sämtliche nicht-kritische Geräte oder Anwendungsdaten in die Backup-Auswahl explizit einschließen oder daraus ausschließen und weiterhin eine vollständige Systemwiederherstellung ausführen. Sie können beispielsweise Microsoft Exchange-Daten von Ihrem Backup ausschließen und dennoch die Backup-Sätze zur Ausführung einer Notfallwiederherstellung verwenden.

Die folgenden Systemressourcen gelten als kritisch und müssen eingeschlossen werden, wenn Sie die Backup-Sätze verwenden möchten, um eine vollständige Systemwiederherstellung durchzuführen:

- Systemdatenträger (einschließlich EFI und Dienstprogrammpartitionen)
- Boot-Datenträger (ausschließlich Betriebssystem)
- Dienst-Anwendungsdatenträger (Boot, System und automatischer Systemstart)
- Systemstatusgeräte und -Datenträger (einschließlich Active Directory, Systemdateien usw.)
- Windows-Wiederherstellungspartition (WinRE) unter einer beliebigen unterstützten Windows-Version

Informationen zu den Best Practices zum Einsatz von Backup Exec zum Schützen wichtiger Systemkomponenten finden Sie unter *Best Practices für Backup Exec*.

Shadow Copy-Dateisystemkomponenten von Backup Exec

Das Schattenkopiekomponenten-Dateisystem von Backup Exec verwendet den Volumeschattenkopie-Dienst von Microsoft, um wichtige Betriebssystem- und Anwendungsdienstprogramme sowie Anwendungs- und Benutzerdaten Dritter auf Computern unter Windows Server 2008 zu schützen.

Der Volume Shadow Copy Service ermöglicht das Backup eines Computers, während Anwendungen und Dienste ausgeführt werden, indem beim Start eines Backup-Auftrags eine Kopie des Datenträgers erstellt wird. Die Anwendungen müssen nicht beendet werden, um ein erfolgreiches Datenträger-Backup zu garantieren. Volume Shadow Copy Service versetzt Drittanbieter in die Lage, Snapshot-Plugins oder Writer zu erstellen und diese mit der Schattenkopie-Technologie zu verwenden.

Bei einem Writer handelt es sich um einen bestimmten Code in einer Anwendung, der in Verbindung mit dem Volume Shadow Copy Service die mit der Wiederherstellung konsistenten Betriebssystem- und Anwendungsdaten zu einem bestimmten Zeitpunkt zur Verfügung stellt. Writer werden als Schattenkopiekomponenten dargestellt, die bei der Backup- und Wiederherstellungsauswahl als Daten aufgeführt werden.

In der Backup-Auswahlliste können nur die Writer ausgewählt werden, die für eine Verwendung mit Backup Exec getestet wurden. Andere Writer werden in den Auswahlen angezeigt, aber sie können nicht für Backups ausgewählt werden.

Wenn Sie einen Datenträger auswählen, der Schattenkopiedateien zum Sichern enthält, wird von Backup Exec festgelegt, welche Schattenkopiedateien bei einem Backup auf Datenträgerebene nicht berücksichtigt werden. Diese Dateien werden automatisch von der Funktion "Ausschließen aktiver Dateien" vom Backup ausgeschlossen. Wenn der Ausschluss nicht während eines Backup ohne Snapshots

erfolgte, werden die Dateien als "Wird gerade benutzt – übersprungen" angezeigt. Wenn der Ausschluss nicht während eines Snapshot-Backups erfolgte, kann dies zu einem inkonsistenten Sichern der Daten und zu Wiederherstellungsproblemen führen.

Die Funktionen der Windows SharePoint-Services verwenden eine SQL-Instanz (MSDE) namens "SharePoint" als Speicher für freigegebene Informationen und gemeinsame Dateien. Wenn SQL Agent nicht unter Windows Server 2008 installiert ist, kann die SQL-SharePoint-Instanz durch das Schattenkopiekomponenten-Dateisystem geschützt werden. Wenn SQL Agent installiert ist, wird die SQL-Instanz SHAREPOINT von diesem geschützt.

Hinweis: Wenn die Windows SharePoint-Services installiert sind und nicht den Standard-Instanz-Namen von SHAREPOINT verwenden, ist kein Schutz über das Schattenkopiekomponenten-Dateisystem möglich. In diesem Fall muss SQL Agent verwendet werden, um die SQL-Instanz SHAREPOINT zu schützen.

Backup-Methoden in Backup Exec

Wenn Sie eine Backup-Definition erstellen, müssen Sie Backup-Methoden für jeden Backup-Auftrag auswählen. Die Backup-Methode bestimmt, welche Daten Backup Exec sichert. Die standardmäßigen Backup-Methoden sind Vollständig, Inkrementell und Differenziell. Sie können jedoch auch bestimmte Typen von Backup-Methoden für einige Agents und Datentypen auswählen.

Backup-Definitionen müssen einen Backup-Auftrag enthalten, der die vollständige Backup-Methode verwendet. Der erste vollständige Backup-Auftrag bildet die Basis, indem alle Daten, die Sie ausgewählt haben, gesichert werden. Dann können Sie der Backup-Definition zusätzliche inkrementelle oder differenzielle Backup-Aufträge hinzufügen. Sie können datenspezifische Backup-Methoden anstelle der Standard-Backup-Methoden anwenden, indem Sie die passende Backup-Methode auf der Seite "Optionen" für diesen Agent auswählen.

Dieses Thema enthält folgende Informationen:

[Vollständiges Backup](#)

[Differenzielles Backups](#)

[Inkrementelles Backup](#)

[Vor- und Nachteile der Backup-Methoden](#)

[Backup-Methoden für bestimmte Datentypen](#)

Vollständiges Backup

Vollständige Backups umfassen alle Daten, die für das Backup ausgewählt wurden. Backup Exec erkennt, dass der Server gesichert wurde.

Hinweis: Als Grundlage für die Notfallwiederherstellung sollten Sie ein vollständiges Backup des Servers durchführen.

Vollständige Backups umfassen auch duplizierte Backups, die alle ausgewählten Daten einschließen. Duplizierte Backups beeinträchtigen nicht Ihre Bandmedienrotationsstrategie, da das Archivbit nicht zurückgesetzt wird.

Es wird empfohlen, dass Sie nach dem Aktualisieren oder Ändern von Backup-Quellen immer ein vollständiges Backup ausführen. Diese Empfehlung gilt für die meisten signifikanten Konfigurationen oder Änderungen von Betriebssystem und Anwendungen.

Tabelle 4-3 Backup-Quellen und Szenarien, für die ein vollständiges Backup empfohlen wird:

Backup-Quelle	Szenarien
Betriebssystem	<p>Sie sollten ein vollständiges Backup ausführen, wenn Sie:</p> <ul style="list-style-type: none">■ auf eine neue Version des Betriebssystems aktualisieren■ das vorhandene Betriebssystem unter Verwendung von Windows Updat aktualisieren <p>Hinweis: Sie sollten ein vollständiges Backup ausführen, bevor Sie die Aktualisierung durchführen. Führen Sie die Aktualisierung aus und starten Sie dann den Computer neu. Dann sollten Sie ein weiteres vollständiges Backup ausführen.</p> <ul style="list-style-type: none">■ Hinzufügen, Ändern oder Entfernen von Serverrollen oder -funktionen
Anwendungen	<p>Sie sollten ein vollständiges Backup ausführen, wenn Sie:</p> <ul style="list-style-type: none">■ neue Anwendungen installieren■ Anwendungen auf neue Versionen aktualisieren■ die vorhandene Version von Anwendungen aktualisieren

Backup-Quelle	Szenarien
Backup Exec	<p>Sie sollten ein vollständiges Backup ausführen, wenn Sie:</p> <ul style="list-style-type: none"> ■ auf eine neue Version von Backup Exec aktualisieren <p>Hinweis: Wiederkehrende Aufträge, die auf eine neue Version von Backup Exec migriert werden, behalten ihre vorhandenen Zeitpläne bei. Sie sollten ein vollständiges Backup für alle vorhandenen Aufträge manuell ausführen, bevor inkrementelle oder differenzielle Backups ausgeführt werden.</p> <ul style="list-style-type: none"> ■ Aktualisieren Sie die vorhandene Version von Backup Exec unter Verwendung von Veritas Update. ■ Nehmen Sie Konfigurationsänderungen vor.

Das Ausführen von vollständigen Backups vor und nach diesen Szenarien hilft, zu garantieren, dass Sie gegebenenfalls die vorherige Konfiguration wiederherstellen können.

Differenzielles Backups

Differenzielle Backups enthalten Dateien, die sich seit dem letzten vollständigen oder inkrementellen Backup geändert haben. Der Unterschied zwischen differenziellen und inkrementellen Backups ist, dass differenzielle Backups kumulativ sind. Nach einem differenziellen Backup sichert jedes folgende differenzielle Backup die gleichen Dateien wie das vorherige. Es sichert auch alle seit dem letzten vollständigen oder inkrementellen Backup neuen oder geänderten Dateien.

Hinweis: In einer Backup-Definition, die eine differenzielle Aufgabe enthält, müssen bei allen Backup-Aufgaben Speichergeräte verwendet werden, auf die der gleiche Backup Exec-Server zugreifen kann.

Standardmäßig verwendet Backup Exec das Windows-Änderungsjournal, um zu bestimmen, ob Dateien zuvor gesichert wurden. Sie können Backup Exec auch so konfigurieren, dass die Eigenschaft "Geändert am" oder das Archivbit verwendet wird, um zu bestimmen, ob die Datei gesichert wurde.

Hinweis: Sie können Backup Exec-Kataloge nicht verwenden, um zu bestimmen, ob Dateien für beliebige differenzielle Backups gesichert wurden.

Siehe ["Konfigurieren von Datei- und Ordneroptionen für Backup-Aufträge"](#) auf Seite 676.

Da weniger Backups benötigt werden, lassen sich mit differenziellen Backups gesamte Geräte leichter wiederherstellen als mit inkrementellen Backups. Die Verwendung von weniger Medien verringert auch das Risiko, dass ein Wiederherstellungsauftrag aufgrund eines Medienfehlers fehlschlägt.

Inkrementelles Backup

Inkrementelle Backups enthalten nur Dateien, die seit dem letzten vollständigen oder inkrementellen Backup geändert wurden. Der Unterschied zwischen einem inkrementellen und einem differenziellen Backup ist, dass inkrementelle Backups nicht kumulativ sind. Jedes inkrementelle Backup stellt eine Basis her. Nach dem inkrementellen Backup sichert das folgende inkrementelle oder differenzielle Backup nur alle seit der Basis neuen oder geänderte Dateien.

Hinweis: In einer Backup-Definition, die eine inkrementelle Aufgabe enthält, müssen bei allen Backup-Aufgaben Speichergeräte verwendet werden, auf die der gleiche Backup Exec-Server zugreifen kann.

Standardmäßig verwendet Backup Exec das Windows-Änderungsjournal, um zu bestimmen, ob Dateien zuvor gesichert wurden. Sie können auch festlegen, dass Backup Exec mithilfe der geänderten Zeit einer Datei, Archivbit, oder Backup Exec-Katalogen bestimmt, ob die Datei gesichert wurde.

Siehe "[Konfigurieren von Datei- und Ordneroptionen für Backup-Aufträge](#)" auf Seite 676.

Inkrementelle Backups nehmen viel weniger Zeit in Anspruch als vollständige oder differenzielle Backups. Sie erfordern auch weniger Speicherplatz für gesicherte Daten, da nur Dateien gesichert werden, die seit dem letzten Backup geändert wurden.

Vor- und Nachteile der Backup-Methoden

Jede Backup-Methode hat Vorteile und Nachteile.

Tabelle 4-4 Vor- und Nachteile der Backup-Methoden

Methode	Vorteile	Nachteile
Vollständiges Backup	<ul style="list-style-type: none"> ■ Dateien sind einfach zu finden Vollständige Backups schließen alle Daten ein, die Sie für das Backup ausgewählt haben. Deshalb müssen Sie nicht mehrere Backup-Sätze nach Dateien durchsuchen, die wiederhergestellt werden müssen. ■ Ein aktuelles Backup Ihres gesamten Systems ist in einem Backup-Satz verfügbar Wenn Sie ein vollständiges Backup Ihres gesamten Systems durchführen und es anschließend wiederherstellen müssen, befinden sich alle aktuellen Informationen an einem Ort. 	<ul style="list-style-type: none"> ■ Überflüssige Backups Die meisten Dateien auf Ihrem Dateiserver ändern sich nicht. Jedes vollständige Backup nach dem ersten ist lediglich eine Kopie der bereits gesicherten Daten. Vollständige Backups erfordern mehr Speicherplatz. ■ Vollständige Backups nehmen mehr Zeit in Anspruch Vollständige Backups können zeitaufwendig sein, besonders wenn sich andere Server im Netzwerk befinden, die gesichert werden müssen (z. B. Arbeitsstationen von Agents, Remote-Server).

Methoden	Vorteile	Nachteile
Differenzielles Backup	<ul style="list-style-type: none"> ■ Dateien sind einfach zu finden Das Wiederherstellen eines Computers, der differenziell gesichert wird, erfordert weniger Backups. Bei differenziellen Backups sind das neueste vollständige Backup, alle folgenden inkrementellen und das neueste differenzielle Backup erforderlich. Das Wiederherstellen aus differenziellen Backups nimmt weniger Zeit in Anspruch als aus inkrementellen. Für das Wiederherstellen aus inkrementellen Backups sind das neueste vollständige Backup und alle inkrementellen Backups erforderlich, die seit dem vollständigen Backup erstellt wurden. ■ Weniger Zeit für Backup und Wiederherstellung erforderlich Differenzielle Backups nehmen weniger Zeit als vollständige Backups in Anspruch. Schnellere Wiederherstellung ist bei Systemausfällen möglich, weil Sie nur Backup-Sätze vom neuesten vollständigen Backup, von allen folgenden inkrementellen Backups und vom neuesten differenziellen Backup benötigen, um einen Server vollständig wiederherzustellen. 	<ul style="list-style-type: none"> ■ Überflüssige Backups Es werden alle Dateien eingeschlossen, die seit dem letzten vollständigen Backup erstellt oder geändert wurden. So werden überflüssige Backups erstellt.

Methode	Vorteile	Nachteile
Inkrementelles Backup	<ul style="list-style-type: none"> ■ Bessere Speichernutzung Es werden nur Dateien eingeschlossen, die seit dem letzten Backup geändert wurden. Somit ist erheblich weniger Datenspeicherplatz erforderlich. ■ Weniger Zeit für Backup erforderlich Inkrementelle Backups nehmen viel weniger Zeit in Anspruch als vollständige und differenzielle Backups. 	<ul style="list-style-type: none"> ■ Backups werden auf mehrere Backup-Sätze aufgeteilt Da mehrere Backup-Sätze bei Systemausfall benötigt werden, kann das Wiederherstellen eines Servers länger dauern. Außerdem müssen die Backup-Sätze in der richtigen Reihenfolge wiederhergestellt werden, um das System effektiv auf den neuesten Stand zu bringen.

Beachten Sie das folgende Beispiel einer Backup-Strategie:

Sie möchten eine Backup-Strategie für den Bürodateiserver implementieren. Alle Backup-Strategien fangen mit einem vollständigen Backup an (Backup eines gesamten Servers unter Verwendung der vollständigen Backup-Methode). Erstellen und senden Sie einen vollständigen Backup-Auftrag so, dass er freitagabends ausgeführt wird.

Die meisten Dateien auf dem Server, wie die Betriebssystemdateien und Anwendungsdateien, werden selten geändert. Deshalb entscheidet Sie sich, inkrementelle oder differenzielle Backups zu verwenden, um Zeit und Speicherplatz zu sparen. Sie entscheiden sich für inkrementelle Backups. Planen Sie den Auftrag so, dass er Montag bis Donnerstag am Ende des Tages mit der inkrementellen Backup-Methode ausgeführt wird.

Am Freitag enthalten Ihre Backup-Sätze alle Daten auf dem Dateiserver. Backup Exec ändert den Status aller Dateien in "Gesichert". Am Montagabend wird das inkrementelle Backup ausgeführt und es werden nur die Dateien, die erstellt oder geändert wurden, gesichert. Nach dem inkrementellen Backup setzt Backup Exec das Archivbit zurück und kennzeichnet die Dateien auf diese Weise als gesichert. Der gleiche Vorgang wird dienstags bis donnerstags wiederholt.

Sollte Ihr Dateiserver am Donnerstag abstürzen, würden Sie die Backups in der Reihenfolge wiederherstellen, in der sie erstellt wurden. Sie würden mit dem Backup vom Freitag anfangen bis hin zum Backup vom Mittwoch.

Wenn Sie sich für differenzielle Backups von Montag bis Donnerstag entschieden haben, würden Sie nur die Backup-Sätze von Freitag und Mittwoch benötigen. Die Backup-Sätze von Freitag würden alle Daten des ursprünglichen Backups enthalten. Die Backup-Sätze vom Mittwoch würden jede Datei enthalten, die seit dem Backup am Freitag erstellt oder geändert wurde.

Backup-Methoden für bestimmte Datentypen

Agents und Funktionen verfügen möglicherweise über bestimmte Backup-Methoden.

Standarmäßig enthält jede Backup-Definition einen Backup-Auftrag, der die verfügbare Backup-Methode auf das erste vollständige Backup für die meisten Datentypen begrenzt. Sie können zusätzliche Backup-Aufträge konfigurieren, die Backup-Methoden für bestimmte Datentypen enthalten. Sie können die Auftragsvorlagen für diese Backup-Aufträge so benennen, dass sie die Organisierung Ihrer Backup-Strategie erleichtert.

Siehe "[Konfigurieren von Backup-Methoden für Backup-Aufträge](#)" auf Seite 215.

Wenn Sie eine Backup-Definition erstellen, die mehr als eine Backup-Methode für mehrfache Datentypen enthält, wird diese in "Auftragsüberwachung" als ein gemischtes Backup bezeichnet.

Tabelle 4-5 Verfügbare Backup-Methoden nach Datentyp

Datentyp	Auftragstyp und Backup-Methode
Dateien und Ordner	<p>Erstes vollständiges:</p> <ul style="list-style-type: none"> ■ Vollständig – Dateien sichern <p>Zusätzliche Backup-Methoden für Dateien und Ordner:</p> <ul style="list-style-type: none"> ■ Vollständig – Dateien sichern ■ Vollständige Kopie – Dateien (Kopie) sichern ■ Differenziell: Seit letztem vollständigen oder inkrementellen Backup geänderte Dateien sichern ■ Inkrementell: Seit dem letzten vollständigen oder inkrementellen Backup geänderte Dateien sichern
Enterprise Vault	<p>Erstes vollständiges:</p> <ul style="list-style-type: none"> ■ Vollständig - Komponenten sichern <p>Zusätzliche Backup-Methoden für Enterprise Vault:</p> <ul style="list-style-type: none"> ■ Vollständig - Komponenten sichern ■ Differenziell - Nur seit dem letzten vollständigen Backup geänderte Komponenten sichern ■ Inkrementell - Nur seit dem letzten vollständigen oder inkrementellen Backup geänderte Komponenten sichern

Datentyp	Auftragstyp und Backup-Methode
Microsoft Exchange	<p>Erstes vollständiges:</p> <ul style="list-style-type: none"> ■ Vollständig – Backup-Datenbanken und Protokolle (Protokolle abschneiden) ■ Vollständige Kopie – Backup-Datenbanken und Protokolle <p>Zusätzliche Backup-Methoden für Microsoft Exchange:</p> <ul style="list-style-type: none"> ■ Vollständig – Backup-Datenbanken und Protokolle (Protokolle abschneiden) ■ Vollständige Kopie – Backup-Datenbanken und Protokolle ■ Differenziell - Protokolle sichern ■ Inkrementell – Protokolle sichern (Protokolle kürzen)
Virtuelle Computer	<p>Erstes vollständiges:</p> <ul style="list-style-type: none"> ■ Vollständig - Virtuelle Computer sichern <p>Zusätzliche Backup-Methoden für virtuelle Computer:</p> <ul style="list-style-type: none"> ■ Vollständig - Virtuelle Computer sichern ■ Differenziell - Änderungen am virtuellen Computer seit letztem vollständigen Backup sichern ■ Inkrementell - Änderungen am virtuellen Computer seit letztem vollständigen oder inkrementellen Backup sichern
Microsoft SharePoint	<p>Erstes vollständiges:</p> <ul style="list-style-type: none"> ■ Vollständig - Datenbanken sichern ■ Vollständige Kopie - Datenbanken (Kopie) sichern <p>Zusätzliche Backup-Methoden für Microsoft SharePoint:</p> <ul style="list-style-type: none"> ■ Vollständig - Datenbanken sichern ■ Vollständige Kopie - Datenbanken (Kopie) sichern ■ Differenziell - Nur seit dem letzten vollständigen Backup vorgenommene Datenbankänderungen sichern ■ Differenziell (Blockebene) - Änderungen an der Datenbank seit dem letzten vollständigen Backup sichern - zusammen mit Auftrag zum Konvertieren in virtuellen Computer ■ Inkrementell (Blockebene): Änderungen an der Datenbank seit dem letzten vollständigen oder inkrementellen Backup sichern - zusammen mit Auftrag zum Konvertieren in virtuellen Computer ■ Protokoll - Transaktionsprotokoll sichern und kürzen

Datentyp	Auftragstyp und Backup-Methode
Microsoft SQL	<p>Erstes vollständiges:</p> <ul style="list-style-type: none"> ■ Vollständig - Datenbanken sichern ■ Vollständige Kopie - Datenbanken (Kopie) sichern <p>Zusätzliche Backup-Methoden für Microsoft SQL:</p> <ul style="list-style-type: none"> ■ Vollständig - Datenbanken sichern ■ Vollständige Kopie - Datenbanken (Kopie) sichern ■ Automatisch: Transaktionsprotokoll sichern, wenn aktiviert und dann Datenbankänderungen seit dem letzten vollständigen oder inkrementellen Backup sichern ■ Protokoll - Transaktionsprotokoll sichern und kürzen ■ Protokoll nicht kürzen - Sichern ohne Kürzen des Transaktionsprotokolls ■ Differenziell - Nur seit dem letzten vollständigen Backup vorgenommene Datenbankänderungen sichern ■ Differenziell (Blockebene) - Änderungen an der Datenbank seit dem letzten vollständigen Backup sichern - zusammen mit Auftrag zum Konvertieren in virtuellen Computer ■ Inkrementell (Blockebene): Änderungen an der Datenbank seit dem letzten vollständigen oder inkrementellen Backup sichern - zusammen mit Auftrag zum Konvertieren in virtuellen Computer ■ Datenbank-Snapshot - schreibgeschützte Zeitpunktkopie von Datenbanken

Datentyp	Auftragstyp und Backup-Methode
NDMP (alle)	<p>Erstes vollständiges:</p> <ul style="list-style-type: none"> ■ Stufe 0 - Vollständiges Backup <p>Zusätzliche Backup-Methoden für NDMP:</p> <ul style="list-style-type: none"> ■ Stufe 0 - Vollständiges Backup ■ Stufe 1 - Inkrementell (sichert neue oder seit letztem Backup der Stufe 0 geänderte Dateien) ■ Stufe 2 - Inkrementell (sichert neue oder seit letztem Backup der Stufe 1 geänderte Dateien) ■ Stufe 3 - Inkrementell (sichert neue oder seit letztem Backup der Stufe 2 geänderte Dateien) ■ Stufe 4 - Inkrementell (sichert neue oder seit letztem Backup der Stufe 3 geänderte Dateien) ■ Stufe 5 - Inkrementell (sichert neue oder seit letztem Backup der Stufe 4 geänderte Dateien) ■ Stufe 6 - Inkrementell (sichert neue oder seit letztem Backup der Stufe 5 geänderte Dateien) ■ Stufe 7 - Inkrementell (sichert neue oder seit letztem Backup der Stufe 6 geänderte Dateien) ■ Stufe 8 - Inkrementell (sichert neue oder seit letztem Backup der Stufe 7 geänderte Dateien) ■ Stufe 9 - Inkrementell (sichert neue oder seit letztem Backup der Stufe 8 geänderte Dateien)
Oracle	<p>Erstes vollständiges:</p> <ul style="list-style-type: none"> ■ Vollständig - Backup-Auswahl <p>Zusätzliche Backup-Methoden für Oracle:</p> <ul style="list-style-type: none"> ■ Vollständig - Backup-Auswahl ■ Differentiell - Änderungen seit dem letzten vollständigen Backup sichern ■ Inkrementell - Änderungen seit letztem vollständigen oder inkrementellen Backup sichern

Konfigurieren von Backup-Methoden für Backup-Aufträge

Wenn Sie eine Backup-Definition erstellen, müssen Sie Backup-Methoden für jeden Backup-Auftrag auswählen. Die Backup-Methode bestimmt, welche Daten Backup Exec sichert. Die standarmäßigen Backup-Methoden sind Vollständig, Inkrementell

und Differenzial. Sie können jedoch auch bestimmte Backup-Methoden für einige Agents oder Datentypen auswählen.

Siehe ["Backup-Methoden in Backup Exec"](#) auf Seite 205.

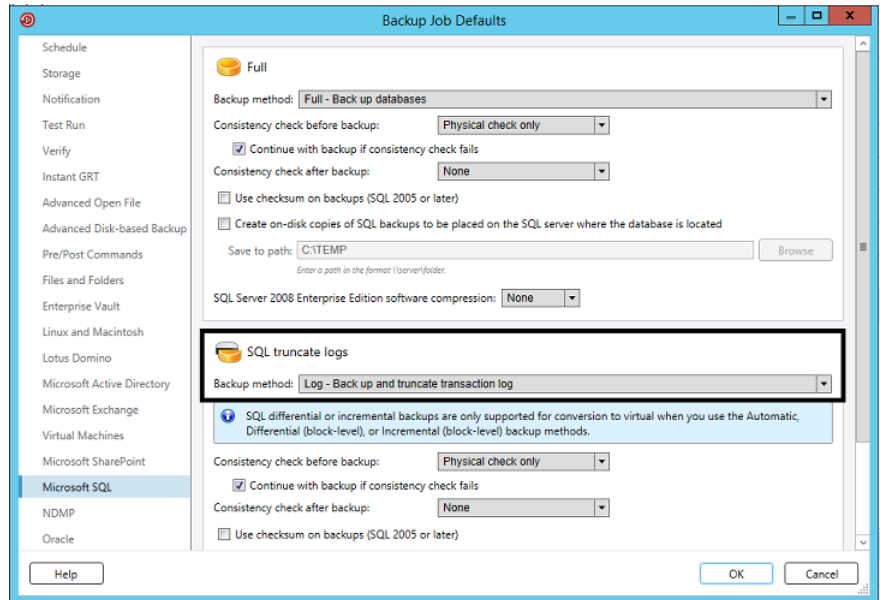
Standardmäßig enthält jede Backup-Definition einen Backup-Auftrag mit einer vollständigen Backup-Methode, die nicht geändert werden kann, sowie einen Backup-Auftrag mit einer inkrementellen Backup-Methode. Sie können den inkrementellen Auftrag durch einen Differenzial-Auftrag ersetzen, zusätzliche inkrementelle- oder Differenzial-Backup-Aufträge hinzufügen, oder die Backup-Methoden zu Daten-spezifischen Backup-Methoden für bestimmte Datentypen ändern. Jede Backup-Methode kann einen eindeutigen Namen erhalten, damit sie leichter zu identifizieren ist.

So konfigurieren Sie Backup-Methoden für Backup-Aufträge

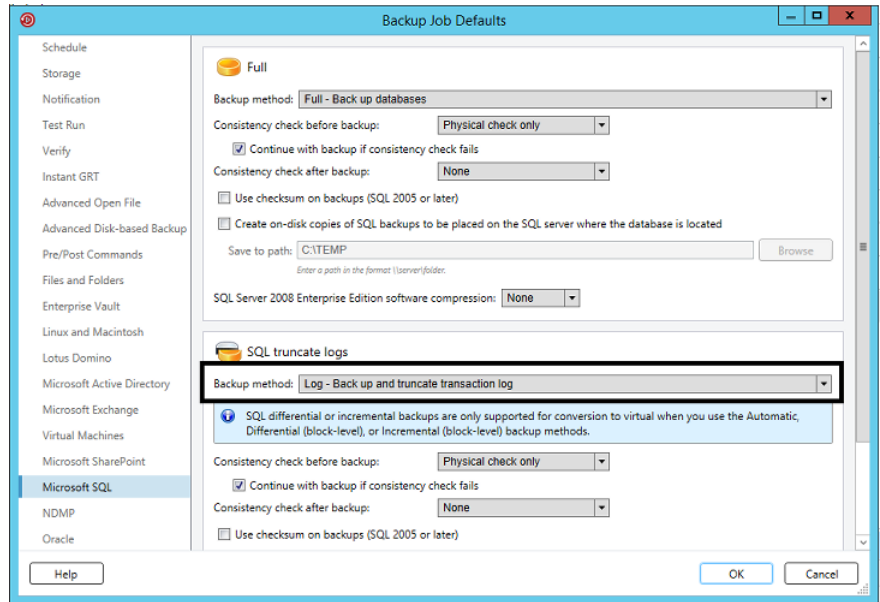
- 1** Erstellen oder bearbeiten Sie eine Definition.
- 2** Klicken Sie im Dialogfeld "Backup" auf "Bearbeiten".
- 3** Klicken Sie im linken Teilfenster auf "Planen".
- 4** (Optional) Um zusätzliche Backup-Aufträge der Backup-Definition hinzuzufügen, gehen Sie wie folgt vor:
 - Klicken Sie auf "Backup-Auftrag hinzufügen".
 - Wählen Sie die Backup-Methode aus, die Sie für den neuen Backup-Auftrag verwenden möchten.

Hinweis: Sie können die Backup-Methode später für bestimmte Agents und Typen zu einer Daten-spezifischen Methode ändern.

- 5 Geben Sie einen Namen für jeden Backup-Auftrag, für den Sie eine Backup-Methode konfigurieren möchten, in das Feld "Auftragsvorlagenname" ein.



- 6 (Optional) Um eine der Backup-Methoden zu ändern, für die Sie eine Daten-spezifische Backup-Methode ausgewählt haben, gehen Sie wie folgt vor:
- Wählen Sie im linken Teilfenster den Agent oder Datentyp, für den Sie eine Daten-spezifische Backup-Methode konfigurieren möchten. Wenn Sie beispielsweise eine Daten-spezifische Backup-Methode für SQL-Daten auswählen möchten, wählen Sie "Microsoft SQL" aus.
 - Wählen Sie im Feld "Backup-Methode" die Daten-spezifische Backup-Methode für jeden anwendbaren Backup-Auftrag aus.



7 Klicken Sie auf "OK".

Ermittlung des Backup-Status von Dateien in Backup Exec

Wenn Sie in Ihrer Backup-Strategie inkrementelle oder Differenzial-Backups verwenden, benötigt Backup Exec Informationen darüber, wann eine Datei geändert worden ist. Vollständige Backups umfassen alle Daten, die Sie für das Backup ausgewählt haben. Darauf folgende inkrementelle und Differenzial-Backups sichern nur neue Dateien und alle Dateien, die geändert wurden.

Wenn eine Datei erstellt oder geändert wird, wird diese Änderung im Dateisystem des Computers registriert und aufgezeichnet. Sie können die Methode angeben, anhand derer Backup Exec ermittelt, ob eine Datei beim Erstellen eines Backup-Auftrags in den Optionen unter "Dateien und Ordner" gesichert werden muss. Backup Exec verwendet bei der Erstellung oder Änderung einer Datei die von Ihnen festgelegte Methode.

Dieses Thema enthält folgende Informationen:

[Geänderte Uhrzeit](#)

[Archivbit](#)

Kataloge

Verwenden des Änderungslogs in Backup Exec, um zu ermitteln, welche Dateien geändert wurden

Auflösen von Änderungslogfehlern

Geänderte Uhrzeit

Wenn Backup Exec einen vollständigen oder inkrementellen Backup-Auftrag ausführt, wird die Startzeit des Backup-Auftrags in der Backup Exec-Datenbank aufgezeichnet. Backup Exec fügt den Zeitpunkt des Backup-Auftrags nur dann der Backup Exec-Datenbank hinzu, wenn der vollständige Backup-Auftrag erfolgreich abgeschlossen wird. Beim nächsten inkrementellen oder Differenzial-Backup-Auftrag vergleicht Backup Exec die Dateisystemzeit mit der Backup-Zeit. Wenn die Dateisystemzeit einen späteren als den in der Datenbank aufgezeichneten Zeitpunkt angibt, wird die Datei gesichert. Wenn das Änderungsdatum der Datei älter als das Änderungsdatum des vorherigen Backups ist, wird diese Datei nicht gesichert. Wird der Auftrag nicht erfolgreich abgeschlossen, werden bei folgenden inkrementellen oder Differenzial-Backup-Aufträgen sämtliche Daten anstatt nur der geänderten Daten gesichert.

Hinweis: Das Datum und der Zeitstempel der letzten Änderung ändern sich nicht, wenn die Datei kopiert oder verschoben wird. Um sicherzustellen, dass die Dateien geschützt sind, führen Sie nach dem Kopieren oder Verschieben der Dateien ein vollständiges Backup aus.

Wenn Sie einen inkrementellen Backup-Auftrag ausführen, zeichnet Backup Exec eine neue Zeit in der Backup Exec-Datenbank auf. Die Datenbankzeit wird bei Differenzial-Backup-Aufträgen nicht aktualisiert.

Wenn Sie die Methode "Geänderte Uhrzeit" auswählen, verwendet Backup Exec das Windows-Änderungslog, um zu ermitteln, ob eine Datei seit ihrer letzten Sicherung geändert wurde. Wenn das Änderungslog nicht verfügbar ist, vergleicht Backup Exec die Dateiinformationen mit der vorherigen Backup-Zeit, um zu ermitteln, ob die Datei geändert wurde.

Bei Verwendung der Methode "Geänderte Uhrzeit" kann Backup Exec präzisere inkrementelle oder Differenzial-Backups ausführen, selbst wenn andere Vorgänge Archivbits von geänderten Dateien haben.

Archivbit

Backup Exec verwendet das Archivbit des Dateisystems, um zu ermitteln, ob eine Datei seit ihrer letzten Sicherung geändert wurde.

Verwenden Sie das Archivbit, setzt Backup Exec das Archivbit zurück, wenn eine Datei gesichert wird. Durch das Zurücksetzen wird Backup Exec angezeigt, dass die Datei gesichert wurde. Wenn die Datei vor dem nächsten Backup wieder geändert wird, wird das Bit wieder aktiviert. Backup Exec sichert die Datei im nächsten Backup.

Wenn der nächste Backup-Auftrag ein vollständiger oder ein inkrementeller Backup-Auftrag ist, wird das Bit bei Abschluss des Backup-Auftrags deaktiviert. Wenn der nächste Backup-Auftrag ein Differenzial-Backup-Auftrag ist, bleibt das Archivbit intakt.

Kataloge

Backup Exec vergleicht Pfadnamen, Änderungszeit, gelöschte und umbenannte Dateien und Ordner sowie andere Attribute. Wenn Sie die Katalog-Methode auswählen, verwendet Backup Exec das Windows-Änderungsjournal, um zu ermitteln, ob eine Datei seit ihrer letzten Sicherung geändert wurde. Wenn das Änderungsjournal nicht verfügbar ist, vergleicht Backup Exec die Dateiinformatoren mit vorherigen Katalogen, um festzustellen, ob eine Änderung stattgefunden hat.

Die Katalog-Methode ist nur dann verfügbar, wenn Advanced Disk-based Backup Feature (ADBO) installiert ist.

Hinweis: Die Offhost-Backup-Funktion von ADBO unterstützt die Katalogmethode nicht.

Siehe "[Konfigurieren von Datei- und Ordneroptionen für Backup-Aufträge](#)" auf Seite 676.

Verwenden des Änderungslogs in Backup Exec, um zu ermitteln, welche Dateien geändert wurden

Wenn Sie die Backup-Methode "Geänderte Uhrzeit" oder "Katalog" für Dateien wählen, verwendet Backup Exec das USN-Änderungsjournal (Update Sequence Number). Backup Exec scannt das Änderungsjournal, um eine Liste der zu sichernden geänderten Dateien zu erhalten, anstatt alle Dateien zu scannen. Die Verwendung des Änderungslogs verringert die Zeit, die Backup Exec für ein inkrementelles Backup oder ein Differenzial-Backup benötigt.

Bei den Backup-Methoden "Geänderte Uhrzeit" und "Katalog" kann die Verwendung des Änderungslogs nicht deaktiviert werden. Wenn das Änderungsjournal auf dem Datenträger noch nicht aktiviert ist, wird es von Backup Exec automatisch aktiviert. Der Datenträger muss Änderungslogs unterstützen. Beispielsweise werden Änderungslogs von NTFS- und ReFS-Datenträgern, nicht jedoch von FAT-Datenträgern unterstützt.

Wenn Backup Exec Änderungsjournale aktiviert, legt es die Standardeinstellungen für die Änderungsjournale wie in [Tabelle 4-6](#) gezeigt fest. Backup Exec ändert die Einstellungen für ein bereits vorhandenes Änderungsjournal nicht.

Tabelle 4-6 Von Backup Exec festgelegte Standardeinstellungen für Änderungsjournale

Datenträgergröße	Standardeinstellungen
128 GB oder größer	<ul style="list-style-type: none">■ Maximale Größe des Änderungsjournals: 32 MB■ Reservierungsdelta: 4 MB
Über 64 GB - 127 GB	<ul style="list-style-type: none">■ Maximale Größe des Änderungsjournals: 16 MB■ Reservierungsdelta: 2 MB
Über 4 GB - 63 GB	<ul style="list-style-type: none">■ Maximale Größe des Änderungsjournals: 8 MB■ Reservierungsdelta: 1 MB
4 GB oder kleiner	<ul style="list-style-type: none">■ Maximale Größe des Änderungsjournals: 1 MB■ Reservierungsdelta: 256 KB

Hinweis: Der Windows-Startdatenträger ist von Windows mit Standardwerten vorkonfiguriert.

Auflösen von Änderungsjournalfehlern

Wenn Fehler beim Änderungsjournal auftreten, verwendet Backup Exec die Backup-Methode "Geänderte Uhrzeit" oder "Katalog", ohne das Änderungsjournal zu verwenden.

Wenn Fehler beim Änderungsjournal auftreten, können Sie Folgendes versuchen:

- Wählen Sie die Backup-Methode "Archivbit verwenden" für Dateien.
- Wählen Sie eine Datei-Backup-Methode, die nicht verwendet wurde, als die Fehler beim Änderungsjournal auftraten. Beispiel: Wenn Sie die Methode "Geänderte Uhrzeit" ausgewählt hatten und Fehler beim Änderungsjournal auftraten, wählen Sie die Methode "Kataloge verwenden" und führen Sie das Backup erneut aus.
- Vergrößern Sie die Änderungsjournal-Datenbank.
Informationen zur Verwendung von fsutil zum Abfragen, Erstellen, Ändern oder Löschen des Änderungsjournals finden Sie in Ihrer Dokumentation von Microsoft.
- Vermeiden Sie die Verwendung des lokalen Backup Exec-Servers, um diesen selbst zu sichern, wenn der Backup Exec-Server auf dem Windows-Startdatenträger installiert ist. Verwenden Sie stattdessen einen Backup

Exec-Remote-Server zum Sichern des lokalen Servers oder installieren Sie den Backup Exec-Server auf einem Datenvolume.

Hinweis: Die Off-Host-Backup-Funktion von ADBO unterstützt die Katalog-Backup-Methode für Dateien nicht.

Konfigurieren von Backup Exec, um Dateien nach einem Backup automatisch zu löschen

Wenn Sie einen vollständigen Backup ausführen, können Sie die Dateien sichern und dann löschen. Mit der Option "Ausgewählte Dateien und Ordner nach erfolgreichem Backup löschen" können Sie auf dem Server durch Löschen von Dateien und Ordnern von dem Server, nachdem sie erfolgreich gesichert wurden, Speicherplatz freigeben. Backup Exec sichert die ausgewählten Daten, überprüft die Backup-Sätze und löscht dann die Daten vom Server. Sie können Dateien nur für vollständige Backups sichern und löschen.

Siehe ["Konfigurieren von Datei- und Ordneroptionen für Backup-Aufträge"](#) auf Seite 676.

Backup Exec führt nach dem Sichern der Daten eine Überprüfung durch. Schlägt diese Überprüfung fehl, wird der Auftrag beendet und eine entsprechende Benachrichtigung eingeblendet. Zeigen Sie im Falle eines Überprüfungsfehlers das Auftragsprotokoll an. Beheben Sie den Fehler, und wiederholen Sie den Auftrag. Nachdem die Daten gesichert und überprüft wurden, löscht Backup Exec die ausgewählten Daten. Das Auftragsprotokoll enthält eine Liste der gelöschten Daten.

Sie können die Auftragswiederaufnahme-Option für einen vollständigen Backup-Auftrag aktivieren, der die Option "Ausgewählte Dateien und Ordner nach erfolgreichem Backup löschen" verwendet. Wenn der Auftrag fehlschlägt und wieder aufgenommen wird, werden die Dateien nicht aus dem Quelldatenträger gelöscht, nachdem das Backup abgeschlossen ist.

So konfigurieren Sie Backup Exec, dass Dateien nach einem Backup automatisch gelöscht werden

1 Sie haben folgende Möglichkeiten:

So konfigurieren Sie Backup Exec, dass Dateien nach allen Backup-Aufträgen automatisch gelöscht werden

Führen Sie die folgenden Schritte durch:

- Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- Wählen Sie "Auftragsstandardeinstellungen" aus und wählen Sie dann den Backup-Typ aus, für den Sie Backup Exec so konfigurieren möchten, dass Dateien automatisch gelöscht werden.

So konfigurieren Sie Backup Exec, dass Dateien für bestimmte Backup-Aufträge automatisch gelöscht werden

Führen Sie die folgenden Schritte durch:

- Erstellen Sie eine neue Backup-Definition oder bearbeiten Sie eine vorhandene Backup-Definition.
- Klicken Sie im Dialogfeld "Backup" auf "Bearbeiten".

- 2 Im linken Teilfenster klicken Sie auf "Dateien und Ordner".
- 3 Wählen Sie "Ausgewählte Dateien und Ordner nach erfolgreichem Backup löschen".

Hinweis: Sie können angeben, dass Dateien und Ordner nur bei vollständigen Backups gelöscht werden.

- 4 Klicken Sie auf "OK".

Konfigurieren erweiterter Optionen für Backup-Aufträge

Sie können festlegen, wie Backup Exec mit Ihrem Netzwerk arbeitet. Backup Exec enthält globale Netzwerk- und Sicherheitseinstellungen, die für alle Aufträge gelten.

Siehe ["Netzwerk- und Sicherheitsoptionen für Backup Exec ändern"](#) auf Seite 713.

Sie können die globalen Netzwerkeinstellungen übergehen, wenn Sie Backup-Aufträge erstellen, wenn die globalen Einstellungen in einer bestimmten Instanz nicht zutreffen. Schließen Sie die Schritte in der folgenden Prozedur ab, um Netzwerkooptionen für einzelne Backup-Aufträge zu konfigurieren.

Hinweis: In CAS-Umgebungen gelten andere Netzwerkooptionen.

So konfigurieren Sie Netzwerkooptionen für Backup-Jobs

- Erstellen Sie eine neue Backup-Definition oder bearbeiten Sie eine vorhandene Backup-Definition.
- Klicken Sie im Dialogfeld "Backup" auf "Bearbeiten".
- Klicken Sie im linken Teilfenster auf "Netzwerk".
- Konfigurieren Sie folgende Optionen:

Netzwerkschnittstelle	Gibt den Namen der Netzwerkkarte an, die den Backup Exec-Server mit dem Netzwerk, das Sie für diesen Backup-Auftrag verwenden möchten, verbindet. Die Liste umfasst alle verfügbaren Netzwerkschnittstellen auf dem Backup Exec-Server.
Protokoll	<p>Gibt das Protokoll an, das Sie für diesen Backup-Auftrag verwenden möchten.</p> <p>Folgende Optionen sind verfügbar:</p> <ul style="list-style-type: none"> ■ Beliebiges verfügbares Protokoll verwenden ■ IPv4 ■ IPv6
Subnetz	Hier können Sie die 32-Bit-Nummer auswählen, die das Subnetz festlegt, zu dem die Netzwerkkarte gehört.
Einsatz von beliebigen verfügbaren Netzwerkschnittstellen, Subnetzen oder Protokollen für Backup Exec-Agents zulassen, die nicht an die oben genannten Netzwerkschnittstellen, Subnetze oder Protokolle gebunden sind	<p>Wählen Sie diese Option aus, damit Backup Exec jedes verfügbare Netzwerk nutzen kann, wenn das Remote-System, das Sie für Backup oder Wiederherstellung ausgewählt haben, nicht Teil des angegebenen Backup-Netzwerks ist.</p> <p>Wenn Sie diese Option nicht auswählen und das Remote-System nicht Teil des angegebenen Backup-Netzwerks ist, schlägt der Auftrag fehl. Backup Exec kann auf die Daten vom Remote-System nicht zugreifen.</p>
Schnittstellendetails	Klicken Sie auf diese Option, um die MAC-Adresse, den Adaptertyp, die Beschreibung, die IP-Adresse und die Subnetzpräfixe für die Schnittstelle anzuzeigen, die Sie für das Backup-Netzwerk auswählen.

Ausführen des nächsten geplanten Backup-Auftrags vor seiner geplanten Zeit

Zulassen, dass der verwaltete Backup Exec-Server eine beliebige Netzwerkschnittstelle für den Zugriff auf Backup Exec Agents verwendet

Wählen Sie diese Option, um zuzulassen, dass ein Auftrag eine beliebige Netzwerkschnittstelle zum Zugriff auf Backup Exec-Agents verwendet, wenn die ausgewählte Netzwerkschnittstelle nicht verfügbar ist. Durch das Aktivieren dieser Option kann der verwaltete Backup Exec-Server eine alternative Netzwerkschnittstelle verwenden, um alle wichtigen Backup-Aufträge auszuführen, die andernfalls fehlschlagen würden.

Diese Option ist nur verfügbar, wenn Central Admin Server Feature (CAS) installiert ist.

Siehe ["Infos zu Central Admin Server Feature"](#) auf Seite 1450.

5 Klicken Sie auf "OK".

Siehe ["Backup-Netzwerke"](#) auf Seite 711.

Ausführen des nächsten geplanten Backup-Auftrags vor seiner geplanten Zeit

Sie können den nächsten geplanten Backup-Auftrag in einer Backup-Definition jederzeit ausführen. Sie können z. B. einen geplanten Backup-Auftrag früher als vorgesehen ausführen, um sicherzustellen, dass wichtige Daten gesichert werden oder dass ein geplanter Auftrag erfolgreich abgeschlossen wird. Die vorzeitige Ausführung eines geplanten Backup-Auftrags wirkt sich nicht auf dessen normalen Zeitplan aus. Der Auftrag wird nach wie vor wie geplant ausgeführt.

So führen Sie den nächsten geplanten Backup-Auftrag aus

- 1** Auf der Registerkarte "Backup und Wiederherstellung" haben Sie folgende Möglichkeiten:
 - Um das nächste geplante Backup für die Backup-Aufträge eines einzelnen Servers auszuführen, klicken Sie mit der rechten Maustaste auf den Namen des Servers.
 - Um das nächste geplante Backup für die Backup-Aufträge mehrerer Server auszuführen, klicken Sie bei gedrückter Umschalt- oder Strg-Taste auf die

Servernamen und klicken Sie dann mit der rechten Maustaste auf einen der ausgewählten Server.

- 2 Klicken Sie auf "Nächstes Backup jetzt ausführen".
- 3 Klicken Sie auf "Ja", um zu bestätigen, dass Sie den Auftrag oder die Aufträge jetzt ausführen möchten.

Siehe ["Sichern von Daten"](#) auf Seite 174.

Bearbeiten von Backup-Definitionen

Sie können vorhandene Backup-Definitionen bearbeiten. Sie können die Backup-Auswahl jeder vorhandenen Backup-Definition oder die Backup-Auftragseinstellungen für sämtliche darin enthaltene Backup-Aufträge ändern. Die Backup-Auswahl umfasst alle Server, Datenträger oder Daten, die Sie für ein Backup ausgewählt haben. Die Einstellungen für Backup-Aufträge können beispielsweise Planungsoptionen, Optionen für Speichergeräte oder Backup-Methoden für ausgewählte Datentypen umfassen.

Sie können auch einer vorhandenen Backup-Definition eine Stufe hinzufügen, um die Backup-Daten zu kopieren oder virtuelle Computer mit den Backup-Daten herzustellen.

Siehe ["Hinzufügen einer Stufe zu einer Backup-Definition"](#) auf Seite 244.

Wenn Sie mehrere Backup-Definitionen auf einmal bearbeiten möchten, können Sie nur diejenigen Eigenschaften bearbeiten, die die Definitionen gemeinsam haben. Wenn Sie z. B. beschließen, zwei Backup-Definitionen zusammen zu bearbeiten, für diese Definitionen jedoch unterschiedliche Zeitpläne verwendet wurden, können Sie die Zeitpläne nicht bearbeiten. Wenn Sie die Einstellungen, die Sie bearbeiten möchten, nicht sehen, wiederholen Sie diesen Vorgang, wobei Sie jedoch nur eine Definition auf einmal auswählen.

Hinweis: Sie können eine Backup-Definition nicht bearbeiten, während einer ihrer Backup-Aufträge ausgeführt wird.

Dieses Thema umfasst die folgende Vorgehensweise:

[So bearbeiten Sie die Backup-Auswahl einer Backup-Definition oder wählen zu sichernde Benutzerfreigaben aus](#)

[So bearbeiten Sie die Auftragseinstellungen einer Backup-Definition](#)

So bearbeiten Sie die Backup-Auswahl einer Backup-Definition oder wählen zu sichernde Benutzerfreigaben aus

- 1 Sie haben folgende Möglichkeiten:

So bearbeiten Sie Backups auf der Registerkarte "Backup und Wiederherstellung"

Führen Sie die folgenden Schritte durch:

- Auf der Registerkarte "Backup und Wiederherstellung" haben Sie folgende Möglichkeiten:
 - Um Backups für einen einzelnen Server zu bearbeiten, klicken Sie mit der rechten Maustaste auf den Servernamen.
 - Um Backups für mehrere Server zu bearbeiten, klicken Sie bei gedrückter Umschalttaste oder Strg-Taste auf die Servernamen und klicken Sie dann mit der rechten Maustaste auf einen der ausgewählten Server.
- Klicken Sie auf "Backups bearbeiten".

Hinweis: Wenn der Server bzw. die Server, die Sie ausgewählt haben, über mehrere Backup-Definitionen verfügen, wählen Sie die zu bearbeitenden Definitionen im Dialogfeld "Backup-Auftrag-Auswahl" aus und klicken Sie anschließend auf "OK".

So bearbeiten Sie Backups auf der Registerkarte "Auftragsüberwachung"

Führen Sie die folgenden Schritte durch:

- Auf der Registerkarte "Auftragsüberwachung" führen Sie einen der folgenden Schritte aus:
 - Klicken Sie zum Bearbeiten eines einzelnen Backups mit der rechten Maustaste auf den Auftragsnamen.
 - Zum gleichzeitigen Bearbeiten mehrerer Backups wählen Sie die Auftragsnamen bei gedrückter Umschalt- bzw. Strg-Taste aus, und klicken Sie dann mit der rechten Maustaste auf einen der ausgewählten Aufträge.
- Klicken Sie auf "Bearbeiten".

So bearbeiten Sie Backups
auf der Registerkarte
"Speicher"

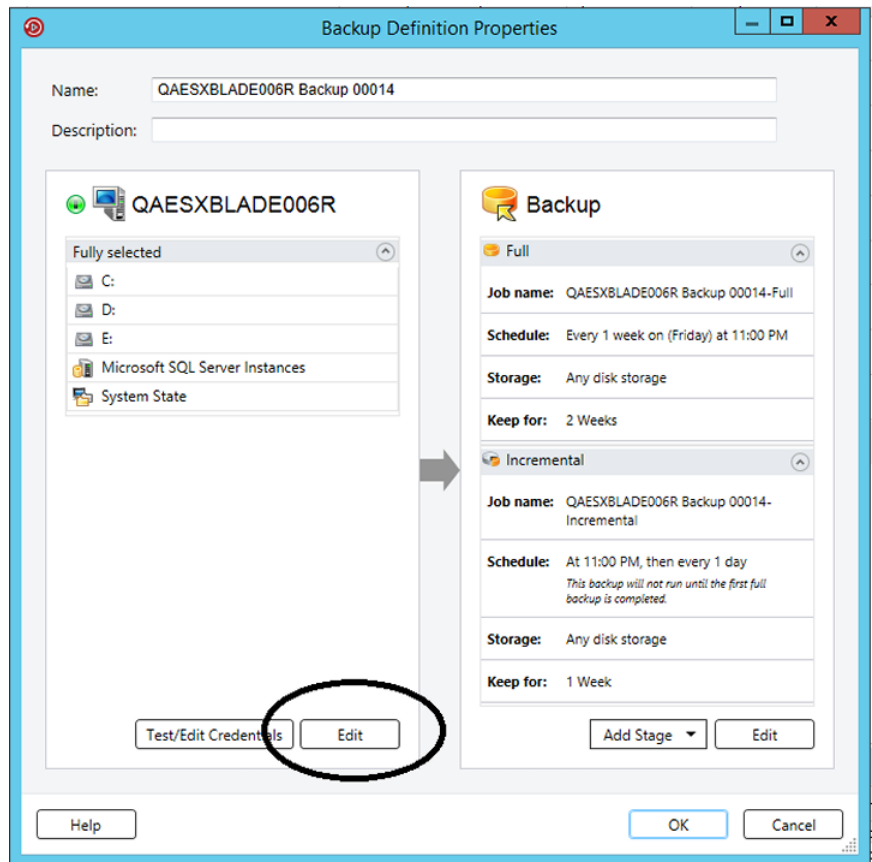
Führen Sie die folgenden Schritte durch:

- Doppelklicken Sie auf der Registerkarte "Speicher" auf das Speichergerät bzw. den Speicherpool, für das zu bearbeitende Backup.
- Führen Sie im Teilfenster "Auftragsverlauf" einen der folgenden Schritte aus:
 - Klicken Sie zum Bearbeiten eines einzelnen Backups mit der rechten Maustaste auf das Backup.
 - Zum Bearbeiten mehrerer Backups wählen Sie die Backups bei gedrückter Umschalt- bzw. Strg-Taste aus, und klicken Sie dann mit der rechten Maustaste auf eines der ausgewählten Backups.

Hinweis: Sie können nur jene Backup-Aufträge bearbeiten, die bereits über die Registerkarte "Speicher" ausgeführt wurden.

- Klicken Sie auf "Backup bearbeiten".

- 2 Klicken Sie im Dialogfeld "Auswahl" auf "Bearbeiten".



- 3 So fügen Sie der Backup-Definition zusätzliche Server hinzu
 - Klicken Sie auf die Schaltfläche "Hinzufügen (+)".
 - Wählen Sie die Server aus, die der Backup-Definition hinzugefügt werden sollen. Klicken Sie auf "Neuer Server", um Backup Exec einen neuen Server hinzuzufügen.
 - Klicken Sie auf "OK".

4 Wählen Sie die Daten aus, die Sie sichern möchten.

Server werden standardmäßig in ihrer Gesamtheit ausgewählt. Wenn Sie nicht den gesamten Server sichern möchten, doppelklicken Sie auf den Servernamen, um den gesamten Inhalt anzuzeigen. Wählen Sie die Kontrollkästchen für jedes Element aus, das Sie sichern möchten.

Hinweis: Das Aufheben der Auswahl für die kritischen Systemkomponenten eines Servers führt zu der Erstellung von Backup-Sätzen, die für einige Wiederherstellungszenarien nicht verwendet werden können.

Siehe ["Info zum Sichern von wichtigen Systemkomponenten"](#) auf Seite 200.

5 Klicken Sie auf "OK".

6 Wenn Sie die Backup-Definition konfiguriert haben, klicken Sie im Dialogfeld "Backup-Eigenschaften" auf "OK".

So bearbeiten Sie die Auftragseinstellungen einer Backup-Definition

1 Sie haben folgende Möglichkeiten:

So bearbeiten Sie Backups auf der Registerkarte "Backup und Wiederherstellung"

Führen Sie die folgenden Schritte durch:

- Auf der Registerkarte "Backup und Wiederherstellung" haben Sie folgende Möglichkeiten:
 - Um Backups für einen einzelnen Server zu bearbeiten, klicken Sie mit der rechten Maustaste auf den Servernamen.
 - Um Backups für mehrere Server zu bearbeiten, klicken Sie bei gedrückter Umschalttaste oder Strg-Taste auf die Servernamen und klicken Sie dann mit der rechten Maustaste auf einen der ausgewählten Server.
- Klicken Sie auf "Backups bearbeiten".

Hinweis: Wenn der Server bzw. die Server, die Sie ausgewählt haben, über mehrere Backup-Definitionen verfügen, wählen Sie die zu bearbeitenden Definitionen im Dialogfeld "Backup-Auftrag-Auswahl" aus und klicken Sie anschließend auf "OK".

So bearbeiten Sie Backups
auf der Registerkarte
"Auftragsüberwachung"

Führen Sie die folgenden Schritte durch:

- Auf der Registerkarte "Auftragsüberwachung" führen Sie einen der folgenden Schritte aus:
 - Klicken Sie zum Bearbeiten eines einzelnen Backups mit der rechten Maustaste auf den Auftragsnamen.
 - Zum gleichzeitigen Bearbeiten mehrerer Backups wählen Sie die Auftragsnamen bei gedrückter Umschalt- bzw. Strg-Taste aus, und klicken Sie dann mit der rechten Maustaste auf einen der ausgewählten Aufträge.
- Klicken Sie auf "Bearbeiten".

So bearbeiten Sie Backups
auf der Registerkarte
"Speicher"

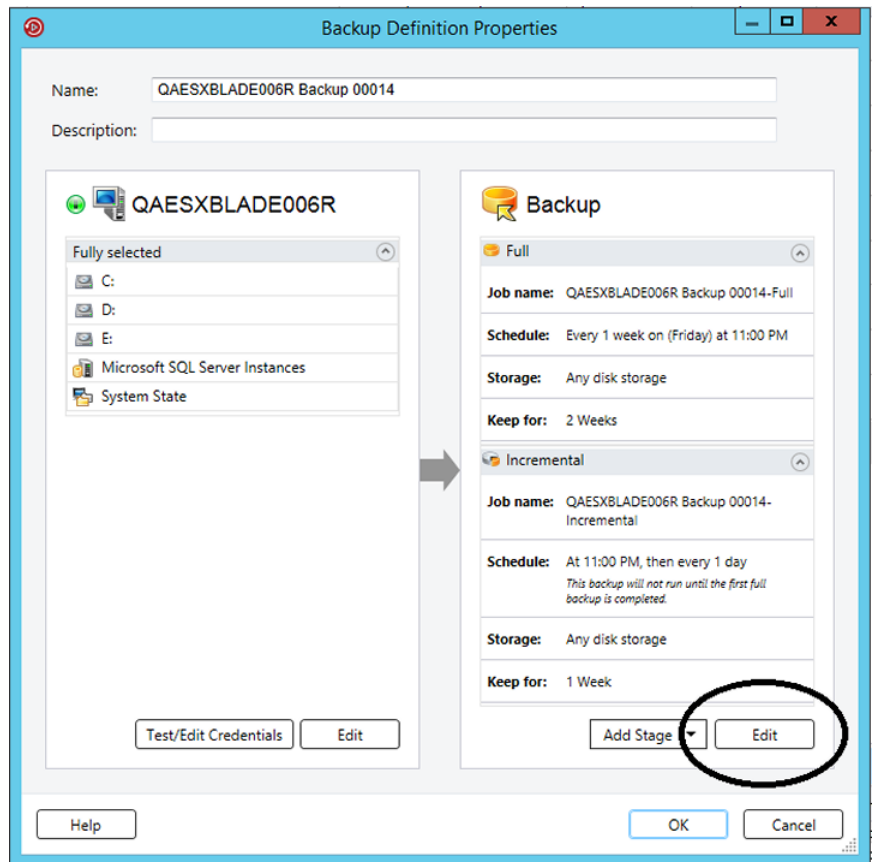
Führen Sie die folgenden Schritte durch:

- Doppelklicken Sie auf der Registerkarte "Speicher" auf das Speichergerät bzw. den Speicherpool, für das zu bearbeitende Backup.
- Führen Sie im Teilfenster "Auftragsverlauf" einen der folgenden Schritte aus:
 - Klicken Sie zum Bearbeiten eines einzelnen Backups mit der rechten Maustaste auf das Backup.
 - Zum Bearbeiten mehrerer Backups wählen Sie die Backups bei gedrückter Umschalt- bzw. Strg-Taste aus, und klicken Sie dann mit der rechten Maustaste auf eines der ausgewählten Backups.

Hinweis: Sie können nur jene Backup-Aufträge bearbeiten, die bereits über die Registerkarte "Speicher" ausgeführt wurden.

- Klicken Sie auf "Backup bearbeiten".

- 2 Klicken Sie im Dialogfeld "Backup" auf "Bearbeiten".



- 3 Wählen Sie im linken Teilfenster die zu ändernde Backup-Auftragseinstellung aus.
 Die Optionen hängen von den zu sichernden Elementen ab.
 - 4 Nehmen Sie die notwendigen Änderungen vor.
 - 5 Wenn Sie die gewünschten Optionen für das Backup ausgewählt haben, klicken Sie auf "OK".
 - 6 Wenn Sie die Backup-Definition konfiguriert haben, klicken Sie im Dialogfeld "Backup-Eigenschaften" auf "OK".
- Siehe ["Sichern von Daten"](#) auf Seite 174.

Prüfung der Identifikationsdaten für Backup-Quellen

Backup Exec listet die Backup-Quellen und die damit verbundenen Identifikationsdaten für alle Server auf, die Sie im Teilfenster "Identifikationsdaten" überwachen. Wenn Backup Exec nicht die korrekten Identifikationsdaten hat, um auf die Inhalte zuzugreifen, schlagen Versuche den Inhalt zu sichern, fehl.

Es wird empfohlen, dass Sie testen, ob Sie die passende Identifikationsdaten zum Zugreifen auf die zu sichernden Inhalte haben. Wenn der Test fehlschlägt, können Sie neue Identifikationsdaten für die Inhalte eingeben, damit Backup Exec darauf zugreifen kann.

Sie können die Identifikationsdaten, die mit einer Backup-Quelle verknüpft sind, jederzeit vom Teilfenster "Identifikationsdaten" aus prüfen. Sie können die Identifikationsdaten auch überprüfen, wenn Sie eine Backup-Definition erstellen.

Hinweis: Sie können Identifikationsdaten nicht für virtuelle Computer prüfen. Der Auftrag wird jedoch ausgeführt, wenn Sie die richtigen Identifikationsdaten angeben. Schlägt die Ausführung des Auftrags fehl, müssen Sie möglicherweise versuchen, den Auftrag mit anderen Identifikationsdaten auszuführen.

Sie haben folgende Möglichkeiten, um Identifikationsdaten für eine Backup-Quelle zu prüfen:

[Prüfen der Identifikationsdaten, die mit einer Backup-Quelle verknüpft sind](#)

[So testen Sie die Identifikationsdaten für alle Backup-Quellen in einer bestimmten Backup-Definition](#)

[So prüfen Sie die Identifikationsdaten für eine bestimmte Backup-Quelle in einer bestimmten Backup-Definition](#)

Prüfen der Identifikationsdaten, die mit einer Backup-Quelle verknüpft sind

- 1 Doppelklicken Sie auf der Registerkarte "Backup und Wiederherstellung" auf den Server, dessen Identifikationsdaten Sie prüfen möchten.
- 2 Klicken Sie im linken Teilfenster auf "Identifikationsdaten".
- 3 Wählen Sie die Backup-Quelle aus, die Sie prüfen möchten.
- 4 Klicken Sie in der Gruppe "Identifikationsdaten" auf "Identifikationsdaten testen".

Im Feld "Status der Identifikationsdaten" werden die Ergebnisse des Tests angezeigt.

So testen Sie die Identifikationsdaten für alle Backup-Quellen in einer bestimmten Backup-Definition

- 1 Erstellen Sie ein neues Backup oder bearbeiten Sie ein vorhandenes.
- 2 Klicken Sie im Dialogfeld "Auswahl" auf "Identifikationsdaten testen/bearbeiten".
- 3 Klicken Sie auf "Alle Identifikationsdaten testen".

Im Feld "Status der Identifikationsdaten" werden die Ergebnisse des Tests angezeigt.

- 4 Klicken Sie auf "OK".

So prüfen Sie die Identifikationsdaten für eine bestimmte Backup-Quelle in einer bestimmten Backup-Definition

- 1 Erstellen Sie ein neues Backup oder bearbeiten Sie ein vorhandenes.
- 2 Klicken Sie im Dialogfeld "Auswahl" auf "Identifikationsdaten testen/bearbeiten".
- 3 Wählen Sie die Backup-Quelle aus.
- 4 Klicken Sie auf "Ausgewählte Identifikationsdaten testen".

Im Feld "Status der Identifikationsdaten" werden die Ergebnisse des Tests angezeigt.

- 5 Klicken Sie auf "OK".

Siehe ["Ersetzen der Identifikationsdaten für eine Backup-Quelle"](#) auf Seite 235.

Siehe ["Erstellen neuer Identifikationsdaten für eine Backup-Quelle"](#) auf Seite 236.

Siehe ["Löschen ausrangierter oder nicht genutzter Backup-Quellen aus dem Teilfenster "Identifikationsdaten""](#) auf Seite 238.

Ersetzen der Identifikationsdaten für eine Backup-Quelle

Backup Exec listet die Backup-Quellen und die damit verbundenen Identifikationsdaten für alle Server auf, die Sie im Teilfenster "Identifikationsdaten" überwachen. Wenn Backup Exec nicht die korrekten Identifikationsdaten hat, um auf die Inhalte zuzugreifen, schlagen Versuche den Inhalt zu sichern, fehl.

Es wird empfohlen, dass Sie testen, ob Sie die passende Identifikationsdaten zum Zugreifen auf die zu sichernden Inhalte haben. Wenn der Test fehlschlägt, können Sie neue Identifikationsdaten für die Inhalte eingeben, damit Backup Exec darauf zugreifen kann. Wenn Sie die Identifikationsdaten ändern müssen, die mit einer Backup-Quelle verknüpft sind, können Sie dies jederzeit auf der Registerkarte "Backup und Wiederherstellung" im Teilfenster "Identifikationsdaten" tun. Sie können

die Identifikationsdaten einer Backup-Quelle auch ändern, wenn Sie Backups erstellen oder bearbeiten.

So ersetzen Sie die Identifikationsdaten für eine Backup-Quelle

- ◆ Sie haben folgende Möglichkeiten:

So ersetzen Sie das Login-Konto, das mit einer Backup-Quelle im Teilfenster "Identifikationsdaten" verknüpft ist

Führen Sie die folgenden Schritte durch:

- Doppelklicken Sie auf der Registerkarte "Backup und Wiederherstellung" auf den Server, dessen Identifikationsdaten Sie anzeigen möchten.
- Klicken Sie im linken Teilfenster auf "Identifikationsdaten".
- Wählen Sie im Feld "Login-Konto" das Login-Konto aus, das Sie für die Backup-Quelle verwenden möchten.
- Klicken Sie auf "Übernehmen".

So ersetzen Sie das Login-Konto an, das mit einer Backup-Quelle in einer Backup-Definition verbunden ist

Führen Sie die folgenden Schritte durch:

- Erstellen Sie ein neues Backup oder bearbeiten Sie ein vorhandenes.
- Klicken Sie im Dialogfeld "Auswahl" auf "Identifikationsdaten testen/bearbeiten".
- Wählen Sie im Feld "Login-Konto" das Login-Konto aus, das Sie für die Backup-Quelle verwenden möchten.
- Klicken Sie auf "OK".

Siehe ["Prüfung der Identifikationsdaten für Backup-Quellen"](#) auf Seite 234.

Siehe ["Erstellen neuer Identifikationsdaten für eine Backup-Quelle"](#) auf Seite 236.

Siehe ["Löschen ausrangierter oder nicht genutzter Backup-Quellen aus dem Teilfenster "Identifikationsdaten""](#) auf Seite 238.

Erstellen neuer Identifikationsdaten für eine Backup-Quelle

Backup Exec listet die Backup-Quellen und ihre verbundenen Identifikationsdaten für alle Server auf, die Sie im Teilfenster "Identifikationsdaten" überwachen. Wenn Backup Exec nicht die korrekten Bescheinigungen hat, um auf des Inhalts zuzugreifen, beliebige Versuche zu unterstützen dass Inhaltsausfallung.

Wenn die Bescheinigungen für eine Backup-Quelle ändern, müssen Sie die neuen Bescheinigungen in Backup Exec anmelden und sie mit der Backup-Quelle verbinden. Sie können jederzeit neue Identifikationsdaten für eine Backup-Quelle vom Teilfenster "Identifikationsdaten" aus prüfen. Sie können neue Bescheinigungen für eine Backup-Quelle auch herstellen, wenn Sie Backup-Definitionen erstellen oder bearbeiten.

Erstellen neuer Identifikationsdaten für eine Backup-Quelle

1 Sie haben folgende Möglichkeiten:

Erstellen neuer Identifikationsdaten für eine Backup-Quelle im Teilfenster "Identifikationsdaten"

Führen Sie die folgenden Schritte durch:

- Doppelklicken Sie auf der Registerkarte "Backup und Wiederherstellung" auf den Server, für den Sie neue Identifikationsdaten erstellen möchten.
- Klicken Sie im linken Teilfenster auf "Identifikationsdaten".

Erstellen neuer Identifikationsdaten für eine Backup-Quelle in einer Backup-Definition

Führen Sie die folgenden Schritte durch:

- Erstellen Sie ein neues Backup oder bearbeiten Sie ein vorhandenes.
- Klicken Sie im Dialogfeld "Auswahl" auf "Identifikationsdaten testen/bearbeiten".

- 2 Wählen Sie Sie im Feld "Login-Konto" neben der Backup-Quelle auf "Neues Login-Konto" aus.
- 3 Geben Sie im Feld "Benutzername" den Benutzernamen für das neue Login-Konto ein.
- 4 Geben Sie im Feld "Kennwort" das Kennwort für das neue Login-Konto ein.
- 5 Geben Sie im Feld "Kennwort bestätigen" das Kennwort erneut ein, um es zu bestätigen.
- 6 Geben Sie im Feld "Kontoname" einen eindeutigen Namen für das neue Login-Konto ein.
- 7 Geben Sie im Feld "Notizen" ein, wie das Backup Exec-Login-Konto verwendet werden soll.
- 8 Wählen Sie die Option "Dies ist ein eingeschränktes Login-Konto", wenn das Backup Exec-Login-Konto nur vom Besitzer des Login-Kontos, und denen, die das Kennwort kennen, genutzt werden soll.

Wenn diese Option nicht ausgewählt ist, wird das Backup Exec-Login-Konto als gemeinsames Konto erstellt. Alle Benutzer können auf gemeinsam genutzte Konten zugreifen.

- 9 Aktivieren Sie "Dies ist mein Standardkonto", wenn Sie dieses Backup Exec-Login-Konto zum Durchsuchen, Auswählen oder Wiederherstellen von Daten auf lokalen und Remote-Computern verwenden möchten.

- 10 Klicken Sie auf "OK".

Siehe ["Prüfung der Identifikationsdaten für Backup-Quellen"](#) auf Seite 234.

Siehe ["Ersetzen der Identifikationsdaten für eine Backup-Quelle"](#) auf Seite 235.

Siehe ["Löschen ausrangierter oder nicht genutzter Backup-Quellen aus dem Teilfenster "Identifikationsdaten""](#) auf Seite 238.

Löschen ausrangierter oder nicht genutzter Backup-Quellen aus dem Teilfenster "Identifikationsdaten"

Backup Exec listet die Backup-Quellen und die damit verbundenen Identifikationsdaten für alle Server auf, die Sie im Teilfenster "Identifikationsdaten" überwachen. Wenn Sie eine der Backup-Quellen aus Ihrer Umgebung entfernen, wird sie weiterhin in der Liste der Backup-Quellen im Teilfenster "Identifikationsdaten" angezeigt. Sie können ausrangierte oder ungenutzte Backup-Quellen aus dem Teilfenster löschen, um das Verwalten zu vereinfachen. Backup Exec durchsucht und erkennt Ressourcen während des Normalbetriebs. Wenn die gelöschte Backup-Quelle noch in Ihrer Umgebung existiert, fügt Backup Exec sie der Liste der Ressourcen hinzu, wenn Sie das nächste Mal erkannt wird. Sie sollten Backup-Quellen aus dem Teilfenster "Identifikationsdaten" nur löschen, wenn sie nicht mehr in Ihrer Umgebung existieren.

So löschen Sie die ausrangierten oder ungenutzten Backup-Quellen aus dem Teilfenster "Identifikationsdaten"

- 1 Auf der Registerkarte "Backup und Wiederherstellung" doppelklicken Sie auf den Server, der die Backup-Quelle enthält, die Sie aus dem Teilfenster "Identifikationsdaten" löschen möchten.
- 2 Klicken Sie im linken Teilfenster auf "Identifikationsdaten".

- 3 Wählen Sie die Backup-Quelle aus, die Sie aus dem Teilfenster "Identifikationsdaten" löschen möchten.
- 4 Klicken Sie auf in der Gruppe "Identifikationsdaten" auf "Ausgewählte Ressource löschen".

Backup Exec entfernt die Backup-Quelle aus der Liste.

Hinweis: Wenn Sie versuchen, eine Backup-Quelle zu löschen, die in einer Backup-Definition verwendet wird, löscht Backup Exec diese Backup-Quelle nicht. Wenn Sie eine Backup-Quelle löschen, die noch in Ihrer Umgebung existiert, fügt Backup Exec diese Backup-Quelle wieder in die Liste ein, wenn Sie Ihre Umgebung das nächste Mal durchsuchen.

Siehe ["Prüfung der Identifikationsdaten für Backup-Quellen"](#) auf Seite 234.

Siehe ["Ersetzen der Identifikationsdaten für eine Backup-Quelle"](#) auf Seite 235.

Siehe ["Erstellen neuer Identifikationsdaten für eine Backup-Quelle"](#) auf Seite 236.

Wie die Joborganisation in Backup Exec arbeitet

Mit Backup Exec können Sie Zeitpunkt und Häufigkeit für Backup-Aufträge konfigurieren. Sie können Aufträge sofort, einmalig an einem bestimmten Tag und zu einer bestimmten Uhrzeit oder mehrmals gemäß einem Zeitplan ausführen. Mit Backup Exec können Sie ein Wiederholungsmuster für den Zeitplan mit Minuten, Stunden, Tagen, Wochen, Monaten oder Jahren als Messeinheit erstellen. Alternativ können Sie bestimmte Tage im Monat auswählen, um einen wiederkehrenden Zeitplan zu erstellen, nach dem Aufträge ausgeführt werden sollen.

Dieses Thema enthält folgende Informationen:

[Verfügbarkeitszeiträumen](#)

[Schedulingkonflikte](#)

[Daten einschließen und ausschließen](#)

Verfügbarkeitszeiträumen

Backup Exec bietet zusätzliche Zeitplanoptionen, mit denen Sie sicherstellen können, dass der Auftrag nicht außerhalb Ihres Verfügbarkeitszeitrahmens ausgeführt wird. Das Verfügbarkeitszeitrahmen ist der Zeitraum, in dem Ihre Backup-Quellen gesichert werden können. Sie können konfigurieren, wie lange ein unvollständiger Auftrag geplant bleiben soll, bevor Backup Exec den Auftrag neu plant und den Abschlussstatus in "Verpasst" ändert. Sie können auch festlegen, dass der Auftrag automatisch abgebrochen wird, wenn er zu lange nach seiner geplanten Startzeit

ausgeführt wird. Mit diesen Optionen können Sie sicherstellen, dass Ihre Systemressourcen in kritischen Zeiträumen nicht von Backup-Aufträgen beeinträchtigt werden.

Siehe ["Konfigurieren von Zeitplänen für Backup-Jobs"](#) auf Seite 635.

Schedulungskonflikte

Backup Exec löst Planungskonflikte zwischen zwei Backup-Aufträgen, indem es den weniger häufigen Auftrag ausführt und den häufigeren Auftrag überspringt. Wenn ein vollständiges Backup und ein inkrementelle bzw. Differenzial-Backup gleichzeitig ausgeführt werden sollen, führt Backup Exec das vollständige Backup aus. Das inkrementelle bzw. Differenzial-Backup wird übersprungen und zum nächsten geplanten Zeitpunkt ausgeführt. Vollständige Backups haben immer Vorrang vor inkrementellen und Differenzial-Backups. Wenn zwei Backup-Aufträge des gleichen Typs zum gleichen Zeitpunkt geplant sind, führt Backup Exec den weniger häufig geplanten Auftrag aus. Der häufiger geplante Auftrag wird übersprungen. Der übersprungene Backup-Auftrag wird zum nächsten geplanten Zeitpunkt ausgeführt. Beispiel: Wenn ein monatlicher Auftrag und ein täglicher Auftrag gleichzeitig geplant sind, führt Backup Exec den monatlichen Auftrag aus. Der tägliche Auftrag wird am folgenden Tag entsprechend des normalen Zeitplans ausgeführt.

Daten einschließen und ausschließen

Mithilfe der Option "Auszuschließende Tage" können Sie bestimmte Daten von Ihrem Zeitplan ausschließen. Beispielsweise können Sie Feiertage von Ihrem normalen Backup-Zeitplan ausschließen.

Mit der Option "Daten einschließen" können Sie Daten in den Backup-Zeitplan einzuschließen. Wenn Sie ein Datum in den Backup-Zeitplan einschließen, wird der Backup-Auftrag an diesem Datum ausgeführt, selbst wenn er nicht normalerweise an diesem Datum geplant ist. Sie können mit einem eingeschlossenen Datum eine zusätzliche Ausführung eines Backup-Auftrags außerhalb seines normalen Zeitplans planen.

Siehe ["Durchführung von Backup-Aufträgen zu einem bestimmten Datum verhindern"](#) auf Seite 242.

Siehe ["Einschließlich ein spezifisches Datum im Zeitplan für einen Backup-Auftrag"](#) auf Seite 240.

Einschließlich ein spezifisches Datum im Zeitplan für einen Backup-Auftrag

Sie können bestimmte Tage in den Backup-Zeitplan für einen Backup-Auftrag einschließen. Wenn Sie ein Datum in den Backup-Zeitplan einschließen, wird der

Backup-Auftrag an diesem Datum ausgeführt, selbst wenn er nicht normalerweise an diesem Datum geplant ist. Sie können mit einem eingeschlossenen Datum eine zusätzliche Ausführung eines Backup-Auftrags außerhalb seines normalen Zeitplans planen. Das Planen eines zusätzlichen Datums hat keinen Einfluss auf den normalen Zeitplan eines Backup-Auftrags.

Hinweis: Eingeschlossene Daten werden vor den ausgeschlossenen Daten auf die Auftragsplanung angewendet. Wenn alle ausgeschlossenen Daten angewandt sind, überschreiben sie möglicherweise die eingeschlossenen Daten, wenn es Konflikte gibt. Wenn Sie das gleiche Datum sowohl als eingeschlossenes als auch als ausgeschlossenes Datum auswählen, schließt Backup Exec das Datum von Ihrem Backup-Zeitplan aus.

Siehe ["Durchführung von Backup-Aufträgen zu einem bestimmten Datum verhindern"](#) auf Seite 242.

So schließen Sie ein bestimmtes Datum in den Zeitplan für einen Backup-Auftrag ein

- 1 Erstellen oder bearbeiten Sie eine Definition.
- 2 Klicken Sie im Dialogfeld "Backup" auf "Bearbeiten".
- 3 Klicken Sie im linken Teilfenster auf "Planen".
- 4 Klicken Sie für den Auftrag, in den Sie ein Datum einschließen möchten, auf das Feld "Wiederkehrend".
- 5 Klicken Sie auf die Registerkarte "Daten ein-/ausschließen" und dann auf "Daten einschließen".
- 6 Sie haben folgende Möglichkeiten:

So geben Sie das Datum
manuell ein

Führen Sie die folgenden Schritte durch:

- Geben Sie im Feld "Datum auswählen" das Datum ein, das Sie in dem Backup-Zeitplan einschließen möchten.
- Klicken Sie auf "Hinzufügen".

Hinweis: Sie können nur ein Datum auf einmal hinzufügen.

So wählen Sie das Datum im Kalender Klicken Sie auf das Datum, das Sie in den Backup-Zeitplan einschließen möchten.

Der Kalender zeigt 3 Monate auf einmal an. Sie können vorwärts oder rückwärts navigieren und zusätzliche Monate ansehen, indem Sie die Pfeile anklicken.

Hinweis: Sie können immer nur ein Datum auf einmal auswählen.

7 Klicken Sie auf "OK".

Siehe ["Wie die Joborganisation in Backup Exec arbeitet"](#) auf Seite 239.

Durchführung von Backup-Aufträgen zu einem bestimmten Datum verhindern

Sie können bestimmte Tage, wie etwa Feiertage, von Ihrem Backup-Zeitplan für einzelne Backup-Aufträge ausschließen.

Wenn Sie Tage für einen bestimmten Backup-Auftrag ausschließen, ist nur dieser Backup-Auftrag von den auszuschließenden Tagen betroffen. Der Auftrag wird nicht am ausgeschlossenen Datum ausgeführt, selbst wenn er normalerweise gemäß dem Zeitplan ausgeführt werden müsste. Nach dem ausgeschlossenen Datum wird die Ausführung des Auftrags nach dem normalen Zeitplan fortgesetzt.

Hinweis: Eingeschlossene Daten werden vor den ausgeschlossenen Daten auf die Auftragsplanung angewendet. Wenn alle ausgeschlossenen Daten angewandt sind, überschreiben sie möglicherweise die eingeschlossenen Daten, wenn es Konflikte gibt. Wenn Sie das gleiche Datum sowohl als eingeschlossenes als auch als ausgeschlossenes Datum auswählen, schließt Backup Exec das Datum von Ihrem Backup-Zeitplan aus.

Siehe ["Einschließlich ein spezifisches Datum im Zeitplan für einen Backup-Auftrag"](#) auf Seite 240.

Durchführung von Backup-Aufträgen zu einem bestimmten Datum verhindern

- 1** Erstellen oder bearbeiten Sie eine Definition.
- 2** Klicken Sie im Dialogfeld "Backup" auf "Bearbeiten".
- 3** Klicken Sie im linken Teilfenster auf "Planen".
- 4** Klicken Sie für den Auftrag, dem Sie ein Ausschlussdatum hinzufügen möchten, auf das Feld "Wiederkehrend".

5 Klicken Sie auf der Registerkarte "Daten ein-/ausschließen" auf "Daten ausschließen".

6 Sie haben folgende Möglichkeiten:

So geben Sie das Datum
manuell ein

Führen Sie die folgenden Schritte durch:

- Geben Sie im Feld "Datum auswählen" das Datum des Tags ein, das Sie aus dem Backup-Zeitplan ausschließen möchten.
- Klicken Sie auf "Hinzufügen".

Hinweis: Sie können nur ein Datum auf einmal hinzufügen.

So wählen Sie das Datum im
Kalender

Klicken Sie auf das auszuschließende Datum.

Der Kalender zeigt 3 Monate auf einmal an. Sie können vorwärts oder rückwärts navigieren und zusätzliche Monate ansehen, indem Sie die Pfeile anklicken.

Hinweis: Sie können immer nur ein Datum auf einmal auswählen.

7 Klicken Sie auf "OK".

Siehe ["Wie die Joborganisation in Backup Exec arbeitet"](#) auf Seite 239.

Anzeigen aller geplanten Backup-Aufträge im Kalender

Sie können alle Ihre Backup-Aufträge für einen Monat, eine Woche oder einen Tag im Kalender anzeigen lassen. Es kann hilfreich sein, Ihre Backup-Aufträge im Kalenderformat anzeigen zu lassen, um sicherzustellen, dass es keinen Konflikt im Zeitplan gibt. Werfen Sie einen Blick auf den Kalender, bevor Sie einen neuen Auftrag erstellen.

Anzeigen aller geplanten Backup-Aufträge im Kalender:

1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" in der Gruppe "Backups" auf "Backup-Kalender".

2 Klicken Sie anschließend auf "Schließen".

Siehe ["Wie die Joborganisation in Backup Exec arbeitet"](#) auf Seite 239.

Hinzufügen einer Stufe zu einer Backup-Definition

Stufen sind die zusätzlichen Aufgaben, die Sie mit Backup-Aufträgen als Teil der Backup-Definition ausführen können. Sie können die Backup-Definition anpassen und ihr eine zusätzliche Stufe hinzufügen. Sie können eine oder mehrere Stufen für Virtualisierung und Duplizierung hinzufügen, wenn Sie eine Backup-Definition erstellen. Sie können auch den vorhandenen Backup-Definitionen Stufen hinzufügen.

Wenn Sie beispielsweise einen Backup-Auftrag zur Sicherung wichtiger Daten erstellen können, die an einen anderen Standort gesendet werden sollen, dann können Sie der Backup-Definition, die diesen Auftrag enthält, eine doppelte Phase hinzufügen. Die doppelte Phase schickt automatisch die Backup-Daten zum Bandspeicher, sobald der Backup-Auftrag vollständig ist. Dann können Sie das Band an einen anderen Standort mitnehmen, um sicherzugehen, dass Ihre Daten sicher sind.

Tabelle 4-7 Phasenarten

Phase	Beschreibung
Auf Festplatte duplizieren	Erstellt ein Duplikat Ihres Backups und sendet es an den Festplattenspeicher.
Auf Band duplizieren	Erstellt ein Duplikat Ihres Backups und sendet es an den Bandspeicher.
Auf Cloud duplizieren	Erstellt eine Kopie Ihrer Sicherung und sendet sie an den Cloud-Speicher.
In virtuellen Computer konvertieren	Erstellt mit Ihren Backup-Sätzen einen virtuellen Computer, nachdem das Backup abgeschlossen ist. Siehe "Funktionsweise der Konvertierung eines physischen Computers in einen virtuellen in Backup Exec" auf Seite 581.
Gleichzeitig mit Backups in virtuellen Computer konvertieren	Erstellt mit Ihren Backup-Sätzen einen virtuellen Computer, während das Backup ausgeführt wird. Siehe "Funktionsweise der Konvertierung eines physischen Computers in einen virtuellen in Backup Exec" auf Seite 581.

So fügen Sie einer Backup-Definition Stufen hinzu

- 1 Erstellen oder bearbeiten Sie eine Definition.

Hinweis: Sie können einem einmaligen Backup keine Stufe hinzufügen.

- 2 Klicken Sie im Dialogfeld "Backup" auf "Stufe hinzufügen".
- 3 Wählen Sie den Stufentyp aus, den Sie hinzufügen möchten.
Sie können mehrere Stufen einer Backup-Definition hinzufügen.
- 4 Klicken Sie in dem Feld der Stufe auf "Bearbeiten".
- 5 Klicken Sie im linken Teilfenster auf "Planen" und wählen Sie dann aus, wann Sie die Stufe ausführen möchten.
- 6 Klicken Sie im linken Teilfenster auf "Speicher" und wählen Sie dann das Speichergerät aus, das Sie für diese Stufe verwenden möchten.
- 7 Wählen Sie alle Zusatzfunktionen aus, die auf diese Stufe angewendet werden sollen.
- 8 Wenn Sie mit der Konfiguration dieser Stufe fertig sind, klicken Sie auf "OK".
Wiederholen Sie diese Vorgehensweise für jede Stufe, die Sie der Backup-Definition hinzufügen möchten.

Siehe ["Sichern von Daten"](#) auf Seite 174.

Siehe ["Bearbeiten von Stufen"](#) auf Seite 245.

Bearbeiten von Stufen

Sie können eine Stufe bearbeiten, die Bestandteil einer Backup-Definition ist.

So bearbeiten Sie eine Stufe

- 1 Sie haben folgende Möglichkeiten:

So bearbeiten Sie eine Stufe Führen Sie die folgenden Schritte durch:

über die Registerkarte
 "Backup und
 Wiederherstellung"

- Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" mit der rechten Maustaste auf den Server, der die Backup-Definition mit der zu bearbeitenden Stufe enthält.
- Klicken Sie auf "Backups bearbeiten".
- Wenn auf dem Server mehrere Backup-Definitionen vorhanden sind, wählen Sie die Definition mit der zu bearbeitenden Stufe und klicken Sie auf "OK".

So bearbeiten Sie eine Stufe Führen Sie die folgenden Schritte durch:

auf der Registerkarte
"Auftragsüberwachung"

- Klicken Sie mit der rechten Maustaste auf die Registerkarte "Auftragsüberwachung" auf den Auftrag, der die Stufe enthält, die Sie bearbeiten möchten.
- Klicken Sie auf "Bearbeiten".

- 2 Klicken Sie in dem Feld, das die zu bearbeitende Stufe anzeige, auf "Bearbeiten".
- 3 Nehmen Sie alle notwendigen Änderungen vor.
- 4 Wenn Sie alle erforderlichen Änderungen an der Stufe vorgenommen haben, klicken Sie im Dialogfeld "Backup-Eigenschaften" auf "OK".

Siehe ["Hinzufügen einer Stufe zu einer Backup-Definition"](#) auf Seite 244.

Manuelles Duplizieren von Backup-Sätzen bzw. Auftragsverläufen

Sie können eine Duplizierungsstufe zum automatischen Duplizieren von Backup-Daten nach dem Ausführen eines Backup-Auftrags konfigurieren. Sie sollten Daten duplizieren, damit Sie z. B. eine zusätzliche Kopie off-site ablegen können.

Siehe ["Hinzufügen einer Stufe zu einer Backup-Definition"](#) auf Seite 244.

Sie können Backup-Daten aus abgeschlossenen Aufträgen auch jederzeit manuell kopieren. Wenn Sie gesicherte Daten aus abgeschlossenen Aufträgen duplizieren, wählen Sie die gewünschten Backup-Sätze oder den Auftragsverlauf aus. Die ausgewählten Daten werden von der Quelle gelesen und auf das ausgewählte Ziel geschrieben, wie etwa ein Laufwerk, ein Laufwerkpool oder ein Backup-Ordner. Sie können die duplizierten Daten verschlüsseln. Sie können planen, wann dieser Auftragsstyp ausgeführt wird. Er wird jedoch nur einmal ausgeführt.

Sie können entweder eine oder mehrere einzelne Backup-Sätze oder einen gesamten Auftragsverlauf duplizieren. Sie sollten Backup-Sätze duplizieren, wenn Sie nur die Daten duplizieren möchten, die in einer bestimmten Backup-Auftrags-Instanz gesichert wurden. Wenn Sie einen Auftragsverlauf duplizieren, schließt Backup Exec alle abhängigen Backup-Sätze einer Backup-Definition ein. Beispiel: Wenn Sie ein inkrementelles Backup auswählen, dupliziert Backup Exec automatisch alle inkrementellen Backups bis einschließlich zum letzten vollständigen Backup.

Dieses Thema enthält folgende Informationen:

Duplizieren von Daten aus einem virtuellen auf ein physisches Gerät

So duplizieren Sie Backup-Sätze

Deduplizierungsauftrags-Verlauf

Duplizieren von Daten aus einem virtuellen auf ein physisches Gerät

Sie können einen duplizierten Backup-Auftrag verwenden, um Daten direkt von einem virtuellen Gerät auf ein physisches Gerät zu kopieren.

Softwareverschlüsselung kann nicht auf einen doppelten Backup-Auftrag angewendet werden, wenn Sie Daten direkt von einem virtuellen Gerät auf ein physisches Gerät kopieren. Sie müssen entweder DirectCopy deaktivieren oder festlegen, dass der Auftrag nicht verschlüsselt wird.

Siehe ["Kopieren von Daten von einer virtuellen Bandbibliothek auf ein physisches Bandgerät mit DirectCopy"](#) auf Seite 255.

Wenn Sie mit mehreren Datenströmen erstellte Oracle-Backup-Sätze duplizieren, beachten Sie Folgendes:

- Backup Exec wandelt mehrere Datenströme beim Kopieren in einen sequenziellen Datenstrom um.
- Eine Wiederherstellung von der Kopie kann durchaus mehr Zeit in Anspruch nehmen, als wenn die Wiederherstellung vom ursprünglichen Medium erfolgt.

So duplizieren Sie Backup-Sätze

- 1 Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, das mit den zu duplizierenden Backup-Sätzen verbunden ist.
- 2 Klicken Sie im linken Teilfenster auf "Backup-Sätze".
- 3 Sie haben folgende Möglichkeiten:
 - Klicken Sie zum Duplizieren eines einzelnen Backup-Satzes mit der rechten Maustaste auf den Backup-Satz.
 - Um mehrere Backup-Sätze zu duplizieren, klicken Sie bei gedrückter Umschalttaste oder Strg-Taste auf die Backup-Sätze und klicken Sie dann mit der rechten Maustaste auf einen der ausgewählten Backup-Sätze.
- 4 Wählen Sie "Kopie" aus.

- 5** Wählen Sie im Gruppenfeld "Planen" aus, wann Backup Exec den Duplizierungsauftrag ausführen soll:

So führen Sie den Duplizierungsauftrag sofort aus	Wählen Sie "Jetzt ausführen".
So planen Sie den Auftrag für einen späteren Zeitpunkt	Wählen Sie "Am x um y ausführen" und geben Sie Datum und Uhrzeit ein.
So planen Sie den Auftrag mit einem externen Tool so, dass er zu einem späteren Zeitpunkt ausgeführt wird	Wählen Sie "Ohne Zeitplan erstellen". Sie können den Auftrag zu einem späteren Zeitpunkt mithilfe eines externen Planungs-Tools planen.
So geben Sie den Auftrag auf Griff ein	Klicken Sie auf "Auftrag in Wartestellung senden". Der Auftrag wird mit dem Status "In Wartestellung" erstellt. Er verbleibt in Wartestellung, bis Sie den Status aufheben.

- 6** Wählen Sie im Feld "Speicher" das Speichergerät aus, auf das Sie die Backup-Sätze kopieren möchten.

- 7** Wählen Sie im Feld "Aufbewahren für" aus, wie lange Backup Exec die Backup-Sätze aufbewahren soll.

Für den angegebenen Zeitraum ist das Medium vor Überschreiben geschützt.

Wählen Sie "Quellaufbewahrung verwenden", um die Backup-Sätze genauso lange aufzubewahren wie die zu duplizierenden Quell-Backup-Sätze.

- 8** Sie haben folgende Möglichkeiten:

So aktivieren Sie die Komprimierung für die duplizierten Backup-Sätze	Wählen Sie im Feld "Komprimierung" den Typ der Komprimierung aus.
So aktivieren Sie die Verschlüsselung für die duplizierten Backup-Sätze	<p>Führen Sie die folgenden Schritte durch:</p> <ul style="list-style-type: none"> ■ Wählen Sie im Feld "Verschlüsselungstyp" den Typ der Verschlüsselung aus. ■ Wählen Sie im Feld "Verschlüsselungsschlüssel" den gewünschten Verschlüsselungsschlüssel aus oder wählen Sie "Schlüssel verwalten", um einen neuen Schlüssel zu erstellen.

So verifizieren Sie die
duplizierten Backup-Sätze

Wählen Sie "Am Ende des Auftrags prüfen".

9 Klicken Sie im Dialogfeld "Auftrag duplizieren" auf "OK".

Deduplizierungsauftrags-Verlauf

1 Sie haben folgende Möglichkeiten:

So kopieren Sie den
Auftragsverlauf aus der
Registerkarte "Backup und
Wiederherstellung bzw.
"Speicher"

Führen Sie die folgenden Schritte durch:

- Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, das mit dem zu duplizierenden Auftragsverlauf verbunden ist.
- Im linken Teilfenster klicken Sie auf "Auftragsverlauf".
- Sie haben folgende Möglichkeiten:
 - Klicken Sie mit der rechten Maustaste auf den gewünschten Auftragsverlauf, um eine einzelne Auftragsverläufe zu kopieren.
 - Um mehrere Auftragsverläufe zu duplizieren, klicken Sie bei gedrückter Umschalttaste oder Strg-Taste auf die Auftragsverläufe und klicken Sie dann mit der rechten Maustaste auf einen der ausgewählten Auftragsverläufe.

So kopieren Sie den
Auftragsverlauf aus der
Registerkarte
"Auftragsüberwachung"

Führen Sie die folgenden Schritte durch:

- Auf der Registerkarte "Auftragsüberwachung" führen Sie einen der folgenden Schritte aus:
 - Klicken Sie mit der rechten Maustaste auf den gewünschten Auftragsverlauf, um eine einzelne Auftragsverläufe zu kopieren.
 - Um mehrere Auftragsverläufe zu duplizieren, klicken Sie bei gedrückter Umschalttaste oder Strg-Taste auf die Auftragsverläufe und klicken Sie dann mit der rechten Maustaste auf einen der ausgewählten Auftragsverläufe.

2 Klicken Sie auf "Duplizieren".

- 3** Wählen Sie im Gruppenfeld "Planen" aus, wann Backup Exec den Duplizierungsauftrag ausführen soll:

So führen Sie den Duplizierungsauftrag sofort aus	Wählen Sie "Jetzt ausführen".
So planen Sie den Auftrag für einen späteren Zeitpunkt	Wählen Sie "Am x um y ausführen" und geben Sie Datum und Uhrzeit ein.
So planen Sie den Auftrag mit einem externen Tool so, dass er zu einem späteren Zeitpunkt ausgeführt wird	Wählen Sie "Ohne Zeitplan erstellen". Sie können den Auftrag zu einem späteren Zeitpunkt mithilfe eines externen Planungs-Tools planen.
So geben Sie den Auftrag auf Griff ein	Klicken Sie auf "Auftrag in Wartestellung senden". Der Auftrag wird mit dem Status "In Wartestellung" erstellt. Er verbleibt in Wartestellung, bis Sie den Status aufheben.

- 4** Wählen Sie im Feld "Speicher" das Speichergerät aus, auf das Sie den Auftragsverlauf kopieren möchten.

- 5** Wählen Sie im Feld "Aufbewahren für" aus, wie lange Backup Exec den Auftragsverlauf speichern soll.

Für den angegebenen Zeitraum ist das Medium vor Überschreiben geschützt.

Wählen Sie "Quellaufbewahrung verwenden", um den Auftragsverlauf genauso lange aufzubewahren wie den zu duplizierenden Quellauftragsverlauf.

- 6** Sie haben folgende Möglichkeiten:

So aktivieren Sie die Komprimierung für den Auftragsverlauf	Wählen Sie im Feld "Komprimierung" den Typ der Komprimierung aus.
So aktivieren Sie die Verschlüsselung für den Auftragsverlauf	<p>Führen Sie die folgenden Schritte durch:</p> <ul style="list-style-type: none"> ■ Wählen Sie im Feld "Verschlüsselungstyp" den Typ der Verschlüsselung aus. ■ Wählen Sie im Feld "Verschlüsselungsschlüssel" den gewünschten Verschlüsselungsschlüssel aus oder wählen Sie "Schlüssel verwalten", um einen neuen Schlüssel zu erstellen.

So verifizieren Sie den
Auftragsverlauf

Wählen Sie "Am Ende des Auftrags prüfen".

- 7 Klicken Sie im Dialogfeld "Auftrag duplizieren" für jeden Duplizierungsauftrag, den Sie erstellen, auf "OK".

Manuelle Ausführung von Probelaufaufträgen

Mithilfe von Aufträgen für Testläufe wird versucht, festzustellen, ob ein geplanter Backup während des Ausführens fehlschlagen kann. Bei der Ausführung von Testaufträgen werden keine Daten gesichert. Stattdessen prüft Backup Exec Ihre Speicherkapazität, Login-Daten und Medien, um potenzielle Fehler zu finden. Wenn ein Fehler auftritt, wird der Auftrag weiterhin ausgeführt, bis er abgeschlossen ist. Der Fehler wird im Auftragsprotokoll angezeigt. Sie können Backup Exec auch konfigurieren, um eine Benachrichtigung an einen designierten Empfänger zu schicken.

Wenn es während eines Probelaufauftrags zu Fehlern kommt, können folgende Gründe vorliegen:

- Login-Daten sind falsch.
- Speicherkapazität reicht nicht aus.
- Bandkassettemedien oder -Datenträgermedien sind nicht verfügbar.
- Überschreibbare Medien sind nicht für einen Überschreibungsauftrag verfügbar.
- Anhängbare Medien sind nicht für einen Anhängauftrag verfügbar.

Ein Probelaufauftrags prüft die Medienkapazität, die für den ausgewählten Auftrag verfügbar ist. Sie können jedoch prüfen, ob ausreichend Medien für mehrere Probelaufaufträge im Bericht "Probelaufergebnisse" verfügbar sind.

Siehe "[Bericht "Probelaufergebnisse"](#)" auf Seite 849.

Sie können Probelaufaufträge so konfigurieren, dass sie vor Ihren geplanten Backup-Aufträgen ausgeführt werden. Oder Sie können einen Probelaufauftrag manuell jederzeit ausführen.

Es wird empfohlen, dass Sie vor dem Ausführen eines Probelaufauftrags zunächst Backup-Aufträge auf Ihren Speichergeräten ausführen. Backup Exec kann die Kapazität eines Speichergeräts erst bestimmen, wenn ein tatsächlicher Backup-Auftrag Daten an das Gerät sendet. Wenn Sie vor dem Erstellen anderer Aufträge zunächst einen Probelaufauftrag erstellen, kann Backup Exec nicht überprüfen, ob genügend Speicherkapazität zum Ausführen des Backup-Auftrags

zur Verfügung steht. Nachdem mindestens ein Backup-Auftrag Daten an ein Gerät gesendet hat, kann Backup Exec die Speicherkapazität bestimmen.

So führen Sie einen Testauftrag manuell aus

1 Sie haben folgende Möglichkeiten:

So führen Sie einen Testauftrag von der Registerkarte "Backup und Wiederherstellung" aus

Führen Sie die folgenden Schritte durch:

- Auf der Registerkarte "Backup und Wiederherstellung" doppelklicken Sie auf den Server, der den Auftrag enthält, den Sie testen möchten.
- Klicken Sie im linken Teilfenster auf "Aufträge".

So führen Sie einen Testauftrag von der Registerkarte "Auftragsüberwachung" aus

Wählen Sie die Registerkarte "Auftragsüberwachung".

- 2** Klicken Sie mit der rechten Maustaste auf den Auftrag, den Sie testen möchten, und klicken Sie dann auf "Testlauf".
- 3** Klicken Sie auf "Ja", um zu bestätigen, dass Sie den Testauftrag jetzt ausführen möchten.

Siehe ["Konfigurieren automatischer Testlaufaufträge für Backup-Aufträge"](#) auf Seite 653.

Gesicherte Daten manuell überprüfen

Backup Exec kann eine Überprüfung durchführen, um sicherzustellen, ob die Medien gelesen werden können, sobald der Backup-Auftrag abgeschlossen wurde. Es wird empfohlen, dass Sie alle gesicherten Daten verifizieren, um die Integrität der Datenerfassung und der Medien sicherzustellen, auf denen sie sich befindet. Standardmäßig verifiziert Backup Exec automatisch gesicherte Daten am Ende eines Backup-Auftrags. Sie können aber auch festlegen, dass die Überprüfung zu einem späteren Zeitpunkt ausgeführt werden soll, oder sie komplett deaktivieren. Sie können die Prüfungsoptionen von Backup Exec als Teil der Standardbackupeinstellungen oder für einzelne Backup-Aufträge anpassen.

Siehe ["Konfigurieren der automatischen Prüfung von Aufträgen"](#) auf Seite 655.

Sie können einen Backup-Satz oder Auftragsverlauf jederzeit manuell verifizieren. Sie können Backup-Sätze überprüfen, wenn Sie nur die Daten überprüfen möchten, die in einer bestimmten Backup-Auftrags-Instanz gesichert wurden. Wenn Sie einen Auftrag und alle seine abhängigen Backup-Sätze prüfen möchten, können Sie einen Auftragsverlauf prüfen. Beispiel: Wenn Sie eine Backup-Definition prüfen möchten,

die inkrementelle Backups nutzte, überprüft Backup Exec alle entsprechenden Backups, einschließlich des letzten vollständigen.

Dieses Thema umfasst die folgenden Vorgänge:

[Überprüfen bestimmter Backup-Sätze](#)

[So prüfen Sie einen Auftragsverlauf](#)

Überprüfen bestimmter Backup-Sätze

- 1 Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder auf das Speichergerät, das mit dem Backup-Satz oder den Backup-Sätzen verknüpft ist, die Sie überprüfen möchten.
- 2 Klicken Sie im linken Teilfenster auf "Backup-Sätze".
- 3 Sie haben folgende Möglichkeiten:
 - Um einen einzelnen Backup-Satz zu überprüfen, klicken Sie mit der rechten Maustaste auf den Backup-Satz.
 - Um mehrere Backup-Sätze zu überprüfen, klicken Sie bei gedrückter Umschalt- oder Steuerungstaste auf die Backup-Sätze und klicken dann mit der rechten Maustaste auf einen der ausgewählten Backup-Sätze.
- 4 Klicken Sie auf "Überprüfen".
- 5 Wählen Sie im Gruppenfeld "Zeitplan" aus, wann Backup Exec die Verifizierung ausführen soll:

So führen Sie die Verifizierung sofort aus

Wählen Sie "Jetzt ausführen".

So planen Sie den Vorgang für einen späteren Zeitpunkt

Wählen Sie "Ausführen am" aus und geben Sie Datum und Uhrzeit zum Ausführen des Auftrags ein.

So planen Sie den Auftrag mit einem externen Tool so, dass er zu einem späteren Zeitpunkt ausgeführt wird

Wählen Sie "Ohne Zeitplan erstellen". Sie können die Verifizierung zu einem späteren Zeitpunkt mithilfe eines externen Planungs-Tools planen.

- 6 Klicken Sie auf "OK".

So prüfen Sie einen Auftragsverlauf

- 1 Sie haben folgende Möglichkeiten:

So prüfen Sie einen Auftragsverlauf auf der Registerkarte "Backup und Wiederherstellung" oder "Speicher"

Führen Sie die folgenden Schritte durch:

- Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, das mit dem zu verifizierenden Auftragsverlauf verbunden ist.
- Im linken Teilfenster klicken Sie auf "Auftragsverlauf".
- Sie haben folgende Möglichkeiten:
 - Klicken Sie mit der rechten Maustaste auf einen Auftragsverlauf, um diesen zu verifizieren.
 - Um mehrere Auftragsverläufe zu verifizieren, klicken Sie bei gedrückter Umschalt- oder Strg-Taste auf die Auftragsverläufe und klicken Sie dann mit der rechten Maustaste auf einen der ausgewählten Auftragsverläufe.

So prüfen Sie einen Auftragsverlauf auf der Registerkarte "Auftragsüberwachung"

Auf der Registerkarte "Auftragsüberwachung" führen Sie einen der folgenden Schritte aus:

- Klicken Sie mit der rechten Maustaste auf einen Auftragsverlauf, um diesen zu verifizieren.
- Um mehrere Auftragsverläufe zu überprüfen, klicken Sie bei gedrückter Umschalttaste oder Strg-Taste auf die Auftragsverläufe und klicken Sie dann mit der rechten Maustaste auf einen der ausgewählten Auftragsverläufe.

- 2** Klicken Sie auf "Überprüfen".
- 3** Wählen Sie im Gruppenfeld "Zeitplan" aus, wann Backup Exec die Verifizierung ausführen soll:

So führen Sie die Verifizierung sofort aus

Wählen Sie "Jetzt ausführen".

So planen Sie den Vorgang für einen späteren Zeitpunkt

Wählen Sie "Ausführen am" aus und geben Sie Datum und Uhrzeit zum Ausführen des Auftrags ein.

So planen Sie den Auftrag mit einem externen Tool so, dass er zu einem späteren Zeitpunkt ausgeführt wird

Wählen Sie "Ohne Zeitplan erstellen".

Sie können die Verifizierung zu einem späteren Zeitpunkt mithilfe eines externen Planungs-Tools planen.

- 4** Klicken Sie auf "OK".

Kopieren von Daten von einer virtuellen Bandbibliothek auf ein physisches Bandgerät mit DirectCopy

Mithilfe der Backup Exec-Option "DirectCopy auf Band" können Sie Daten während eines Auftrags zum Duplizieren von Backups direkt von einer virtuellen Bandbibliothek auf ein physisches Bandgerät kopieren. Der Backup Exec-Server koordiniert den Duplizierungsauftrag, aber er kopiert nicht die Daten. Stattdessen kopiert die virtuelle Bandbibliothek das virtuelle Band-Image direkt auf das physische Gerät. Der Backup Exec-Server zeichnet Informationen über die Daten im Katalog auf. Da die Informationen über die kopierten Daten im Katalog sind, können Sie Daten entweder von der virtuellen Bandbibliothek oder vom physischen Gerät wiederherstellen. Das Auftragsprotokoll für den Duplizierungs-Backup-Auftrag gibt an, dass "DirectCopy auf Band" aktiviert ist.

Um "DirectCopy auf Band" verwenden zu können, müssen das Quellgerät und das Zielgerät NDMP-fähig sein. Wenn die Geräte nicht NDMP-fähig sind, führt Backup Exec einen herkömmlichen Duplizierungs-Backup-Auftrag durch.

Hardware- und Software-Verschlüsselung werden mit "DirectCopy auf Band" unterstützt. Zur Softwareverschlüsselung ist es erforderlich, dass sowohl der Quell-Backup-Satz als auch der Ziel-Backup-Satz verwendet werden.

Hinweis: Wenn Sie einen Datenträgerspeicher als Zielgerät für einen duplizierten Auftrag mit der aktivierter Option "DirectCopy auf Band" auswählen, führt Backup Exec einen regulären Duplizierungsauftrag durch.

Tabelle 4-8 Verwenden von "DirectCopy auf Band", um Daten von einer virtuellen Bandbibliothek auf ein physisches Gerät zu kopieren

Schritt	Hinweise	Weitere Informationen
Erstellen Sie einen herkömmlichen Backup-Auftrag.	Wählen Sie eine virtuelle Bandbibliothek als das Speicherziel aus.	Siehe "Sichern von Daten" auf Seite 174. Siehe "Konfigurieren von Speicheroptionen für Backup-Aufträge" auf Seite 645.

Kopieren von Daten von einer virtuellen Bandbibliothek auf ein physisches Bandgerät mit DirectCopy

Schritt	Hinweise	Weitere Informationen
Erstellen Sie einen Duplizierungs- Backup-Auftrag.	<p>Einstellungen für DBA-initiierte Aufträge:</p> <ul style="list-style-type: none"> ■ Wählen Sie ein physisches Bandgerät als Ziel aus. ■ Wählen Sie DirectCopy auf Band aktivieren. 	<p>Siehe "DBA-initiierte Auftragsvorlagen" auf Seite 746.</p> <p>Siehe "Speicheroptionen für von DBA gestartete Aufträge" auf Seite 748.</p> <p>Siehe "Duplizieren von Auftragseinstellungen für DBA-initiierte Aufträge" auf Seite 755.</p>

Wiederherstellungen

In diesem Kapitel werden folgende Themen behandelt:

- Methoden für das Wiederherstellen von Daten in Backup Exec
- Suchen nach Daten zum Wiederherstellen
- Wiederherstellen von Daten aus einem Server, einem Backup-Satz, einem Backup-Auftrag oder einem Speichergerät
- Wiederherstellen von Dateisystemdaten
- Vollständige Online-Wiederherstellung eines Microsoft Windows-Computers
- Wiederherstellen des Systemstatus
- Installieren eines Windows Server-Domänencontrollers in einer vorhandenen Domäne durch die Anwendung einer umgeleiteten Wiederherstellung
- Wiederherstellen der Shadow Copy-Komponenten von Backup Exec
- Wiederherstellen von Dienstprogrammpartitionen oder Unified Extensible Firmware Interface-Systempartition
- Informationen zum Wiederherstellen verschlüsselter Daten
- Info zur Wiederherstellung von NetWare SMS-Datenträger-Backups auf andere als SMS-Datenträger mit Backup Exec
- Abbrechen eines Wiederherstellungsauftrags
- Funktionsweise der Backup Exec-Kataloge
- Katalogisieren von Backup-Sätzen

Methoden für das Wiederherstellen von Daten in Backup Exec

In Backup Exec stehen Methoden zum Suchen und Wiederherstellen mit Anleitung für den Benutzer zur Verfügung, die die Suche nach und Wiederherstellung von gesicherten Daten erleichtern.

Über die Funktionen "Suchen" oder "Wiederherstellen" auf der Registerkarte "Backup und Wiederherstellung" können Sie Folgendes tun:

- Wiederherstellen von Daten an dem Speicherort, von dem aus sie ursprünglich gesichert wurden, oder Umleiten des Wiederherstellungsvorgangs an einen anderen Speicherort.
- Sofortiges Starten des Wiederherstellungsauftrags oder Planen für einen zukünftigen Zeitpunkt.

Hinweis: Der Wiederherstellungsassistent zeigt nur bis zu 30.000 Elemente an. Wenn Sie Daten aus einem Ordner wiederherstellen möchten, der mehr als 30.000 Elemente enthält, sollten Sie das Element suchen, das Sie wiederherstellen möchten. Sie können Suchkriterien wie den Datentyp und das Datum des ursprünglichen Backup verwenden, um die Anzahl der ausgegebenen Elemente zu verringern.

Tabelle 5-1 Datenwiederherstellungs- und Suchmethoden mit Anleitung

Methode	Beschreibung
Suchen	<p>Ermöglicht die Suche nach Backup-Sätzen auf mehreren Servern. Anschließend können Sie die Daten wiederherstellen oder die Suchkriterien und die Ergebnisse in die Zwischenablage kopieren und speichern. Sie können die Ergebnisse per E-Mail an die Person weiterleiten, die die Wiederherstellung angefordert hat, um sich vor der Wiederherstellung zu vergewissern, dass die richtigen Daten gefunden wurden.</p> <p>Um den Suchassistent zu starten, müssen Sie auf der Registerkarte "Backup und Wiederherstellung" einen oder mehr Server auswählen und anschließend in der Gruppe "Wiederherstellung" auf "Suchen" klicken.</p> <p>Siehe "Suchen nach Daten zum Wiederherstellen" auf Seite 260.</p>

Methode	Beschreibung
Wiederherstellen	<p>Durchsucht die Backup-Sätze von einem einzelnen Server und stellt dann die Daten wieder her. Sie können Dateisystemdaten, Systemstatusdaten, Backup Exec Shadow Copy-Komponenten, Dienstpartitionen oder UEFI-Systempartitionen und mehr wiederherstellen.</p> <p>Sie können eine vollständige Online-Wiederherstellung eines Windows-Computers durchführen, wenn der Computer vollständig für ein Backup ausgewählt wurde. Standardmäßig umfassen Backup-Aufträge alle notwendigen Komponenten, die für eine vollständige Wiederherstellung erforderlich sind.</p> <p>Um den Assistent für Wiederherstellungsaufträge zu starten, müssen Sie auf der Registerkarte "Backup und Wiederherstellung" einen Server auswählen und anschließend in der Gruppe "Wiederherstellung" auf "Wiederherstellen" klicken.</p> <p>Siehe "Wiederherstellen von Daten aus einem Server, einem Backup-Satz, einem Backup-Auftrag oder einem Speichergerät" auf Seite 261.</p> <p>Siehe "Vollständige Online-Wiederherstellung eines Microsoft Windows-Computers" auf Seite 267.</p>
Simplified Disaster Recovery	<p>Ermöglicht die Wiederherstellung von Windows-Computern nach einem Festplattenausfall. Die Simplified Disaster Recovery-Assistenten führen Sie durch die Vorbereitungen für eine Notfallwiederherstellung und durch die Wiederherstellung des Zustandes eines lokalen oder standortfernen Computers vor dem Notfall.</p> <p>Siehe "Info zu Simplified Disaster Recovery" auf Seite 941.</p>

Siehe ["Wiederherstellen von Dateisystemdaten"](#) auf Seite 265.

Siehe ["Wiederherstellen des Systemstatus "](#) auf Seite 268.

Siehe ["Wiederherstellen der Shadow Copy-Komponenten von Backup Exec"](#) auf Seite 274.

Siehe ["Wiederherstellen von Dienstprogrammpartitionen oder Unified Extensible Firmware Interface-Systempartition"](#) auf Seite 275.

Siehe ["Wiederherstellen von Exchange-Daten"](#) auf Seite 1309.

Siehe ["SQL-Datenbanken und Transaktionsprotokolle wiederherstellen"](#) auf Seite 1256.

Siehe ["Wiederherstellen von Oracle-Ressourcen"](#) auf Seite 1368.

Siehe ["Wiederherstellen virtueller VMware-Computer und VMDK-Dateien"](#) auf Seite 1121.

Siehe ["Wiederherstellen eines Deduplizierungs-Plattenspeichergeräts oder von deduplizierten Daten"](#) auf Seite 1085.

Siehe ["Wiederherstellen von Microsoft SharePoint-Daten"](#) auf Seite 1329.

Siehe ["Wiederherstellen von Enterprise Vault"](#) auf Seite 1400.

Siehe ["Info zum Wiederherstellen von Daten auf Linux-Computern"](#) auf Seite 1582.

Suchen nach Daten zum Wiederherstellen

Sie können einen oder mehrere Server für die Suche nach Backup-Sätzen auswählen. Anschließend können Sie die Daten wiederherstellen oder die Suchkriterien und die Ergebnisse in die Zwischenablage kopieren und speichern. Sie können die Ergebnisse per E-Mail an die Person weiterleiten, die die Wiederherstellung angefordert hat, um sich vor der Wiederherstellung zu vergewissern, dass die richtigen Daten gefunden wurden.

Backup Exec erstellt separate Wiederherstellungsaufträge für jeden Server, auf dem Sie Daten wiederherstellen.

Der Suchassistent unterstützt nur die folgenden Typen von Daten:

- Dateien und Ordner
- Exchange- und SharePoint-Backup-Sätze, für die Granular Recovery Technology aktiviert wurde

Hinweis: Sie können die Backup-Sätze nach Daten durchsuchen, die aus einem virtuellen Computer gesichert wurden, wenn auf der Seite "Optionen für Instant GRT und Vollständige Katalogisierung" die Option "Vollständige Katalogisierung" gewählt und abgeschlossen wurde. Die Suchfunktion ist jedoch nur im Wiederherstellungsassistenten verfügbar, wenn Sie eine auf dem virtuellen Computer installierte Anwendung zum Wiederherstellen auswählen.

Die Suchfunktion ist nicht verfügbar, wenn auf der Seite "Optionen für Instant GRT und Vollständige Katalogisierung" die Option "Instant GRT aktivieren" ausgewählt wurde.

Dateien und Ordner: Wenn Sie den Zugriff auf gesicherte Dateien mit dem BEMCLI-Befehl `Import-BEItemsToBlock` blockiert haben, sind die blockierten Elemente nicht verfügbar, wenn Sie Dateien zum Wiederherstellen suchen.

So suchen Sie nach Daten zum Wiederherstellen

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" mit der rechten Maustaste auf den bzw. die zu durchsuchenden Server. und klicken Sie dann auf "Suchen".
- 2 Folgen Sie den Anweisungen des Suchassistenten, um nach Daten zu suchen und Daten wiederherzustellen.

Wiederherstellen von Daten aus einem Server, einem Backup-Satz, einem Backup-Auftrag oder einem Speichergerät

Sie können Daten wiederherstellen, indem Sie den Wiederherstellungsassistenten direkt von einem Server, einem Backup-Satz, einem abgeschlossenen Backup-Auftrag oder einem Speichergerät starten.

Sie können eine vollständige Online-Wiederherstellung eines Windows-Computers durchführen, wenn der Computer vollständig für ein Backup ausgewählt wurde. Standardmäßig umfassen Backup-Aufträge alle notwendigen Komponenten, die für eine vollständige Wiederherstellung erforderlich sind.

Dateien und Ordner: Wenn Sie den Zugriff auf gesicherte Dateien mit dem BEMCLI-Befehl `Import-BEItemsToBlock` blockiert haben, werden die blockierten Elemente nicht in den Suchergebnissen angezeigt.

Siehe ["Vollständige Online-Wiederherstellung eines Microsoft Windows-Computers"](#) auf Seite 267.

Tabelle 5-2 Wiederherstellungsmethoden

Wiederherstellungsmethode	Weitere Informationen
So stellen Sie Daten aus einem Server wieder her	Wiederherstellen von Daten aus einem Server
So stellen Sie Daten aus einem Backup-Satz wieder her	So stellen Sie Daten aus einem Backup-Satz wieder her
So stellen Sie Daten aus einem abgeschlossenen Backup-Auftrag wieder her	Wiederherstellen von Daten aus einem abgeschlossenen Backup-Auftrag
So stellen Sie Daten aus einem Speichergerät wieder her	Wiederherstellen von Daten aus Speichergeräten

Hinweis: Wenn Ressourcen-Manager für Dateiserver (FSRM) auf dem Server ausgeführt wird, den Sie wiederherstellen, kann der Auftrag mit dem Fehler "Nicht genügend Speicherplatz." fehlschlagen. Ist dies der Fall, deaktivieren Sie RSRM und führen Sie dann den Auftrag erneut aus.

Wiederherstellen von Daten aus einem Server

Sie können die Backup-Sätze aus einem einzelnen Server durchsuchen und dann die Daten wiederherstellen.

Hinweis: Wenn Sie einen Server sichern und dann umbenennen, werden sowohl der neue als auch der alte Servername auf der Registerkarte "Backup und Wiederherstellung" angezeigt. Der Status neben dem neuen Servernamen gibt an, dass er gesichert wird. Jedoch sollten Sie das Symbol mit dem alten Servernamen auswählen, um Daten wiederherzustellen, die Sie gesichert haben, bevor der Servername geändert wurde.

So stellen Sie Daten aus einem Server wieder her

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" in der Serverliste oder auf der Registerkarte "Auftragsüberwachung" mit der rechten Maustaste auf einen Server, der gesichert wurde.
- 2 Klicken Sie auf "Wiederherstellen".
- 3 Folgen Sie im Assistenten für Wiederherstellungsaufträge den Anweisungen zum Wiederherstellen der Daten.

Wiederherstellen von Daten aus einem abgeschlossenen Backup-Auftrag

Sie können Daten aus einem abgeschlossenen Backup-Auftrag wiederherstellen. Wenn Sie Daten aus Backup-Aufträgen wiederherstellen, können Sie nur Daten auswählen, die in den Backup-Sätzen enthalten sind, die der Backup-Auftrag erstellte.

So stellen Sie Daten aus einem abgeschlossenen Backup-Auftrag wieder her

- 1 Sie haben folgende Möglichkeiten:

- So stellen Sie Daten aus der Registerkarte "Backup und Wiederherstellung" wieder her
 - Doppelklicken Sie auf der Registerkarte "Backup und Wiederherstellung" in der Serverliste auf einen Server, der gesichert wurde.
 - Erweitern Sie in der Ansicht "Aufträge" Sie eine Backup-Definition.
 - Unter der Backup-Definition klicken Sie mit der rechten Maustaste auf den Backup-Auftrag, aus dem Sie Daten wiederherstellen möchten.
 - Wählen Sie die Option "Durch diesen Auftrag erstellte Backup-Sätze wiederherstellen".
- So stellen Sie Daten aus der Registerkarte "Auftragsüberwachung" wieder her
 - Klicken Sie auf der Registerkarte "Auftragsüberwachung" im Teilfenster "Aufträge" mit der rechten Maustaste auf einen Server, der gesichert wurde.
 - Wählen Sie die Option "Durch diesen Auftrag erstellte Backup-Sätze wiederherstellen".

- 2 Folgen Sie im Assistenten für Wiederherstellungsaufträge den Anweisungen zum Wiederherstellen der Daten.

Wiederherstellen von Daten aus einem Backup-Satz

Sie können Daten aus den Backup-Sätzen wiederherstellen, die auf der Registerkarte "Backup und Wiederherstellung" angezeigt werden. Wenn Sie Daten aus Backup-Sätzen wiederherstellen, können Sie nur Daten auswählen, die in den Backup-Sätzen enthalten wird.

So stellen Sie Daten aus einem Backup-Satz wieder her

- 1 Doppelklicken Sie auf der Registerkarte "Backup und Wiederherstellung" in der Serverliste auf einen Server, der gesichert wurde.
- 2 Erweitern Sie in der Ansicht "Backup-Sätze" einen Backup-Satz, aus dem Sie Daten wiederherstellen möchten.
- 3 Klicken Sie mit der rechten Maustaste auf den Backup-Satz, aus dem Sie Daten wiederherstellen möchten.
- 4 Klicken Sie auf "Wiederherstellen".
- 5 Folgen Sie im Assistenten für Wiederherstellungsaufträge den Anweisungen zum Wiederherstellen der Daten.

Wiederherstellen von Daten aus Speichergeräten

Sie können Daten aus den Medien wiederherstellen, die in den Speichergeräten auf der Registerkarte "Speicher" enthalten sind. Wenn Sie Daten direkt aus den Speichergerätmedien wiederherstellen, können Sie nur Daten wiederherstellen,

die in den Backup-Sätzen auf den Medien enthalten sind. Der Wiederherstellungsassistent fordert Sie auf, Optionen für jeden Datentyp auszuwählen und sendet dann einen separaten Auftrag für jeden Datentyp.

Wenn Sie Daten aus Speichergeräten wiederherstellen, können Sie mehrere Datentypen wiederherstellen. Für jeden Datentyp wird ein separater Wiederherstellungsauftrag gesendet.

So stellen Sie Daten aus einem Speichergerätmedium wieder her

1 Sie haben folgenden Möglichkeiten:

So stellen Sie Daten aus einem Plattenspeichergerät wieder her

Gehen Sie dazu in folgender Reihenfolge vor:

- Wählen Sie auf der Registerkarte "Speicher" in der Ansicht "Gesamter Speicher" das Speichergerät aus, aus dem Sie wiederherstellen möchten.
- Doppelklicken Sie auf das Plattenspeichergerät und klicken Sie dann links auf "Backup-Sätze".
- Klicken Sie mit der rechten Maustaste auf den Backup-Satz, aus dem Sie Daten wiederherstellen möchten, und klicken Sie dann auf "Wiederherstellen".

So stellen Sie Daten aus einem Bandlaufwerk oder Plattenkassettengerät wieder her

Gehen Sie dazu in folgender Reihenfolge vor:

- Erweitern Sie auf der Registerkarte "Speicher" in der Ansicht "Gesamter Speicher" den Eintrag "Band- und Plattenspeichermedien".
- Öffnen Sie das Medium, das die Daten enthält, die Sie wiederherstellen möchten.
- Klicken Sie mit der rechten Maustaste auf die Medien, aus denen Sie Daten wiederherstellen möchten, und klicken Sie dann auf "Wiederherstellen".

So stellen Sie Daten aus Medien eines Wechslers wieder her

Gehen Sie dazu in folgender Reihenfolge vor:

- Wählen Sie auf der Registerkarte "Speicher" in der Ansicht "Gesamter Speicher" den Wechsler aus, aus dem Sie wiederherstellen möchten.
- Erweitern Sie den Wechsler.
- Doppelklicken Sie auf "Schächte".
- Klicken Sie in der Ansicht "Schächte" mit der rechten Maustaste auf den Schacht, der die Medien enthält, aus denen Sie Daten wiederherstellen möchten, und klicken Sie dann auf "Wiederherstellen".

- 2 Folgen Sie im Assistenten für Wiederherstellungsaufträge den Anweisungen zum Wiederherstellen der Daten.
- 3 (Optional) Zum Wiederherstellen mehrerer Datentypen verwenden Sie den "Wiederherstellungsassistent" und wählen die passenden Optionen für den ausgewählten Datentyp.

Dann tun Sie Folgendes:

- Klicken Sie auf der Übersichtsseite auf "Weiter", um den Auftrag zu senden und die Seite mit den verschiedenen Datentypen aufzurufen.
Das Symbol in der Spalte "Auftrag gesendet" gibt an, dass der Wiederherstellungsauftrag für den ersten Datentyp gesendet wurde.
- Wählen Sie den nächsten Datentyp und die entsprechenden Wiederherstellungsoptionen aus. Wenn Sie die anderen Datentypen nicht wiederherstellen möchten, klicken Sie auf "Abbrechen", um den Wiederherstellungsassistenten zu schließen. Die bereits gesendeten Aufträge werden davon nicht beeinträchtigt.
- Wenn Sie Aufträge für alle Datentypen konfiguriert haben, ändert sich die Schaltfläche "Weiter" in "Fertigstellen". Wenn Sie auf "Fertigstellen" klicken, sendet Backup Exec den letzten Wiederherstellungsauftrag und schließt den Wiederherstellungsassistenten.

Wiederherstellen von Dateisystemdaten

Wenn Sie Dateien, Ordner oder Datenträger wiederherstellen, können Sie zu einem bestimmten Zeitpunkt oder aus einem Backup-Satz wiederherstellen.

Wenn Sie wissen, welcher Backup-Satz, welcher abgeschlossene Backup-Auftrag oder welches Speichermedium die Daten enthält, die Sie wiederherstellen möchten, können Sie den "Assistent für Wiederherstellungsaufträge" von dort aus starten.

Andernfalls können Sie einen Server auswählen und dann den Wiederherstellungsassistenten starten.

Siehe ["Wiederherstellen von Daten aus einem Server, einem Backup-Satz, einem Backup-Auftrag oder einem Speichergerät"](#) auf Seite 261.

So stellen Sie Dateisystemdaten wieder her

- 1** Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" mit der rechten Maustaste auf den Server, aus dem Sie Daten wiederherstellen möchten, und klicken Sie dann auf "Wiederherstellen".
- 2** Wählen Sie "Dateien, Ordner oder Datenträger" und klicken auf "Weiter".
- 3** Sie haben folgende Möglichkeiten:

So stellen Sie die Daten zu einem Zeitpunkt wieder her, an dem der Backup-Satz erstellt wurde

Wählen Sie "Datei- und Ordner-Backups zu einem Zeitpunkt".

Hinweis: Wenn Sie Dateisystemdaten zu einem Zeitpunkt wiederherstellen, wählen Sie einen wiederherzustellenden Backup-Satz aus. Der Backup-Satz stellt die Dateisystemdaten an dem Zeitpunkt dar, an dem er gesichert wurde. Backup Exec stellt automatisch alle zugehörigen Backup-Sätze wieder her, die erforderlich sind, um die Dateisystemdaten in dem Zustand am Zeitpunkt wiederherzustellen.

So stellen Sie Datei- und Ordner-Backups aus einem Backup-Satz wieder her

Wählen Sie "Datei- und Ordner-Backups aus einem Backup-Satz".

Hinweis: Wenn Sie Dateisystemdaten aus einem Backup-Satz wiederherstellen, wählen Sie einen wiederherzustellenden Backup-Satz aus. Backup Exec stellt die Dateisystemdaten genau so wieder her, wie sie im ausgewählten Backup-Satz vorliegen. Keine abhängigen Backup-Sätze werden für die Wiederherstellung ausgewählt.

So suchen Sie nach Dateien und Ordnern

Wählen Sie "Gefundene Dateien und Ordner".

So stellen Sie blockierte Dateien wieder her

Gehen Sie dazu in folgender Reihenfolge vor:

- Blockierte Elemente enthalten persönliche Informationen. Standardmäßig sind blockierte Elemente nicht zum Wiederherstellen verfügbar.
- Nur der Eigentümer eines System-Login-Kontos ist berechtigt, diese blockierten Elemente wiederherzustellen. Der Grund für die Wiederherstellung wird im Überwachungsprotokoll aufgezeichnet.
- 1** Aktivieren Sie das Kontrollkästchen "Wiederherstellen blockierter Elemente zulassen".
 - 2** Geben Sie im Dialogfeld "Blockierte Elemente wiederherstellen" einen Grund ein und klicken Sie dann auf "OK".
- Siehe ["Info zu GDPR Guard"](#) auf Seite 869.

4 Klicken Sie auf "Weiter".

Wenn Sie den Zugriff auf gesicherte Dateien mit dem BEMCLI-Befehl `Import-BEItemsToBlock` blockiert haben, sind die blockierten Dateien nicht verfügbar, wenn Sie Dateien zum Wiederherstellen suchen.

5 Folgen Sie im Assistenten für Wiederherstellungsaufträge den Anweisungen zum Wiederherstellen der Daten.

Vollständige Online-Wiederherstellung eines Microsoft Windows-Computers

Sie können eine vollständige Online-Wiederherstellung eines Microsoft Windows-Computers durchführen, wenn der Computer vollständig für ein Backup ausgewählt wurde. Wählen Sie die Zeit im Backup aus, ab der Sie den Computer wiederherstellen möchten. Alle erforderlichen Backup-Sätze werden automatisch ausgewählt. Sie können zusätzliche Backup-Sätze auswählen, um sie dementsprechend wiederherzustellen. Eine Wiederherstellung kann nicht umgeleitet werden.

Hinweis: Bei einer Online-Wiederherstellung mit Agent for Windows werden unter Windows 8 und höher die WindowsApps-Ordner nicht wiederhergestellt. Der Wiederherstellungsauftrag ist aber dennoch erfolgreich. Microsoft empfiehlt, die WindowsApps-Ordner in den Einstellungen mit der Option "Gerät - Zurücksetzen" wiederherzustellen.

Bei der Wiederherstellung werden möglicherweise die folgenden WindowsApps-Ordner ignoriert:

Der in

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Appx\PackageRoot`
erwähnte Ordner

Der in

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Appx\PackageRepositoryRoot`
erwähnte Ordner

`%SystemRoot%\InfusedApps`

So führen Sie eine vollständige Online-Wiederherstellung eines Microsoft Windows-Computers aus

- 1** Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" mit der rechten Maustaste auf den wiederherzustellenden Computer, und klicken Sie dann auf "Wiederherstellen".
- 2** Wählen Sie "Ein Windows-Computer, der vollständig für ein Backup ausgewählt wurde" und klicken Sie auf "Weiter".
- 3** Klicken Sie auf "Vollständige Online-Wiederherstellung eines Computers oder Wiederherstellen von Systemkomponenten" und dann auf "Weiter".
- 4** Folgen Sie im Assistenten für Wiederherstellungsaufträge den Anweisungen zum Wiederherstellen der Daten.

Wenn Sie blockierte Elemente angegeben haben, werden diese nicht wiederhergestellt.

Siehe ["Info zum Sichern von wichtigen Systemkomponenten"](#) auf Seite 200.

Siehe ["Methoden für das Wiederherstellen von Daten in Backup Exec"](#) auf Seite 258.

Wiederherstellen des Systemstatus

Je nachdem, welche Version von Microsoft Windows, welche Service Pack Levels und welche Funktionen installiert sind können Sie die folgenden Systemstatusdaten wiederherstellen:

- Active Directory

- Automatisierte Systemwiederherstellung
- Intelligenter Hintergrundübertragungsdienst
- COM+-Klassenregistrierungsdatenbank
- Dynamic Host Configuration Protocol
- Ereignisprotokolle
- Ressourcen-Manager für Dateiserver
- Internet Information Service (IIS)
- Microsoft Search-Dienst
- Netzwerkrichtlinienserver
- Registrierung
- Remote-Speicher
- Wechselmedien-Manager
- Shadow Copy Optimization Writer
- Systemdateien
- Terminalserver-Lizenzierung
- Terminaldienste-Gateway
- Windows-Bereitstellungsdienste
- Windows-Verwaltungsinstrumentation (WMI)

Hinweis: Zum Wiederherstellen von Windows Internet Name Service (WINS) müssen Sie auch die Registrierung wiederherstellen. Sie können WINS nicht separat wiederherstellen.

Wenn der Server ein Zertifikatsserver ist, dann umfasst der Systemstatus die Datenbank für Zertifikatdienste.

Wenn der Server ein Domänencontroller ist, dann umfasst der Systemstatus die Active Directory-Dienstdatenbank und das SYSVOL-Verzeichnis.

Siehe "[Info zum Agent for Microsoft Active Directory](#)" auf Seite 1439.

Sie müssen den Computer neu starten, nachdem Sie die Systemstatusdaten wiederhergestellt haben.

Warnung: Brechen Sie den Wiederherstellungsauftrag des Systemstatus nicht ab. Durch Abbrechen dieses Auftrags kann der Server unbrauchbar werden.

Wenn Sie wissen, welcher Backup-Satz, welcher abgeschlossene Backup-Auftrag oder welches Speichermedium die Daten enthält, die Sie wiederherstellen möchten, können Sie den "Assistent für Wiederherstellungsaufträge" von dort aus starten. Andernfalls können Sie einen Server auswählen und dann den "Assistent für Wiederherstellungsaufträge" starten.

Siehe ["Wiederherstellen von Daten aus einem Server, einem Backup-Satz, einem Backup-Auftrag oder einem Speichergerät"](#) auf Seite 261.

Hinweis: Wenn Sie den Systemzustand wiederherstellen, erstellt Backup Exec möglicherweise folgendes temporäres Verzeichnis:

%SystemRoot%\F52E2DD5-CE7D-4e54-8766-EE08A709C28E

Sie können dieses Verzeichnis nach Abschluss des Wiederherstellungsauftrags löschen.

So stellen Sie den Systemstatus wieder her

- 1** Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" mit der rechten Maustaste auf den Computer, dessen Systemstatus Sie wiederherstellen möchten und klicken Sie dann auf "Wiederherstellen".
- 2** Klicken Sie auf "Vollständige Online-Wiederherstellung eines Computers oder Wiederherstellen von Systemkomponenten" und dann auf "Weiter".
- 3** Befolgen Sie die Anweisungen des "Assistenten für Wiederherstellungsaufträge", um die Daten wiederherzustellen.
- 4** Nachdem Sie Systemstatusdaten wiederherstellen, starten Sie den Computer neu.

Siehe ["Info zum Sichern von wichtigen Systemkomponenten"](#) auf Seite 200.

Siehe ["Vollständige Online-Wiederherstellung eines Microsoft Windows-Computers"](#) auf Seite 267.

Wiederherstellen des Systemstatus auf einem Domänencontroller

Um den Systemstatus auf einem Computer wiederherzustellen, der ein Domänencontroller ist, müssen Sie den Computer im abgesicherter Modus starten. Verwenden Sie dann den Wiederherstellungsmodus für die Verzeichnisdienste, um die Wiederherstellung durchzuführen.

Um Active Directory auf den anderen Domänencontrollern in der Domäne zu replizieren, müssen Sie eine autoritative Wiederherstellung von Active Directory durchführen. Bei einer autoritativen Wiederherstellung wird sichergestellt, dass die wiederhergestellten Daten auf allen Servern repliziert werden. Zu einer autoritativen Wiederherstellung gehört die Ausführung des Ntdsutil-Dienstprogramms von Microsoft, nachdem Backup Exec des Systemstatus wiederhergestellt hat, aber bevor der Server neu gestartet wird. Weitere Informationen zu autoritativen Wiederherstellungen und zum Dienstprogramm Ntdsutil finden Sie in der Microsoft-Dokumentation.

So stellen Sie den Systemstatus auf einem Domänencontroller wieder her

- 1** Starten Sie den Zielservers im Verzeichnisdienst-Wiederherstellungsmodus neu.

In Ihrer Microsoft-Dokumentation finden Sie weitere Informationen hierzu.
- 2** Öffnen Sie die Dienste.
- 3** Gehen Sie bei jedem der aufgelisteten Backup Exec Services in der folgenden Reihenfolge vor:
 - Klicken Sie auf "Eigenschaften".
 - Klicken Sie auf der Registerkarte "Login" auf "Dieses Konto".
 - Geben Sie ein Benutzerkonto mit lokalen Administratorrechten ein und klicken Sie dann auf "OK".
 - Klicken Sie mit der rechten Maustaste auf den Dienst und dann auf "Starten".
- 4** Führen Sie nach dem Start der Backup Exec Services den Assistent für Wiederherstellungsaufträge aus, um den Systemstatus wiederherzustellen.

Siehe "[Methoden für das Wiederherstellen von Daten in Backup Exec](#)" auf Seite 258.
- 5** Aktivieren Sie im Assistent für Wiederherstellungsaufträge die Option "Bei Wiederherstellung von SYSVOL im Systemstatus diesen Server zum primären Vermittler für die Replikation bestimmen".
- 6** Starten Sie den Server neu, bevor Sie weitere Daten wiederherstellen.

Installieren eines Windows Server-Domänencontrollers in einer vorhandenen Domäne durch die Anwendung einer umgeleiteten Wiederherstellung

Um einen Windows Server-Domänencontroller in eine vorhandene Domäne zu installieren, müssen Active Directory- und SYSVOL-Daten auf den neuen Domänencontroller repliziert werden. Wenn die zu replizierende Datenmenge sehr groß oder die Verbindung zwischen den Domänencontrollern langsam ist, kann die Replikation eine gewisse Zeit in Anspruch nehmen. Die Menge der zu replizierenden Daten und die Verbindungsgeschwindigkeit beeinflusst auch die Replikationszeit des Active Directory Application Mode. Um die Replikationszeit für Active Directory und Active Directory Application Mode zu reduzieren, können Sie die Microsoft Windows-Funktion "Installieren von Medium" verwenden.

Verwenden Sie für Active Directory die Funktion "Installieren von Medium". Stellen Sie die Systemstatus-Backup-Sätze eines vorhandenen Domänencontrollers in der Domäne wieder her, in der Sie einen neuen Domänencontroller hinzufügen möchten. Anschließend können Sie eine umgeleitete Wiederherstellung der Systemstatus-Backup-Sätze auf den Ziel-Domänencontroller durchführen.

Für Active Directory Application Mode können die Daten unter Verwendung des ADAM-Writers gesichert werden. Anschließend können Sie eine umgeleitete Wiederherstellung der Daten aus dem ADAM-Backup auf den Zielcomputer vornehmen.

Siehe ["Info zum Agent for Microsoft Active Directory"](#) auf Seite 1439.

Weitere Informationen dazu finden Sie in der Microsoft-Dokumentation.

Tabelle 5-3

Information zum Installieren eines Windows Server-Domänencontrollers in eine vorhandene Domäne durch die Anwendung einer umgeleiteten Wiederherstellung

Schritt	Beschreibung
Schritt 1	<p>Sichern Sie die Systemstatusdaten eines aktiven Windows Server-Domänencontrollers in der Zieldomäne. Sichern Sie die Daten auf einen Wechseldatenträger, beispielsweise ein Plattenkassettengerät oder ein Band.</p> <p>Siehe "Sichern von Daten" auf Seite 174.</p>

Schritt	Beschreibung
Schritt 2	<p>Hängen Sie den Speicher an, der die Systemstatusdaten des Computers enthält, die Sie in der Zieldomäne installieren möchten.</p> <p>Hinweis: Es wird empfohlen, dass Sie den Speicher verschlüsseln. Gehen Sie beim Transport des Speichers zum Speicherort in der Zieldomäne vorsichtig vor.</p>
Schritt 3	<p>Inventarisieren und Katalogisieren Sie den Speicher.</p> <p>Siehe "Inventarisieren und Katalogisieren von Speichergeräten" auf Seite 552.</p>
Schritt 4	<p>Leiten Sie die Wiederherstellung der Systemstatus-Backup-Sätze zu einem temporärem Speicherort auf einem Datenträger oder einem Verzeichnis auf dem Zielcomputer um.</p> <p>Siehe "Wiederherstellen des Systemstatus " auf Seite 268.</p>
Schritt 5	<p>Starten Sie die Domänencontrollerinstallation, indem Sie in die folgenden Schritte durchführen:</p> <ul style="list-style-type: none"> ■ Auf dem Zielcomputer klicken Sie auf "Start" und dann auf "Ausführen". ■ Geben Sie <code>dcpromo /advein</code> und klicken Sie auf OK. ■ Wenn der Installationsassistent für Active Directory angezeigt wird, klicken Sie auf Weiter. ■ Wählen Sie Zusätzlicher Domänencontroller für eine vorhandene Domäne und klicken Sie auf Weiter. ■ Wählen Sie Von diesen wiederhergestellten Backup-Dateien, geben den temporären Speicherort an, an den Sie die Systemstatus-Daten wiederherstellen möchten und klicke Sie auf Weiter. ■ Befolgen Sie die Anweisungen auf dem Bildschirm, um den Installationsassistenten für Active Directory abzuschließen.
Schritt 6	Schließen Sie die Installation des Domänencontrollers ab.
Schritt 7	Starten Sie den Computer mit dem neuen Domänencontroller neu.
Schritt 8	<p>Lassen Sie die verbliebenen Systemstatus-Backup-Sätze ablaufen, die Sie zum temporären Speicherort umgeleitet haben.</p> <p>Siehe "Ändern des Ablaufdatums von Backup-Sätzen auf plattenbasierten Speichergeräten" auf Seite 404.</p>

Wiederherstellen der Shadow Copy-Komponenten von Backup Exec

Das Schattenkopiekomponenten-Dateisystem von Backup Exec verwendet den Volumeschattenkopie-Dienst (VSS) von Microsoft, um Drittanbieteranwendungen und Benutzerdaten auf Windows-Computern zu schützen. Sie können die Elemente in Backup Exec-Schattenkopiekomponenten einzeln oder zusammen wiederherstellen.

Die folgenden Elemente sind in Backup Exec-Schattenkopiekomponenten enthalten:

- Backup Exec-Deduplizierungsspeicher
- Verteilte Dateisystemreplikation (DFSR)
- OSISoft PI-Serverdaten

Wenn Sie domänenbasierte Microsoft Distributed File System(DFS)-Namespaces wiederherstellen, müssen Sie auch das Active Directory zum gleichen Zeitpunkt wiederherstellen. Domänenbasierte DFS-Namespaces verweisen auf Daten im Active Directory. Wenn Sie die Namespaces wiederherstellen, ohne das Active Directory auf denselben Zeitpunkt wiederherzustellen, werden diese Informationen nicht wiederhergestellt und es werden eventuell Fehler in der DFS-Management-Konsole ausgegeben.

Wenn Sie wissen, welcher Backup-Satz, welcher abgeschlossene Backup-Auftrag oder welches Speichermedium die Daten enthält, die Sie wiederherstellen möchten, können Sie den "Assistent für Wiederherstellungsaufträge" von dort aus starten. Andernfalls können Sie einen Server auswählen und dann den "Assistent für Wiederherstellungsaufträge" starten.

Siehe ["Wiederherstellen von Daten aus einem Server, einem Backup-Satz, einem Backup-Auftrag oder einem Speichergerät"](#) auf Seite 261.

So stellen Sie Shadow Copy-Komponenten von Backup Exec wieder her

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" mit der rechten Maustaste auf den Server und klicken Sie dann auf "Wiederherstellen".
- 2 Wählen Sie "Shadow Copy-Komponenten" und klicken Sie auf dann auf "Weiter".
- 3 Befolgen Sie die Anweisungen des "Assistenten für Wiederherstellungsaufträge", um die Daten wiederherzustellen.

Siehe ["Methoden für das Wiederherstellen von Daten in Backup Exec"](#) auf Seite 258.

Siehe ["Wiederherstellen des Systemstatus "](#) auf Seite 268.

Wiederherstellen von Dienstprogrammpartitionen oder Unified Extensible Firmware Interface-Systempartition

Sie können Dienstprogrammpartitionen oder Unified Extensible Firmware Interface (UEFI)-Partition für die Wiederherstellung auswählen. Dienstprogrammpartitionen sind kleine Partitionen, die OEM-Händler wie zum Beispiel Dell, Hewlett-Packard und IBM-Installation auf der Festplatte installieren. Diese Partitionen enthalten Systemdiagnostik- und Konfigurationsdienstprogramme. UEFI-Partitionen sind die kleinen Partitionen, die das Betriebssystem erstellt. Die UEFI-Systempartitionen enthalten die kritischen Systemdateien wie etwa "bootmgr" und "BOOT\BCD".

Für die Wiederherstellung von Dienstprogrammpartitionen gelten die folgenden Anforderungen:

- Sie müssen die Dienstprogrammpartitionen neu erstellen, bevor Sie Daten wiederherstellen.
- Sie müssen Administratorrechte haben.
- Sie können die Wiederherstellung einer Dienstprogrammpartition nicht zu einem anderen Computer umleiten.
- Sie können nur Dienstprogrammpartitionen desselben Anbieters wiederherstellen. So können Sie z. B. Dell-Dienstprogrammpartitionen nicht auf einer Compaq-Dienstprogrammpartition wiederherstellen.
- Die Dienstprogrammpartition, auf der Sie die Daten wiederherstellen, muss mindestens dieselbe Größe wie die Dienstprogrammpartition aufweisen, die gesichert wurde.

Wenn Sie wissen, welcher Backup-Satz, welcher abgeschlossene Backup-Auftrag oder welches Speichermedium die Daten enthält, die Sie wiederherstellen möchten, können Sie den "Assistent für Wiederherstellungsaufträge" von dort aus starten. Andernfalls können Sie einen Server auswählen und dann den "Assistent für Wiederherstellungsaufträge" starten.

Siehe ["Wiederherstellen von Daten aus einem Server, einem Backup-Satz, einem Backup-Auftrag oder einem Speichergerät"](#) auf Seite 261.

So stellen Sie Dienstprogrammpartitionen oder UEFI-Systempartitionen wieder her

- 1** Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" mit der rechten Maustaste auf den Computer, dessen Dienstprogrammpartitionen oder UEFI-Systempartitionen Sie wiederherstellen möchten und klicken Sie dann auf "Wiederherstellen".
- 2** Wählen Sie eine der folgenden Optionen aus und klicken Sie auf "Weiter" :
 - Dienstprogrammpartition
 - Unified Extensible Firmware Interface-Systempartition
- 3** Befolgen Sie die Anweisungen des "Assistenten für Wiederherstellungsaufträge", um die Daten wiederherzustellen.

Siehe ["Methoden für das Wiederherstellen von Daten in Backup Exec"](#) auf Seite 258.

Informationen zum Wiederherstellen verschlüsselter Daten

Verschlüsselte Backup-Sätze sind in der Auswahlliste für die Wiederherstellung durch ein Schlosssymbol gekennzeichnet. Wenn Sie verschlüsselte Daten wiederherstellen möchten, validiert Backup Exec automatisch den dazugehörigen Verschlüsselungsschlüssel. Befindet sich der zum Sichern der Daten verwendete Verschlüsselungsschlüssel nach wie vor in der Backup Exec-Datenbank, wählt Backup Exec automatisch diesen Verschlüsselungsschlüssel. Wird dieser Verschlüsselungsschlüssel jedoch nicht gefunden, fordert Backup Exec Sie auf, den Kennsatz für den zum Sichern der Daten verwendeten Verschlüsselungsschlüssel anzugeben. Wenn Sie diesen Satz korrekt eingeben, erstellt Backup Exec den Schlüssel neu.

Wenn Sie einen eingeschränkten Verschlüsselungsschlüssel verwenden, um Daten zu sichern, müssen Benutzer, die den Schlüssel nicht besitzen, die Passphrase eingeben, um Daten wiederherzustellen.

Siehe ["Verwendung von Verschlüsselung mit Backup Exec"](#) auf Seite 727.

Siehe ["Verwaltung von Verschlüsselungscodes"](#) auf Seite 731.

Info zur Wiederherstellung von NetWare SMS-Datenträger-Backups auf andere als SMS-Datenträger mit Backup Exec

In Backup Exec wird die Wiederherstellung von NetWare SMS-Datenträger-Backups auf andere als SMS-Datenträger unterstützt. So können z. B. Daten, die mit Backup Exec for NetWare Servers oder SBackup von Novell gesichert wurden, auf dem Backup Exec-Server oder einer anderen Netzwerkfreigabe wiederhergestellt werden.

Die unterstützten Betriebssysteme, Plattformen und Anwendungen finden Sie in der Liste der mit Backup Exec kompatiblen Software.

Abbrechen eines Wiederherstellungsauftrags

Warnung: Durch das Abbrechen eines laufenden Wiederherstellungsauftrags werden die Daten und das Laufwerk möglicherweise unbrauchbar.

Um den Abbruch eines Wiederherstellungsauftrags zu vermeiden, können Sie die Wiederherstellung zu einem nicht kritischen Ziel umleiten. Wenn der Auftrag erfolgreich abgeschlossen ist, kopieren Sie die Daten an den endgültigen Bestimmungsort.

Brechen Sie Wiederherstellungsaufträge des Systemstatus nicht ab. Durch das Abbrechen eines Wiederherstellungsauftrags des Systemstatus wird das System möglicherweise beschädigt.

So brechen Sie einen Wiederherstellungsauftrag ab:

- 1 Klicken Sie auf der Registerkarte "Auftragsüberwachung" mit der rechten Maustaste auf den abzubrechenden Auftrag.
- 2 Wenn Sie vom System gefragt werden, ob Sie den Auftrag abbrechen möchten, klicken Sie auf "Ja".

Siehe ["Abbrechen eines aktiven Auftrags"](#) auf Seite 291.

Funktionsweise der Backup Exec-Kataloge

Beim Sichern von Daten erstellt Backup Exec einen Katalog mit Informationen über die Backup-Sätze und über das Speichergerät, auf dem die Backup-Sätze gespeichert sind. Wenn Sie die wiederherzustellenden Daten auswählen, verwendet Backup Exec die Kataloginformationen für die Suche nach den ausgewählten

Elementen für die Wiederherstellung und den Speichergeräte, auf denen diese sich befinden.

Wenn ein Speichergerät vollständig katalogisiert ist, können Sie folgende Schritte durchführen:

- Anzeigen von Informationen zu allen Verzeichnissen und Dateien eines Backup-Satzes
- Suchen nach Dateien für die Wiederherstellung

Backup Exec katalogisiert jeden Backup-Auftrag. Wenn die Kataloge jedoch gekürzt werden, werden nur Informationen zu Backup-Sätzen aufgelistet. Sie können Dateien oder Dateiattribute nicht anzeigen. Die Menge der Informationen im Katalog ist davon abhängig, ob Sie festlegen, dass Kataloge nach einer bestimmten Frist gekürzt werden sollen.

Kataloge befinden sich auf dem Backup Exec-Server und auf dem Speichergerät, an das Sie den Backup-Auftrag geschickt haben.

Um die Daten wiederherzustellen die durch eine andere Installation von Backup Exec gesichert wurden, müssen Sie zuerst einen Katalogvorgang auf dem Speichergerät auf dem lokalen Backup Exec-Server ausführen. Der Katalog für einen Backup-Auftrag, der auf einer Installation von Backup Exec ausgeführt wurde, ist in anderen Installationen von Backup Exec nicht vorhanden.

Wenn Sie Granular Recovery Technology (GRT) für Exchange, SharePoint oder Backups virtueller Computer aktivieren, wird nach Abschluss des Backups standardmäßig eine Katalogisierung ausgeführt.

Für Exchange- und SharePoint-Backups mit Agent wird die vollständige Katalogisierung sofort nach allen vollständigen Backups ausgeführt. Sie wird einmal alle 24 Stunden für alle inkrementellen und differenziellen Backups ausgeführt, selbst wenn Sie mehr als einen GRT-Auftrag für diesen Zeitraum planen.

Für Hyper-V- und VMware-Backups wird die vollständige Katalogisierung standardmäßig sofort nach allen vollständigen, inkrementellen und differenziellen Backups ausgeführt. Sie können auch eine vollständige Katalogisierung planen.

Informationen zu den Best Practices zum Verwalten von Katalogen in Backup Exec finden Sie unter *Best Practices für Backup Exec*.

Siehe ["Konfigurieren der Standardoptionen für Kataloge"](#) auf Seite 279.

Siehe ["Katalogisieren eines Speichergeräts"](#) auf Seite 548.

Siehe ["Info zum Katalogisieren von Band- oder Plattenspeichermédien, die verschlüsselte Backup-Sätze enthalten"](#) auf Seite 505.

Siehe ["Konfigurieren der Optionen für Instant GRT und Vollständige Katalogisierung zum Verbessern der Backup-Leistung von GRT-Aufträgen"](#) auf Seite 656.

Konfigurieren der Standardoptionen für Kataloge

Sie können die Standardoptionen für Kataloge konfigurieren, um die für Ihre Umgebung am besten geeigneten Standardwerte festzulegen.

Siehe ["Funktionsweise der Backup Exec-Kataloge"](#) auf Seite 277.

Konfigurieren der Standardoptionen für Kataloge

- 1** Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Backup Exec-Einstellungen".
- 2** Klicken Sie im linken Teilfenster auf "Katalog".
- 3** Bearbeiten Sie eine der folgenden Optionen:

Alle Medien in der Reihenfolge für Katalogisierungsvorgänge anfordern

Katalogisiert die Medien in Bandlaufwerken und Plattenkassetten beginnend mit der niedrigsten bekannten Bandnummer in der Bandfamilie. Wenn beispielsweise das erste Band nicht verfügbar ist, beginnt der Katalogisierungsauftrag mit dem zweiten. Wenn Sie diese Option deaktivieren, beginnt der Katalogisierungsauftrag mit dem von Ihnen angegebenen Medium.

Wenn Sie "Alle Medien in der Reihenfolge für Katalogvorgänge anfordern" deaktivieren, können Sie die Option "Speicherbasierte Kataloge verwenden" nicht auswählen.

Diese Option ist standardmäßig aktiviert.

Speicherbasierte Kataloge
verwenden

Ermöglicht es Backup Exec, die Kataloginformationen vom Speichergerät zu lesen.

Speicherbasierte Kataloge ermöglichen die schnelle Katalogisierung der Backup-Sätze, die nicht im serverbasierten Katalog von Backup Exec enthalten sind. Ein Beispiel hierfür ist die Katalogisierung von Backup-Sätzen, die durch eine andere Installation von Backup Exec erstellt wurden.

Speicherbasierte Kataloge ermöglichen die Katalogisierung von Backup-Sätzen in Minuten, anders als die herkömmlichen Katalogisierungsverfahren für einzelne Dateien, die Stunden in Anspruch nehmen.

Wenn Backup Exec die einzelnen Dateiblöcke lesen soll, um einen neuen Katalog zu erstellen, deaktivieren Sie diese Option. Sie sollten diese Option nur deaktivieren, wenn normale Katalogisierungsmethoden nicht zum gewünschten Ergebnis führen.

Hinweis: Es wird empfohlen, dass Sie immer zuerst speicherbasierte Kataloge verwenden, bevor Sie diese Option löschen.

Wenn Sie "Alle Medien in der Reihenfolge für Katalogvorgänge anfordern" deaktivieren, steht die Option "Speicherbasierte Kataloge verwenden" nicht zur Verfügung.

Diese Option ist standardmäßig aktiviert.

Die Option "Speicherbasierte Kataloge verwenden" muss für die folgenden Wiederherstellungsszenarien aktiviert werden:

- Diese Option muss aktiviert sein, wenn Sie die NDMP Feature verwenden, damit NAS-Server-Backup-Sätze katalogisiert werden können.
 Siehe "[Wiederherstellen und Umleiten von Wiederherstellungsdaten für NDMP-Server](#)" auf Seite 1550.
- Diese Option muss aktiviert sein, wenn Sie Advanced Disk-based Backup Feature verwenden, damit Sie die True Image-Wiederherstellung nutzen können.
 Siehe "[Infos zur True Image-Wiederherstellung für synthetische Backups](#)" auf Seite 1524.
- Diese Option muss aktiviert sein, wenn Sie Simplified

Disaster Recovery verwenden, um die Backup-Sätze als Teil eines SDR-Wiederherstellungsvorgangs zu nutzen.

Siehe "[Vorbereiten von Computern für die Verwendung mit Simplified Disaster Recovery](#)" auf Seite 946.

- Diese Option muss aktiviert sein, um eine Wiederherstellung der Backup-Sätze mit Granular Recovery Technology durchzuführen, wenn ein virtueller Computer auf Band gesichert werden soll. Siehe "[Granular Recovery Technology](#)" auf Seite 737.

Kataloge kürzen nach

Behält nur die Kopfdaten bei und entfernt nach Ablauf der angegebenen Zeit alle Datei- und Verzeichnisdetails. Mit dieser Option wird die Kataloggröße beträchtlich verringert. Nachdem einer Kürzung der Kataloge können die Dateien und die Verzeichnisse nicht mehr wiederhergestellt werden, bis Sie den Speicher neu katalogisieren.

Siehe "[Katalogisieren eines Speichergeräts](#)" auf Seite 548.

Bei gekürzten Katalogen wird das Datum des letzten Zugriffs nicht zurückgesetzt.

Sie können aus gekürzten Katalogen eine vollständige Wiederherstellung der Backup-Sätze durchführen.

Diese Option gilt nicht für Aufträge für synthetische Backups.

Diese Option ist standardmäßig deaktiviert.

Katalogpfad

Legt den Pfad auf dem Datenträger für die Katalogdateien fest. Wenn der Pfad nicht existiert, werden Sie aufgefordert, ihn zu erstellen.

Der Standardpfad ist "C:<Backup Exec-Installationsordner>\Backup Exec\Catalogs".

Hinweis: Es wird empfohlen, dass Sie Backup Exec Utility verwenden, um den Katalogspeicherort zu ändern. Wenn Sie den Speicherort unter Verwendung des Felds "Katalogpfad" ändern, müssen Sie die vorhandenen Kataloge auf dem neuen Speicherort auch manuell kopieren und dann die Backup Exec-Dienste neu starten.

Siehe ["Verschieben der Backup Exec-Kataloge in einen neuen Ordner"](#) auf Seite 283.

- 4 Klicken Sie auf "OK".

Verschieben der Backup Exec-Kataloge in einen neuen Ordner

Es ist möglicherweise notwendig, die Kataloge in einen anderen Speicherort zu verschieben, falls der Speicherplatz nicht ausreicht oder andere Probleme vorliegen. Sie können Backup Exec so konfigurieren, dass ein anderer Ordner für die Katalogdateien verwendet wird.

Der Ordner auf Backup Exec-Server, in dem Kataloge gespeichert werden, kann auch geändert werden. Wenn Sie den Katalogordner auf dem Backup Exec-Server ändern, müssen Sie zuerst alle Backup Exec-Dienste beenden, alle vorhandenen Kataloge manuell in den neuen Katalogordner kopieren.

So verschieben Sie die Backup Exec-Kataloge in einen neuen Ordner

- 1 Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Backup Exec-Einstellungen".
- 2 Klicken Sie im linken Teilfenster auf "Katalog".
- 3 Geben Sie im Feld "Katalogpfad" den neuen Pfad für die Kataloge ein oder wählen Sie ihn aus.

Hinweis: Der Ordner muss unter Windows vorhanden sein. Erstellen Sie das Verzeichnis mithilfe von Windows Explorer, bevor Sie ihn im Feld "Katalogpfad" eingeben.

- 4 Klicken Sie auf "OK".

- 5 Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Backup Exec Services".
- 6 Klicken Sie auf "Alle Dienste beenden".
- 7 Klicken Sie auf "OK".

Nachdem alle Backup Exec Services beendet wurde, kopiere Sie die Katalogdateien aus dem alten Ordner in den neuen.
- 8 Öffnen Sie in Windows Explorer den Ordner, in dem die Kataloge derzeit gespeichert sind.
- 9 Kopieren Sie alle Elemente im Ordner, einschließlich aller Unterordner und aller Dateien.
- 10 Öffnen Sie in Windows Explorer den Ordner, in den die Kataloge verschoben werden sollen.
- 11 Fügen Sie alle Elemente im Ordner ein.

Starten Sie anschließend alle Backup Exec Services wieder.
- 12 Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Backup Exec Services".
- 13 Klicken Sie auf "Alle Dienste starten".
- 14 Klicken Sie auf "OK".

Katalogisieren von Backup-Sätzen

Bevor Sie die Daten wiederherstellen oder überprüfen können, müssen diese katalogisiert werden. Beim Sichern von Daten erstellt Backup Exec einen Katalog mit Informationen über die Backup-Sätze und über das Speichergerät, auf dem die Backup-Sätze gespeichert werden. Sie können Backup-Sätze jedoch jederzeit manuell katalogisieren.

Katalogisieren von Backup-Sätzen

- 1 Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, das mit den zu katalogisierenden Backup-Sätzen verbunden ist.
- 2 Klicken Sie im linken Teilfenster auf "Backup-Sätze".
- 3 Sie haben folgende Möglichkeiten:
 - Klicken Sie zum Katalogisieren eines einzelnen Backup-Satzes mit der rechten Maustaste auf den Backup-Satz.

- Um mehrere Backup-Sätze zu katalogisieren, klicken Sie bei gedrückter Umschalttaste oder Strg-Taste auf die Backup-Sätze und klicken Sie dann mit der rechten Maustaste auf einen der ausgewählten Backup-Sätze.

4 Klicken Sie auf "Katalogisieren".

Backup Exec führt Katalogisierung aus.

Siehe ["Backup-Sätze"](#) auf Seite 401.

Siehe ["Funktionsweise der Backup Exec-Kataloge"](#) auf Seite 277.

Verwalten und Überwachen von Aufträgen

In diesem Kapitel werden folgende Themen behandelt:

- [So überwachen und verwalten Sie Aufträge in Backup Exec](#)
- [Informationen zur Auftragsüberwachung](#)
- [Informationen zum Auftragsverlauf](#)
- [Anzeigen des Auftragsprotokolls](#)
- [Fehlerbehandlungsregeln für fehlgeschlagene oder abgebrochene Aufträge](#)
- [Liste von Auftragsstatus in Backup Exec](#)
- [Festlegen von Auftragsstatus- und Wiederherstellungsoptionen](#)

So überwachen und verwalten Sie Aufträge in Backup Exec

Backup Exec liefert viele Methoden, Ihr Backup, Wiederherstellung und Speicheraufträge zu überwachen und zu verwalten.

Auftragsüberwachung

Sie können Ihre aktiven und geplanten Aufträge von der Registerkarte "Auftragsüberwachung", von der Liste "Aufträge" auf der Registerkarte "Backup und Wiederherstellung" oder von der Registerkarte "Speicher" aus überwachen.

Sie können die aktiven und geplanten Aufträge, Zustand und Status der Aufträge, den Zeitplan und andere Details überwachen. Der Status von Berichten kann von der Registerkarte "Berichte" überwacht werden.

Tabelle 6-1 Orte, von denen Sie Aufträge überwachen können

Speicherort, in dem Sie Aufträge überwachen können	Weitere Informationen
Die Registerkarte "Auftragsüberwachung"	<p>Mit der Auftragsüberwachung können Sie alle Backup-, Wiederherstellungs-, Installations- und Speicheraufträge an einem einzigen Ort überwachen und verwalten. Die Auftragsüberwachung ist in zwei Teilfenster unterteilt. Das Teilfenster "Aufträge" zeigt Details zu allen aktiven sowie geplanten Aufträgen an. Das Teilfenster "Auftragsverlauf" zeigt Details zu allen kürzlich ausgeführten Aufträgen an. Standardmäßig werden alle aktuellen Aufträge im Teilfenster "Auftragsverlauf" angezeigt. Sie können den Standard ändern, indem Sie die Ansicht "Auftragsverlauf" filtern.</p> <p>Hinweis: Berichtsaufträge werden nicht in der Auftragsüberwachung angezeigt. Sie können Berichtsaufträge über die Registerkarte "Berichte" überwachen und verwalten.</p>
Die Registerkarte "Backup und Wiederherstellung"	<p>Wenn Sie auf einen Servernamen auf der Registerkarte "Backup und Wiederherstellung" doppelklicken, werden Details für diesen Server verfügbar. Sie können die Backup- und -Wiederherstellungsaufträge anzeigen, die geplant und für den ausgewählten Server aktiv sind. Sie können auch den Verlauf der Backup- und -Wiederherstellungsaufträge anzeigen, die auf dem ausgewählten Server verarbeitet wurden.</p>

Speicherort, in dem Sie Aufträge überwachen können	Weitere Informationen
Die Registerkarte "Speicher".	Wenn Sie auf eine Speichergerätgerätebezeichnung auf der Registerkarte "Speicher" doppelklicken, werden Details für dieses Speichergerät verfügbar. Sie können die Speichervorgangsaufträge anzeigen, die geplant und für das ausgewählte Speichergerät aktiv sind. Sie können auch den Verlauf von Speichervorgangsaufträgen, die für das ausgewählte Speichergerät verarbeitet wurden, anzeigen.
Die Registerkarte "Berichte".	Auf der Registerkarte "Berichte" können Sie siehe die geplanten Berichte in der Berichtgruppe "Anstehende aufrufen" und eine Liste von Berichten, die in der Berichtgruppe "Abgeschlossene aufrufen" abgeschlossen wurden, anzeigen.

Auftragsverwaltung

Backup Exec verfügt über Funktionen, mit denen Sie Backup-Aufträge, Wiederherstellungsaufträge und Speicheraufträge verwalten können.

Sie können Aufträge in der folgenden Weise verwalten:

- Bearbeiten Sie geplante Aufträge.
- Löschen Sie geplante Aufträge.
- Brechen Sie aktive Aufträge ab.
- Ändern Sie die Priorität von geplanten Aufträgen.
- Führen Sie einen geplanten Auftrag sofort aus.
- Halten Sie einen Auftrag oder die Auftragswarteschlange an.
- Führen Sie einen Test des Backup-Auftrags aus.
- Zeigen Sie die Auftragaktivitätsdetails, wie zum Beispiel Auftragstatistiken und Systeminformationen, für einen aktiven Auftrag an.
- So zeigen Sie den Verlauf eines Auftrags an.
- Nur fehlgeschlagene Aufträge wiederholen.
- Führen Sie einen Backup-Auftrag mit aktiviertem Debugging aus.

Siehe ["Bearbeiten von Backup-Definitionen"](#) auf Seite 226.

Siehe ["Anzeigen der Details zur Auftragsaktivität für aktive Aufträge"](#) auf Seite 290.

Siehe ["Löschen von geplanten Aufträgen"](#) auf Seite 299.

Siehe ["Abbrechen eines aktiven Auftrags"](#) auf Seite 291.

Siehe ["Ändern der Priorität für geplante Aufträge"](#) auf Seite 297.

Siehe ["Sofortiges Ausführen von geplanten Aufträgen"](#) auf Seite 297.

Siehe ["Aufträge anhalten"](#) auf Seite 292.

Siehe ["Anhalten der Auftragswarteschlange"](#) auf Seite 295.

Siehe ["Manuelle Ausführung von Probelaufaufträgen"](#) auf Seite 251.

Informationen zur Auftragsüberwachung

Mit der Auftragsüberwachung können Sie alle Backup-, Wiederherstellungs-, Installations- und Speicheraufträge an einem einzigen Ort überwachen und verwalten. Die Auftragsüberwachung ist in zwei Teilfenster unterteilt. Das Teilfenster "Aufträge" zeigt Details zu allen aktiven sowie geplanten Aufträgen an. Das Teilfenster "Auftragsverlauf" zeigt Details zu allen kürzlich ausgeführten Aufträgen an. Standardmäßig werden alle aktuellen Aufträge im Teilfenster "Auftragsverlauf" angezeigt. Sie können den Standard ändern, indem Sie die Ansicht "Auftragsverlauf" filtern.

Hinweis: Berichtsaufträge werden nicht in der Auftragsüberwachung angezeigt. Sie können Berichtsaufträge über die Registerkarte "Berichte" überwachen und verwalten.

Im Teilfenster "Aufträge" der Auftragsüberwachung können Sie aktive und geplante Aufträge folgendermaßen verwalten:

- Bearbeiten Sie geplante Aufträge.
- Löschen Sie geplante Aufträge.
- Brechen Sie aktive Aufträge ab.
- Ändern Sie die Priorität von geplanten Aufträgen.
- Führen Sie einen geplanten Auftrag sofort aus.
- Halten Sie einen Auftrag oder die Auftragswarteschlange an.
- Führen Sie einen Test-Backup-Auftrag aus.
- Zeigen Sie die Details zu den Auftragsaktivitäten für einen aktiven Auftrag an.
- So zeigen Sie den Verlauf eines Auftrags an

- Nur fehlgeschlagene Aufträge wiederholen.
- Führen Sie einen Backup-Auftrag mit aktiviertem Debugging aus.

Im Teilfenster "Auftragsverlauf" der Auftragsüberwachung können Sie abgeschlossene Aufträge folgendermaßen verwalten:

- Führen Sie den Auftrag sofort erneut aus.
- Zeigen Sie das Auftragsprotokoll an.
- Löschen Sie den Auftrag.
- Zeigen Sie die Auftragsverlaufdetails an.
- Aktivieren Sie die Fehlerbehandlungsregeln.
- Duplizieren Sie Auftragsverläufe.
- Verifizieren Sie einen Backup-Auftrag.
- Bearbeiten Sie die Einstellungen für einen Backup-Auftrag.
- Nur fehlgeschlagene Aufträge wiederholen.
- Führen Sie einen Backup-Auftrag mit aktiviertem Debugging aus.

Über die "Auftragsüberwachung" können Sie Daten aus den Backup-Sätzen eines abgeschlossenen Backup-Auftrags wiederherstellen. Zusätzlich können Sie den Backup-Kalender anzeigen.

Siehe ["So überwachen und verwalten Sie Aufträge in Backup Exec"](#) auf Seite 286.

Siehe ["Manuelle Ausführung von Probelaufaufträgen"](#) auf Seite 251.

Siehe ["Manuelles Duplizieren von Backup-Sätzen bzw. Auftragsverläufen"](#) auf Seite 246.

Siehe ["Gesicherte Daten manuell überprüfen"](#) auf Seite 252.

Siehe ["Bearbeiten von Backup-Definitionen"](#) auf Seite 226.

Anzeigen der Details zur Auftragsaktivität für aktive Aufträge

Bei Ausführung eines Auftrags können Sie Details für den Auftrag anzeigen, wie etwa abgeschlossener Prozentsatz, Auftragsrate und Byte-Anzahl.

So zeigen Sie Details für aktive Aufträge an

- 1 Sie haben folgende Möglichkeiten:

So zeigen Sie die Auftragsaktivität auf der Registerkarte "Auftragsüberwachung" an: Wählen Sie die Registerkarte "Auftragsüberwachung".

So zeigen Sie die Auftragsaktivität auf der Registerkarte "Backup und Wiederherstellung" oder der Registerkarte "Speicher" an

Gehen Sie wie folgt vor:

- Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, auf dem der Auftrag ausgeführt wird.
- Klicken Sie im linken Teilfenster auf "Aufträge".

- 2 Klicken Sie mit der rechten Maustaste auf den Auftrag und klicken Sie anschließend auf "Auftragsaktivität anzeigen".

Abbrechen eines aktiven Auftrags

Aufträge, die gerade ausgeführt werden, können abgebrochen werden. Wenn es sich um einen geplanten Auftrag handelt, wird er zum nächsten geplanten Zeitpunkt erneut ausgeführt.

Das Abbrechen eines Auftrags kann mehrere Minuten dauern. Während Backup Exec den Auftragsabbruch verarbeitet, wird in der Spalte "Auftragsstatus" der Status "Abbrechen steht aus" angezeigt.

So brechen Sie einen aktiven Auftrag ab

- 1 Sie haben folgende Möglichkeiten:

So brechen Sie den Auftrag von der Registerkarte "Auftragsüberwachung" aus ab

Wählen Sie die Registerkarte "Auftragsüberwachung" aus.

So brechen Sie den Auftrag auf der Registerkarte "Backup und Wiederherstellung" oder der Registerkarte "Speicher" ab

Gehen Sie wie folgt vor:

- Doppelklicken Sie auf der Registerkarte "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, auf dem der Auftrag läuft.
- Klicken Sie im linken Teilfenster auf "Aufträge".

- 2 Klicken Sie mit der rechten Maustaste auf den aktiven Auftrag, den Sie abbrechen möchten, und klicken Sie dann auf "Abbrechen".

- 3 Klicken Sie auf "Ja", um den Abbruch des Auftrags zu bestätigen.

Siehe ["Liste von Auftragsstatus in Backup Exec"](#) auf Seite 322.

Aufträge anhalten

Aktive und geplante Aufträge können angehalten werden. Wenn Sie einen aktiven Auftrag anhalten, wird er bis zum Abschluss weiter ausgeführt. Jedoch wird die nächste geplante Ausführung dieses Auftrags angehalten. Wenn Sie einen Auftrag anhalten, ändert sich der Status in der Spalte "Auftragsstatus" in "In Wartestellung".

So halten Sie Aufträge an

- 1 Sie haben folgende Möglichkeiten:

So halten Sie einen Auftrag von der	Wählen Sie die Registerkarte
Registerkarte "Auftragsüberwachung" aus	"Auftragsüberwachung" aus.
an	

So halten Sie einen Auftrag von der Registerkarte "Backup und Wiederherstellung" oder "Speicher" aus an

Gehen Sie wie folgt vor:

- Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, auf dem der Auftrag ausgeführt wird oder seine Ausführung geplant ist.
- Klicken Sie im linken Teilfenster auf "Aufträge".

2 Sie haben folgende Möglichkeiten:

So halten Sie einen einzelnen Auftrag an

Wählen Sie den Auftrag aus der Liste mit Aufträgen und klicken Sie dann in der Gruppe "Aufträge" auf "In Wartestellung". Wählen Sie dann "Auftrag in Wartestellung" aus.

So halten Sie alle aktiven Aufträge an

In der Gruppe "Aufträge" klicken Sie auf "In Wartestellung" und dann auf "Alle aktiven Aufträge anhalten". Sie müssen möglicherweise auf "Ja" klicken, um zu bestätigen, dass Sie alle aktiven Aufträge anhalten möchten.

Hinweis: Diese Option ist nur von der Registerkarte "Auftragsüberwachung" aus verfügbar.

So halten Sie alle geplanten Aufträge an

In der Gruppe "Aufträge" klicken Sie auf "In Wartestellung" und dann auf "Alle geplanten Aufträge anhalten". Sie müssen möglicherweise auf "Ja" klicken, um zu bestätigen, dass Sie alle geplanten Aufträge in Wartestellung versetzen möchten.

Hinweis: Diese Option ist nur von der Registerkarte "Auftragsüberwachung" aus verfügbar.

Siehe ["Aufheben der Wartestellung von Aufträgen"](#) auf Seite 294.

Aufheben der Wartestellung von Aufträgen

Sie können die Wartestellung eines geplanten Auftrags jederzeit aufheben. Wenn Sie die Wartestellung eines Auftrags aufheben, ändert sich der Status in der Spalte "Auftragsstatus" in den ursprünglichen Status des Auftrags, zum Beispiel "Aktiv" oder "Geplant".

So heben Sie die Wartestellung von Aufträgen auf

1 Sie haben folgende Möglichkeiten:

So entfernen Sie die Wartestellung von Aufträgen auf der Registerkarte "Auftragsüberwachung"

Wählen Sie die Registerkarte "Auftragsüberwachung" aus.

So entfernen Sie die Wartestellung von Aufträgen auf der Registerkarte "Backup und Wiederherstellung" oder "Speicher"

Gehen Sie wie folgt vor:

- Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, auf dem der Auftrag angehalten wurde.
- Klicken Sie im linken Teilfenster auf "Aufträge".

2 Sie haben folgende Möglichkeiten:

So entfernen Sie die Wartestellung von Aufträgen bei einem einzelnen Auftrag

Wählen Sie den Auftrag aus der Liste mit Aufträgen und klicken Sie dann in der Gruppe "Aufträge" auf "In Wartestellung". Wählen Sie dann "Auftrag in Wartestellung" aus, um das Häkchen zu entfernen.

Hinweis: Wenn der Auftrag, den Sie anhalten möchten, ein Teil einer Backup-Definition ist, müssen Sie möglicherweise auf die Auftragsdefinition doppelklicken, um den Auftrag anzuzeigen.

So heben Sie die Wartestellung bei allen aktiven Aufträgen auf

In der Gruppe "Aufträge" klicken Sie auf "In Wartestellung" und dann auf "Alle aktiven Aufträge anhalten", um das Häkchen zu entfernen. Sie müssen möglicherweise auf "Ja" klicken, um zu bestätigen, dass Sie die Wartestellung bei allen aktiven Aufträge aufheben möchten.

Hinweis: Diese Option ist nur von der Registerkarte "Auftragsüberwachung" aus verfügbar.

So heben Sie die Wartestellung bei allen geplanten Aufträgen auf

In der Gruppe "Aufträge" klicken Sie auf "In Wartestellung" und dann auf "Alle geplanten Aufträge anhalten", um das Häkchen zu entfernen. Sie müssen möglicherweise auf "Ja" klicken, um zu bestätigen, dass Sie die Wartestellung bei allen geplanten Aufträge aufheben möchten.

Hinweis: Diese Option ist nur von der Registerkarte "Auftragsüberwachung" aus verfügbar.

Siehe ["Aufträge anhalten"](#) auf Seite 292.

Anhalten der Auftragswarteschlange

Sie können die gesamte Auftragswarteschlange anhalten, um die Umgebung zu ändern. Der Server wurde angehalten, um die Auftragswarteschlange anzuhalten. Wenn Sie die Auftragswarteschlange anhalten, werden nur aktive Aufträge weiterhin ausgeführt, es sei denn, Sie brechen sie ab. Weitere Aufträge können erst wieder ausgeführt werden, wenn die Auftragswarteschlange fortgesetzt wird.

So halten Sie die Auftragswarteschlange an

1 Sie haben folgende Möglichkeiten:

So halten Sie die Auftragswarteschlange auf der Registerkarte "Auftragsüberwachung" an	Klicken Sie auf die Registerkarte "Auftragsüberwachung".
--	--

So halten Sie die Auftragswarteschlange auf der Registerkarte "Backup und Wiederherstellung" oder "Speicher" an

Gehen Sie wie folgt vor:

- Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, auf dem der Auftrag ausgeführt wird oder seine Ausführung geplant ist.
- Im linken Teilfenster klicken Sie auf "Aufträge".

- 2 Klicken Sie unter "Aufträge" auf "Anhalten" und dann auf "Auftragswarteschlange anhalten".
- 3 Klicken Sie auf "Ja".
- 4 Wenn aktive Aufträge ausgeführt werden, wählen Sie die abzubrechenden aus und klicken Sie auf "OK".

Siehe ["Fortsetzen einer angehaltenen Auftragswarteschlange"](#) auf Seite 296.

Fortsetzen einer angehaltenen Auftragswarteschlange

Wenn Sie das Anhalten der Auftragswarteschlange entfernen, wird der Server wieder gestartet und die Aufträge werden gemäß des Zeitplans ausgeführt.

So entfernen Sie das Anhalten der Auftragswarteschlange

- 1 Sie haben folgende Möglichkeiten:

So setzen Sie die Auftragswarteschlange auf der Registerkarte "Auftragsüberwachung" fort

Klicken Sie auf die Registerkarte "Auftragsüberwachung".

So setzen Sie die Auftragswarteschlange auf der Registerkarte "Backup und Wiederherstellung" oder "Speicher"

Gehen Sie wie folgt vor:

- Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, auf dem der Auftrag angehalten wurde.
- Im linken Teilfenster klicken Sie auf "Aufträge".

- 2 Klicken Sie in der Gruppe "Aufträge" auf "Anhalten" und dann auf "Auftragswarteschlange anhalten", um das Kontrollkästchen zu deaktivieren.

Siehe ["Anhalten der Auftragswarteschlange"](#) auf Seite 295.

Sofortiges Ausführen von geplanten Aufträgen

Sie können einen geplanten Auftrag sofort ausführen. Der Auftrag wird auch zum nächsten geplanten Zeitpunkt ausgeführt.

So führen Sie einen geplanten Auftrag sofort aus:

1 Sie haben folgende Möglichkeiten:

So führen Sie den Auftrag von der Registerkarte "Auftragsüberwachung" aus

Wählen Sie die Registerkarte "Auftragsüberwachung" aus.

So führen Sie den Auftrag auf der Registerkarte "Backup und Wiederherstellung" oder der Registerkarte "Speicher" aus

Gehen Sie wie folgt vor:

- Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, auf dem die Ausführung des Auftrags geplant ist.
- Klicken Sie im linken Teilfenster auf "Aufträge".

2 Klicken Sie mit der rechten Maustaste auf den geplanten Auftrag, den Sie ausführen möchten, und klicken Sie dann auf "Jetzt ausführen".

Hinweis: Wenn der geplante Auftrag Teil einer Backup-Definition ist, müssen Sie möglicherweise auf die Auftragsdefinition doppelklicken, um den geplanten Auftrag anzuzeigen.

Siehe ["Ändern der Priorität für geplante Aufträge"](#) auf Seite 297.

Siehe ["Löschen von geplanten Aufträgen"](#) auf Seite 299.

Ändern der Priorität für geplante Aufträge

Mit der Priorität legen Sie die Reihenfolge der auszuführenden Aufträge fest. Wenn zwei Aufträge, gleichzeitig ausgeführt werden sollen, wird durch die Priorität festgelegt, welcher Auftrag zuerst ausgeführt wird. Die Priorität wird für alle Vorkommen eines geplanten Auftrags geändert.

Die Priorität des Auftrags wird in der Auftragsliste in der Spalte "Priorität" angezeigt.

Diese Option ist besonders sinnvoll, wenn in Ihrer Umgebung eine beschränkte Anzahl von Geräten verfügbar ist, Sie aber wünschen, dass bestimmte Aufträge einen prioritären Zugriff auf die Geräte haben sollen. Ein bereiteter Auftrag mit einer

höheren Priorität wird vor einem bereiten Auftrag mit einer niedrigeren Priorität ausgeführt. Ein bereiter Auftrag mit einer höheren Priorität wird auch dann vor einem bereiten Auftrag mit niedrigerer Priorität ausgeführt, wenn dieser eine frühere geplante Startzeit aufweist.

Wenn mehrere Aufträge für die Ausführung bereit sind, aber auf die Verfügbarkeit eines Geräts warten müssen, legt Backup Exec fest, welche Aufträge zuerst ausgeführt werden. Backup Exec überprüft die Auftragspriorität und die geplante Startzeit des Auftrags.

Sie können die Auftragspriorität festlegen, wenn Sie folgende Schritte durchführen:

- Wählen Sie Speicheroptionen aus, wenn Sie einen Backup-Auftrag erstellen oder bearbeiten.
- Zeigen Sie geplante Aufträge auf der Registerkarte "Auftragsüberwachung" an.
- Zeigen Sie die geplanten Aufträge eines Servers im Bereich "Aufträge" auf der Registerkarte "Backup und Wiederherstellung" an.

Wenn Sie die Auftragspriorität in den Speicheroptionen oder im Bereich "Aufträge" ändern, können Sie von folgenden Prioritätsstufen auswählen:

- Höchste
- Hohe
- Mittlere
- Niedrige
- Niedrigste

Wenn Sie die Auftragspriorität in "Auftragsüberwachung" ändern, können Sie die Auftragspriorität nur erhöhen oder verringern. Sie können eine Stufe nicht angeben.

So ändern Sie die Priorität für einen geplanten Auftrag

- 1 Sie haben folgende Möglichkeiten:

So ändern Sie die Auftragspriorität von der Registerkarte "Auftragsüberwachung" Wählen Sie die Registerkarte "Auftragsüberwachung".

So ändern Sie die Auftragspriorität auf der Registerkarte "Backup und Wiederherstellung" oder der Registerkarte "Speicher" Gehen Sie wie folgt vor:

- Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, auf dem die Ausführung des Auftrags geplant ist.
- Klicken Sie im linken Teilfenster auf "Aufträge".

- 2 Klicken Sie mit der rechten Maustaste auf den geplanten Auftrag und klicken Sie dann auf "Priorität ändern".

Hinweis: Wenn der Auftrag ein Teil einer Backup-Definition ist, müssen Sie möglicherweise auf die Auftragsdefinition doppelklicken, um den Auftrag anzuzeigen.

- 3 Wählen Sie die neue Priorität aus.

Löschen von geplanten Aufträgen

Durch Löschen eines geplanten Auftrags werden alle geplanten Instanzen dieses Auftrags gelöscht. Um einen geplanten Auftrag nur an einem bestimmten Datum zu löschen, können Sie den Zeitplan entsprechend bearbeiten, um dieses Datum zu löschen.

Hinweis: Wenn eine Backup-Definition mehr als einen Auftragstyp umfasst, können Sie einen einzelnen Auftrags nicht mit der Option "Löschen" aus der Definition löschen. Stattdessen müssen Sie die Auftragsdefinition bearbeiten, um den geplanten Auftrag zu entfernen.

So löschen Sie einen geplanten Auftrag

- 1 Sie haben folgende Möglichkeiten:

So löschen Sie einen geplanten Auftrag auf der Registerkarte "Auftragsüberwachung"

Wählen Sie die Registerkarte "Auftragsüberwachung".

So löschen Sie einen Auftrag von der Registerkarte "Backup und Wiederherstellung" oder der Registerkarte "Speicher"

Gehen Sie wie folgt vor:

- Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, auf dem die Ausführung des Auftrags geplant ist.
- Klicken Sie im linken Teilfenster auf "Aufträge".

- 2 Klicken Sie mit der rechten Maustaste auf den geplanten Auftrag und klicken Sie dann auf "Löschen".

Hinweis: Wenn der Auftrag ein Teil einer Backup-Definition ist, müssen Sie möglicherweise auf die Auftragsdefinition doppelklicken, um den Auftrag anzuzeigen.

- 3 Klicken Sie auf "Ja".

Siehe ["So überwachen und verwalten Sie Aufträge in Backup Exec"](#) auf Seite 286.

Wiederholen nur fehlgeschlagener Aufträge

Sie können einen Backup-Auftrag nur für die Ressourcen wiederholen, die beim direkt vorhergehenden Durchgang nicht gesichert werden konnten. Diese Option ist nur für fehlgeschlagene oder abgebrochene Backup-Aufträge verfügbar. Wenn ein Backup-Auftrag erfolgreich war, ist diese Option ausgegraut.

Beispiel: Sie haben einen VMware-Backup-Auftrag, der fünf virtuelle Computer sichert. Es werden allerdings nur drei virtuelle Computer gesichert. Sie können das Auftragsprotokoll auf die Ursache des Fehlers prüfen, das Problem beheben und dann die Option "Nur fehlgeschlagene Aufträge wiederholen" verwenden. Diesmal werden nur die beiden virtuellen Computer gesichert, die beim vorherigen Durchgang nicht gesichert werden konnten. Die drei virtuellen Computer, die bereits gesichert wurden, werden nicht erneut gesichert.

Wenn Simplified Disaster Recovery für einen Backup-Auftrag aktiviert ist, und ein Fehler in mindestens einer der wichtigen Ressourcen auftrat, werden diese beim Wiederholen des fehlgeschlagenen Backup-Auftrags erneut gesichert. Dies gilt auch für die wichtigen Ressourcen, die bereits im vorherigen Durchgang gesichert wurden.

In einer CAS-MMS-Umgebung für Aufträge, die vom CAS-Server delegiert wurden, ist die Option zum Wiederholen eines fehlgeschlagenen Auftrags nur über die

CAS-Benutzeroberfläche verfügbar. Die Option ist für delegierte Aufträge in der MMS-Benutzeroberfläche deaktiviert.

So wiederholen Sie einen Auftrag für fehlgeschlagene Ressourcen

1 Sie haben folgende Möglichkeiten:

So wiederholen Sie den Auftrag über die Registerkarte "Auftragsüberwachung"

Klicken Sie auf die Registerkarte "Auftragsüberwachung".

So wiederholen Sie den Auftrag über die Registerkarte "Backup und Wiederherstellung" bzw. "Speicher"

Gehen Sie wie folgt vor:

- Doppelklicken Sie auf der Registerkarte "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, auf dem der Auftrag läuft.
- Klicken Sie im linken Teilfenster auf "Aufträge".

2 Sie haben folgende Möglichkeiten:

- Klicken Sie mit der rechten Maustaste auf den zu wiederholenden Auftrag und klicken Sie dann auf "Nur fehlgeschlagene Aufträge wiederholen".
- Klicken Sie auf der Registerkarte "Auftragsüberwachung" auf den zu wiederholenden Auftrag und klicken Sie dann auf "Nur fehlgeschlagene Aufträge wiederholen".

Es wird gemeldet, dass der Auftrag sofort sowie im Rahmen des festgelegten Zeitplans ausgeführt wird.

3 Klicken Sie auf "Ja".

Der Auftrag wird gestartet und jetzt wird nur die Ressource, die im vorherigen Durchgang nicht gesichert wurde, gesichert

Führen Sie den Backup-Auftrag mit aktiviertem Debugging aus

Sie können ein Backup ausführen und den Auftrag wiederherstellen, während das automatische Debugging aktiviert ist. Sollten Sie den technischen Support wegen eines Problems anrufen, das mit einem Backup- oder Wiederherstellungs-Auftrag zu tun hat, werden die Support-Mitarbeiter Sie dazu auffordern, die Debug-Protokolle zu beschaffen. Mit Hilfe der Debug-Protokolle, kann der Support Änderungen an den Aufträgen vornehmen, mit denen es ein Problem gibt. Nach Abschluss des Auftrags liegen Ihnen alle Debug-Protokolle vor, die der Support anfragt.

So führen Sie einen Auftrag mit aktiviertem Debugging aus

1 Sie haben folgende Möglichkeiten:

So führen Sie den Auftrag mit aktiviertem Debugging auf der Registerkarte "Auftragsüberwachung" aus

Klicken Sie auf die Registerkarte "Auftragsüberwachung".

So führen Sie den Auftrag mit aktiviertem Debugging auf der Registerkarte "Backup und Wiederherstellung" oder der Registerkarte "Speicher" aus

Gehen Sie wie folgt vor:

- Doppelklicken Sie auf der Registerkarte "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, auf dem der Auftrag läuft.
- Klicken Sie im linken Teilfenster auf "Aufträge".

2 Sie haben folgende Möglichkeiten:

- Klicken Sie mit der rechten Maustaste auf den Auftrag und dann auf "Mit aktiviertem Debugging ausführen".
- Wählen Sie auf der Registerkarte "Auftragsüberwachung" den Auftrag aus und klicken dann auf "Mit aktiviertem Debugging ausführen".

Wenn für den Auftrag kein Zeitplan definiert wurde, erscheint ein Dialogfeld, das besagt, dass der Auftrag umgehend ausgeführt wird.

Wenn für den Auftrag ein Zeitplan festgelegt wurde, erscheint ein Dialogfeld, in dem Sie auswählen müssen, ob der Auftrag sofort oder gemäß dem Zeitplan ausgeführt werden soll. Der Auftrag mit aktiviertem Debugging läuft nur, wenn Sie die Option zum ersten Mal aktivieren. Der Auftrag läuft nicht gemäß den darauf folgenden Zeitplänen ab.

3 Klicken Sie auf "OK".

Der Auftrag wurde abgeschlossen und die Debug-Protokolle werden generiert. Gibt es mit dem Backup- oder Wiederherstellungsauftrag Probleme, können Sie dem technischen Support die Debug-Protokolle zukommen lassen.

Informationen zum Auftragsverlauf

Im Auftragsverlauf wird eine Liste abgeschlossener und fehlgeschlagener Backup-, Wiederherstellungs- und Speichervorgangsaufträge angezeigt. Der Auftragsverlauf wird im unteren Teilfenster der Registerkarte "Auftragsüberwachung" angezeigt. Er wird auch angezeigt, wenn Sie auf der Registerkarte "Backup und

Wiederherstellung" einen Server und auf der Registerkarte "Speicher" ein Speichergerät auswählen.

Ausgehend vom Auftragsverlauf haben Sie die folgenden Möglichkeiten:

- Anzeigen des Auftragsprotokolls.
- Löschen eines Auftrags.
- Erneute Ausführung eines Auftrags.
- Kopieren der Daten eines vollständigen Backup-Auftrags.
- Überprüfen eines Backup-Auftrags.
- Aktivieren von Fehlerbehandlungsregeln für einen fehlgeschlagenen Auftrag.

Siehe ["Ausführen eines Auftrags über den Auftragsverlauf"](#) auf Seite 305.

Siehe ["Anzeigen des Auftragsprotokolls "](#) auf Seite 308.

Siehe ["Löschen eines Auftrags aus dem Auftragsverlauf"](#) auf Seite 304.

Siehe ["Aktivieren einer Fehlerbehandlungsregel für einen fehlgeschlagenen Auftrag"](#) auf Seite 319.

Siehe ["Manuelles Duplizieren von Backup-Sätzen bzw. Auftragsverläufen"](#) auf Seite 246.

Siehe ["Gesicherte Daten manuell überprüfen"](#) auf Seite 252.

Anzeigen des Verlaufs eines Auftrags

Der Auftragsverlauf zeigt Statistiken für alle Vorkommnisse eines Auftrags an.

So zeigen Sie den Verlauf eines Auftrags an

- 1 Sie haben folgende Möglichkeiten:

So zeigen Sie auf der Registerkarte
"Auftragsüberwachung" den Verlauf eines
Auftrags an

Suchen sie auf der Registerkarte
"Auftragsüberwachung" im Teilfenster
"Auftragsverläufe" den Auftrag.

So zeigen Sie den Verlauf eines Auftrags auf der Registerkarte "Backup und Wiederherstellung" oder "Speicher" an

Gehen Sie wie folgt vor:

- Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, auf dem der Auftrag ausgeführt wurde.
- Im linken Teilfenster klicken Sie auf "Auftragsverlauf".

- 2 Klicken Sie mit der rechten Maustaste auf den Auftrag und klicken Sie anschließend auf "Auftragsverlauf anzeigen".

Löschen eines Auftrags aus dem Auftragsverlauf

Sie können einen Auftrag aus dem Auftragsverlauf löschen oder festlegen, dass Backup Exec den Auftragsverlauf automatisch mithilfe der Datenbankverwaltung löscht.

Beim Löschen eines Auftrags wird dieser auf dem Computer gelöscht und kann nicht wiederhergestellt werden.

So löschen Sie einen Auftrag aus dem Auftragsverlauf

- 1 Sie haben folgende Möglichkeiten:

So löschen Sie einen Auftrag aus dem Auftragsverlauf auf der Registerkarte "Auftragsüberwachung"

Suchen Sie auf der Registerkarte "Auftragsüberwachung" den Auftrag im Teilfenster "Auftragsverläufe".

So löschen Sie einen Auftrag aus dem Auftragsverlauf auf der Registerkarte "Backup und Wiederherstellung" oder der Registerkarte "Speicher"

Gehen Sie wie folgt vor:

- Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, auf dem der Auftrag ausgeführt wurde.
- Im linken Teilfenster klicken Sie auf "Auftragsverlauf".

- 2** Klicken Sie mit der rechten Maustaste auf den Auftrag, den Sie löschen möchten, und klicken Sie dann auf "Löschen".

Sie können mehrere Aufträge auswählen, indem Sie zunächst einen Auftrag auswählen und dann die <Strg-Taste> oder <Umschalttaste> drücken, während Sie auf andere Aufträge klicken, die Sie auswählen möchten. Dadurch können Aufgaben, z. B. Löschen, für mehrere Aufträge mit ähnlichem Auftragsstyp gleichzeitig ausgeführt werden.

Sie können bis zu 2.500 Aufträge aus dem Auftragsverlauf löschen. Wenn Sie versuchen, mehr als 2.500 Aufträge zu löschen, werden Sie aufgefordert, mit dem Löschen fortzufahren.

- 3** Klicken Sie auf "Ja".

Siehe ["Informationen zum Auftragsverlauf"](#) auf Seite 302.

Siehe ["Konfigurieren der Datenbankverwaltung und -sicherheit"](#) auf Seite 694.

Ausführen eines Auftrags über den Auftragsverlauf

Nachdem ein Auftrag ausgeführt wurde, wird er in den "Auftragsverlauf" verschoben. Sie können einen abgeschlossenen Auftrag aus dem "Auftragsverlauf" erneut ausführen.

So führen Sie einen Auftrag aus dem Auftragsverlauf aus

- 1** Sie haben folgende Möglichkeiten:

So führen Sie auf der Registerkarte "Auftragsüberwachung" einen Auftrag aus dem "Auftragsverlauf" aus

Suchen Sie auf der Registerkarte "Auftragsüberwachung" den Auftrag im Teilfenster "Auftragsverläufe".

So führen Sie von der Registerkarte "Auftragsverlauf" auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" aus

- Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, auf dem der Auftrag ausgeführt wurde.
- Im linken Teilfenster klicken Sie auf "Auftragsverlauf".

- 2 Klicken Sie mit der rechten Maustaste auf den Auftrag, den Sie ausführen möchten, und klicken Sie dann auf "Jetzt ausführen".

Siehe ["Informationen zum Auftragsverlauf"](#) auf Seite 302.

Wiederholt nur fehlgeschlagener Aufträge aus dem Auftragsverlauf

Sie können einen Auftrag nur für die Ressourcen aus dem Auftragsverlauf wiederholen, die beim direkt vorhergehenden Durchgang nicht gesichert werden konnten. Diese Option ist nur für fehlgeschlagene oder abgebrochene Backup-Aufträge verfügbar. Wenn ein Backup-Auftrag erfolgreich war, ist diese Option ausgegraut.

Beispiel: Sie haben einen VMware-Backup-Auftrag, der fünf virtuelle Computer sichert. Es werden allerdings nur drei virtuelle Computer gesichert. Sie können das Auftragsprotokoll auf die Ursache des Fehlers prüfen, das Problem beheben und dann die Option "Nur fehlgeschlagene Aufträge wiederholen" verwenden. Diesmal werden nur die beiden virtuellen Computer gesichert, die beim vorherigen Durchgang nicht gesichert werden konnten. Die drei virtuellen Computer, die bereits gesichert wurden, werden nicht erneut gesichert.

Wenn Simplified Disaster Recovery für einen Backup-Auftrag aktiviert ist, und ein Fehler in mindestens einer der wichtigen Ressourcen auftrat, werden diese beim Wiederholen des fehlgeschlagenen Backup-Auftrags erneut gesichert. Dies gilt auch für die wichtigen Ressourcen, die bereits im vorherigen Durchgang gesichert wurden.

In einer CAS-MMS-Umgebung für Aufträge, die vom CAS-Server delegiert wurden, ist die Option zum Wiederholen eines fehlgeschlagenen Auftrags nur über die CAS-Benutzeroberfläche verfügbar. Die Option ist für delegierte Aufträge in der MMS-Benutzeroberfläche deaktiviert.

So wiederholen Sie einen Auftrag für fehlgeschlagene Ressourcen aus dem Auftragsverlauf

- 1 Sie haben folgende Möglichkeiten:

So wiederholen Sie den Auftrag über die Registerkarte "Auftragsüberwachung"

Suchen Sie auf der Registerkarte "Auftragsüberwachung" den Auftrag im Teilfenster "Auftragsverläufe".

So wiederholen Sie den Auftrag über die Registerkarte "Backup und Wiederherstellung" bzw. "Speicher"

Gehen Sie wie folgt vor:

- Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, auf dem der Auftrag ausgeführt wurde.
- Im linken Teilfenster klicken Sie auf "Auftragsverlauf".

2 Sie haben folgende Möglichkeiten:

- Klicken Sie mit der rechten Maustaste auf den zu wiederholenden Auftrag und klicken Sie dann auf "Nur fehlgeschlagene Aufträge wiederholen".
- Klicken Sie auf der Registerkarte "Auftragsüberwachung" auf den zu wiederholenden Auftrag und klicken Sie dann auf "Nur fehlgeschlagene Aufträge wiederholen".

Es wird gemeldet, dass der Auftrag sofort sowie im Rahmen des festgelegten Zeitplans ausgeführt wird.

3 Klicken Sie auf "Ja".

Der Auftrag wird gestartet und jetzt wird nur die Ressource, die im vorherigen Durchgang nicht gesichert wurde, gesichert

Führen Sie den Backup-Auftrag mit aktiviertem Debugging im Auftragsverlauf aus.

Sie können ein Backup ausführen und den Auftrag wiederherstellen, während das automatische Debugging aktiviert ist. Sollten Sie den technischen Support wegen eines Problems anrufen, das mit einem Backup- oder Wiederherstellungs-Auftrag zu tun hat, werden die Support-Mitarbeiter Sie dazu auffordern, die Debug-Protokolle zu beschaffen. Mit Hilfe der Debug-Protokolle, kann der Support Änderungen an den Aufträgen vornehmen, mit denen es ein Problem gibt. Nach Abschluss des Auftrags liegen Ihnen alle Debug-Protokolle vor, die der Support anfragt.

So führen Sie einen Auftrag mit aktiviertem Debugging aus

1 Sie haben folgende Möglichkeiten:

So führen Sie den Auftrag mit aktiviertem Debugging auf der Registerkarte "Auftragsüberwachung" aus

Suchen Sie auf der Registerkarte "Auftragsüberwachung" den Auftrag im Teilfenster "Auftragsverläufe".

So führen Sie den Auftrag mit aktiviertem Debugging auf der Registerkarte "Backup und Wiederherstellung" oder der Registerkarte "Speicher" aus

Gehen Sie wie folgt vor:

- Doppelklicken Sie auf der Registerkarte "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, auf dem der Auftrag läuft.
- Im linken Teilfenster klicken Sie auf "Auftragsverlauf".

2 Sie haben folgende Möglichkeiten:

- Klicken Sie mit der rechten Maustaste auf den Auftrag und dann auf "Mit aktiviertem Debugging ausführen".
- Wählen Sie auf der Registerkarte "Auftragsüberwachung" den Auftrag aus und klicken dann auf "Mit aktiviertem Debugging ausführen".

Wenn für den Auftrag kein Zeitplan definiert wurde, erscheint ein Dialogfeld, das besagt, dass der Auftrag umgehend ausgeführt wird.

Wenn für den Auftrag ein Zeitplan festgelegt wurde, erscheint ein Dialogfeld, in dem Sie auswählen müssen, ob der Auftrag sofort oder gemäß dem Zeitplan ausgeführt werden soll. Der Auftrag mit aktiviertem Debugging läuft nur, wenn Sie die Option zum ersten Mal aktivieren. Der Auftrag läuft nicht gemäß den darauf folgenden Zeitplänen ab.

3 Klicken Sie auf "OK".

Der Auftrag wurde abgeschlossen und die Debug-Protokolle werden generiert. Gibt es mit dem Backup-oder Wiederherstellungsauftrag Probleme, können Sie dem technischen Support die Debug-Protokolle zukommen lassen.

Anzeigen des Auftragsprotokolls

Sie können detaillierte, auftragsbezogene Eigenschaften für jeden verarbeiteten Auftrag anzeigen. Sie können eine Kopie des Auftragsprotokolls an einem Speicherort Ihrer Wahl speichern oder das Auftragsprotokoll drucken.

So zeigen Sie das Auftragsprotokoll an

1 Sie haben folgende Möglichkeiten:

So rufen Sie das Auftragsprotokoll von der Registerkarte "Auftragsüberwachung" aus auf

Suchen Sie auf der Registerkarte "Auftragsüberwachung" den Auftrag im Teilfenster "Auftragsverläufe".

So rufen Sie das Auftragsprotokoll von der Registerkarte "Backup und Wiederherstellung" oder von der Registerkarte "Speicher" aus auf

Gehen Sie wie folgt vor:

- Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, auf dem der Auftrag ausgeführt wurde.
- Im linken Teilfenster klicken Sie auf "Auftragsverlauf".

- 2 Klicken Sie mit der rechten Maustaste auf den Auftrag und wählen Sie "Auftragsprotokoll anzeigen".
- 3 Führen Sie einen der folgenden Schritte aus:
 - Klicken Sie auf "Suchen", um nach einem bestimmten Wort, einer Phrase oder einem Dateinamen zu suchen.
 - Klicken Sie auf "Speichern unter", um eine Kopie des Auftragsprotokolls am Speicherort Ihrer Wahl zu speichern.
 - Klicken Sie auf "Drucken", um das Auftragsprotokoll zu drucken.

Suchen nach Text im Auftragsprotokoll

Sie können nach einem bestimmtem Text im Auftragsprotokoll suchen. Backup Exec durchsucht nur die Abschnitte, die erweitert sind. Um den gesamten Auftrag zu suchen, sollten Sie die Option "Alle erweitern" auswählen.

So suchen Sie nach Text im Auftragsprotokoll

- 1 Sie haben folgende Möglichkeiten:

So suchen Sie Text im Auftragsprotokoll von der Registerkarte "Auftragsüberwachung" aus

Suchen Sie auf der Registerkarte "Auftragsüberwachung" im Bereich "Auftragsverläufe" den Auftrag, dessen Auftragsprotokoll Sie suchen.

So suchen Sie Text im Auftragsprotokoll von der Registerkarte "Backup und Wiederherstellung" oder von der Registerkarte "Speicher" aus

Gehen Sie wie folgt vor:

- Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, auf dem der Auftrag ausgeführt wurde.
- Im linken Teilfenster klicken Sie auf "Auftragsverlauf".

- 2** Klicken Sie mit der rechten Maustaste auf den Auftrag und klicken Sie anschließend auf "Auftragsprotokoll anzeigen".
- 3** Klicken Sie auf "Suchen".
- 4** Geben Sie im Feld "Suchen" den Text ein, den Sie suchen möchten.

5 Wählen Sie beliebige Zusatzfunktionen aus, um Ihre Suche zu erleichtern:

Nur ganzes Wort suchen

Aktivieren Sie dieses Kontrollkästchen, wenn Backup Exec nur nach dem vollständigen Wort suchen soll, das Sie eingegeben haben. Wenn Sie diese Option nicht auswählen, findet Backup Exec Text, der dieses Wort enthält. Wenn Sie beispielsweise das Wort "Datei" suchen und diese Option nicht auswählen, findet Backup Exec alle Vorkommen von "Datei", "Dateien", "Protokolldatei" und andere Wörter, die "Datei" enthalten. Wenn Sie diese Option auswählen, findet Backup Exec nur Vorkommen von "Datei".

Groß- und Kleinschreibung beachten

Aktivieren Sie dieses Kontrollkästchen, wenn Backup Exec nur nach Wörtern mit genau der gleichen Groß- und Kleinschreibung suchen soll. Wenn Sie beispielsweise das Wort "Datei" suchen und diese Option auswählen, findet Backup Exec alle Vorkommen von "Datei", aber keine Vorkommen von "datei".

Alle Übereinstimmungen hervorheben

Aktivieren Sie dieses Kontrollkästchen, wenn Backup Exec den mit den Suchkriterien übereinstimmenden Text hervorheben soll. Die Option wird standardmäßig ausgewählt.

6 Klicken Sie auf "Weiter", um das nächste Vorkommen des Textes zu suchen.

Siehe ["Anzeigen des Auftragsprotokolls"](#) auf Seite 308.

Drucken des Auftragsprotokolls

Wenn Ihr Backup Exec-Server mit einem Drucker verbunden ist, können Sie das Auftragsprotokoll für einen abgeschlossenen Auftrag drucken.

So drucken Sie das Auftragsprotokoll

1 Sie haben folgende Möglichkeiten:

So greifen Sie auf der Registerkarte "Auftragsüberwachung" auf das Auftragsprotokoll zu

Suchen sie auf der Registerkarte "Auftragsüberwachung" im Teilfenster "Auftragsverläufe" den Auftrag.

So greifen Sie auf der Registerkarte "Backup und Wiederherstellung" bzw. "Speicher" auf das Auftragsprotokoll zu

Gehen Sie wie folgt vor:

- Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, auf dem der Auftrag ausgeführt wurde.
- Im linken Teilfenster klicken Sie auf "Auftragsverlauf".

- 2 Klicken Sie mit der rechten Maustaste auf den Auftrag und wählen Sie "Auftragsprotokoll anzeigen".
- 3 Klicken Sie auf "Drucken".
- 4 Wählen Sie den Drucker, den Sie verwenden möchten, und klicken Sie dann auf "Drucken".

Siehe ["Speichern des Auftragsprotokolls"](#) auf Seite 312.

Speichern des Auftragsprotokolls

Mit Backup Exec können Sie das Auftragsprotokoll auf der Festplatte oder im Netzwerk speichern. Außerdem können Sie das Format für die Datei auswählen: als vollständige Webseite, Webarchiv, Webseite nur mit HTML oder Textdatei.

So speichern Sie das Auftragsprotokoll

- 1 Sie haben folgende Möglichkeiten:

So greifen Sie auf der Registerkarte "Auftragsüberwachung" auf das Auftragsprotokoll zu

Suchen sie auf der Registerkarte "Auftragsüberwachung" im Teilfenster "Auftragsverläufe" den Auftrag.

So greifen Sie auf der Registerkarte "Backup und Wiederherstellung" bzw. "Speicher" auf das Auftragsprotokoll zu

Gehen Sie wie folgt vor:

- Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, auf dem der Auftrag ausgeführt wurde.
- Im linken Teilfenster klicken Sie auf "Auftragsverlauf".

- 2 Klicken Sie mit der rechten Maustaste auf den Auftrag und wählen Sie "Auftragsprotokoll anzeigen".

- 3 Klicken Sie auf "Speichern unter".
- 4 Wählen Sie den Speicherort aus, in dem Sie das Auftragsprotokoll speichern möchten.

Siehe ["Drucken des Auftragsprotokolls"](#) auf Seite 311.

Verknüpfung des Auftragsprotokolls mit der Website des technischen Supports von Veritas

Die im Auftragsprotokoll aufgeführten Fehler weisen jeweils einen eindeutigen Code auf, die so genannte eindeutige Meldungskennung (Unique Message Identifier – UMI). Diese Codes enthalten Hyperlinks zum technischen Support von Veritas. Hier haben Sie Zugriff auf technische Hinweise und Tipps zur Fehlerbehebung, die in direktem Bezug zu Ihrer Fehlermeldung stehen. UMI-Codes sorgen für eindeutige MeldungsCodes bei allen Veritas-Produkten.

Einige Warnmeldungen enthalten ebenfalls einen UMI. Wenn beispielsweise bei Fehlschlagen eines Auftrags eine Warnmeldung angezeigt wird, enthält die Warnmeldung den UMI-Code.

Sie können für Fehler eine Fehlerbehandlungsregel erstellen oder aktivieren. Mithilfe dieser Regeln können Sie Optionen festlegen, um beim Auftreten des Fehlers den Auftrag erneut auszuführen oder anzuhalten.

Siehe ["Fehlerbehandlungsregeln für fehlgeschlagene oder abgebrochene Aufträge"](#) auf Seite 316.

So verknüpfen Sie das Auftragsprotokoll mit der Website des technischen Supports von Veritas

- 1 Sie haben folgende Möglichkeiten:

So rufen Sie das Auftragsprotokoll von der Registerkarte "Auftragsüberwachung" aus "Auftragsüberwachung" auf

So rufen Sie das Auftragsprotokoll von der Registerkarte "Backup und Wiederherstellung" oder von der Registerkarte "Speicher" aus auf

Gehen Sie wie folgt vor:

- Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, auf dem der Auftrag ausgeführt wurde.
 - Im linken Teilfenster klicken Sie auf "Auftragsverlauf".
- 2 Klicken Sie mit der rechten Maustaste auf einen Auftrag und wählen Sie "Auftragsprotokoll anzeigen".
 - 3 Scrollen Sie zum Abschnitt "Auftragsabschlussstatus".
 - 4 Klicken Sie auf den UMI-Code, der als blauer Hyperlink angezeigt wird.

So verwendet man Auftragsprotokolle mit vertikalen Anwendungen

In der Backup Exec-Administratorkonsole werden die Auftragsprotokolle im HTML-Format angezeigt. Bei Bedarf können Sie die Auftragsprotokolle in ein Textformat umwandeln, um sie mit vertikalen Anwendungen zu verwenden.

Um eine Auftragsprotokolldatei in ein Textformat umzuwandeln, laden Sie die Backup Exec-Befehlszeilenschnittstelle und geben Sie dann Folgendes an einer Eingabeaufforderung ein:

Get-BEJobLog "Pfadname\Dateiname des Auftragsprotokolls"

Beispiel: Geben Sie den folgenden Befehl ein, um das Auftragsprotokoll "C:<Backup Exec-Installationsordner>\Backup Exec\Data\bex00001.xml" als Text in der Eingabeaufforderung anzuzeigen:

Get-BEJobLog "C:<Backup Exec-Installationsordner>\Backup Exec\Data\bex00001.xml"

Geben Sie zum Umleiten des Auftragsprotokolls in eine Datei einen der folgenden Befehle ein:

Get-BEJobLog "C:<Backup Exec-Installationsordner>\Backup Exec\Data\bex00001.xml" > bex00001.txt

Siehe ["Anzeigen des Auftragsprotokolls"](#) auf Seite 308.

Konfigurieren von standardmäßigen Auftragsprotokolloptionen

Sie können Standardoptionen für Auftragsprotokolle konfigurieren, mit denen Sie festlegen können, welche Details in das fertige Auftragsprotokoll aufgenommen

werden sollen. Für die Aufträge, die große Auftragsprotokolle produzieren, empfiehlt es sich eventuell, die Menge des Details im Auftragsprotokoll zu reduzieren. Die Größe des Auftragsprotokolls nimmt proportional mit dem Umfang der für das Protokoll konfigurierten Details zu.

So konfigurieren Sie standardmäßige Auftragsprotokolloptionen

- 1** Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Backup Exec-Einstellungen".
- 2** Klicken Sie im linken Teilfenster auf "Auftragsprotokoll".
- 3** Wählen Sie die entsprechenden Optionen aus.

Nur Kurz-Info

Wählen Sie diese Option aus, um die folgenden Informationen im Auftragsprotokoll aufzunehmen:

- Auftragsname
- Auftragstyp
- Name des Auftragsprotokolls
- Backup Exec-Server-Name
- Speichergerät
- Startdatum und -uhrzeit
- Aufgetretene Fehler
- Abschlussdatum und -uhrzeit
- Abschlussstatistiken

Außerdem gehören dazu die Namen der übersprungenen Dateien, der Mediensatzname, der Backup-Typ und die Ergebnisse der Überprüfung (falls ausgeführt).

Kurzinfo und verarbeitete Verzeichnisse

Wählen Sie diese Option aus, um zusammenfassende Informationen und eine Liste aller verarbeiteten Unterverzeichnisse in das Auftragsprotokoll aufzunehmen.

Kurzinfo und verarbeitete Verzeichnisse und Dateien

Wählen Sie diese Option aus, um zusammenfassende Informationen, verarbeitete Unterverzeichnisse und eine Liste aller Dateinamen, die verarbeitet wurden, im Auftragsprotokoll aufzunehmen.

Kurzinfo, Verzeichnisse, Dateien und Dateiangaben	Wählen Sie diese Option aus, um zusammenfassende Informationen, verarbeitete Unterverzeichnisse, eine Liste aller Dateinamen und ihre Attribute in das Auftragsprotokoll aufzunehmen. Durch diese Option wird die Größe des Auftragsprotokolls stark erhöht.
Präfix für Dateiname des Auftragsprotokolls	Geben Sie das Präfix an, das den verarbeiteten Auftragsprotokollen vorangestellt wird. Das Standardpräfix ist "BEX". Der Auftragsprotokolldateiname besteht aus Präfix_Servername_Anzahl. Das Präfix ist die Bezeichnung, die Sie in diesem Feld eingeben, "Servername" ist der Name des Backup Exec-Servers, der den Auftrag ausgeführt hat, und "Anzahl" ist die Anzahl der für diesen Auftrag produzierten Auftragsprotokolle.
Auftragsprotokolle als HTML-Datei anhängen	Wählen Sie diese Option aus, um die Auftragsprotokolle im HTML-Format an die E-Mail-Benachrichtigung anzuhängen, wenn diese gesendet wird.
Auftragsprotokolle als Textdatei anhängen	Wählen Sie diese Option aus, um die Auftragsprotokolle in einem Textformat an die E-Mail-Benachrichtigung anzuhängen, wenn diese gesendet wird.
Pfad des Auftragsprotokolls	Zeigt den aktuellen Speicherort des Auftragsprotokolls an. Den Pfad können Sie mithilfe von BE Utility ändern.

Siehe ["Anzeigen des Auftragsprotokolls"](#) auf Seite 308.

Fehlerbehandlungsregeln für fehlgeschlagene oder abgebrochene Aufträge

Sie können Standardregeln aktivieren oder benutzerdefinierte Regeln erstellen, um Wiederholungsoptionen und die endgültige Auftragsbehandlung für fehlgeschlagene oder abgebrochene Aufträge festzulegen. Über die Wiederholungsoptionen können Sie angeben, wie oft ein fehlgeschlagener Auftrag wiederholt wird und nach welchem Zeitraum die einzelnen Wiederholungen durchgeführt werden. Mit der endgültigen

Auftragsbehandlung können Sie den Auftrag anhalten, bis der Fehler behoben werden kann, oder für den nächsten geplanten Dienst neu planen.

Jede Standard-Fehlerbehandlungsregel gilt für eine Kategorie von Fehlern, z. B. Netzwerk- oder Sicherheitsfehler. Standard-Fehlerbehandlungsregeln sind standardmäßig deaktiviert, Sie müssen Regeln daher bearbeiten und die Regeln aktivieren, die Sie verwenden möchten. Es ist nicht möglich, Standard-Fehlerbehandlungsregeln zu löschen, einer Kategorie bestimmte Fehlercodes hinzuzufügen oder neue Fehlerkategorien hinzuzufügen. Fehlerbehandlungsregeln können erst angewendet werden, wenn der endgültige Fehlercode in einer Fehlerkategorie enthalten ist, die einer aktivierten Regel zugeordnet ist.

Erstellen Sie eine benutzerdefinierte Fehlerbehandlungsregel, wenn Sie eine Fehlerbehandlungsregel für einen bestimmten Fehlercode in einer Fehlerkategorie anwenden möchten. Sie können bis zu 28 Fehlercodes in einer Fehlerkategorie auswählen, auf die eine benutzerdefinierte Fehlerbehandlungsregel angewendet werden kann. Sie können darüber hinaus Fehlercodes zu einer vorhandenen benutzerdefinierten Regel hinzufügen.

Eine benutzerdefinierte Fehlerbehandlungsregel mit dem Namen "Wiederhergestellte Aufträge" wird bei der Installation von Backup Exec erstellt und in der Standardeinstellung aktiviert. Über diese Regel werden Wiederholungsoptionen und eine endgültige Auftragsbehandlung auf Aufträge angewendet, die fehlschlagen und nicht so geplant sind, dass sie erneut ausgeführt werden.

Siehe ["Erstellen einer benutzerdefinierten Fehlerbehandlungsregel"](#) auf Seite 317.

Wenn bei einem fehlgeschlagenen Auftrag eine benutzerdefinierte und eine Standard-Fehlerbehandlungsregel vorliegen, werden die Einstellungen der benutzerdefinierten Regel auf den Auftrag angewendet.

Hinweis: Wenn sich der Server, auf dem Backup Exec installiert ist, in einer Clusterumgebung befindet, wird in der Liste der Fehlerbehandlungsregeln die Regel "Cluster-Failover" aufgeführt. Diese Regel ist standardmäßig aktiviert.

Siehe ["Info zur Fehlerbehandlungsregel für Cluster-Failover"](#) auf Seite 321.

Erstellen einer benutzerdefinierten Fehlerbehandlungsregel

Sie können benutzerdefinierte Regeln erstellen, um Wiederholungsoptionen und die endgültige Auftragsbehandlung für fehlgeschlagene oder abgebrochene Aufträge festzulegen.

Siehe ["Fehlerbehandlungsregeln für fehlgeschlagene oder abgebrochene Aufträge"](#) auf Seite 316.

So erstellen Sie eine benutzerdefinierte Fehlerbehandlungsregel

- 1** Klicken Sie auf die Schaltfläche "Backup Exec" und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Fehlerbehandlungsregeln".
- 2** Klicken Sie auf "Neu".
- 3** Aktivieren Sie "Fehlerbehandlungsregel aktivieren".
- 4** Geben Sie im Feld "Name" einen Namen für die Regel ein.
- 5** Wählen Sie in der Liste "Fehlerkategorie" die Fehlerkategorie aus, für die diese Regel gelten soll.
- 6** Aktivieren Sie unter "Verfügbare Fehler" das Kontrollkästchen des Fehlercodes, für den diese Regel gelten soll. Es können bis zu 28 Fehlercodes ausgewählt werden.
- 7** Wenn Backup Exec den Auftrag nach einem Ausfall erneut ausführen soll, müssen Sie das Kontrollkästchen "Auftrag wiederholen" aktivieren und angeben, wie oft der Auftrag wiederholt werden soll.

Die Höchstzahl von Wiederholungen ist 99. Der maximale Wiederholungsabstand ist 1440 Minuten.
- 8** Unter "Endgültige Auftragsbehandlung" wählen Sie die Methode aus, mit der Sie den Auftrag nach der Höchstzahl von Wiederholungen bearbeiten möchten.

Wenn Sie auswählen, den Auftrag anzuhalten, bis der Fehler manuell behoben ist, müssen Sie die Wartestellung für den Auftrag manuell aufheben, nachdem Sie den Fehler behoben haben.
- 9** Klicken Sie auf "OK".

Siehe ["Benutzerdefinierte Fehlerbehandlungsregel für wiederhergestellte Aufträge"](#) auf Seite 320.

Siehe ["Info zur Fehlerbehandlungsregel für Cluster-Failover"](#) auf Seite 321.

Aktivieren oder Deaktivieren von Fehlerbehandlungsregeln

Folgen Sie diesen Schritten, um bestimmte Fehlerbehandlungsregeln zu aktivieren oder zu deaktivieren.

So aktivieren bzw. deaktivieren Sie Fehlerbehandlungsregeln

- 1** Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Fehlerbehandlungsregeln".
- 2** Wählen Sie die Regel, die Sie aktivieren oder deaktivieren möchten, und klicken Sie auf "Bearbeiten".
- 3** Sie haben folgende Möglichkeiten:

- Um die Regel zu aktivieren, markieren Sie das Kontrollkästchen "Fehlerbehandlungsregel aktivieren".
- Um die Regel zu deaktivieren, entfernen Sie die Markierung für "Fehlerbehandlungsregel aktivieren" check box

4 Klicken Sie auf "OK".

Siehe ["Fehlerbehandlungsregeln für fehlgeschlagene oder abgebrochene Aufträge"](#) auf Seite 316.

Löschen einer benutzerdefinierten Fehlerbehandlungsregel

Eine benutzerdefinierte Fehlerbehandlungsregel kann jederzeit gelöscht werden. Standardfehlerbehandlungsregeln können nicht gelöscht werden.

So löschen Sie eine benutzerdefinierte Fehlerbehandlungsregel

- 1** Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Fehlerbehandlungsregeln".
- 2** Wählen Sie die Fehlerbehandlungsregel aus, die Sie löschen möchten, und klicken Sie dann auf "Löschen".
- 3** Sie werden gefragt, ob die Fehlerbehandlungsregel wirklich gelöscht werden soll. Bestätigen Sie mit "Ja".

Siehe ["Fehlerbehandlungsregeln für fehlgeschlagene oder abgebrochene Aufträge"](#) auf Seite 316.

Aktivieren einer Fehlerbehandlungsregel für einen fehlgeschlagenen Auftrag

Sie können benutzerdefinierte Regeln erstellen, um Wiederholungsoptionen und die endgültige Auftragsbehandlung für fehlgeschlagene Aufträge festzulegen.

So aktivieren Sie eine Fehlerbehandlungsregel für einen fehlgeschlagenen Auftrag

1 Sie haben folgende Möglichkeiten:

So aktivieren Sie eine Fehlerbehandlungsregel auf der Registerkarte "Auftragsüberwachung"

Wählen Sie die Registerkarte "Auftragsüberwachung" aus.

So aktivieren Sie eine Fehlerbehandlungsregel auf der Registerkarte "Backup und Wiederherstellung" oder "Speicher".

Klicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" im linken Teilfenster auf "Auftragsverlauf".

- 2** Klicken Sie mit der rechten Maustaste auf den fehlgeschlagenen Auftrag und wählen Sie "Fehlerbehandlung".
- 3** Aktivieren Sie das Kontrollkästchen "Fehlerbehandlungsregel aktivieren".
- 4** Geben Sie die restlichen Optionen für diese Regel an.

Benutzerdefinierte Fehlerbehandlungsregel für wiederhergestellte Aufträge

In Backup Exec wird eine benutzerdefinierte Fehlerbehandlungsregel namens "Wiederhergestellte Aufträge" bereitgestellt, die zur Wiederherstellung von Aufträgen dient, die mit bestimmten Fehlern fehlgeschlagen sind. Diese Regel wird bei der Installation von Backup Exec erstellt und ist standardmäßig aktiviert.

Durch die Wiederholungsoptionen für diese Regel wird festgelegt, dass der Auftrag jeweils zweimal mit einem Intervall von fünf Minuten wiederholt wird. Die endgültige Auftragsbehandlung ist so definiert, dass der Auftrag angehalten wird, bis die Fehlerbedingung manuell gelöscht wurde.

In der folgenden Tabelle werden die standardmäßig für die benutzerdefinierte Fehlerbehandlungsregel "Wiederhergestellte Aufträge" ausgewählten Fehlercodes aufgeführt und erläutert.

Tabelle 6-2 Fehlercodes für die benutzerdefinierte Fehlerbehandlungsregel "Wiederhergestellte Aufträge"

Fehlercode	Beschreibung
0xE00081D9 E_JOB_ENGINE_DEAD	Angezeigte Fehlermeldung: Der Systemdienst der Backup Exec-Auftragsengine reagiert nicht.

Fehlercode	Beschreibung
0xE0008820 E_JOB_LOCAL RECOVERNORMAL	Angezeigte Fehlermeldung: Der lokale Auftrag wurde wiederhergestellt. Es ist keine Benutzeraktion erforderlich.
0xE000881F E_JOB_REMOTE RECOVERNORMAL	Angezeigte Fehlermeldung: Der Remoteauftrag wurde wiederhergestellt. Es ist keine Benutzeraktion erforderlich.
0xE0008821 E_JOB_STARTUP RECOVERY	Angezeigte Fehlermeldung: Der Auftrag wurde durch das Starten des Backup Exec-RPC-Dienstes wiederhergestellt. Es ist keine Benutzeraktion erforderlich.

Hinweis: Wenn Central Admin Server Feature installiert ist, werden zusätzliche Fehlercodes ausgewählt.

Siehe ["Fehlerbehandlungsregeln für fehlgeschlagene oder abgebrochene Aufträge"](#) auf Seite 316.

Siehe ["Info zur Fehlerbehandlungsregel für Cluster-Failover"](#) auf Seite 321.

Info zur Fehlerbehandlungsregel für Cluster-Failover

Wenn sich der Server, auf dem Backup Exec installiert ist, in einer Clusterumgebung befindet, wird in der Liste der Fehlerbehandlungsregeln die Cluster-Failover-Regel aufgeführt. Diese Regel ist standardmäßig aktiviert.

Bei dieser Regel können keine Optionen konfiguriert werden. Die Fehlerbehandlungsregel für den Cluster-Failover kann nur aktiviert oder deaktiviert werden.

Die Fehlerbehandlungsregel für Cluster-Failover und die Option "Auftragswiederaufnahme aktivieren" in den Advanced Open File -Backup-Optionen wirken zusammen und ermöglichen die Wiederaufnahme von Aufträgen vom Failover an. Da die Option "Auftragswiederaufnahme aktivieren" von der Fehlerbehandlungsregel für den Cluster-Failover abhängt, wird sie bei Deaktivierung der Regel automatisch ebenfalls deaktiviert.

Siehe ["Fehlerbehandlungsregeln für fehlgeschlagene oder abgebrochene Aufträge"](#) auf Seite 316.

Liste von Auftragsstatus in Backup Exec

Backup Exec zeigt die verschiedenen Auftragsstatus für aktive, abgeschlossene und geplante Aufträge an.

Siehe „[Statusmeldungen für aktive Aufträge](#)“ auf Seite 322.

Siehe „[Statusmeldungen für abgeschlossene Aufträge](#)“ auf Seite 323.

Siehe „[Statusmeldungen für geplante Aufträge](#)“ auf Seite 325.

Statusmeldungen für aktive Aufträge

Die folgenden Status können für aktive Aufträge angezeigt werden:

Tabelle 6-3 Statusmeldungen für aktive Aufträge

Status	Beschreibung
Wird ausgeführt	Der Vorgang wird ausgeführt.
In der Warteschlange	Der Auftrag wurde initiiert, aber Backup Exec sucht nach einem geeigneten Laufwerk oder Medien.
Abbruch wartend	Die Anforderung zum Abbruch kann nicht sofort verarbeitet werden. Dieser Status wird angezeigt, bis der Auftrag tatsächlich abgebrochen wird. Anschließend wird der Auftrag im Auftragsverlauf mit dem Status "Abgebrochen" angezeigt.
Medium wird geladen	Das Medium wird geladen und im Zielgerät positioniert.
Vorbearbeitung	<p>Dieser Status kann auf ein oder alle folgenden Elemente hinweisen:</p> <ul style="list-style-type: none">■ Backup Exec berechnet die Menge von Daten, die gesichert werden, wenn die Option "Fortschrittsanzeige für Backup-Aufträge einblenden" im Abschnitt "Einstellungen" der Backup Exec-Einstellungen aktiviert ist. Siehe "Ändern der Standardeinstellungen" auf Seite 692.■ Backup Exec wartet auf einen Befehl vor oder nach dem Auftrag, um diesen abzuschließen.■ Backup Exec fragt die festgelegten Zuordnungen ab und positioniert das Band am Anhängepunkt für Anhängenaufträge.
Snapshot-Verarbeitung	Backup Exec verarbeitet einen Snapshot-Vorgang.

Status	Beschreibung
Gerät angehalten	Das Gerät wurde angehalten, an das der Auftrag gesendet wurde. Siehe "Ein Speichergerät anhalten und wieder starten" auf Seite 552.
Server angehalten	Der Backup Exec-Server ist angehalten. Siehe "Anhalten oder Wiederaufnehmen eines verwalteten Backup Exec-Servers" auf Seite 1507.
Verzögert	Die Backup Exec Services reagieren nicht mehr. Siehe "Festlegen von Auftragsstatus- und Wiederherstellungsoptionen" auf Seite 330.
Medienanforderung	Damit der Auftrag weitergeführt werden kann, müssen Medien eingelegt werden.
Verbindung verzögert	Die Verbindung zwischen dem verwalteten Backup Exec-Server und dem zentralen Administrationsserver konnte nicht innerhalb der festgelegten Zeitspanne hergestellt werden. Siehe "Aktivieren bzw. Deaktivieren der Kommunikation zwischen dem verwalteten Backup Exec-Server und dem zentralen Administrationsserver" auf Seite 1492.
Keine Verbindung	Der zentrale Administrationsserver erhält vom verwalteten Backup Exec-Server keine Auftragsinformationen. Der konfigurierte Schwellenwert wurde erreicht. Siehe "Aktivieren bzw. Deaktivieren der Kommunikation zwischen dem verwalteten Backup Exec-Server und dem zentralen Administrationsserver" auf Seite 1492.
Konsistenzprüfung	Backup Exec führt gerade eine Konsistenzprüfung der Datenbanken vor dem Backup aus.
Aktualisieren von Katalogen	Backup Exec aktualisiert die Kataloginformationen.

Statusmeldungen für abgeschlossene Aufträge

Die folgenden Status können für abgeschlossene Aufträge angezeigt werden:

Tabelle 6-4 Auftragsabschlussstatus

Status	Beschreibung
Erfolgreich	Der Auftrag wurde fehlerfrei abgeschlossen.

Status	Beschreibung
Mit Ausnahmen abgeschlossen	Der Auftrag wurde abgeschlossen, aber einige Dateien wurden gerade verwendet, wurden übersprungen oder waren beschädigt.
Failover erfolgt	Der Auftrag wurde in einer Clusterumgebung ausgeführt und war auf einem Computer aktiv. Im Cluster wurde dann ein Failover ausgeführt und der Auftrag auf einem anderen Server im Cluster neu gestartet. Bei einem Failover für einen Auftrag sind zwei separate Auftragsverlaufssätze verfügbar. Im ersten Auftragsverlauf wird der Failover-Status angegeben, im zweiten der Status, der dem abgeschlossenen Auftrag entspricht.
Wiederaufgenommen	Der Status ist identisch mit dem Failover-Status, allerdings wurde die Option "Auftragswiederaufnahme anwenden" aktiviert.
Abgebrochen	Der Vorgang wurde beim Ausführen durch den Administrator beendet.
Abgebrochen (Zeitüberschreitung)	Die Funktion "Auftrag abbrechen, falls x Stunden nach geplantem Start noch ausgeführt" wurde aktiviert und der Auftrag wurde nicht im angegebenen Zeitrahmen abgeschlossen.

Status	Beschreibung
Fehlgeschlagen	<p>Der Vorgang wurde durchgeführt, jedoch sind ein oder mehrere schwerwiegende Fehler aufgetreten. Im Auftragsprotokoll sollte die Fehlerursache vermerkt sein, sodass Sie entscheiden können, ob Sie den Auftrag erneut ausführen möchten. Wenn ein Auftrag beispielsweise aufgrund einer unterbrochenen Verbindung während der Auftragsausführung fehlgeschlagen ist, können Sie ihn nach dem Wiederherstellen der Verbindung erneut senden.</p> <p>Falls während eines Backup-Vorgangs die Stromversorgung eines Laufwerks gestört ist, sollten Sie den Backup-Auftrag mit einem anderen Band neu starten. Sie können die Daten wiederherstellen, die bis zum Zeitpunkt des Stromausfalls auf das Band geschrieben wurden. Das Band sollte jedoch für nachfolgende Backup-Vorgänge nicht mehr verwendet werden.</p> <p>Bei einem fehlgeschlagenen Auftrag wird im Bereich "Fehler" des Auftragsprotokolls eine Fehlermeldung mit einem Hyperlink zur Website des technischen Supports von Veritas angegeben.</p> <p>Aufträge können aus folgenden Gründen fehlschlagen:</p> <ul style="list-style-type: none"> ■ Das für den Auftrag gewählte Speichergerät war nicht verfügbar, als der Auftrag ausgeführt wurde. ■ Das Login-Konto, das im Backup-Auftrag verwendet wurde, ist falsch. Überprüfen Sie, ob die Login-Konto-Informationen für die zu sichernde Ressource gültig sind. ■ Ein Problem trat mit dem Speichergerät auf, als der Auftrag ausgeführt wurde. ■ Der Computer wurde vor oder während der Ausführung des Backup-Auftrags heruntergefahren.
Wiederhergestellt	<p>Der Auftrag war aktiv, als der Status des verwalteten Backup Exec-Servers von "Verbindung verzögert" in "Keine Verbindung" geändert wurde. Die benutzerdefinierte Fehlerbehandlungsregel für wiederhergestellte Aufträge wurde auf den Auftrag angewendet.</p>
Ausgelassen	<p>Der Auftrag wurde nicht während des festgelegten Zeitfensters ausgeführt. Der Auftrag wird erneut geplant, um gemäß des von Ihnen festgelegten Zeitfensters ausgeführt zu werden.</p>

Statusmeldungen für geplante Aufträge

Die folgenden Status können für geplante Aufträge angezeigt werden:

Tabelle 6-5 Statusmeldungen für geplante Aufträge

Status	Beschreibung
Ungültiger Plan	<p>Der geplante Auftrag wird aufgrund eines Planungsproblems nicht ausgeführt.</p> <p>Siehe "Standardmäßige Zeitplanoptionen für richtliniengesteuerte Aufträge und für Aufträge zum sofortigen Ausführen einstellen" auf Seite 685.</p>
Nicht in Zeitrahmen	<p>Der Auftrag sollte zum Verarbeiten gesendet werden, der Zeitrahmen für den Auftrag war jedoch geschlossen.</p> <p>Siehe "Standardmäßige Zeitplanoptionen für richtliniengesteuerte Aufträge und für Aufträge zum sofortigen Ausführen einstellen" auf Seite 685.</p>
Angehalten	<p>Der Auftrag wurde angehalten.</p>
In der Warteschlange	<p>Ein temporärer Status, der beim Anwenden einer für die Wiederherstellung des Auftrags aktivierten Fehlerbehandlungsregel angezeigt wird.</p> <p>Siehe "Benutzerdefinierte Fehlerbehandlungsregel für wiederhergestellte Aufträge" auf Seite 320.</p>

Status	Beschreibung
Bereit	

Status	Beschreibung
	<p>Der Auftrag ist zum Ausführen bereit, kann jedoch aus einem der angezeigten Gründe nicht ausgeführt werden:</p> <ul style="list-style-type: none"> ■ Interner Fehler Es stehen keine Geräte zur Verfügung, die Ursache dafür ist jedoch unbekannt. ■ Ungültiger Auftrag. Der Auftragsstyp ist unbekannt. Möglicherweise ist ein interner Fehler aufgetreten oder die Datenbank ist beschädigt. ■ Ungültiges Ziel. Dieser Typ des Speichergeräts existiert nicht mehr. ■ Backup Exec-Server nicht verfügbar. ■ Keine Lizenz für Optionsnamen. Eine Lizenz muss erworben und auf dem Backup Exec-Server installiert werden. ■ Keine Backup Exec-Server verfügbar. ■ Im Backup Exec-Serverpool sind keine Backup Exec-Server verfügbar. ■ Der angegebene Zielspeichergerätepool ist leer. ■ Das angegebene Zielgerät befindet sich nicht im Backup Exec-Serverpool. ■ Angegebenes Zielgerät nicht auf lokalem Backup Exec-Server. ■ Angegebener Zielspeichergerätepool auf lokalem Backup Exec-Server ist leer. ■ Das Zielspeichergerät darf kein Speicherpool sein. ■ Das Zielspeichergerät darf kein Backup Exec-Server sein. ■ Ein anderer Auftrag wird im System ausgeführt und blockiert die Ausführung dieses Auftrags. Dieser Auftrag wird ausgeführt, nachdem der andere Auftrag abgeschlossen wurde. ■ Ungültige Eingabe. ■ Inkompatible Wiederaufnahmen. ■ Keine Serverlizenz verfügbar. ■ Keine Lizenz für mehrere Server verfügbar. ■ Keine Windows-Lizenz. ■ Kein Windwos-Server. ■ Ein lokaler Backup Exec-Server wird benötigt. ■ Lokaler Server ist kein Backup Exec-Server. ■ Es stehen keine nicht aktiven Speichergeräte zur Verfügung. ■ Es stehen keine passenden Speichergeräte im

Status	Beschreibung
	<p>Speicherpool zur Verfügung.</p> <ul style="list-style-type: none"> ■ Blockiert durch einen aktiven, verknüpften Auftrag zum Kopieren von Backup-Sätzen.
Geplant	<p>Der Auftrag ist zum Ausführen zu einem späteren Zeitpunkt geplant. Geplante Aufträge, die mit einem anderen Auftrag verknüpft sind (z. B. einem Auftrag zum Kopieren von Backup-Sätzen), werden nicht mit dem Status für einen geplanten Auftrag angezeigt.</p>
Server angehalten	<p>Der Auftrag kann ausgeführt werden, der Backup Exec-Server wurde jedoch angehalten. Keine Aufträge werden geschickt, während der Backup Exec-Server angehalten ist.</p> <p>Siehe "Anhalten oder Wiederaufnehmen eines verwalteten Backup Exec-Servers" auf Seite 1507.</p>
Soll geplant werden	<p>Der Status des geplanten Auftrags beim Senden zur Verarbeitung.</p>

Status	Beschreibung
Regel blockiert	<p>Der Auftrag kann nicht ausgeführt werden, weil eine oder mehrere der Einstellungen in der Backup-Definition nicht erfüllt sind.</p> <p>Der Status "Regel blockiert" erscheint möglicherweise aus den folgenden Gründen:</p> <ul style="list-style-type: none"> Ein Auftrag kann erst ausgeführt werden, wenn ein anderer abgeschlossen ist. Beispiel: Wenn Sie einer Backup-Definition ein Duplizierungsstadium hinzufügten und der Quell-Backup-Auftrag noch nicht abgeschlossen ist, wird der Duplizierungsauftrag blockiert, bis der Quell-Backup-Auftrag abgeschlossen ist. Beispiel: Enthält eine Auftragsdefinition ein vollständiges und ein inkrementelles Backup, muss zuerst das vollständige ausgeführt werden. Wenn Sie versuchen, das inkrementelle Backup zuerst auszuführen, wird dieser blockiert, bis das vollständige Backup abgeschlossen ist. Ein Server für einen Auftrag kann erst geändert werden, wenn die verbundenen Aufträge abgeschlossen sind. Ein Server für einen Auftrag kann erst geändert werden, wenn ein anderer Auftrag abgeschlossen ist. Ein Auftrag kann nicht ausgeführt werden, da mehrere Aufträge so geplant sind, dass sie gleichzeitig ausgeführt werden sollen.

Festlegen von Auftragsstatus- und Wiederherstellungsoptionen

Wenn die Backup Exec-Dienste nicht mehr reagieren oder Aufträge nicht mehr ausgeführt werden, können Sie den Schwellenwert festlegen, bei dem Exec den Status von aktiven Aufträgen zu "verzögert" ändert. Sie können darüber hinaus den Schwellenwert festlegen, an dem die verzögerten Aufträge fehlschlagen und anschließend wiederhergestellt werden.

Indem Sie den Zeitraum, bevor Backup Exec den Schwellenwert zum Ändern des Status eines Auftrags in "Verzögert" erreicht, verkürzen, werden Sie zu einem früheren Zeitpunkt auf verzögerte Aufträge hingewiesen. Durch einen kürzeren Zeitraum zwischen dem Schwellenwert für die Verzögerung und für die Wiederherstellung können die verzögerten Aufträge zu einem früheren Zeitpunkt fehlschlagen und anschließend wiederhergestellt werden. Durch zu niedrige

Schwellenwerte werden Aufträge jedoch möglicherweise unnötigerweise wiederhergestellt.

Die Aufträge werden in Backup Exec mit der benutzerdefinierten Fehlerbehandlungsregel "Wiederhergestellte Aufträge" wiederhergestellt. Diese benutzerdefinierte Fehlerbehandlungsregel wird bei der Installation von Backup Exec erstellt und aktiviert und gibt an, dass verzögerte, fehlgeschlagene und wiederhergestellte Aufträge jeweils zweimal mit einem Intervall von fünf Minuten wiederholt werden.

Verzögerte Aufträge, die in Backup Exec fehlschlagen und dann wiederhergestellt werden, da die Backup Exec-Dienste nicht reagieren, werden in Backup Exec auf andere Weise angezeigt als Aufträge, bei denen Fehler im normalen Arbeitsablauf auftreten. Die verzögerten, fehlgeschlagenen oder wiederhergestellten Aufträge werden nicht wie andere fehlgeschlagene Aufträge im Auftragsverlauf rot angezeigt. Stattdessen werden sie mit grauem Text und dem Auftragsstatus "Wiederhergestellt" angezeigt.

Im Auftragsverlauf wird "Auftragsfehler" als Fehlerkategorie aufgeführt. Im Auftragsverlauf wird der entsprechende Fehler bei der internen Verbindung sowie eine Meldung dazu angezeigt, dass der Auftrag wiederhergestellt wurde. Je nach Typ des aufgetretenen Fehlers kann mit dem wiederhergestellten Auftrag eine Protokolldatei verknüpft sein.

So legen Sie Auftragsstatus- und -wiederherstellungsoptionen fest

- 1** Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Backup Exec-Einstellungen".
- 2** Klicken Sie im linken Teilfenster auf "Auftragsstatus und Wiederherstellung".

3 Stellen Sie die Schwellenwerte für die verzögerten und wiederhergestellten Aufträge ein.

Verzögert

Geben Sie an, wie lange gewartet werden soll, bevor Backup Exec den Status eines nicht reagierenden Auftrags in "Verzögert" ändern soll.

Wiederhergestellt

Geben Sie an, wie lange gewartet werden soll, bevor Backup Exec verzögerte Aufträge als fehlgeschlagen markiert und anschließend wiederherstellt. Auf die wiederhergestellten Aufträge wird die benutzerdefinierte Fehlerbehandlungsregel mit dem Namen "Wiederhergestellte Aufträge" angewendet. Wenn diese Regel deaktiviert ist, werden die anderen aktivierten Fehlerbehandlungsregeln auf die wiederhergestellten Aufträge angewendet. Wenn keine Fehlerbehandlungsregeln auf den Auftrag zutreffen, schlägt dieser fehl.

4 Klicken Sie auf "OK".

Siehe ["Liste von Auftragsstatus in Backup Exec"](#) auf Seite 322.

Siehe ["Benutzerdefinierte Fehlerbehandlungsregel für wiederhergestellte Aufträge"](#) auf Seite 320.

Warnmeldungen und Benachrichtigungen

In diesem Kapitel werden folgende Themen behandelt:

- Warnmeldungen und Benachrichtigungen in Backup Exec
- Warnmeldungen in Backup Exec
- Aktivieren der Anzeige aktiver Warnmeldungen und des Warnmeldungsverlaufs auf der Registerkarte "Startseite"
- Anzeigen des Warnmeldungsverlaufs für einen Server oder ein Speichergerät
- Löschen einer Warnmeldung aus dem Warnmeldungsverlauf
- Kopieren der Warnmeldung in ein Dokument oder eine E-Mail
- Filtern von Warnmeldungen
- Anzeigen des Auftragsprotokolls für Warnmeldungen
- Reagieren auf aktive Warnmeldungen
- Manuelles Löschen aller Informationsmeldungen
- Einrichten von Benachrichtigungen für Warnmeldungen
- Konfigurieren von E-Mail- oder SMS-Benachrichtigungen für Warnmeldungen
- Hinzufügen von Empfängern für die Benachrichtigung
- Hinzufügen einer Empfängergruppe für Warnmeldungen
- Deaktivieren von Warnmeldungen per E-Mail oder SMS für einen Empfänger
- Bearbeiten der Benachrichtigungseigenschaften für Empfänger

- Löschen von Empfängern
- Konfigurieren von Warnmeldungskategorien
- Zuweisen von bestimmten Warnmeldungskategorien an bestimmte Empfänger
- Senden einer Benachrichtigung beim Abschluss eines Auftrags
- Deaktivieren von Benachrichtigungen für eine bestimmte Meldungskategorie
- Konfigurieren von Standardeinstellungen für Warnmeldungen
- Aktivieren oder Deaktivieren von Popup-Warnmeldungen
- SNMP-Traps für Backup Exec-Warnmeldungen

Warnmeldungen und Benachrichtigungen in Backup Exec

Als Warnmeldungen werden alle Ereignisse oder Zustände in Backup Exec bezeichnet, die wichtig genug sind, dass eine Meldung ausgegeben wird, oder auf die der Benutzer reagieren muss. In Backup Exec stehen zahlreiche Warnmeldungskategorien und vier Warnmeldungstypen zur Verfügung. Warnmeldungskategorien sind Ereignisse oder Zustände, die Warnmeldungen verursachen. Dazu gehören Zustände oder Probleme, die sich auf das System, auf Aufträge, Medien oder Speicherquellen auswirken. Zu jeder Warnmeldungskategorie können ein oder mehr Ereignisse gehören, für die Warnmeldungen ausgegeben werden. So können z. B. Fehler wegen fehlgeschlagener Aufträge aus vielen Gründen auftreten. Die Schweregrade der Warnmeldungen können Ihnen helfen, festzulegen, welche Warnmeldungen unmittelbare Aufmerksamkeit benötigen und auf welche Warnmeldungen reagiert werden muss.

Die folgenden Schweregrade der Warnmeldungen werden in Backup Exec verwendet:

Tabelle 7-1 Schweregrad der Meldung

Element	Beschreibung
Bedienereingriff erforderlich	Dieser Warnmeldungstyp zeigt die Probleme an, auf die der Benutzer reagieren muss, bevor der Auftrag oder Vorgang fortgesetzt werden kann.

Element	Beschreibung
Fehler	Zeigt die Probleme an, die die Verarbeitung von Aufträgen oder die Integrität des Backup beeinträchtigen. Diese Warnmeldungen können nicht deaktiviert werden und es ist nicht möglich, ihre automatische Löschung zu konfigurieren. Sie müssen auf sie manuell reagieren.
Warnung	Zeigt Bedingungen an, unter denen Aufträge fehlschlagen können, was aber nicht notwendigerweise der Fall ist. Sie sollten diese Bedingungen überwachen und Maßnahmen für deren Lösung ergreifen.
Informationsmeldung	Enthält Statusmeldungen über die Bedingungen, über die Sie vielleicht Bescheid wissen möchten.

Standardmäßig sind die meisten Warnmeldungen aktiviert, d. h., sie werden im Bereich "Aktive Warnmeldungen" angezeigt. Sie können Warnmeldungen der Typen "Warnung" und "Informatorisch" deaktivieren, indem Sie die Eigenschaften der Warnmeldungskategorien bearbeiten. Die Warnmeldungstypen "Fehler" und "Bedienereingriff erforderlich" können jedoch nicht deaktiviert werden. Sie können die Warnmeldungen filtern, damit nur bestimmte Warnmeldungen angezeigt werden.

Siehe ["Konfigurieren von Warnmeldungskategorien"](#) auf Seite 354.

Über die Registerkarte "Startseite" können Sie alle aktiven Warnmeldungen anzeigen oder die Warnmeldungen nach Typ und Datum filtern. Wenn Sie auf der Registerkarte "Backup und Wiederherstellung" auf einen Server doppelklicken, können Sie die aktiven Warnmeldungen für diesen Server anzeigen.

Dementsprechend können Sie auf der Registerkarte "Speicher" auf einen Speichertyp doppelklicken, um die aktiven Warnmeldungen für dieses Speichergerät anzuzeigen.

Warnmeldungen verbleiben in der Ansicht "Aktive Warnmeldungen", bis auf sie reagiert wird. Sie können auf Warnmeldungen manuell reagieren oder Backup Exec für einige Warnmeldungen so konfigurieren, dass nach Ablauf einer festgelegten Zeit eine automatische Reaktion erfolgt. Ob eine Antwort erforderlich ist, hängt vom Schweregrad der Warnmeldung ab. Bei Informationsmeldungen ist dies beispielsweise nicht der Fall. Nachdem Sie auf eine Warnmeldung reagiert haben, verschiebt Backup Exec sie in den Warnmeldungsverlauf. Der Warnmeldungsverlauf ist auf den Registerkarten "Startseite", "Backup und Wiederherstellung" und "Speicher" verfügbar. Darüber hinaus ist ein Bericht zum Warnmeldungsverlauf auf der Registerkarte "Berichte" verfügbar.

Siehe ["Bericht "Warnmeldungsverlauf"](#) auf Seite 819.

Siehe ["Reagieren auf aktive Warnmeldungen"](#) auf Seite 343.

Sie können Benachrichtigungen so konfigurieren, dass beim Auftreten von Warnmeldungen bestimmte Empfänger benachrichtigt werden. Sie könnten z. B. einen Backup-Administrator mithilfe einer Benachrichtigung per E-Mail oder einer SMS-Nachricht auf dem Mobiltelefon auf wichtige Warnmeldungen hinweisen.

Siehe ["Einrichten von Benachrichtigungen für Warnmeldungen"](#) auf Seite 344.

Um die Fehlerbehebung für die Hardware zu erleichtern, zeigt Backup Exec Warnmeldungen für die SCSI-Ereignisse mit ID 9 (Speicherzeitüberschreitung), ID 11 (Controller-Fehler), und ID 15 (Speicher nicht bereit) an.

Warnmeldungen in Backup Exec

Warnmeldungen werden an verschiedenen Stellen in der Backup Exec-Administratorkonsole angezeigt.

Tabelle 7-2 Warnmeldungen in der Backup Exec-Administratorkonsole

Anzeigeort der Warnmeldungen	Details
Registerkarte "Startseite"	<p>Damit eine Liste von aktiven Warnmeldungen auf der Registerkarte "Startseite" angezeigt wird, stellen Sie sicher, dass das Kontrollkästchen "Aktive Warnmeldungen" in der Gruppe "Systemzustand" aktiviert ist.</p> <p>Damit eine Liste von Warnmeldungen im Verlauf angezeigt wird, stellen Sie sicher, dass das Kontrollkästchen "Warnmeldungsverlauf" in der Gruppe "Systemzustand" aktiviert ist.</p> <p>Im Widget "Aktive Warnmeldungen" auf der Registerkarte "Startseite" können Sie auf Warnmeldungen reagieren, das Auftragsprotokoll anzeigen, alle Info-Warnmeldungen löschen oder die Details von bestimmten Warnmeldungen anzeigen.</p>

Anzeigeort der Warnmeldungen	Details
Registerkarte "Backup und Wiederherstellung"	<p>Auf der Registerkarte "Backup und Wiederherstellung" werden aktive Warnmeldungen für jeden Server in der Liste aufgelistet. Wenn Sie auf einen Server doppelklicken, können Sie im linken Teilfenster "Aktive Warnmeldungen" auswählen, um alle aktiven Warnmeldungen für diesen Server anzuzeigen. Wenn Sie "Aktive Warnmeldungen" im linken Teilfenster auswählen, ist die Option "Warnmeldungsverlauf anzeigen" auch in der Gruppe "Warnmeldungen" oben im Dialogfeld verfügbar.</p> <p>Zusätzlich können Sie auf das Warnsymbol neben einem Servernamen klicken, um die Warnmeldungen für diesen Server anzuzeigen.</p>
Registerkarte "Speicher"	<p>Auf der Registerkarte "Speicher" werden aktive Warnmeldungen für die Speichergeräte in der Liste aufgelistet. Wenn Sie auf ein Speichergerät doppelklicken, können Sie im linken Teilfenster "Aktive Warnmeldungen" auswählen, um alle aktiven Warnmeldungen für dieses Gerät anzuzeigen. Wenn Sie "Aktive Warnmeldungen" im linken Teilfenster auswählen, ist die Option "Warnmeldungsverlauf anzeigen" auch in der Gruppe "Warnmeldungen" oben im Dialogfeld verfügbar.</p> <p>Zusätzlich können Sie auf das Warnsymbol neben einem Speichergerät klicken, um die Warnmeldungen für dieses Gerät anzuzeigen.</p>
Backup Exec-Statusleiste	<p>Die Backup Exec-Statusleiste zeigt die Anzahl von aktiven Warnmeldungen für jeden Typ an. Doppelklicken Sie im Abschnitt "Warnmeldungen" der Backup Exec-Statusleiste, um eine Liste aller aktiven Warnmeldungen, den Warnmeldungsverlauf sowie Details zu diesen Warnmeldungen anzuzeigen.</p>

Anzeigeort der Warnmeldungen	Details
Windows-Statusleiste	Wenn Sie Backup Exec minimiert haben, blinkt das Backup Exec-Symbol in der Windows-Statusleiste, wenn eine Backup Exec-Warnmeldung ausgelöst wird. Wenn Sie Backup Exec maximieren, werden die Popup-Warnmeldungen angezeigt.
Popup-Fenster	Popup-Fenster werden angezeigt, wenn eine Warnmeldung ausgelöst wird. Die Farbe des Popup entspricht dem Typ der Warnmeldung: Rot für Fehler, Gelb für Warnungen, Purpur für "Eingreifen erforderlich" und Blau für Informationen. Wenn mehr als drei Warnmeldungen verfügbar sind, listet das Popup die Anzahl der ausstehenden Warnmeldungen auf und die Farbe des Popup weist auf den schwersten Warnmeldungstyp hin. Beispiel: Wenn drei Infomeldungen und zwei Fehlermeldungen aufgetreten sind, zeigt das Popup fünf Warnmeldungen an. Das Popup ist rot, da Fehlermeldungen enthalten sind. Sie können direkt aus dem Popup auf Warnmeldungen zugreifen, die ein Eingreifen erfordern.

Aktivieren der Anzeige aktiver Warnmeldungen und des Warnmeldungsverlaufs auf der Registerkarte "Startseite"

Das Teilfenster "Aktive Warnmeldungen" wird standardmäßig auf der Registerkarte "Startseite" angezeigt. Wenn es nicht angezeigt wird, zeigen Sie die Details zu Warnmeldungen wie folgt an. Sie können auch die Anzeige des Verlaufs aller Warnmeldungen für den Server auf der Registerkarte "Startseite" aktivieren.

So zeigen Sie aktive Warnmeldungen und den Warnmeldungsverlauf auf der Registerkarte "Startseite" an

- ◆ Führen Sie auf der Registerkarte "Startseite" unter "Systemzustand" einen der folgenden Schritte aus:
 - Aktivieren Sie das Kontrollkästchen "Aktive Warnmeldungen", um eine Liste der aktiven Warnmeldungen anzuzeigen.

- Aktivieren Sie das Kontrollkästchen "Warnmeldungsverlauf", um eine Liste aller Warnmeldungen anzuzeigen, die auf dem Server auftraten.

Siehe ["Eigenschaften für aktive Warnmeldungen "](#) auf Seite 339.

Eigenschaften für aktive Warnmeldungen

Eigenschaften für aktive Warnmeldungen können auf der Registerkarte "Startseite" oder in den Details für einen Backup-Auftrag, einen Wiederherstellungsauftrag oder einen Speichertyp angezeigt werden.

Siehe ["Aktivieren der Anzeige aktiver Warnmeldungen und des Warnmeldungsverlaufs auf der Registerkarte "Startseite" "](#) auf Seite 338.

Tabelle 7-3 Eigenschaften für aktive Warnmeldungen

Element	Beschreibung
Schweregrad	<p>Weist auf den Schweregrad der Meldung hin. Anhand des Schweregrads können Sie festlegen, wie dringend eine Reaktion ist.</p> <p>Die folgenden Schweregrade für Warnmeldungen werden möglicherweise angezeigt:</p> <ul style="list-style-type: none"> ■ Fehler ■ Warnung ■ Informationen ■ Bedienereingriff erforderlich
Kategorie	Gibt die Bedingung an, die die Warnmeldung verursachte. Die Kategorien umfassen "Datenbankverwaltung", "Allgemeine Informationen", Gerätefehler und "Auftrag fehlgeschlagen".
Meldung	Zeigt den Text der Fehlermeldung an.
Datum/Uhrzeit	Zeigt das Datum und die Uhrzeit an, als die Warnmeldung erhalten wurde.
Auftragsname	Zeigt den Namen des Auftrags an, der die Warnmeldung auslöste. Diese Spalte ist leer, wenn ein Auftrag die Warnmeldung auslöste, wie zum Beispiel für Warnmeldungen zur allgemeinen Information.
Speicherort	Zeigt den Namen des Speichergeräts an, auf dem die Warnmeldung aufgetreten ist.
Server	Gibt den Namen des Servers an, auf dem die Warnmeldung aufgetreten ist.

Element	Beschreibung
Quelle	<p>Gibt den Grund für die Ausgabe der Meldung an.</p> <p>Meldungen können aus folgenden Quellen stammen:</p> <ul style="list-style-type: none"> ■ System ■ Auftrag ■ Speicherort ■ Medien

Anzeigen des Warnmeldungsverlaufs für einen Server oder ein Speichergerät

Nachdem Sie auf eine Warnmeldung reagiert haben, verschiebt Backup Exec sie in den Warnmeldungsverlauf.

So zeigen Sie den Warnmeldungsverlauf für einen Server oder ein Speichergerät an

- 1 Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, dessen Warnmeldungsverlauf Sie anzeigen möchten.
- 2 Im linken Teilfenster klicken Sie auf "Aktive Warnmeldungen".
- 3 Wählen Sie unter "Warnmeldungen" die Option "Warnmeldungsverlauf anzeigen".

Löschen einer Warnmeldung aus dem Warnmeldungsverlauf

Gehen Sie wie folgt vor, um eine Warnmeldung aus dem Warnmeldungsverlauf zu löschen.

So löschen Sie eine Warnmeldung aus dem Warnmeldungsverlauf

- 1 Rufen Sie den Warnmeldungsverlauf an einer der folgenden Stellen auf:
 - In der Backup Exec-Statusleiste doppelklicken Sie in den Bereich "Warnmeldungen".
 - Auf der Registerkarte "Backup und Wiederherstellung" doppelklicken Sie auf einen Server. Im linken Teilfenster klicken Sie auf "Aktive Warnmeldungen" und dann auf "Warnmeldungsverlauf anzeigen".

- Auf der Registerkarte "Speicher" doppelklicken Sie auf ein Speichergerät. Im linken Teilfenster klicken Sie auf "Aktive Warnmeldungen" und dann auf "Warnmeldungsverlauf anzeigen".
- 2 Wählen Sie im Dialogfeld "Warnmeldungen" die Registerkarte "Warnmeldungsverlauf" aus.
 - 3 Klicken Sie mit der rechten Maustaste auf die Warnmeldung, die Sie aus dem Warnmeldungsverlauf entfernen möchten, und klicken Sie dann auf "Löschen".
 - 4 Sie werden gefragt, ob die Warnmeldung wirklich gelöscht werden soll. Bestätigen Sie mit "Ja".

Kopieren der Warnmeldung in ein Dokument oder eine E-Mail

In Backup Exec können Sie Warnmeldungsinformationen in ein Textverarbeitungsprogramm (z. B. Editor oder Microsoft Word) oder in eine E-Mail kopieren. Dabei formatiert Backup Exec den Text als Tabelle. Im Editor wird der Text unformatiert eingefügt.

So kopieren Sie den Text einer Warnmeldung in ein Dokument oder eine E-Mail

- 1 Rufen Sie die Liste der Warnmeldungen an einer der folgenden Stellen auf:
 - In der Backup Exec-Statusleiste doppelklicken Sie in den Bereich "Warnmeldungen".
 - Auf der Registerkarte "Backup und Wiederherstellung" doppelklicken Sie auf einen Server. Im linken Teilfenster klicken Sie auf "Aktive Warnmeldungen".
 - Auf der Registerkarte "Speicher" doppelklicken Sie auf ein Speichergerät. Im linken Teilfenster klicken Sie auf "Aktive Warnmeldungen".
- 2 Im Dialogfeld "Warnmeldungen" klicken Sie entweder auf die Registerkarte "Aktive Warnmeldungen" oder "Warnmeldungsverlauf", abhängig davon, wo sich die Warnmeldung befindet, die Sie kopieren möchten.

- 3 Klicken Sie mit der rechten Maustaste auf die Warnmeldung, die Sie kopieren möchten, und klicken Sie dann auf "Kopieren".

Hinweis: Sie können auch eine Warnmeldung auswählen und dann Strg+C drücken, um den Text zu kopieren. Darüber hinaus können Sie mehrere Warnmeldungen kopieren, indem Sie die Umschalt- bzw. Strg-Taste gedrückt halten und auf die einzelnen Meldungen klicken.

- 4 Öffnen Sie das Dokument oder die E-Mail, klicken Sie mit der rechten Maustaste hinein und wählen Sie im Kontextmenü die Option "Einfügen".

Filtern von Warnmeldungen

Sie können die Warnmeldungen filtern, die auf der Registerkarte "Startseite" unter "Aktive Warnmeldungen" angezeigt werden. Filter sind sinnvoll, wenn zahlreiche Warnmeldungen vorhanden sind und Sie nur bestimmte Typen von Warnmeldungen anzeigen möchten. Warnmeldungen können nach Schweregrad, Zeit und Quelle gefiltert werden. Beispielsweise können Sie festlegen, dass nur die Fehlerwarnmeldungen angezeigt werden sollen, die in den letzten 12 Stunden für Aufträge ausgegeben wurden.

So filtern Sie Warnmeldungen:

- 1 Suchen Sie auf der Registerkarte "Startseite" das Teilfenster "Aktive Warnmeldungen".

Wenn das Teilfenster "Aktive Warnmeldungen" nicht angezeigt wird, müssen Sie die Warnmeldungsdetails aktivieren.

Siehe ["Aktivieren der Anzeige aktiver Warnmeldungen und des Warnmeldungsverlaufs auf der Registerkarte "Startseite" "](#) auf Seite 338.

- 2 Sie können beliebige Kombinationen der folgenden Optionen verwenden, um die Warnmeldungsliste zu filtern:
 - Wählen Sie im Feld "Quelle" die Quelle der Warnmeldungen aus, die Sie anzeigen möchten.
 - Wählen Sie im Feld "Uhrzeit" den Zeitrahmen aus, für den Sie Warnmeldungen anzeigen möchten.
 - Wählen Sie im Feld "Schweregrad" die Schweregrade der anzuzeigenden Warnmeldungen, z. B. "Fehler" oder "Warnung".

Anzeigen des Auftragsprotokolls für Warnmeldungen

Das Auftragsprotokoll enthält ausführliche Informationen zum Auftrag, zu Speicher und Medien sowie Auftragsoptionen, Dateistatistiken und Auftragsabschlussstatus (bei abgeschlossenen Aufträgen). Sie können von den Warnmeldungen aus, die für Aufträge generiert wurden, auf das Auftragsprotokoll zugreifen.

So zeigen Sie das Auftragsprotokoll von einer Warnmeldung aus an

- 1 Wechseln Sie auf der Registerkarte "Startseite", "Backup und Wiederherstellung" oder "Speicher" zum Teilfenster "Aktive Warnmeldungen".
- 2 Klicken Sie mit der rechten Maustaste auf die Warnmeldung, für die Sie das Auftragsprotokoll anzeigen möchten, und wählen Sie dann "Auftragsprotokoll anzeigen" aus.
- 3 Führen Sie einen der folgenden Schritte aus:
 - Klicken Sie auf "Suchen", um nach bestimmten Wörtern zu suchen. Geben Sie den gewünschten Text ein und klicken Sie auf "Weiter".
Stellen Sie sicher, dass alle Abschnitte des Auftragsprotokolls erweitert sind. Die Suchfunktion sucht nur in den erweiterten Abschnitten des Auftragsprotokolls.
 - Soll das Auftragsprotokoll gedruckt werden, klicken Sie auf "Drucken". Zum Drucken des Protokolls müssen Sie einen an Ihr System angeschlossenen und ordnungsgemäß konfigurierten Drucker haben.
 - Um das Auftragsprotokoll als eine HTML- oder TXT-Datei zu speichern, klicken Sie auf "Speichern unter" und wählen Sie Dateinamen, Speicherort und Dateityp aus.

Reagieren auf aktive Warnmeldungen

Sie können auf aktive Warnmeldungen reagieren und den Vorgang je nach Warnmeldungsbedingung fortsetzen oder abbrechen. Backup Exec zeigt standardmäßig alle aktivierten Warnmeldungen sowie jene Meldungen an, die eine Reaktion des Benutzers erfordern. Wenn Sie Filter festgelegt haben, werden außer den Warnmeldungen, die eine Reaktion erfordern, nur die ausgewählten Warnmeldungen angezeigt.

Wenn Sie im Dialogfeld für die Reaktion auf die Warnmeldung auf "Schließen" klicken, wird das Dialogfeld geschlossen, die Warnmeldung bleibt jedoch aktiv. Um die Warnmeldung zu löschen, müssen Sie eine Reaktion wählen, z. B. "OK", "Ja",

"Nein" oder "Abbrechen". Für einige Warnmeldungskategorien können automatische Reaktionen konfiguriert werden.

Siehe ["Konfigurieren von Warnmeldungskategorien"](#) auf Seite 354.

Manche Warnmeldungen weisen einen Code mit eindeutiger Meldungskennung (Unique Message Identifier, UMI) auf. Dieser Code ist ein Hyperlink zur Website des technischen Supports von Veritas. Hier finden Sie technische Hinweise in direktem Bezug auf die Meldung.

So reagieren Sie auf eine aktive Warnmeldung:

- 1 Wechseln Sie auf der Registerkarte "Startseite", "Backup und Wiederherstellung" oder "Speicher" zum Teilfenster "Aktive Warnmeldungen".
- 2 Klicken Sie mit der rechten Maustaste auf die Warnmeldung, auf die Sie reagieren möchten auf, und klicken Sie dann auf "Beantworten" oder auf "Mit 'OK' beantworten".
- 3 Klicken Sie auf eine Reaktion für die Warnmeldung, wie zum Beispiel "Mit 'OK' antworten" oder "Antworten".

Manuelles Löschen aller Informationsmeldungen

Sie können einzelne Warnmeldungskategorien so konfigurieren, dass sie automatisch nach einer gewissen Zeit gelöscht werden. Informationsmeldungen werden möglicherweise häufig generiert, Sie sollten daher eventuell alle Informationsmeldungen manuell löschen, bevor das System sie automatisch verschiebt.

So löschen Sie alle Informationsmeldungen manuell

- 1 Wechseln Sie auf der Registerkarte "Startseite", "Backup und Wiederherstellung" oder "Speicher" zum Teilfenster "Aktive Warnmeldungen".
- 2 Klicken Sie mit der rechten Maustaste auf eine Informationsmeldung und wählen Sie "Alle Informationen löschen".

Siehe ["Konfigurieren von Warnmeldungskategorien"](#) auf Seite 354.

Einrichten von Benachrichtigungen für Warnmeldungen

Sie können Backup Exec so konfigurieren, dass beim Auftreten von Warnmeldungen bestimmte Empfänger benachrichtigt werden. Benachrichtigungen für Warnmeldungen einzurichten ist ein dreistufiger Prozess:

Tabelle 7-4 So richten Sie Benachrichtigungen für Warnmeldungen ein

Schritt	Aktion
Schritt 1	<p>Konfigurieren Sie die Methode, die für die Benachrichtigung des Empfängers verwendet werden soll. Die Benachrichtigungsmethoden sind Textmeldung oder E-Mail.</p> <p>Siehe "Konfigurieren von E-Mail- oder SMS-Benachrichtigungen für Warnmeldungen" auf Seite 345.</p>
Schritt 2	<p>Fügen Sie die Kontaktdaten für die Personen oder die Gruppen hinzu, die Benachrichtigungen erhalten sollen.</p> <p>Siehe "Hinzufügen von Empfängern für die Benachrichtigung" auf Seite 348.</p> <p>Siehe "Hinzufügen einer Empfängergruppe für Warnmeldungen" auf Seite 351.</p>
Schritt 3	<p>Weisen Sie jedem Empfänger die entsprechende Warnmeldungskategorie zu, deren Benachrichtigungen er erhalten soll.</p> <p>Siehe "Zuweisen von bestimmten Warnmeldungskategorien an bestimmte Empfänger" auf Seite 356.</p> <p>Siehe "Konfigurieren von Warnmeldungskategorien" auf Seite 354.</p> <p>Siehe "Senden einer Benachrichtigung beim Abschluss eines Auftrags" auf Seite 357.</p>

Konfigurieren von E-Mail- oder SMS-Benachrichtigungen für Warnmeldungen

Sie können Backup Exec so einrichten, dass E-Mails oder SMS an die angegebenen Empfänger geschickt werden, wenn eine Warnmeldung auftritt. Für die E-Mail-Benachrichtigung muss ein E-Mail-Konto als Absender verwendet werden. Sie könnten z. B. ein E-Mail-Konto für den Backup-Administrator oder den IT-Administrator verwenden. Um E-Mail-Benachrichtigungen zu konfigurieren, geben Sie den Namen des E-Mail-Servers des Absenders, die vom Server verwendete Port-Nummer und den Namen und die E-Mail-Adresse des Absenders ein. Sie können Backup Exec auch für die Authentifizierung der für Warnmeldungen verwendeten E-Mails einrichten.

Tabelle 7-5 Typen der Benachrichtigung

Benachrichtigungstyp	Beschreibung
E-Mail-Benachrichtigung	Backup Exec verwendet SMTP für E-Mail-Benachrichtigungen und unterstützt Authentifizierung und Transport Layer Security (TLS). E-Mail-Benachrichtigungen können an Microsoft Outlook und webbasierte E-Mail-Anwendungen wie zum Beispiel Gmail oder Yahoo geschickt werden.
Benachrichtigungen per SMS	<p>Für Benachrichtigungen per Text-Messages versucht Backup Exec, die Meldung so zu formatieren, dass sie weniger als 144 Zeichen enthält, damit die Einschränkungen für das Text-Messaging-Protokoll eingehalten werden. Durch Begrenzen einer Benachrichtigung auf weniger als 144 Zeichen wird mit größerer Wahrscheinlichkeit erreicht, dass diese in einer einzelnen Text-Message verschickt anstatt in mehrere Messages unterteilt wird. Jedoch legt der Anbieter des Text-Messaging-Service fest, wie die Benachrichtigungen verschickt werden.</p> <p>SMS-Benachrichtigungen werden in den folgenden Formaten gesendet:</p> <ul style="list-style-type: none"> ■ Auftragsbezogene Benachrichtigung: Backup Exec: <Servername> : <Auftragsname> : <Status> ■ Benachrichtigungen zu Warnmeldungen: Backup Exec: <Servername> : <Warnmeldungstyp>

Nachdem die E-Mail-Informationen des Absenders eingegeben wurden, können Informationen über Empfänger eingerichtet werden.

Hinweis: Ein SMTP-kompatibles E-Mail-System, z. B. ein POP3-E-Mail-Server, ist für E-Mail-Benachrichtigungen erforderlich.

Hinweis: Nachdem Sie die E-Mail- oder Textbenachrichtigung konfiguriert haben, können Sie die Konfiguration nicht entfernen, um Benachrichtigungen zu deaktivieren. Sie können jedoch die Benachrichtigungen für einzelne Empfänger deaktivieren.

So konfigurieren Sie Backup Exec, um E-Mail oder Textbenachrichtigung für Warnmeldungen zu senden

- 1** Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- 2** Wählen Sie "Warnmeldungen und Benachrichtigungen", und dann "E-Mail- und Textbenachrichtigung".
- 3** Geben Sie die Daten des Absenders der E-Mail oder der SMS ein.

Wenn Sie Warnmeldungen per E-Mail senden möchten

Gehen Sie wie folgt vor:

- Unter "E-Mail-Konfiguration" geben Sie den Namen des E-Mail-Servers, der Port-Nummer, die der E-Mail-Server verwendet, und den Namens und die E-Mail-Adresse des Absenders ein.
- Wenn Sie die E-Mail-Informationen authentifizieren möchten, die Sie eingaben, aktivieren Sie "E-Mail-Authentifizierung aktivieren" und geben Sie dann den Benutzernamen und das Kennwort für das E-Mail-Konto des Absenders ein.

Wenn Sie Warnmeldungen per Textnachricht senden möchten

Unter "Service-Provider-Adresse der Textmeldung" geben Sie den vollqualifizierten Domännennamen des Absenders des Text Messaging Service Providers ein.

Wenn beispielsweise eine Firma namens "MyPhone" Textnachrichtendienste anbietet, geben Sie im Feld "Service-Provider-Adresse der Textmeldung" den Wert "MyPhone.com" ein. Sie können diese Standardadresse für einzelne Benutzer, die diesen Provider nicht verwenden, außer Kraft setzen.

Hinweis: SMS-Benachrichtigungen werden als SMTP-Mail an eine E-Mail-Adresse geschickt, die von einem SMS-Service-Provider zur Verfügung gestellt wird. Um Benachrichtigungen per SMS zu aktivieren, müssen Sie die Informationen über das E-Mail-Konto des Absenders im Abschnitt "E-Mail-Konfiguration" zusätzlich zum vollständig qualifizierten Domännennamen des Standard-Service-Providers für SMS eingeben.

4 Klicken Sie auf "OK".

Sie können Informationen über die Empfänger jetzt hinzufügen, die Warnmeldungsbenachrichtigungen erhalten müssen.

Siehe "[Hinzufügen von Empfängern für die Benachrichtigung](#)" auf Seite 348.

Hinzufügen von Empfängern für die Benachrichtigung

Sie können Einzelpersonen oder Gruppen so einrichten, dass sie Benachrichtigungen erhalten, wenn Warnmeldungen in Backup Exec ausgegeben werden. Wenn Sie einen einzelnen Empfänger einrichten, geben Sie an, ob diese Person Benachrichtigungen per E-Mail, Text-Message oder beides erhalten soll. Ein Gruppenempfänger enthält die einzelnen Empfänger, die Sie auswählen. Jede Einzelperson innerhalb einer Gruppe erhält Benachrichtigungen auf dem für die Einzelperson angegebenen Weg: per E-Mail, Textmeldung oder beides.

Hinweis: Informationen über den Absender der Benachrichtigung müssen konfiguriert werden, bevor Empfänger konfiguriert werden können.

Siehe ["Konfigurieren von E-Mail- oder SMS-Benachrichtigungen für Warnmeldungen"](#) auf Seite 345.

So fügen Sie Empfänger für Benachrichtigung per E-Mail oder Textmeldungen hinzu

- 1** Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- 2** Wählen Sie "Warnmeldungen und Benachrichtigungen", und dann "Empfänger der Benachrichtigung".
- 3** Klicken Sie im Dialogfeld "Empfänger verwalten" auf "Empfänger hinzufügen".
- 4** Geben Sie im Feld "Name" den Namen des Empfängers ein.
- 5** Wählen Sie die Methode der Benachrichtigung für diesen Empfänger aus:

So schicken Sie E-Mails an diesen Empfänger

Aktivieren Sie "Benachrichtigungen per E-Mail senden" und geben Sie anschließend die E-Mail-Adresse der Person an.

Um die Anzahl von E-Mails, die innerhalb eines bestimmten Zeitraums gesendet werden, zu begrenzen, aktivieren Sie "Nicht mehr als X E-Mails innerhalb von X Minuten/Stunden senden" und geben Sie dann die Höchstzahl von E-Mails ein, die innerhalb eines bestimmten Zeitraums gesendet werden sollen.

So senden Sie Textmeldungen an diesen Empfänger

Aktivieren Sie "Benachrichtigungen als Textmeldung senden" und geben Sie anschließend die Handynummer der Person sowie die Adresse des Textnachrichtendienst an.

Hinweis: Wenn sich der Empfänger in einem anderen Land befindet, müssen Sie die Vorwahl für Auslandsgespräche des Landes, von dem die Meldung generiert wird, und die Landesvorwahl, in dem der Empfänger sich befindet, einschließen. Beispielsweise ist die Vorwahl für Auslandsgespräche für die USA 011. Die Landesvorwahl für Italien ist 39. Um eine Nachricht von den USA an einen Empfänger in Italien zu senden, geben Sie **011 39** und die Telefonnummer des Empfängers ein.

Die Telefonnummer kann Leerzeichen und die folgenden Zeichen umfassen:

- Öffnende und schließende Anführungszeichen
- Punkt
- Pluszeichen
- Gedankenstrich
- Öffnende und schließende Klammern
- Schrägstrich

Um die Anzahl von Textmeldungen, die innerhalb eines bestimmten Zeitraums gesendet werden, zu begrenzen, aktivieren Sie "Nicht mehr als X Textmeldungen innerhalb von X Minuten/Stunden senden" und geben Sie dann die Höchstzahl von Textmeldungen ein, die innerhalb eines bestimmten Zeitraums gesendet werden sollen.

6 Klicken Sie auf "OK".

Sie können die Empfänger jetzt den Meldungskategorien zuweisen, für die sie Benachrichtigungen erhalten sollten.

Siehe ["Zuweisen von bestimmten Warnmeldungskategorien an bestimmte Empfänger"](#) auf Seite 356.

Hinzufügen einer Empfängergruppe für Warnmeldungen

Gruppen werden konfiguriert, indem Empfänger als Gruppenmitglieder hinzugefügt werden. Eine Gruppe besteht aus mindestens einem Empfänger. Wenn Sie eine Gruppe als Empfänger konfigurieren, erhält jedes Mitglied der Gruppe die Benachrichtigung. Eine Gruppe kann nur aus Einzelpersonen bestehen. Gruppen können keine anderen Gruppen enthalten.

So fügen Sie eine Empfängergruppe für Warnmeldungen hinzu

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- 2 Wählen Sie "Warnmeldungen und Benachrichtigungen", und dann "Empfänger der Benachrichtigung".
- 3 Klicken Sie im Dialogfeld "Empfänger verwalten" auf "Gruppe hinzufügen".
- 4 Geben Sie im Feld "Name" einen eindeutigen Namen für die Benachrichtigungsgruppe ein.
- 5 Um der Gruppe Mitglieder hinzuzufügen, wählen Sie in der Liste "Alle Empfänger" die gewünschten Empfänger aus und klicken Sie auf "Hinzufügen", um diese in die Liste "Gruppenmitglieder" zu verschieben.

Wenn Sie Empfänger aus der Gruppe entfernen möchten, wählen Sie diese in der Liste "Ausgewählte Empfänger" aus und klicken auf "Entfernen". Die Empfängernamen werden daraufhin in die Liste mit allen Empfängern verschoben.

- 6 Wenn die Gruppe die gewünschten Empfänger umfasst, klicken Sie auf "OK". Die Gruppe wird der Liste der Empfänger im Dialogfeld "Empfänger verwalten" hinzugefügt.

Siehe ["Hinzufügen von Empfängern für die Benachrichtigung"](#) auf Seite 348.

Entfernen eines Empfängers aus einer Gruppe

Wenn Sie einen Empfänger aus einer Gruppe entfernen, erhält dieser nicht die Benachrichtigungen, die die Gruppe entsprechend ihrer Konfiguration erhält, nicht mehr. Der Empfänger erhält weiterhin die für ihn konfigurierten Benachrichtigungen.

So entfernen Sie einen Empfänger aus einer Gruppe

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- 2 Wählen Sie "Warnmeldungen und Benachrichtigungen", und dann "Empfänger der Benachrichtigung".
- 3 Doppelklicken Sie im Dialogfeld "Empfänger verwalten" auf die Gruppe, die den Empfänger enthält.
- 4 Wählen Sie unter "Ausgewählte Empfänger" den zu entfernenden Empfänger und klicken Sie auf "Entfernen".

Deaktivieren von Warnmeldungen per E-Mail oder SMS für einen Empfänger

Wenn eine Person keine Warnmeldungen mehr erhalten möchte, können Sie diese Benachrichtigungen deaktivieren.

Hinweis: Anstatt Benachrichtigungen vollständig zu deaktivieren, können Sie die Warnmeldungskategorien ändern, für die ein Benutzer Benachrichtigungen erhält.

Siehe ["Deaktivieren von Benachrichtigungen für eine bestimmte Meldungskategorie"](#) auf Seite 358.

So deaktivieren Sie Warnmeldungen per E-Mail oder SMS für einen Empfänger

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- 2 Wählen Sie "Warnmeldungen und Benachrichtigungen", und dann "Empfänger der Benachrichtigung".
- 3 Wählen Sie im Dialogfeld "Empfänger verwalten" den Namen des Empfängers aus und klicken Sie dann auf "Bearbeiten".
- 4 Führen Sie einen der folgenden Schritte aus:
 - Deaktivieren Sie das Kontrollkästchen "Benachrichtigungen per E-Mail senden", um E-Mail-Benachrichtigungen zu deaktivieren.
 - Deaktivieren Sie das Kontrollkästchen "Benachrichtigungen als Textmeldung senden", um Benachrichtigungen als Textmeldung zu deaktivieren.
- 5 Klicken Sie auf "OK".

Bearbeiten der Benachrichtigungseigenschaften für Empfänger

Sie können die Benachrichtigungseigenschaften für Empfänger jederzeit bearbeiten und dabei Empfängerinformationen wie zum Beispiel eine E-Mail-Adresse oder Mobiltelefonnummer ändern. In Gruppen können Sie Empfänger hinzufügen oder daraus entfernen.

So bearbeiten Sie die Benachrichtigungseigenschaften für einen Empfänger:

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- 2 Wählen Sie "Warnmeldungen und Benachrichtigungen", und dann "Empfänger der Benachrichtigung".
- 3 Wählen Sie im Dialogfeld "Empfänger verwalten" den Empfänger aus, den Sie bearbeiten möchten.
- 4 Klicken Sie auf "Bearbeiten".
- 5 Bearbeiten Sie die Eigenschaften für den ausgewählten Empfänger.
- 6 Klicken Sie auf OK.

Löschen von Empfängern

Sie können Empfänger, die keine Benachrichtigungen erhalten sollen, entfernen. Beachten Sie, dass diese Empfänger dauerhaft gelöscht werden. Außerdem können Sie Benachrichtigung für Empfänger deaktivieren.

Siehe ["Deaktivieren von Benachrichtigungen für eine bestimmte Meldungskategorie"](#) auf Seite 358.

Siehe ["Deaktivieren von Warnmeldungen per E-Mail oder SMS für einen Empfänger"](#) auf Seite 352.

So löschen Sie einen Empfänger

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- 2 Wählen Sie "Warnmeldungen und Benachrichtigungen", und dann "Empfänger der Benachrichtigung".
- 3 Wählen Sie im Dialogfeld "Empfänger verwalten" den Empfänger aus, den Sie löschen möchten.
- 4 Klicken Sie auf "Löschen".

- 5 Klicken Sie auf "Ja", um das Löschen des Empfängers zu bestätigen.
- 6 Klicken Sie auf "OK".

Konfigurieren von Warnmeldungskategorien

Warnmeldungskategorien sind Ereignisse oder Zustände, die Warnmeldungen verursachen. Dazu gehören Zustände oder Probleme, die sich auf das System, auf Aufträge, Medien oder Speicherquellen auswirken. Zu jeder Warnmeldungskategorie können ein oder mehr Ereignisse gehören, für die Warnmeldungen ausgegeben werden. So können z. B. Fehler wegen fehlgeschlagener Aufträge aus vielen Gründen auftreten. Die Warnmeldungstypen können Ihnen helfen, festzulegen, welche Warnmeldungen unmittelbare Aufmerksamkeit benötigen und auf welche Warnmeldungen reagiert werden muss. Sie können Warnmeldungskategorien einrichten, um Meldungen zu aktivieren oder zu deaktivieren und festzulegen, welche Aktionen stattfinden sollen, wenn eine Meldung auftritt.

Die meisten Warnmeldungen sind standardmäßig aktiviert. Die folgenden Warnmeldungskategorien sind jedoch anfangs deaktiviert:

- Backup-Auftrag enthält keine Daten
- Auftragsbeginn
- Auftrag erfolgreich

Sie können Meldungskategorien deaktivieren, wenn sie informatorische oder warnende Warnmeldungen sind. Sie können Meldungskategorien nicht deaktivieren, wenn sie Fehler oder Aufmerksamkeit erfordern Warnmeldungen sind.

Bei jeder Änderung der Warnmeldungskonfiguration wird dies im Überwachungsprotokoll gespeichert. Sie können jederzeit das Überwachungsprotokoll anzeigen, um festzustellen, welche Änderungen an der Warnmeldungskategorie vorgenommen wurden.

So konfigurieren Sie Eigenschaften von Warnmeldungskategorien

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- 2 Wählen Sie "Warnmeldungen und Benachrichtigungen" und dann "Warnmeldungskategorien".
- 3 Wählen Sie unter "Warnmeldungskategorie" die Warnmeldung aus, die Sie konfigurieren möchten.

4 Wählen Sie unter "Kategorieneigenschaften" die passenden Optionen aus.

Meldungen für diese Kategorie aktivieren	Aktiviert oder deaktiviert die Warnmeldung. Warnmeldungstypen wie "Fehler" und "Bedienereingriff erforderlich" können nicht deaktiviert werden.
Auftragsprotokoll in E-Mail-Benachrichtigungen einschließen	Sendet das Auftragsprotokoll an den Empfänger, der für den Erhalt der Benachrichtigung konfiguriert ist. Wenn Sie diese Option auswählen, stellen Sie sicher, dass mindestens ein Empfänger aus dem Bereich "Benachrichtigung an folgende Empfänger senden" am Ende des Dialogfeldes ausgewählt ist.
Ereignis im Windows-Ereignisprotokoll aufzeichnen	Gibt die Warnmeldung in die Windows-Ereignisanzeige ein. Im Windows-Ereignisprotokoll werden alle Eigenschaftsinformationen für die Warnmeldung angezeigt. Wenn im Windows-Ereignisprotokoll kein Link angezeigt wird, können Sie auf der Website für den technischen Support nach Informationen zur Ereignis-ID suchen.
SNMP-Benachrichtigungen senden	Weist darauf hin, ob SNMP-Benachrichtigungen für die Meldung aktiviert sind oder nicht. Diese Option kann nur verwendet werden, wenn SNMP installiert wurde.
Automatisch löschen nach X Tagen/Stunden/Minuten	Hier können Sie in Minuten, Stunden oder Tagen angeben, wie lange die Warnmeldung aktiv bleiben soll, bevor sie gelöscht wird. Hinweis: Fehlerwarnmeldungen können nicht automatisch gelöscht werden, deshalb ist diese Option hier deaktiviert.

Antworten mit

Gibt die Reaktion an, die Backup Exec automatisch senden soll, wenn die Warnmeldung gelöscht wird. Diese Option ist nur für die Warnmeldungskategorien "Medien überschreiben" und "Medien einlegen" und nur bei aktivierter Option "Automatisch löschen nach x Tagen/Stunden/Minuten" verfügbar. Die Möglichkeiten sind "Abbrechen", "Nein", "Ja" oder "OK".

Benachrichtigung an folgende Empfänger senden

Hier können Sie den Namen eines Empfängers auswählen, der benachrichtigt werden soll, wenn dieser Typ der Warnmeldung auftritt. Diese Option kann nur verwendet werden, wenn zuvor Empfänger konfiguriert wurden.

Wenn der Empfänger, an den Sie Benachrichtigungen schicken möchten, nicht in der Liste ist, klicken Sie auf "Empfänger verwalten", um den Empfänger hinzuzufügen.

- 5 Wiederholen Sie Schritt 2 bis 4, um weitere Warnmeldungskategorien zu konfigurieren.
- 6 Klicken Sie auf "OK", um die von Ihnen ausgewählten Eigenschaften zu speichern.

Zuweisen von bestimmten Warnmeldungskategorien an bestimmte Empfänger

Nachdem Sie die Empfänger der Benachrichtigungen eingerichtet haben, müssen Sie die Warnmeldungskategorien festlegen, für die sie Benachrichtigungen erhalten sollen. Es könnte beispielsweise sein, dass einige Empfänger nur Benachrichtigungen über fehlgeschlagene Aufträge und Bandfehler erhalten möchten, während andere Benachrichtigungen für alle Warnmeldungskategorien erhalten möchten.

So weisen Sie bestimmte Warnmeldungskategorien bestimmten Empfängern zu

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- 2 Wählen Sie "Warnmeldungen und Benachrichtigungen" und dann "Warnmeldungskategorien".
- 3 Wählen Sie eine Warnmeldungskategorie in der Liste aus.
- 4 Ist die Kategorie nicht aktiviert, klicken Sie auf "Warnmeldungen für diese Kategorie aktivieren".
- 5 Aktivieren Sie unter "Benachrichtigung an folgende Empfänger senden" das Kontrollkästchen neben dem Namen jedes Empfängers, der für die ausgewählte Warnmeldungskategorie Benachrichtigungen erhalten möchte.
- 6 Klicken Sie auf "OK".

Senden einer Benachrichtigung beim Abschluss eines Auftrags

Sie können die Empfänger angeben, die beim Abschluss eines Auftrags benachrichtigt werden sollen. Die Empfänger müssen eingerichtet sein, bevor Sie die Benachrichtigung einrichten können.

So senden Sie eine Benachrichtigung, wenn ein Auftrag abgeschlossen ist

- 1 Erstellen Sie einen neuen Auftrag oder bearbeiten Sie einen vorhandenen Auftrag.
- 2 Klicken Sie im Dialogfeld "Backup-Optionen" im linken Teilfenster auf "Benachrichtigung".
- 3 Wählen Sie das Kontrollkästchen für jeden Empfänger aus, den Sie beim Abschluss des jeweiligen Auftragsstyps benachrichtigen möchten.
- 4 Um das Auftragsprotokoll mit der Benachrichtigung an eine E-Mail-Adresse zu senden, aktivieren Sie "Auftragsprotokoll in E-Mail-Benachrichtigungen einschließen".
- 5 Wählen Sie im Dialogfeld "Optionen" bei Bedarf weitere Optionen aus, oder klicken Sie auf "OK".

Benachrichtigungsoptionen für Aufträge

Wenn Sie einen Auftrag einrichten oder bearbeiten, können Sie die Empfänger auswählen, die nach Abschluss des Auftrags eine Benachrichtigung erhalten sollen.

Siehe ["Senden einer Benachrichtigung beim Abschluss eines Auftrags"](#) auf Seite 357.

Tabelle 7-6 Benachrichtigungsoptionen für Aufträge

Element	Beschreibung
Empfängername	Zeigt die Namen der Empfänger (Einzelpersonen und Gruppen) an.
Empfängertyp	Zeigt "Empfänger" für einen Einzelpersonempfänger oder "Gruppe" für einen Gruppenempfänger an.
Auftragsprotokoll in E-Mail-Benachrichtigungen einschließen	<p>Ermöglicht, dass Backup Exec die Benachrichtigung zusammen mit einer Kopie des Auftragsprotokolls sendet. Diese Option gilt nur für E-Mail-Empfänger. Die maximale Anhanggröße (in KB) kann im Folgenden Registrierungsschlüssel konfiguriert werden:</p> <p>HKLM\Software\Symantec\Backup Exec for Windows\Backup Exec\Server\Max Notification Attachment Size</p> <p>Die Anhanggröße kann auch durch die Einstellungen auf Ihrem E-Mail-Server festgelegt werden.</p>
Empfänger verwalten	Hier können Sie Empfänger hinzufügen, bearbeiten oder löschen.
Eigenschaften	Ermöglicht die Anzeige oder das Ändern der Eigenschaften eines ausgewählten Empfängers.

Deaktivieren von Benachrichtigungen für eine bestimmte Meldungskategorie

Wenn ein Empfänger keine Benachrichtigungen mehr für eine Warnmeldungskategorie erhalten soll, können Sie die Benachrichtigung beenden.

So deaktivieren Sie Benachrichtigungen für eine bestimmte Meldungskategorie

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- 2 Wählen Sie "Warnmeldungen und Benachrichtigungen" und dann "Warnmeldungskategorien".

- 3 Wählen Sie unter "Warnmeldungskategorie" die Kategorie, für die der Empfänger keine Benachrichtigungen mehr erhalten soll.
- 4 Deaktivieren Sie unter "Benachrichtigung an folgende Empfänger senden" das Kontrollkästchen neben der Empfänger, für den Sie die Benachrichtigungen beenden möchten.
- 5 Klicken Sie auf "OK".

Siehe ["Deaktivieren von Warnmeldungen per E-Mail oder SMS für einen Empfänger"](#) auf Seite 352.

Konfigurieren von Standardeinstellungen für Warnmeldungen

Mit den Standardeinstellungen für Warnmeldungen können Sie die Popup-Warnmeldungen für die vier Typen von Warnmeldungen aktivieren oder deaktivieren und auch festlegen, wie lange die Popup-Warnmeldungen auf dem Bildschirm verbleiben. Wenn Sie die Popup-Warnmeldungen für einen bestimmten Warnmeldungstyp deaktivieren, wird dieser Warnmeldungstyp noch in der Liste der aktiven Warnmeldungen in anderen Teilen der Backup Exec-Administratorkonsole angezeigt, es sei denn, Sie haben den gleichen Warnmeldungstyp aus der Liste der aktiven Warnmeldungen gefiltert.

So konfigurieren Sie Standardeinstellungen für Warnmeldungen

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- 2 Wählen Sie "Backup Exec-Einstellungen" und dann "Warnmeldungen".
- 3 Wenn Sie eine Erinnerungsmeldung zum Verlängern Ihrer Wartungsverträge erhalten möchten, aktivieren Sie die Option "Erinnerung zum Verlängern der Lizenzverträge an diesem Datum senden" und geben Sie dann ein Datum ein.

- 4 Im Gruppenfeld "Popups für folgende Warnmeldungstypen anzeigen" aktivieren Sie die Kontrollkästchen für die Warnmeldungstypen, die als Popups angezeigt werden sollen. Deaktivieren Sie die Kontrollkästchen für die Warnmeldungstypen, die nicht angezeigt werden sollen.

Informationsmeldung	Enthält Statusmeldungen über Bedingungen, über die Sie vielleicht Bescheid wissen möchten. Sie erfordern keine Reaktion und sind nicht kritisch. Die Infowarnmeldungs-Popups haben eine blaue Farbe.
Fehler	Zeigt die Probleme an, die die Verarbeitung von Aufträgen oder die Integrität des Backups beeinträchtigen. Sie müssen auf sie manuell reagieren. Die Fehlerwarnmeldungs-Popups haben eine rote Farbe.
Warnung	Zeigt Bedingungen an, unter denen Aufträge fehlschlagen können, was aber nicht notwendigerweise der Fall ist. Sie sollten diese Bedingungen überwachen und Maßnahmen für deren Lösung ergreifen. Diese Warnmeldungs-Popups haben eine gelbe Farbe.
Bedienereingriff erforderlich	Dieser Warnmeldungstyp zeigt die Probleme an, auf die der Benutzer reagieren muss, bevor der Auftrag oder Vorgang fortgesetzt werden kann. Sie können auf diesen Typ von Warnmeldung direkt im Popup reagieren. Die Aufmerksamkeits-Warnmeldungs-Popups haben eine purpurrote Farbe.

- 5 Geben Sie im Feld "Zeit in Sekunden zum Anzeigen von Popups" die Zeit an, für die Popups auf dem Bildschirm angezeigt werden sollen.
- 6 Klicken Sie auf "OK".

Aktivieren oder Deaktivieren von Popup-Warnmeldungen

Standardmäßig zeigt Backup Exec Informations- und Fehlermeldungen, Warnungen oder die Meldung "Eingreifen erforderlich" in einem Popup an, wenn ein Fehler auftritt. Sie können die Standardeinstellungen ändern, damit nur die gewünschten Warnmeldungstypen angezeigt werden.

So aktivieren oder deaktivieren Sie Popup-Warnmeldungen

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- 2 Wählen Sie "Backup Exec-Einstellungen" und "Warnmeldungen".
- 3 Im Gruppenfeld "Popups für folgende Warnmeldungstypen anzeigen" aktivieren Sie die Kontrollkästchen für die Warnmeldungstypen, die als Popups angezeigt werden sollen. Deaktivieren Sie die Kontrollkästchen für die Warnmeldungstypen, die nicht angezeigt werden sollen.
- 4 Klicken Sie auf "OK".

SNMP-Traps für Backup Exec-Warnmeldungen

SNMP (Simple Network Management Protocol) ist eine Methode zum Überwachen eines Netzwerks von einem zentralen Standort aus. SNMP-kompatible Netzwerkanwendungen (z. B. Backup Exec) senden Berichte an eine SNMP-Konsole (Verwaltungsarbeitsstation). Auf der Konsole gehen Nachrichten (Traps) von Backup Exec mit Statusmeldungen und Fehlerbedingungen ein. Ein MIB steht auf dem Backup Exec-Installationsdatenträger im Verzeichnis "WINNT\SNMP\Sprache" zum Herunterladen auf die SNMP-Konsole zur Verfügung.

Das Präfix für die Objekt-ID für Veritas lautet:

1.3.6.1.4.1.1302

Backup Exec-SNMP-Traps (Nachrichten) verfügen über eindeutige Objekt-IDs und können bis zu vier Zeichenfolgen enthalten.

Folgende SNMP-Trap-Typen werden unterstützt:

Tabelle 7-7 SNMP-Traps

Trap-Typ	Objekt-ID	Zeichenfolge 1	Zeichenfolge 2	Zeichenfolge 3	Zeichenfolge 4
Produktstart	1302.3.1.1.9.1	Backup Exec: Anwendung wird initialisiert	Computername	Produkt, Version, Edition	

Trap-Typ	Objekt-ID	Zeichenfolge 1	Zeichenfolge 2	Zeichenfolge 3	Zeichenfolge 4
Produkthalt	1302.3.1.1.9.2	Backup Exec: Anwendung wird beendet	Computername	Produkt, Version, Edition	
Auftrag abgebrochen	1302.3.1.2.8.2	Backup Exec: Auftrag von Operator abgebrochen	Computername	Auftragsname	Name von lokalem oder remotem Operator
Auftrag fehlgeschlagen	1302.3.1.2.8.1	Backup Exec: Auftrag fehlgeschlagen	Computername	Auftragsname	Detaillierte Meldung
Speichergerät erfordert Benutzereingriff	1302.3.2.5.3.3	Backup Exec: Speichergerät erfordert Benutzereingriff	Computername	Auftragsname	Detaillierte Meldung
Wechsler erfordert Benutzereingriff	1302.3.2.4.3.3	Backup Exec: Wechslergerät erfordert Benutzereingriff	Computername	Auftragsname	Detaillierte Meldung
Simplified Disaster Recovery-Meldung	1302.3.1.4.2.1.2	Vollständiges Backup mit SDR erfolgreich	Computername	Auftragsname	Detaillierte Meldung
Backup Exec-Systemfehler	1302.3.1.1.9.3	Bei der Anwendung ist ein Fehler aufgetreten.	Computername	Auftragsname	Detaillierte Meldung
Allgemeine Informationen zu Backup Exec	1302.3.1.1.9.4	Informationen zu normalen Ereignissen	Computername	Auftragsname	Detaillierte Meldung
Auftrag erfolgreich	1302.3.1.2.8.3	Der Auftrag wurde erfolgreich durchgeführt.	Computername	Auftragsname	Detaillierte Meldung
Auftrag mit Ausnahmen abgeschlossen	1302.3.1.2.8.4	Der Auftrag wurde erfolgreich ausgeführt, jedoch ist ein Problem aufgetreten.	Computername	Auftragsname	Detaillierte Meldung

Trap-Typ	Objekt-ID	Zeichenfolge 1	Zeichenfolge 2	Zeichenfolge 3	Zeichenfolge 4
Auftrag gestartet	1302.3.1.2.8.5	Der Auftrag wurde gestartet.	Computername	Auftragsname	Detaillierte Meldung
Auftrag ausgeführt, keine Daten vorhanden	1302.3.1.2.8.6	Der Auftrag wurde ausgeführt, es waren jedoch keine Daten vorhanden.	Computername	Auftragsname	Detaillierte Meldung
Auftragswarnung	1302.3.1.2.8.7	Für den Auftrag besteht eine Warnung.	Computername	Auftragsname	Detaillierte Meldung
PVL-Gerätefehler	1302.3.1.5.1.1.1	Beim Gerät ist ein Fehler aufgetreten.	Computername	Auftragsname	Detaillierte Meldung
PVL-Gerätewarnung	1302.3.1.5.1.1.2	Beim Gerät ist eine Warnung aufgetreten.	Computername	Auftragsname	Detaillierte Meldung
PVL-Geräteinformationen	1302.3.1.5.1.1.3	Normale Geräteinformationen	Computername	Auftragsname	Detaillierte Meldung
PVL-Geräteeingriff	1302.3.1.5.1.1.4	Gerät erfordert Benutzereingriff	Computername	Auftragsname	Detaillierte Meldung
PVL-Medienfehler	1302.3.1.5.2.1.1	Beim Medium ist ein Fehler aufgetreten.	Computername	Auftragsname	Detaillierte Meldung
PVL-Medienwarnung	1302.3.1.5.2.1.2	Möglicherweise besteht ein Problem mit dem Medium.	Computername	Auftragsname	Detaillierte Meldung
PVL-Medieninformationen	1302.3.1.5.2.1.3	Normale Medieninformationen	Computername	Auftragsname	Detaillierte Meldung
PVL-Medienintervention	1302.3.1.5.2.1.4	Medium erfordert Benutzereingriff	Computername	Auftragsname	Detaillierte Meldung
Katalogfehler	1302.3.1.5.3.1.1	Beim Katalog ist ein Fehler aufgetreten.	Computername	Auftragsname	Detaillierte Meldung

Trap-Typ	Objekt-ID	Zeichenfolge 1	Zeichenfolge 2	Zeichenfolge 3	Zeichenfolge 4
Tape Alert-Fehler	1302.3.1.5.4.1.1	Es ist ein Tape Alert-Fehler aufgetreten.	Computername	Auftragsname	Detaillierte Meldung
Tape Alert-Warnung	1302.3.1.5.4.1.2	Es ist eine Tape Alert-Warnung aufgetreten.	Computername	Auftragsname	Detaillierte Meldung
Tape Alert-Informationen	1302.3.1.5.4.1.3	Normale Tape Alert-Informationen	Computername	Auftragsname	Detaillierte Meldung
Datenbankwarnungsfehler	1302.3.1.5.5.1.1	Es ist ein Datenbankwarnungsfehler aufgetreten.	Computername	Auftragsname	Detaillierte Meldung
Datenbankwarnungsinformationen	1302.3.1.5.5.1.2	Normale Datenbankwarnungsinformationen	Computername	Auftragsname	Detaillierte Meldung
Installationswarnung	1302.3.1.5.7.1.1	Es ist eine Installationswarnung aufgetreten.	Computername	Auftragsname	Detaillierte Meldung
Installationsinformationen	1302.3.1.5.7.1.2	Normale Installationsinformationen	Computername	Auftragsname	Detaillierte Meldung

Siehe ["Installieren und Konfigurieren des SNMP-Systemdienstes"](#) auf Seite 364.

Installieren und Konfigurieren des SNMP-Systemdienstes

Damit Backup Exec-Traps auf der SNMP-Konsole empfangen werden können, müssen Sie den SNMP-Systemdienst mit der IP-Adresse der SNMP-Konsole konfigurieren.

SNMP wird automatisch nach der Installation gestartet. Sie müssen als Administrator oder Mitglied der Administratorengruppe eingeloggt sein, um diesen Vorgang ausführen zu können. Wenn Ihr Computer mit einem Netzwerk verbunden ist, können Sie darüber hinaus auch durch Netzwerkrichtlinien daran gehindert werden, diesen Vorgang auszuführen.

So installieren Sie den SNMP-Systemdienst und konfigurieren ihn zum Senden von Traps an die SNMP-Konsole

- 1 Wählen Sie in der Windows-Systemsteuerung "Software".
- 2 Klicken Sie auf "Windows-Komponenten hinzufügen/entfernen".

- 3 Wählen Sie unter "Windows-Komponenten hinzufügen/entfernen" den Eintrag "Verwaltungs- und Überwachungsprogramme", und klicken Sie auf "Details".
Achten Sie beim Auswählen der Komponente darauf, dass Sie nicht das Kontrollkästchen markieren bzw. die Markierung entfernen.
- 4 Wählen Sie "Simple Network Management Protocol" aus, und klicken Sie auf "OK".
- 5 Klicken Sie auf "Weiter".

Installieren der Leistungszähler-Provider der Windows-Verwaltungsinstrumentation

Die Windows-Verwaltungsinstrumentation (WMI) ist eine Infrastruktur, mit der Sie Systemressourcen beobachten und steuern können. Backup Exec enthält Leistungszähler- und SNMP-Provider, die manuell installiert und mit WMI verwendet werden können.

So installieren Sie den WMI-Leistungszähler-Anbieter

- 1 Legen Sie das Backup Exec-Installationsmedium ein.
- 2 Geben Sie an der Eingabeaufforderung Folgendes ein:

```
mofcomp <CD Drive Letter>:\winnt\wmi\backupexecperfmon.mof
```

Installieren des Windows-Verwaltungsinstrumentation-Providers für SNMP

Die Windows-Verwaltungsinstrumentation (WMI) ist eine Infrastruktur, mit der Sie Systemressourcen beobachten und steuern können. Backup Exec enthält Leistungszähler- und SNMP-Provider, die manuell installiert und mit WMI verwendet werden können.

Zur Benutzung des WMI-SNMP-Providers müssen Sie die SNMP-Benachrichtigung einrichten.

So installieren Sie den WMI-SNMP-Provider

- 1 Bevor Sie den mit Backup Exec mitgelieferten SNMP-Provider installieren können, muss der Microsoft SNMP-Provider auf dem System installiert sein.
Weitere Informationen dazu finden Sie in der Microsoft-Dokumentation.
- 2 Legen Sie das Backup Exec-Installationsmedium ein.
- 3 Geben Sie an der Eingabeaufforderung Folgendes ein:

```
mofcomp <CD Drive Letter>:\winnt\wmi\snmp\eng\bkuexecmib.mof
```

Deinstallieren des WMI-Leistungszähler-Providers

Sie müssen die Leistungszähler-Provider der Windows-Verwaltungsinstrumentation (WMI) und den WMI-SNMP-Provider separat deinstallieren.

So deinstallieren Sie den WMI-Leistungsindikatoren-Anbieter

- ◆ Geben Sie an der Kommandozeile Folgendes ein:

```
mofcomp <CD Drive  
Letter>:\winnt\wmi\deletebackupexecperfmon.mof
```

Deinstallieren des Windows-Verwaltungsinstrumentation-Providers für SNMP

Sie müssen die Leistungszähler-Provider der Windows-Verwaltungsinstrumentation (WMI) und den WMI-SNMP-Provider separat deinstallieren.

So deinstallieren Sie den WMI-SNMP-Provider

- ◆ Geben Sie an der Kommandozeile Folgendes ein:

```
Smi2smir /d Backup_Exec_MIB
```

Plattenbasierter und netzwerkbasierter Speicher

In diesem Kapitel werden folgende Themen behandelt:

- Funktionen und Typen des plattenbasierten und netzwerkbasierten Speichers
- Speichertrendanalysestatus für Plattenspeicher und virtuelle Datenträger
- Festlegen von Schwellenwerten für geringen Speicherplatz auf plattenbasierten Speichern
- Konfigurieren von Festplattenspeicher
- Wiederherstellen von Daten von einem erneut verbundenen oder eingelegten, plattenbasierten Speichergerät
- Konfigurieren des Plattenkassettenspeichers
- Löschen abgelaufener Backup-Sätze auf plattenbasiertem Speicher durch Data Lifecycle Management (DLM)
- Backup-Sätze

Funktionen und Typen des plattenbasierten und netzwerkbasierten Speichers

Der plattenbasierte Speicher hat folgende Funktionen:

- Automatic Discovery von lokal zugänglichen Datenträgern.

- Speicherplatzüberwachung. Ausgabe von Warnmeldungen, wenn die von Ihnen festgelegten Schwellenwerte für Festplattenspeicher erreicht sind.
- Speichertrendanalyse, die Vorhersagen niedrigen Speicherplatzes für Datenträgerspeicher und virtuelle Datenträger liefert.
- Data Lifecycle Management löscht automatisch abgelaufene Backup-Sätze und gibt den Speicherplatz für neue Backup-Sätze frei.

Zum plattenbasierten Speicher gehören die folgenden Speichertypen:

Tabelle 8-1 Plattenbasierter Speicher - Typen

Plattenbasierter Speicher - Typen	Beschreibung
Datenträgerspeicher	<p>Beim Festplattenspeicher handelt es sich um einen Speicherort auf einer lokal verbundenen internen Festplatte, einem USB-Gerät, einem FireWire-Gerät oder einem über ein Netzwerk angehängten Speichergerät, auf dem Sie Daten sichern können.</p> <p>Siehe "Konfigurieren von Festplattenspeicher" auf Seite 372.</p>
Plattenkassettengeräte	<p>Plattenkassetten sind ein Typ Speicher, der normalerweise mit dem Backup Exec-Server verbunden bleibt, während Sie die Datenträger (z. B. RDX) entfernen. Wenn Sie nicht sicher sind, ob Wechseldatenträger im Speicher vorhanden sind, öffnen Sie den Ordner "Computer" auf dem Windows-Computer. Die Geräte, die Wechselmedien enthalten, sind aufgelistet.</p> <p>Siehe "Konfigurieren des Plattenkassettenspeichers" auf Seite 384.</p>
Deduplizierungsspeicher	<p>Der Deduplizierungsspeicher ist ein plattenbasierter Backup-Ordner, der sich auf dem Backup Exec-Server befindet und integrierte Deduplizierung ermöglicht. Sie müssen das Backup Exec Deduplication Feature installieren, um diese Datenreduzierungsstrategie zu verwenden, die Speicher und Netzwerkbandbreite optimiert.</p> <p>Siehe "Info zu Deduplication Feature" auf Seite 1047.</p>

Zum netzwerkbasierten Speicher gehören NDMP-Server, OpenStorage-Geräte, Cloud-Speichergeräte und der Remote Media Agent for Linux.

Tabelle 8-2 Typen des Netzwerkspeichers

Typ des Speichers	Beschreibung
NDMP-Server	NDMP-Server sind NAS-Geräte, die das Network Data Management Protocol (NDMP) unterstützen, um den Einsatz von Geräten zu ermöglichen, die an den Servern angeschlossen sind. Siehe "Funktionen von NDMP Feature" auf Seite 1539.
OpenStorage-Geräte	OpenStorage-Geräte sind mit dem Netzwerk verknüpfte Speicher, die die OpenStorage-Technologie von Veritas unterstützen. Siehe "Konfigurieren eines OpenStorage-Geräts" auf Seite 1058.
Cloud-Speichergeräte	Cloud-Speichergeräte sind die in der Cloud konfigurierten und durch den Service-Provider des Cloud-Speichers gehosteten Speichergeräte.
Remote Media Agent for Linux	Mit Remote Media Agent for Linux können Sie Daten aus Remote-Computern auf Speichergeräte sichern, die direkt an einem Linux-Server angeschlossen sind. Sie können Daten auch auf einer simulierten Bandbibliothek auf einem Linux-Server sichern. Siehe "Info zu Remote Media Agent for Linux" auf Seite 1598.

Informationen zu den Best Practices zum Verwalten von plattenbasierten Speichern in Backup Exec finden Sie unter *Best Practices für Backup Exec*.

Siehe ["Speichertrendanalysestatus für Plattenspeicher und virtuelle Datenträger"](#) auf Seite 369.

Siehe ["Löschen abgelaufener Backup-Sätze auf plattenbasiertem Speicher durch Data Lifecycle Management \(DLM\)"](#) auf Seite 393.

Siehe ["Anzeigen von Aufträgen, Auftragsverläufen, Backup-Sätzen und aktiven Warnmeldungen für Speichergeräte"](#) auf Seite 548.

Siehe ["Backup-Sätze"](#) auf Seite 401.

Speichertrendanalysestatus für Plattenspeicher und virtuelle Datenträger

Backup Exec sammelt Informationen zur Auslastung von Plattenspeichern und virtuellen Datenträgern. Backup Exec führt dann eine statistische Analyse des

verwendeten und des freien Speicherplatzes durch. Die Analyse liefert eine Schätzung, wie viele Tage verbleiben, bevor der Plattenspeicher oder der virtuelle Datenträger voll ist.

Warnmeldungen zeigen an, ob die aktuellen Speicherressourcen ausreichend sind, und helfen Ihnen bei der Planung für die Erweiterung des Speicherplatzes.

Tabelle 8-3 Statuswerte bei der Speichertrendanalyse

Statuswerte bei der Speichertrendanalyse	Beschreibung
Verbleibender Speicher: x Tage	Eine Schätzung der mit dem vorhandenen Speicherplatz verbleibenden Tage, basierend auf der aktuellen Speichernutzung.
Verlaufsdaten zu genutztem Speicher werden noch gesammelt	<p>Dieser Status kann aus den folgenden Gründen angezeigt werden:</p> <ul style="list-style-type: none"> ■ Das Speichergerät wurde noch nicht lange genug konfiguriert, um eine statistische Schätzung zu ermöglichen. <p>Hinweis: Nachdem Sie Plattenspeicher erstellt haben, benötigt Backup Exec möglicherweise ca. einen Monat, um genügend Informationen für eine Speicherschätzung zu sammeln.</p> <ul style="list-style-type: none"> ■ Dieser Speicher befindet sich möglicherweise auf einem verwalteten Backup Exec-Server, auf dem gerade ein paralleles Upgrade durchgeführt wird.
Der aktuelle Speicher reicht aus	Die Umgebung enthält genügend Speicherplatz, um Speicherbedarf während der nächsten 30 Tage zu erfüllen.
Keine Einschätzung aufgrund eines unvollständigen Verlaufs des genutzten Speicherplatzes	Es ist nicht möglich, einen Speichertrend abzurufen. Ungewöhnliche Zu- oder Abnahmen in der Menge des freien Speicherplatzes während der letzten 30 Tage können diesen Status verursachen.

Statuswerte bei der Speichertrendanalyse	Beschreibung
Zu wenig statistische Informationen verfügbar	<p>Backup Exec hat nicht ausreichend Beispieldaten für eine statistische Analyse gesammelt.</p> <p>Hinweis: Nachdem Sie Plattenspeicher erstellt haben, benötigt Backup Exec möglicherweise ca. einen Monat, um genügend Informationen für eine Speicherschätzung zu sammeln.</p>

Siehe ["Konfigurieren von Festplattenspeicher"](#) auf Seite 372.

Festlegen von Schwellenwerten für geringen Speicherplatz auf plattenbasierten Speichern

Sie können die Standardwerte für drei Warnstufen aufgrund von geringem Speicherplatz ändern. Wenn die genutzte Kapazität des Speichergeräts diesen Schwellenwert erreicht, sendet Backup Exec eine Warnmeldung und die Data Lifecycle Management-Funktion durchsucht das Gerät nach abgelaufenen Backup-Sätzen, die gelöscht werden können.

Data Lifecycle Management wird auch auf einer Plattenkassette ausgeführt, wenn diese die entsprechende Kapazität erreicht. Das Backup muss möglicherweise nicht auf eine weitere Plattenkassette ausgedehnt werden, wenn Data Lifecycle Management genügend abgelaufene Backup-Sätze löscht. Wenn ein Auftrag auf eine andere Plattenkassette ausgedehnt werden muss und Sie eine neue Plattenkassette einlegen, die bereits voll ist, löscht Data Lifecycle Management abgelaufene Backup-Sätze auf der neuen Plattenkassette.

So legen Sie Schwellenwerte für geringen Speicherplatz auf plattenbasierten Speichern fest

- 1 Doppelklicken Sie auf der Registerkarte "Speicher" auf den Speicher, für den Sie die Schwellenwerte für geringen Speicherplatz ändern möchten.
- 2 Klicken Sie im linken Teilfenster auf "Eigenschaften".
- 3 Ändern Sie den Wert für eine oder alle folgenden Eigenschaften:
 - Geringer Speicherplatz
Der erste Schwellenwert für geringen Speicherplatz, bei dem Backup Exec eine Warnmeldung senden soll. Der Standardwert ist 25 %.
 - Geringer Speicherplatz – Warnung

Der zweite Schwellenwert für geringen Speicherplatz, bei dem Backup Exec eine Warnmeldung senden soll. Der Standardwert ist 15 %. Dieser Schwellenwert muss kleiner als der Schwellenwert für geringen Speicherplatz sein.

- Geringer Speicherplatz – Kritisch
Der dritte Schwellenwert für geringen Speicherplatz, bei dem Backup Exec eine Warnmeldung senden soll. Der Standardwert ist 5 %. Dieser Schwellenwert muss kleiner als der Schwellenwert für Warnungen sein.

4 Klicken Sie auf "Übernehmen".

Siehe ["Löschen abgelaufener Backup-Sätze auf plattenbasiertem Speicher durch Data Lifecycle Management \(DLM\)"](#) auf Seite 393.

Konfigurieren von Festplattenspeicher

Beim Festplattenspeicher handelt es sich um einen Speicherort auf einer lokal verbundenen internen Festplatte, einem USB-Gerät, einem FireWire-Gerät oder einem über ein Netzwerk angehängten Speichergerät, auf dem Sie Daten sichern können. Wenn Sie den Backup-Auftrag erstellen, geben Sie an, wie lange die im Festplattenspeicher gesicherten Daten erhalten bleiben sollen. Die Data Lifecycle Management-Funktion von Backup Exec löscht automatisch alle abgelaufenen Backup-Sätze und fordert den Speicherplatz zurück. Wenn Sie die Backup-Daten länger als für den bei Erstellung des Backup-Auftrags angegebenen Zeitraum aufbewahren möchten, erstellen Sie einen Duplizierungs-Backup-Auftrag. Ein Duplizierungs-Backup-Auftrag kopiert die Backup-Daten vom ursprünglichen Speichergerät auf ein Band- oder Festplattenkassettendatenträger, den Sie dann zur langfristigen oder externen Aufbewahrung senden können. Sie können auch verhindern, dass Backup-Sätze automatisch ablaufen, indem Sie sie aufbewahren. Backup Exec behält dann auch alle abhängigen Backup-Sätze bei.

Damit ein Datenträger als Datenträgerspeicher konfiguriert werden kann, muss darauf mindestens 1 GB Speicherplatz zur Verfügung stehen und er darf nicht als Deduplizierungsspeicher konfiguriert sein. Es ist zwar möglich, Datenträgerspeicher und Deduplizierungsspeicher auf demselben Datenträger zu konfigurieren, dies wird jedoch nicht empfohlen.

Wenn Sie Speicher auf einem Datenträger erstellen, der mit dem Netzwerk verbunden ist, müssen Sie den Pfad zu einer bestehenden Freigabe angeben. Sie sollten den Servernamen im UNC-Pfad statt einer IP-Adresse verwenden.

Hinweis: Bevor Sie den Datenträgerspeicher auf einer Netzwerkfreigabe erstellen, müssen Sie dem Backup Exec-Dienstkonto Lese- und Schreibberechtigungen zuweisen. Das Backup Exec-Dienstkonto befindet sich auf dem Backup Exec-Server, der auf die Netzwerkfreigabe zugreifen soll.

Informationen zu den Best Practices zum Einsatz von Hot-Plug-Geräten in Backup Exec finden Sie unter *Best Practices für Backup Exec*.

Wenn Sie Festplattenspeicher auf einem lokalen Datenträger erstellen, können Sie in Backup Exec die folgenden Speicherorte angeben:

- Datenträger mit oder ohne Laufwerksbuchstaben.
Sie können auf jedem Datenträger nur einen Plattenspeicher erstellen.
- Unformatierte Partitionen.
Backup Exec formatiert und partitioniert gegebenenfalls das Laufwerk.
- Laufwerk, ohne Partitionen.

Backup Exec erstellt einen Ordner mit dem Namen "BEControl" auf dem Root des Datenträgers. Löschen oder bearbeiten Sie nicht die Inhalte des BEControl-Ordners und kopieren Sie ihn nicht auf andere Datenträger oder Laufwerksbuchstaben.

Im Windows-Explorer werden die Backup-Dateien, die sich auf dem Datenträgerspeichergerät befinden, mit einer .bkf-Dateierweiterung angezeigt. Jedes Datenträgerspeichergerät enthält außerdem die Dateien "changer.cfg" und "folder.cfg", in denen Informationen über die Backup-Dateien gespeichert werden. Die Dateien "changer.cfg" und "folder.cfg" dürfen nicht gelöscht oder geändert werden.

Auf einem Datenträgerspeichergerät wird möglicherweise ein Unterordner angezeigt, dessen Name mit "IMG" beginnt. Dieser Unterordner wird angezeigt, wenn für das Backup Granular Recovery Technology (GRT) aktiviert wurde oder Sie das Datenträgerspeichergerät als Speicher für Backup-Daten ausgewählt haben.

Zum Erstellen von Festplattenspeicher müssen Sie den Assistenten "Speicher konfigurieren" verwenden. Backup Exec stellt im Assistenten "Speicher konfigurieren" eine Liste der Datenträger zur Verfügung, auf denen Sie Festplattenspeicher erstellen können. Die Datenträger werden in der Liste nicht in der alphabetischen Reihenfolge der Laufwerksbuchstaben angezeigt. Stattdessen steht derjenige Datenträger an erster Stelle in der Liste, auf dem der meiste Speicherplatz verfügbar ist. Sie können jeden gewünschten Datenträger wählen; der von Backup Exec empfohlene Datenträger wird jedoch an erster Stelle aufgeführt. Der Datenträger, den Sie als Systemlaufwerk verwenden, steht immer an letzter Stelle. Es wird empfohlen, Plattenspeicher nicht auf dem Systemlaufwerk zu konfigurieren.

Hinweis: Ist die Windows-Deduplizierung auf dem Plattenspeichergerät aktiviert, schließt Backup Exec die Backup-Daten im Ordner "\BEData" aus der Deduplizierung aus, es sei denn, der Ordner "\BEData" ist bereits vorhanden. Backup Exec muss Backup-Daten aus der Deduplizierung ausschließen, damit Sie Simplified Disaster Recovery (SDR) zum Ausführen einer lokalen Wiederherstellung des Backup Exec-Servers verwenden können.

Ist die Windows-Datendeduplizierung auf Datenträger aktiviert, schlägt die lokale Notfallwiederherstellung mit SDR fehl. Die von SDR genutzte Windows Preinstallation Environment (Windows PE) kann die Dateien, die die Windows-Datendeduplizierung verarbeitet, nicht lesen.

So konfigurieren Sie Festplattenspeicher

- 1 Klicken Sie auf der Registerkarte "Speicher" in der Gruppe "Konfigurieren" auf "Speicher konfigurieren".
- 2 Sie haben folgende Möglichkeiten:

Wenn Central Admin Server Feature nicht installiert ist	Klicken Sie auf "Plattenbasierter Speicher" und dann auf "Weiter".
---	--

Wenn Central Admin Server Feature installiert ist	Gehen Sie dazu in folgender Reihenfolge vor:
---	--

- Wählen Sie den Backup Exec-Server aus, auf dem Sie Speicher konfigurieren wollen, und klicken Sie dann auf "Weiter".
- Klicken Sie auf "Plattenbasierter Speicher" und dann auf "Weiter".

- 3 Klicken Sie auf "Plattenspeicher" und dann auf "Weiter".
- 4 Geben Sie einen Namen und eine Beschreibung für das Plattenspeichergerät ein und klicken Sie dann auf "Weiter".
- 5 Geben Sie an, ob das Plattenspeichergerät auf einem lokalen Datenträger oder einer Netzwerkfreigabe erstellt werden soll, geben Sie den Speicherort oder Pfad an und klicken Sie auf "Weiter".
- 6 Geben Sie an, wie viele Schreibvorgänge auf diesem Plattenspeichergerät gleichzeitig ausgeführt werden sollen, und klicken Sie auf "Weiter".
- 7 Lesen Sie die Übersicht und führen einen der folgenden Schritte aus:

So ändern Sie die Konfiguration

Gehen Sie dazu in folgender Reihenfolge vor:

- Klicken Sie auf die Überschrift, die die Elemente enthält, die Sie ändern möchten.
- Nehmen Sie alle Änderungen, vor und klicken Sie dann auf "Weiter", bis die Übersicht angezeigt wird.
- Klicken Sie auf "Fertigstellen".

So konfigurieren Sie das
Plattenspeichergerät

Klicken Sie auf "Fertigstellen".

Siehe ["Ändern des Speicherorts für ein Datenträgerspeichergerät"](#) auf Seite 375.

Siehe ["Löschen abgelaufener Backup-Sätze auf plattenbasiertem Speicher durch Data Lifecycle Management \(DLM\)"](#) auf Seite 393.

Ändern des Speicherorts für ein Datenträgerspeichergerät

Sie können den Speicherort eines vorhandenen Datenträgerspeichergeräts ändern. Sie benötigen einen weiteren Datenträger, auf den Sie die Dateien im Ordner "BEDData" verschieben können.

Hinweis: Wenn Sie Dateien vom ursprünglichen Datenträgerspeichergerät an den neuen Speicherort kopieren, dürfen Sie .cfg-Dateien nicht kopieren.

So ändern Sie den Speicherort eines Datenträgerspeichergeräts

- 1 Klicken Sie auf der Registerkarte "Speicher" in der Gruppe "Konfigurieren" auf "Speicher konfigurieren".
- 2 Klicken Sie auf "Plattenbasierter Speicher" und dann auf "Weiter".
- 3 Geben Sie einen anderen Namen und eine andere Beschreibung als für das ursprüngliche Plattenspeichergerät ein und klicken Sie dann auf "Weiter".
- 4 Geben Sie einen anderen Laufwerksbuchstaben ein und klicken Sie dann auf "Weiter".
- 5 Geben Sie die Anzahl von gleichzeitigen Schreibvorgängen auf diesem Speichergerät ein und klicken Sie auf "Weiter".
- 6 Lesen Sie die Übersicht und führen einen der folgenden Schritte aus:

So ändern Sie die Konfiguration

Gehen Sie dazu nach folgender Reihenfolge vor:

- Klicken Sie auf die Überschrift, die die zu ändernden Elemente enthält.
- Nehmen Sie die Änderungen vor und klicken Sie dann auf "Weiter", bis die Übersicht angezeigt wird.
- Klicken Sie auf "Fertigstellen".

So konfigurieren Sie das Plattenspeichergerät

Klicken Sie auf "Fertigstellen".

- 7 Kopieren Sie im Windows-Explorer die folgenden Dateien aus dem Ordner "BEDData" auf dem ursprünglichen Datenträger und fügen Sie sie in den Ordner "BEDData" auf dem neuen Datenträger ein:
 - . Bkf-Dateien
 - Alle Unterordner mit dem Präfix "IMG" im Namen
- 8 Löschen Sie im Windows-Explorer alle Dateien aus dem ursprünglichen Datenträgerspeichergerät.
- 9 Klicken Sie in der Backup Exec-Administratorkonsole auf der Registerkarte "Speicher" mit der rechten Maustaste auf das neue Plattenspeichergerät, und klicken Sie dann auf "Löschen".
- 10 Benennen Sie das neue Datenträgerspeichergerät um und geben Sie ihm den Namen des ursprünglichen Datenträgerspeichergeräts.
- 11 Klicken Sie mit der rechten Maustaste auf das neue Plattenspeichergerät, und klicken Sie dann auf "Inventar und Katalog".

Siehe ["Inventarisieren und Katalogisieren von Speichergeräten"](#) auf Seite 552.

Siehe ["Konfigurieren von Festplattenspeicher"](#) auf Seite 372.

Bearbeiten der Eigenschaften von Festplattenspeichern

Sie können Speicherplatzverwaltungseinstellungen für das Speichergerät bearbeiten.

So bearbeiten Sie Speichereigenschaften

- 1 Doppelklicken Sie auf der Registerkarte "Speicher" auf den Speicher, dessen Eigenschaften Sie anzeigen möchten.
- 2 Klicken Sie im linken Teilfenster auf "Eigenschaften".
- 3 Bearbeiten Sie eine der folgenden Optionen:

Name	Zeigt den Namen des Speichers an. Sie können dieses Feld bearbeiten.
Beschreibung	Zeigt eine Beschreibung des Datenträgerspeichers an. Sie können dieses Feld bearbeiten.
Backup Exec auf schreibgeschützte Vorgänge begrenzen	<p>Verhindert, dass Backup Exec abgelaufene Backup-Sätze auf diesem Festplattenspeicher löscht, wenn Sie den Festplattenspeicher erneut an den Backup Exec-Server anschließen. Andernfalls löscht die Data Lifecycle Management-Funktion von Backup Exec alle abgelaufenen Backup-Sätze und fordert den Speicherplatz zurück.</p> <p>Der Standardwert ist "Nein".</p> <p>Diese Option ist nur dann anwendbar, wenn der Festplattenspeicher für die in der globalen Einstellung angegebene Anzahl an Tagen vom Backup Exec-Server getrennt wurde. Die standardmäßige Anzahl von Tagen ist 14.</p> <p>Siehe "Löschen abgelaufener Backup-Sätze auf plattenbasiertem Speicher durch Data Lifecycle Management (DLM)" auf Seite 393.</p> <p>Siehe "Backup-Sätze " auf Seite 401.</p> <p>Siehe "Wiederherstellen von Daten von einem erneut verbundenen oder eingelegten, plattenbasierten Speichergerät" auf Seite 383.</p>
Maximale Dateigröße	<p>Zeigt die maximale Dateigröße auf dem Datenträgerspeicher an. Die Daten aus dem Backup-Auftrag sind in einer Datei auf dem Datenträger enthalten.</p> <p>Der Standardwert ist 50 GB oder die Kapazität des Datenträgerspeichers.</p>

Speicherplatz bis zur maximalen Dateigröße inkrementell im Voraus zuordnen

Erstellt die Datei zu Beginn des Backup-Auftrags durch inkrementelle Zuteilung von Speicherplatz gemäß der Größe des von Ihnen in "Inkrement der Vorabzuordnung" festgelegten Werts. Während der Auftrag den Speicherplatz aufbraucht, wird weiterer Speicherplatz vorab zugeteilt, bis die maximale Dateigröße erreicht ist. Wenn der Auftrag abgeschlossen ist, wird die Dateigröße auf den für den Auftrag tatsächlich verwendeten Speicherplatz reduziert.

Wenn Sie die Vorabzuordnung aktivieren und als Inkrement z. B. 4 GB festlegen, werden beim Start des Auftrags 4 GB Speicherplatz im Voraus zugeordnet. Nachdem der Auftrag 4 GB aufgebraucht hat, ordnet Backup Exec weitere 4 GB zu. Weiterer Speicherplatz wird in Schritten von 4 GB zugeteilt, bis der Auftrag abgeschlossen ist. Wenn der Auftrag z. B. nur 13 GB verwendet, obwohl 16 GB zugeordnet wurden, wird die Dateigröße auf 13 GB reduziert.

Die Standardeinstellung ist "Deaktiviert".

Inkrement der Vorabzuordnung

Zeigt den Speicherplatz an, um den die Dateigröße jeweils erhöht wird. Die Dateigröße nimmt entsprechend dem Speicherplatzbedarf für den Auftrag immer wieder um diesen Wert zu, bis die maximale Dateigröße erreicht ist.

Der Standardwert ist 1 GB.

Block- und Puffergröße automatisch erkennen

Gibt an, ob Backup Exec automatisch die bevorzugten Einstellungen für die Block- und Puffergröße für den Plattenspeicher erkennt.

Die Standardeinstellung ist "Aktiviert".

Wenn Sie diese Einstellung deaktivieren, können Sie die zu verwendende Block- und Puffergröße wählen.

Blockgröße

Zeigt die Größe der Datenblöcke an, die auf neue Medien in diesem Speichergerät geschrieben werden, wenn die Option "Block- und Puffergröße automatisch erkennen" deaktiviert wird. Standardeinstellung ist die bevorzugte Blockgröße.

Einige Speichergeräte erreichen eine bessere Leistung, wenn größere Blockgrößen verwendet werden. Die bevorzugte Blockgröße kann zwischen 512 Byte und 64 Kilobyte oder mehr liegen. Wenn Sie ein Speichergerät verwenden, das größere Blockgrößen unterstützt, können Sie die Blockgröße ändern. Wenn jedoch die Option zum Ändern der Blockgröße nicht verfügbar ist, müssen Sie das Gerät so konfigurieren, dass es eine größere Blockgröße verwendet.

Informationen zum Konfigurieren des Geräts finden Sie in der Dokumentation des Herstellers.

Backup Exec stellt nicht sicher, dass die angeforderte Blockgröße vom Speichergerät unterstützt wird. Wenn die angeforderte Blockgröße nicht unterstützt wird, wird die Standardblockgröße des Geräts verwendet.

Wenn das Laufwerk das Konfigurieren der Blockgröße nicht unterstützt, ist diese Option nicht verfügbar.

Puffergröße

Zeigt die Menge der Daten an, die bei jeder Lese- oder Schreibenfrage an das Speichergerät gesendet werden, wenn die Option "Block- und Puffergröße automatisch erkennen" deaktiviert ist. Die Puffergröße muss ein gerades Vielfaches der Blockgröße sein.

Je nach Größe des Arbeitsspeichers in Ihrem System können Sie durch Erhöhen dieses Werts eventuell die Speicherleistung verbessern. Für jeden Gerätetyp ist eine andere, gerätespezifische Puffergröße erforderlich, um optimale Leistungswerte zu erzielen.

Wenn die bevorzugte Blockgröße größer als 64 KB ist, ist die Standardpuffergröße gleich der Standardblockgröße. Wenn die bevorzugte Blockgröße kleiner als 64 KB ist, dann ist die Standardpuffergröße 64 KB.

Geringer Speicherplatz - Kritisch

Gibt den kritischen Schwellenwert für geringen Speicherplatz an, bei dem Backup Exec eine Warnmeldung senden soll. Die Farbe der Kapazitätsleiste auf der Registerkarte "Speicher" ändert sich in rot, um anzuzeigen, dass der freie Speicherplatz ein kritisches Minimum erreicht hat. Backup Exec sendet Warnmeldungen, wenn die Menge des freien Speicherplatzes unter den Schwellenwert für geringen Speicherplatz fällt und erneut, wenn sie unter den Schwellenwert für Warnungen fällt. Die Menge des freien Speicherplatzes umfasst nicht den Speicherplatz, der für nicht mit Backup Exec zusammenhängende Vorgänge reserviert ist.

Sie können den Schwellenwert ändern. Dieser Schwellenwert muss kleiner als der Schwellenwert für Warnungen sein.

Der Standardwert ist 5 %.

Geringer Speicherplatz – Warnung

Gibt den Schwellenwert für geringen Speicherplatz an, bei dem Backup Exec eine Warnmeldung senden soll. Die Farbe der Kapazitätsleiste auf der Registerkarte "Speicher" ändert sich in orange, um anzuzeigen, dass nur noch wenig freier Speicherplatz verfügbar ist. Wenn der freie Speicherplatz unter den Schwellenwert für Warnungen auf den kritischen Schwellenwert abfällt, wird eine weitere Warnmeldung gesendet. Die Menge des freien Speicherplatzes umfasst nicht den Speicherplatz, der für nicht mit Backup Exec zusammenhängende Vorgänge reserviert ist.

Sie können den Schwellenwert ändern. Dieser Schwellenwert muss kleiner als der Schwellenwert für geringen Speicherplatz sein.

Der Standardwert ist 15 %.

Geringer Speicherplatz

Gibt den Schwellenwert für geringen Speicherplatz an, bei dem Backup Exec eine Warnmeldung senden soll. Die Farbe der Kapazitätsleiste auf der Registerkarte "Speicher" ändert sich in gelb, um anzuzeigen, dass die erste von drei Warnstufen aufgrund von geringem Speicherplatz erreicht wurde. Wenn der freie Speicherplatz unter diesen Schwellenwert auf den Wert abfällt, der als Schwellenwert für Warnungen angegeben wurde, wird eine weitere Warnmeldung gesendet. Wenn der freie Speicherplatz unter den Schwellenwert für Warnungen auf den kritischen Schwellenwert abfällt, wird eine weitere Warnmeldung gesendet. Der freie Speicherplatz umfasst nicht den Speicherplatz, der für nicht mit Backup Exec zusammenhängende Vorgänge reserviert ist.

Wenn der geringe Speicherplatz diesen Schwellenwert erreicht, durchsucht Data Lifecycle Management das Gerät nach abgelaufenen Backup-Sätzen, die gelöscht werden können.

Sie können den Schwellenwert ändern.

Der Standardwert ist 25 %.

Siehe "[Löschen abgelaufener Backup-Sätze auf plattenbasiertem Speicher durch Data Lifecycle Management \(DLM\)](#)" auf Seite 393.

Zu reservierender Speicherplatz für Vorgänge, die nicht zu Backup Exec gehören

Zeigt den Speicherplatz an, der für andere Anwendungen als Backup Exec zu reservieren ist.

Der Standardwert ist 10 MB.

Einstellungen automatisch erkennen

Gibt an, ob Backup Exec automatisch die bevorzugten Einstellungen für Lese- und Schreibpuffer für den Datenträgerspeicher erkennt.

Gepufferte Lesevorgänge

Wenn diese Einstellung aktiviert ist, gilt:

- Backup Exec soll die Einstellungen für dieses Speichergerät nicht automatisch erkennen.
- Dieser Festplattenspeicher soll gepufferte Lesevorgänge (das Lesen großer Datenblöcke) zulassen.

Das Aktivieren dieser Option kann zu einer höheren Leistung führen.

Gepufferte Schreibvorgänge

Wenn diese Einstellung aktiviert ist, gilt:

- Backup Exec soll die Einstellungen für dieses Speichergerät nicht automatisch erkennen.
- Dieser Festplattenspeicher soll gepufferte Schreibvorgänge (das Schreiben großer Datenblöcke) zulassen.

Gleichzeitige Schreibvorgänge

Zeigt die Anzahl der gleichzeitigen Schreibvorgänge an, die Sie auf diesem Speichergerät zulassen möchten.

4 Klicken Sie auf "Übernehmen".

Siehe "[Konfigurieren von Festplattenspeicher](#)" auf Seite 372.

Wiederherstellen von Daten von einem erneut verbundenen oder eingelegten, plattenbasierten Speichergerät

Wenn die Backup-Sätze auf einem plattenbasierten Speichergerät oder einer Plattenkassette ablaufen, während dieses Gerät nicht angeschlossen ist, löscht Backup Exec die Kataloge dieser Backup-Sätze. Um zu einem späteren Zeitpunkt eine Wiederherstellung von diesen Backup-Sätzen vornehmen zu können, müssen Sie beim erneuten Verbinden auf dem Gerät einen Inventar- und Katalogvorgang ausführen. Bei der Ausführung des Inventar- und Katalogvorgangs legt Backup Exec für jeden Backup-Satz ein neues Ablaufdatum fest. Dabei werden die ursprünglichen Aufbewahrungseinstellungen des Backup-Satzes verwendet und die Berechnung mit dem Tagesdatum vorgenommen. Backup Exec setzt auch das Ablaufdatum für jeden Backup-Satz auf dem Speichergerät zurück, der innerhalb von sieben Tage ab dem aktuellen Datum abläuft.

Wenn Sie möchten, dass die Backup-Sätze ablaufen, können Sie die Speichergeräteeigenschaft "Backup Exec auf schreibgeschützte Vorgänge begrenzen" deaktivieren. Klicken Sie zum Auffinden dieser Option auf der Registerkarte "Speicher" mit der rechten Maustaste auf das Speichergerät, klicken Sie auf "Details" und dann auf "Eigenschaften". Führen Sie keinen Inventar- und Katalogvorgang aus. Backup Exec fordert im Zuge der Datenlebenszyklusverwaltung den Speicherplatz auf diesem Speichergerät zurück. Sie können die Backup-Sätze auch löschen.

Siehe ["Inventarisieren und Katalogisieren von Speichergeräten"](#) auf Seite 552.

Siehe ["Backup-Sätze"](#) auf Seite 401.

Konfigurieren des Plattenkassettenspeichers

Plattenkassetten sind ein Typ Speicher, der normalerweise mit dem Backup Exec-Server verbunden bleibt, während Sie die Medien, z. B. RDX, entfernen. Wenn Sie nicht sicher sind, ob Wechselmedien im Speicher vorhanden sind, öffnen Sie den Ordner "Computer" auf Ihrem Windows-Computer. Die Geräte, die Wechselmedien enthalten, werden aufgelistet.

Backup Exec nutzt die Datenlebenszyklusverwaltung, um die Backup-Sätze, die auf Plattenkassettenmedien gespeichert sind, automatisch als abgelaufen zu kennzeichnen. Die Backup-Sätze auf Plattenkassettenmedien werden so lange aufbewahrt, wie in den Eigenschaften des Backup-Auftrags angegeben. Backup Exec gibt den Speicherplatz automatisch frei, wenn die Backup-Daten ablaufen. Sie können verhindern, dass Backup-Sätze automatisch ablaufen, indem Sie sie aufbewahren. Backup Exec behält dann auch alle abhängigen Backup-Sätze bei.

Sie müssen den Assistenten "Speicher konfigurieren" verwenden, um ein Plattenkassettengerät zu konfigurieren.

Welche Speichervorgänge für Plattenkassetten verfügbar sind, sind vom Typ der Plattenkassette abhängig. Beispielsweise sind weniger Vorgänge für USB-Sticks als für RDX-Geräte verfügbar.

So konfigurieren Sie Plattenkassettenspeicher

- 1 Klicken Sie auf der Registerkarte "Speicher" in der Gruppe "Konfigurieren" auf "Speicher konfigurieren".
- 2 Sie haben folgende Möglichkeiten:

Wenn Central Admin Server Feature nicht installiert ist Klicken Sie auf "Plattenbasierter Speicher" und dann auf "Weiter".

Wenn Central Admin Server Feature installiert ist

Gehen Sie dazu nach folgender Reihenfolge vor:

- Wählen Sie den Backup Exec-Server aus, für den Sie Speicher konfigurieren möchten, und klicken Sie dann auf "Weiter".
- Klicken Sie auf "Plattenbasierter Speicher" und dann auf "Weiter".

- 3** Klicken Sie auf "Plattenkassettengerät" und dann auf "Weiter".
- 4** Geben Sie einen Namen und eine Beschreibung für das Plattenkassettengerät ein und klicken Sie dann auf "Weiter".
- 5** Geben Sie an, wo sich das Plattenkassettengerät befindet, und klicken Sie dann auf "Weiter".
- 6** Lesen Sie die Übersicht und führen einen der folgenden Schritte aus:

So ändern Sie die Konfiguration

Gehen Sie dazu in folgender Reihenfolge vor:

- Klicken Sie auf die Überschrift, die die Elemente enthält, die Sie ändern möchten.
- Nehmen Sie alle Änderungen, vor und klicken Sie dann auf "Weiter", bis die Übersicht angezeigt wird.
- Klicken Sie auf "Fertigstellen".

So konfigurieren Sie das Plattenkassettengerät

Klicken Sie auf "Fertigstellen".

Siehe ["Bearbeiten der Eigenschaften von Festplattenkassetten"](#) auf Seite 385.

Bearbeiten der Eigenschaften von Festplattenkassetten

Sie können die Einstellungen für den Plattenkassettenspeicher bearbeiten.

Siehe ["Konfigurieren des Plattenkassettenspeichers"](#) auf Seite 384.

So bearbeiten Sie Plattenkassetteneigenschaften

- 1** Doppelklicken Sie auf der Registerkarte "Speicher" auf den Plattenspeicher, dessen Eigenschaften Sie anzeigen möchten.
- 2** Klicken Sie im linken Teilfenster auf "Eigenschaften".

3 Bearbeiten Sie eine der folgenden Optionen:

Name	<p>Zeigt den Namen der Plattenkassette an. Namen von Plattenkassetten dürfen höchstens 128 Zeichen lang sein.</p> <p>Sie können die Plattenkassette umbenennen.</p>
Beschreibung	<p>Zeigt eine Beschreibung der Plattenkassette an.</p> <p>Sie können die Beschreibung ändern.</p>
Maximale Dateigröße	<p>Zeigt die maximale Dateigröße auf der Plattenkassette an. Die Daten des Auftrags befinden sich in einer Datei auf der Plattenkassette.</p> <p>Der Standardwert ist 50 GB oder die Kapazität der Plattenkassettenmedien.</p>
Speicherplatz bis zur maximalen Dateigröße inkrementell im Voraus zuordnen	<p>Erstellt die Datei zu Beginn des Auftrags durch inkrementelle Zuteilung von Speicherplatz gemäß der Größe des von Ihnen in "Inkrement der Vorabzuordnung" festgelegten Werts. Während der Auftrag den Speicherplatz aufbraucht, wird weiterer Speicherplatz vorab zugeteilt, bis die maximale Dateigröße erreicht ist. Wenn der Auftrag abgeschlossen ist, wird die Dateigröße auf den für den Auftrag tatsächlich verwendeten Speicherplatz reduziert.</p> <p>Wenn Sie die Vorabzuordnung aktivieren und als Inkrement z. B. 4 GB festlegen, werden beim Start des Auftrags 4 GB Speicherplatz im Voraus zugeordnet. Nachdem der Auftrag 4 GB aufgebraucht hat, ordnet Backup Exec weitere 4 GB zu. Weiterer Speicherplatz wird in Schritten von 4 GB zugeteilt, bis der Auftrag abgeschlossen ist. Wenn der Auftrag z. B. nur 13 GB verwendet, obwohl 16 GB zugeordnet wurden, wird die Dateigröße auf 13 GB reduziert.</p> <p>Die Standardeinstellung ist "Deaktiviert".</p>

Inkrement der Vorabzuordnung

Zeigt den Speicherplatz an, um den die Dateigröße jeweils erhöht wird, wenn die Option zum Zuteilen von Speicherplatz aktiviert ist. Die Dateigröße nimmt entsprechend dem Speicherplatzbedarf für den Auftrag immer wieder um diesen Wert zu, bis die maximale Dateigröße erreicht ist.

Der Standardwert ist 1 GB.

Block- und Puffergröße automatisch erkennen

Gibt an, ob Backup Exec automatisch die bevorzugten Einstellungen für die Block- und Puffergröße für den Plattenspeicher erkennt.

Die Standardeinstellung ist "Aktiviert".

Wenn Sie diese Einstellung deaktivieren, können Sie die zu verwendende Block- und Puffergröße wählen.

Blockgröße

Zeigt die Größe der Datenblöcke an, die auf neue Medien in dieser Plattenkassette geschrieben werden, wenn die Option "Block- und Puffergröße automatisch erkennen" deaktiviert wird. Standardeinstellung ist die bevorzugte Blockgröße.

Einige Speichergeräte erreichen eine bessere Leistung, wenn größere Blockgrößen verwendet werden. Die bevorzugte Blockgröße kann zwischen 512 Byte und 64 Kilobyte oder mehr liegen. Wenn Sie einen Speicher verwenden, der größere Blockgrößen unterstützt, können Sie die Blockgröße ändern. Wenn jedoch die Option zum Ändern der Blockgröße nicht verfügbar ist, müssen Sie das Gerät so konfigurieren, dass es eine größere Blockgröße verwendet.

Informationen zum Konfigurieren des Speichers finden Sie in der Dokumentation des Herstellers.

Backup Exec stellt nicht sicher, dass die angeforderte Blockgröße vom Speichergerät unterstützt wird. Wenn die angeforderte Blockgröße nicht unterstützt wird, wird die Standardblockgröße verwendet.

Wenn der Speicher das Konfigurieren der Blockgröße nicht unterstützt, ist diese Option nicht verfügbar.

Puffergröße

Zeigt die Menge der Daten an, die bei jeder Lese- oder Schreibanfrage an die Plattenkassette gesendet werden, wenn die Option "Block- und Puffergröße automatisch erkennen" deaktiviert ist. Die Puffergröße muss ein gerades Vielfaches der Blockgröße sein.

Je nach Größe des Arbeitsspeichers in Ihrem System können Sie durch Erhöhen dieses Werts eventuell die Speicherleistung verbessern. Für jeden Speichertyp ist eine andere, spezifische Puffergröße erforderlich, um optimale Leistungswerte zu erzielen.

Wenn die bevorzugte Blockgröße größer als 64 KB ist, ist die Standardpuffergröße gleich der Standardblockgröße. Wenn die bevorzugte Blockgröße kleiner als 64 KB ist, dann ist die Standardpuffergröße 64 KB.

Geringer Speicherplatz - Kritisch

Zeigt den Schwellenwert für Festplattenspeicher an. Die Farbe der Kapazitätsleiste auf der Registerkarte "Speicher" ändert sich in rot, um anzuzeigen, dass der freie Speicherplatz ein kritisches Minimum erreicht hat. Backup Exec sendet keine Warnmeldung aufgrund von geringem Speicherplatz für Plattenkassettengeräte.

Sie können den Wert des Schwellenwerts ändern, aber er muss kleiner als der Warnschwellenwert sein.

Der Standardwert ist 5 %.

Siehe "[Übersicht über die Registerkarte "Speicher" in Backup Exec](#)" auf Seite 520.

Geringer Speicherplatz – Warnung

Zeigt den Schwellenwert für Festplattenspeicher an. Die Farbe der Kapazitätsleiste auf der Registerkarte "Speicher" ändert sich in orange, um anzuzeigen, dass nur noch wenig freier Speicherplatz verfügbar ist. Backup Exec sendet keine Warnmeldung aufgrund von geringem Speicherplatz für Plattenkassettengeräte.

Sie können den Wert des Schwellenwerts ändern, aber er muss kleiner als der Schwellenwert für niedrigen Speicherplatz sein.

Der Standardwert ist 15 %.

Siehe ["Übersicht über die Registerkarte "Speicher" in Backup Exec"](#) auf Seite 520.

Geringer Speicherplatz

Zeigt den Schwellenwert für Festplattenspeicher an. Die Farbe der Kapazitätsleiste auf der Registerkarte "Speicher" ändert sich in gelb, um anzuzeigen, dass die erste von drei Warnstufen aufgrund von geringem Speicherplatz erreicht wurde. Backup Exec sendet keine Warnmeldung aufgrund von geringem Speicherplatz für Plattenkassettengeräte. Wenn die genutzte Kapazität der Datenträgermedien diesen Schwellenwert erreicht, durchsucht die Data Lifecycle Management-Funktion diese Datenträgermedien nach abgelaufenen Backup-Sätzen, die gelöscht werden können.

Sie können den Schwellenwert ändern.

Der Standardwert ist 25 %.

Siehe ["Übersicht über die Registerkarte "Speicher" in Backup Exec"](#) auf Seite 520.

Einstellungen automatisch erkennen

Gibt an, ob Backup Exec automatisch die bevorzugten Einstellungen für Lese- und Schreibpuffer für die Plattenkassette erkennt.

Die Standardeinstellung ist "Aktiviert".

Gepufferte Lesevorgänge

Wenn diese Einstellung aktiviert ist, gilt:

- Backup Exec soll die Einstellungen für diese Plattenkassette nicht automatisch erkennen.
- Diese Festplattenkassette soll gepufferte Lesevorgänge (das Lesen großer Datenblöcke) zulassen.

Das Aktivieren dieser Option kann zu einer höheren Leistung führen.

Die Standardeinstellung ist "Aktiviert". Wenn Sie "Einstellungen automatisch erkennen" deaktivieren, wird für diese Einstellung ebenfalls der Wert "Deaktiviert" festgelegt.

Gepufferte Schreibvorgänge

Wenn diese Einstellung aktiviert ist, gilt:

- Backup Exec soll die Einstellungen für diese Plattenkassette nicht automatisch erkennen.
- Diese Festplattenkassette soll gepufferte Schreibvorgänge (das Schreiben großer Datenblöcke) zulassen.

Die Standardeinstellung ist "Aktiviert". Wenn Sie "Einstellungen automatisch erkennen" deaktivieren, wird für diese Einstellung ebenfalls der Wert "Deaktiviert" festgelegt.

- 4 Klicken Sie auf "Übernehmen".

Bearbeiten der Eigenschaften von Plattenkassetten

Sie können die Eigenschaften von Plattenkassetten bearbeiten.

Siehe "[Konfigurieren des Plattenkassettenspeichers](#)" auf Seite 384.

So bearbeiten Sie die Eigenschaften von Plattenkassetten

- 1 Doppelklicken Sie auf der Registerkarte "Speicher" auf das gewünschte Plattenkassettengerät.
- 2 Klicken Sie im linken Teilfenster auf "Medien".

3 Bearbeiten Sie eine der folgenden Optionen:

Medienkennung	<p>Zeigt die Medienkennung an, die Backup Exec automatisch zuweist, oder die der Administrator zuweist.</p> <p>Sie können die Medienkennung bearbeiten, die aus maximal 32 Zeichen bestehen kann. Das Bearbeiten der Kennung ändert den Namen der Medien in der Backup Exec-Benutzeroberfläche.</p>
Medienbeschreibung	<p>Zeigt die ursprüngliche Medienkennung an, wenn das Medium importiert ist. Sie können die Medienbeschreibung bearbeiten, wenn sie nicht eindeutig genug ist. Die Beschreibung ist auf 128 Zeichen begrenzt.</p>
Beschreibung beibehalten	<p>Behält die Medienbeschreibung bei, wenn Sie in der Dropdown-Liste die Option "Ja" wählen. Die Medienbeschreibung wird beibehalten, bis ein überschreibender Backup-Auftrag bzw. ein Lösch- oder Bezeichnungspeichervorgang ausgeführt wird.</p> <p>Standardmäßig wird die Medienbeschreibung nicht behalten. Der Standardwert dieser Option ist "Nein".</p>

Löschen abgelaufener Backup-Sätze auf plattenbasiertem Speicher durch Data Lifecycle Management (DLM)

Backup Exec auf schreibgeschützte Vorgänge begrenzen

Verhindert, dass Backup Exec abgelaufene Backup-Sätze auf diesem Datenträgermedium löscht, wenn Sie die Kassette wieder einlegen. Wenn Sie im Dropdown-Menü die Option "Ja" wählen, löscht die Data Lifecycle Management-Funktion von Backup Exec alle abgelaufenen Backup-Sätze und fordert den Speicherplatz zurück.

Der Standardwert ist "Nein".

Diese Option ist nur dann anwendbar, wenn die Plattenkassette für die in der globalen Einstellung angegebene Anzahl an Tagen vom Backup Exec-Server getrennt war. Der Standardwert ist 30 Tage.

Siehe "[Löschen abgelaufener Backup-Sätze auf plattenbasiertem Speicher durch Data Lifecycle Management \(DLM\)](#)" auf Seite 393.

Siehe "[Backup-Sätze](#)" auf Seite 401.

Siehe "[Wiederherstellen von Daten von einem erneut verbundenen oder eingelegten, plattenbasierten Speichergerät](#)" auf Seite 383.

4 Klicken Sie auf "Übernehmen".

Löschen abgelaufener Backup-Sätze auf plattenbasiertem Speicher durch Data Lifecycle Management (DLM)

Mithilfe von Data Lifecycle Management (DLM) löscht Backup Exec automatisch abgelaufene Backup-Sätze auf dem Festplattenspeicher, dem Festplattenkassettendatenträger, dem Deduplizierungsspeicher, Speichergruppen und virtuellen Datenträgern. Sie geben an, wie lange Backup-Daten aufbewahrt werden, wenn Sie einen Backup-Auftrag erstellen, der an ein plattenbasiertes Speichergerät geschickt wird. Wenn die Aufbewahrungszeit der Backup-Daten abläuft, löscht Data Lifecycle Management die Backup-Sätze und gibt den Speicherplatz frei, es sei denn, es sind abhängige Backup-Sätze (z. B. inkrementelle) vorhanden.

Standardmäßig bewahrt Backup Exec die neuesten Backup-Sätze, die zum Wiederherstellen von gesicherten Komponenten auf einem Server erforderlich sind, selbst dann auf, wenn die Backup-Sätze abgelaufen sind. Wenn Backup-Sätze von anderen Backup-Sätzen abhängen, löscht Backup Exec die Backup-Sätze erst, wenn das Ablaufdatum für alle Backup-Sätze erreicht ist. Selbst wenn der Backup-Satz als abgelaufen angezeigt wird, sind die Daten verfügbar, bis alle abhängigen Backup-Sätze ebenfalls abgelaufen sind.

Beispiel: Sie erstellen eine Backup-Definition, die ein vollständiges Backup und ein inkrementelles Backup für das Laufwerk C: auf einem Server enthält. Das erste vollständige Backup wird ausgeführt, gefolgt vom ersten inkrementellen Backup und dann vom zweiten inkrementellen Backup. Das zweite vollständige Backup wird ausgeführt, gefolgt vom dritten inkrementellen Backup und dann vom vierten inkrementellen Backup. Es werden keine weiteren Backups ausgeführt. Alle Backup-Sätze, die von diesen Backups erstellt wurden, laufen schließlich ab und werden von DLM gelöscht. Die Backup-Sätze aus dem zweiten vollständigen Backup und dem dritten und vierten inkrementellen Backup werden bleiben jedoch erhalten.

Backup Exec bewahrt diese miteinander verbundenen Backup-Sätze auf, da sie die neuesten Backup-Sätze sind, die zur Wiederherstellung des Laufwerks C: erforderlich sind. Durch Aufbewahrung der neuesten miteinander verbundenen Backup-Sätze haben Sie die Daten zum Wiederherstellen des Datenträgers verfügbar.

Warnung: DLM löscht alle abgelaufenen Backup-Sätze, die von einem einmaligen Backup-Auftrag erstellt wurden. DLM bewahrt den letzten Backup-Satz nicht mehr auf, nachdem der Aufbewahrungszeitraum abgelaufen ist, wenn der Backup-Satz aus einem einmaligen Backup stammt.

Um zu verhindern, dass die Backup-Sätze automatisch gelöscht werden, können Sie spezifische Backup-Sätze manuell aufbewahren oder das Ablaufdatum ändern. Wenn Sie einen Backup-Satz aufbewahren, bewahrt Backup Exec auch alle davon abhängigen Backup-Sätze auf.

Siehe ["Aufbewahren von Backup-Sätzen auf plattenbasierten Speichergeräten zum Vermeiden des Ablaufens"](#) auf Seite 406.

Siehe ["Ändern des Ablaufdatums von Backup-Sätzen auf plattenbasierten Speichergeräten"](#) auf Seite 404.

DLM sucht nach abgelaufenen Backup-Sätzen, um sie zu folgenden Zeiten aus plattenbasierten Speichern zu löschen:

- Jede Stunde.
DLM wird zum ersten Mal eine Stunde nachdem Sie Backup Exec und die Backup Exec Services installiert haben gestartet und anschließend jede Stunde

ausgeführt. Wenn Sie den Backup Exec-Dienst neu starten, wird auch der stündliche DLM-Zyklus neu gestartet.

- Wenn der Schwellwert für geringen Speicherplatz für plattenbasierte Speicher erreicht ist.
Dies ist eine Eigenschaft des Speichergeräts. Wenn die genutzte Kapazität des Speichergeräts diesen Schwellwert erreicht wird, durchsucht DLM sofort das Gerät nach abgelaufenen Backup-Sätzen, die es löschen kann.
- Wenn Sie einen Backup-Satz manuell als abgelaufen kennzeichnen.
Wenn Sie einen Backup-Satz auf einem eigenständigen Backup Exec-Server manuell als abgelaufen kennzeichnen, wird DLM sofort auf dem Speichergerät ausgeführt, auf dem sich der Backup-Satz befindet. Wenn Sie in einer Umgebung mit Central Admin Server Feature (CAS) einen Backup-Satz über den zentralen Administrationsserver als abgelaufen kennzeichnen, wird DLM sofort auf dem Server ausgeführt, auf dem der Backup-Satz erstellt wurde. Bei diesem Server kann es sich um einen zentralen Administrationsserver oder den verwalteten Backup Exec-Server handeln. DLM wird nur auf dem Speichergerät ausgeführt, auf dem der Backup-Satz manuell als abgelaufen gekennzeichnet wurde. Wenn Sie einen Backup-Satz manuell von einem verwalteten Backup Exec-Server aus als abgelaufen kennzeichnen, wird DLM sofort auf dem Speichergerät ausgeführt, von dem aus der Backup-Satz manuell als abgelaufen gekennzeichnet wurde.

Zur Überwachung der Backup-Sätze, die Data Lifecycle Management als abgelaufen kennzeichnet, können Sie die Kategorie "Backup-Satz-Aufbewahrung" im Audit-Protokoll anzeigen. Sie können auch den Audit-Protokollbericht ausführen, um die Backup-Sätze, die Data Lifecycle Management als abgelaufen kennzeichnet, anzuzeigen.

Siehe ["Konfigurieren von Überwachungsprotokollen"](#) auf Seite 779.

Siehe ["Bericht "Überwachungsprotokoll""](#) auf Seite 821.

Speicheroptionen, die sich darauf auswirken können, wie Data Lifecycle Management Backup-Sätze löscht, werden in der folgenden Tabelle beschrieben:

Tabelle 8-4 Speicheroptionen in Backup Exec, die sich auf Data Lifecycle Management auswirken

Speicheroption	Beschreibung
Zulassen, dass Backup Exec alle abgelaufenen Backup-Sätze löscht	

Speicheroption	Beschreibung
	<p>Mit dieser globalen Einstellung kann Backup Exec abgelaufene Backup-Sätze löschen, selbst wenn sie die letzten verbleibenden Backup-Sätze sind, die für die Herstellung eines Servers erforderlich sind. Verwenden Sie diese Option, wenn Sie Backup-Daten nach einem bestimmten Zeitraum löschen möchten. Außerdem können Sie Backup-Sätze manuell löschen.</p> <p>Warnung: Wenn Sie diese Option aktivieren, sind die Daten, die Sie zum Wiederherstellen eines Servers benötigen, möglicherweise nicht verfügbar.</p> <p>Folgende Bedingungen können möglicherweise dazu führen, dass Sie Backup-Sätze verlieren, wenn Sie diese Option aktivieren:</p> <ul style="list-style-type: none"> ■ Die Backup-Sätze des letzten vollständigen Backups laufen ab, bevor das nächste vollständige Backup ausgeführt wird. Stellen Sie beim Erstellen von Aufträgen sicher, dass die Backup-Sätze länger als der Zeitraum zwischen vollständigen Backups aufbewahrt werden. ■ Ein Backup schlägt fehl oder wird übersprungen und wird nicht erneut ausgeführt, bevor die Backup-Sätze ablaufen. Überwachen Sie fehlgeschlagene oder übersprungene Aufträge, und stellen Sie sicher, dass Sie sie erneut ausführen, bevor die Backup-Sätze vom vorherigen vollständigen Backup ablaufen. <p>Hinweis: In einer CAS-Umgebung (Central Admin Server Feature) ist diese Option nur auf dem zentralen Administrationsserver verfügbar. Wenn Sie diese Option auf dem zentralen Administrationsserver aktivieren, löscht DLM alle abgelaufenen Backup-Sätze auf dem zentralen Administrationsserver sowie auf allen verwalteten Backup</p>

Speicheroption	Beschreibung
	<p>Exec-Servern. Diese Option löscht alle abgelaufenen Backup-Sätze auf zentral und lokal verwalteten Backup Exec-Servern in einer CAS-Umgebung.</p> <p>Klicken Sie zum Zugreifen auf diese Option auf Backup Exec-Schaltfläche > "Konfiguration und Einstellungen" > "Backup Exec-Einstellungen" > "Speicher".</p> <p>Siehe "Bearbeiten globaler Einstellungen für Speicher" auf Seite 535.</p>
Backup Exec auf Lesevorgänge auf einem plattenbasierten Speichergerät beschränken, wenn getrennt für x Tage	<p>Diese globale Einstellung verhindert, dass Backup Exec abgelaufene Backup-Sätze auf plattenbasierten Speichergeräten löscht, sobald sie sie wieder anschließen. Wenn Sie Backup Exec auf Lesevorgänge beschränken, haben Sie Zeit, die abgelaufenen Backup-Sätze zu überprüfen und zu entscheiden, ob Sie sie aufbewahren möchten, bevor Data Lifecycle Management sie löscht. Zum Beibehalten abgelaufener Backup-Sätze können Sie sie aufbewahren oder das Ablaufdatum ändern.</p> <p>Siehe "Aufbewahren von Backup-Sätzen auf plattenbasierten Speichergeräten zum Vermeiden des Ablaufens" auf Seite 406.</p> <p>Siehe "Ändern des Ablaufdatums von Backup-Sätzen auf plattenbasierten Speichergeräten" auf Seite 404.</p> <p>Backup Exec ist nur auf plattenbasierten Speichergeräten, die für die festgelegte Anzahl von Tagen vom Backup Exec-Server getrennt werden, auf Lesevorgänge beschränkt.</p> <p>Klicken Sie zum Zugreifen auf diese Option auf Backup Exec-Schaltfläche > "Konfiguration und Einstellungen" > "Backup Exec-Einstellungen" > "Speicher".</p> <p>Siehe "Bearbeiten globaler Einstellungen für Speicher" auf Seite 535.</p>

Speicheroption	Beschreibung
Backup Exec auf Lesevorgänge auf einer Plattenkassette beschränken, wenn nicht eingelegt seit x Tagen	<p>Diese globale Einstellung verhindert, dass Backup Exec abgelaufene Backup-Sätze auf Plattenkassetten löscht, sobald sie sie wieder in ein Plattenkassettengerät einlegen. Wenn Sie Backup Exec auf Lesevorgänge beschränken, haben Sie Zeit, die abgelaufenen Backup-Sätze zu überprüfen und zu entscheiden, ob Sie sie aufbewahren möchten, bevor Data Lifecycle Management sie löscht. Zum Beibehalten abgelaufener Backup-Sätze können Sie sie aufbewahren oder das Ablaufdatum ändern.</p> <p>Siehe "Backup-Sätze " auf Seite 401.</p> <p>Backup Exec ist nur auf Plattenkassetten, die für die festgelegte Anzahl von Tagen vom Backup Exec-Server getrennt werden, auf Lesevorgänge beschränkt.</p> <p>Klicken Sie zum Zugreifen auf diese Option auf Backup Exec-Schaltfläche > "Konfiguration und Einstellungen" > "Backup Exec-Einstellungen" > "Speicher".</p> <p>Siehe "Bearbeiten globaler Einstellungen für Speicher" auf Seite 535.</p>

Speicheroption	Beschreibung
Backup Exec auf schreibgeschützte Vorgänge begrenzen	<p>Diese Geräteeigenschaft verhindert, dass Data Lifecycle Management auf einem bestimmten plattenbasierten Speichergerät oder Plattenkassettenspeichergerät ausgeführt wird, das Sie erneut anschließen oder einlegen. Diese Option ist nur dann anwendbar, wenn das Speichergerät für die in einer der beiden in dieser Tabelle beschriebenen globalen Einstellungen angegebene Anzahl an Tagen vom Backup Exec-Server getrennt war.</p> <p>Klicken Sie zum Zugreifen auf diese Option auf der Registerkarte "Speicher" mit der rechten Maustaste auf das Gerät, klicken Sie auf "Details" und dann auf "Eigenschaften".</p> <p>Siehe "Bearbeiten der Eigenschaften von Festplattenspeichern" auf Seite 376.</p> <p>Siehe "Bearbeiten der Eigenschaften von Festplattenkassetten" auf Seite 385.</p> <p>Siehe "Bearbeiten der Eigenschaften eines Deduplizierungsspeichergeräts" auf Seite 1067.</p>

Speicheroption	Beschreibung
Geringer Speicherplatz	<p>Diese Geräteeigenschaft ist die erste von drei Warnstufen aufgrund von geringem Speicherplatz. Wenn die genutzte Kapazität des Speichergeräts diesen Schwellenwert erreicht, durchsucht die Data Lifecycle Management-Funktion das Gerät nach abgelaufenen Backup-Sätzen, die gelöscht werden können.</p> <p>Data Lifecycle Management wird auch auf einer Plattenkassette ausgeführt, wenn diese die entsprechende Kapazität erreicht. Das Backup muss möglicherweise nicht auf eine weitere Plattenkassette ausgedehnt werden, wenn Data Lifecycle Management genügend abgelaufene Backup-Sätze löscht. Wenn ein Auftrag auf eine andere Plattenkassette ausgedehnt werden muss und Sie eine neue Plattenkassette einlegen, die bereits voll ist, löscht Data Lifecycle Management abgelaufene Backup-Sätze auf der neuen Plattenkassette.</p> <p>Klicken Sie zum Zugreifen auf diese Option auf der Registerkarte "Speicher" mit der rechten Maustaste auf das Gerät, klicken Sie auf "Details" und dann auf "Eigenschaften".</p> <p>Siehe "Festlegen von Schwellenwerten für geringen Speicherplatz auf plattenbasierten Speichern" auf Seite 371.</p>

Informationen zu den Best Practices zur Funktion "Data Lifecycle Management" von Backup Exec finden Sie unter *Best Practices für Backup Exec*.

Backup-Sätze

Ein Backup-Satz ist eine Sammlung der Daten, die Sie aus einer Inhaltsquelle sichern. Eine Inhaltsquelle kann beispielsweise ein Server oder ein Microsoft Exchange-Datensatz sein. Wenn Sie mehrere Inhaltsquellen auswählen, erstellt Backup Exec mehrere Backup-Sätze. Wenn Sie einen Backup-Auftrag ausführen, erstellt Backup Exec die Backup-Sätze und schreibt diese auf Speicher. Wählen Sie zum Wiederherstellen von Daten die Backup-Sätze aus, die die wiederherzustellenden Daten enthalten.

Backup Exec behält die Backup-Sätze, die auf Datenträgerspeicher und Datenträgermedien gespeichert werden solange wie in den Backup-Auftragsseigenschaften angegeben. Standardmäßig wird durch den Typ und den Zeitplan des Backup-Auftrags bestimmt, wie lange die Backup-Sätze gespeichert bleiben.

Zum Beispiel können Sie angeben, dass die Backup-Sätze aus einem vollständigen Backup zwei Wochen lang auf einem plattenbasierten Speichergerät aufbewahrt werden sollen. Nach zwei Wochen laufen die Backup-Sätze ab und Backup Exec nutzt Data Lifecycle Management, um die Backup-Sätze zu löschen und den Speicherplatz freizugeben. Wenn Sie später einen inkrementellen Backup-Auftrag erstellen, bewahrt Backup Exec die vollständigen Backup-Sätze für zwei Wochen plus dem Zeitraum auf, für den inkrementelle Backup-Sätze beibehalten werden. Behalten Sie inkrementelle Backup-Sätze vier Wochen lang bei, bewahrt Backup Exec die vollständigen Backup-Sätze sechs Wochen lang auf. Die Daten aus einem vollständigen Backup-Auftrag werden so lange wie die Daten aus den dazugehörigen inkrementellen Backup-Aufträgen aufbewahrt. Backup Exec fordert den Speicherplatz für Backup-Sätze nicht von einem Auftrag zurück, der von einem anderen Auftrag abhängt, bis die Datenaufbewahrung für alle verbundenen Aufträge abläuft. Selbst wenn der Backup-Satz als abgelaufen angezeigt wird, sind die Daten verfügbar, bis alle abhängigen Backup-Sätze ebenfalls abgelaufen sind.

Backup Exec verwaltet die Aufbewahrung von Backup-Sätzen unterschiedlich, je nachdem, welchen Speichertyp Sie für das Backup der Daten verwenden.

Tabelle 8-5 Speichertypen und Backup-Satz-Aufbewahrung

Typ des Speichers	Backup-Daten-Aufbewahrung
Festplattenspeicher, Plattenkassettengeräte, Deduplizierungsspeicher, Speichergruppen, Cloud-Speicher und virtuelle Festplatten	<p>Backup Exec nutzt Data Lifecycle Management, um die abgelaufenen Backup-Sätze automatisch aus dem plattenbasierten Speicher zu löschen. Standardmäßig bewahrt Backup Exec die neuesten Backup-Sätze, die zum Wiederherstellen von gesicherten Komponenten auf einem Server erforderlich sind, selbst dann auf, wenn die Backup-Sätze abgelaufen sind. Selbst wenn der Backup-Satz als abgelaufen angezeigt wird, sind die Daten verfügbar, bis alle abhängigen Backup-Sätze ebenfalls abgelaufen sind.</p> <p>Für plattenbasierten Speicher, den Sie nach einer angegebenen Anzahl von Tagen wieder mit dem Backup Exec-Server verbinden, können Sie verhindern, dass Backup Exec diesen Speicherplatz zurückfordert. Eine globale Einstellung begrenzt Backup Exec auf schreibgeschützte Vorgänge auf plattenbasiertem Speicher oder Plattenkassette, wenn dieser für eine angegebene Anzahl von Tagen abgetrennt wurde. Sie können Backup Exec auch auf schreibgeschützte Vorgänge pro Speichergerät begrenzen, indem Sie diese Einstellung über die Geräteeigenschaften aktivieren.</p> <p>Siehe "Löschen abgelaufener Backup-Sätze auf plattenbasiertem Speicher durch Data Lifecycle Management (DLM)" auf Seite 393.</p> <p>Siehe "Wiederherstellen von Daten von einem erneut verbundenen oder eingelegten, plattenbasierten Speichergerät" auf Seite 383.</p>
Bandkassettenmedien	<p>Backup Exec verwendet die Advanced Device and Media Management-(ADAMM-)Funktion zur Verwaltung der Datenaufbewahrung auf Bandkassettenmedien. ADAMM lässt die auf Medien gespeicherten Backup-Sätze entsprechend den Regeln, die Sie für die Medien festlegen, ablaufen. Backup-Sätze werden nicht automatisch aus Bandkassetten gelöscht, aber sie können, abhängig von den geltenden Regeln, überschrieben werden. Die Gruppe der Regeln zur Verwaltung von Bandkassettenmedien wird als Mediensatz bezeichnet. Sie erstellen Mediensätze, die Anhängezeiträume, Überschreibschutzzeiträume und Auslagerungszeiträume angeben.</p> <p>Siehe "Standard-Mediansätze" auf Seite 473.</p>

Sie können die folgenden Aktionen auf Backup-Sätze ausführen, die sich auf plattenbasierten Speichern befinden:

- Ändern Sie das Ablaufdatum von Backup-Sätzen für eine längere Aufbewahrung oder einen sofortigen Ablauf.
- Erweitern Sie den Zeitraum zur Aufbewahrung von Backup-Sätzen.
- Alle Backup-Sätze freigeben, die beibehalten werden, damit sie automatisch ablaufen

Für alle Backup-Sätze einschließlich denen auf Bandkassetten können Sie die folgenden Aktionen ausführen:

- Backup-Sätze katalogisieren, sodass Sie die in den Backup-Sätzen enthaltenen Daten anzeigen und nach wiederherzustellenden Dateien suchen können
- Inhalte von Backup-Sätzen anzeigen und die darin gesicherten Daten durchsuchen
- System- und Auftragseigenschaften von Backup-Sätzen anzeigen.

Siehe ["Ändern des Ablaufdatums von Backup-Sätzen auf plattenbasierten Speichergeräten"](#) auf Seite 404.

Siehe ["Aufbewahren von Backup-Sätzen auf plattenbasierten Speichergeräten zum Vermeiden des Ablaufens"](#) auf Seite 406.

Siehe ["Freigeben aufbewahrter Backup-Sätze auf plattenbasierten Speichergeräten"](#) auf Seite 407.

Siehe ["Katalogisieren von Backup-Sätzen"](#) auf Seite 284.

Siehe ["Anzeigen des Inhalts oder der Eigenschaften von Backup-Sätzen"](#) auf Seite 408.

Ändern des Ablaufdatums von Backup-Sätzen auf plattenbasierten Speichergeräten

Sie können das Ablaufdatum von Backup-Sätzen auf plattenbasierten Speichergeräten ändern. Außerdem können Sie Backup-Sätze sofort als abgelaufen kennzeichnen, wenn Sie sie nicht mehr benötigen. Data Lifecycle Management (DLM) löscht automatisch abgelaufene Backup-Sätze aus plattenbasierten Speichern.

Wenn Sie Backup-Sätze manuell als abgelaufen kennzeichnen, prüft Backup Exec diese Backup-Sätze, um sicherzustellen, dass keine anderen Backup-Sätze von ihnen abhängen. Backup-Sätze aus inkrementellen und Differenzial-Aufträgen hängen von den Backup-Sätzen ab, die aus dem vollständigen Backup in der gleichen Backup-Definition stammen. Sie können nicht nur die Backup-Sätze, die

aus dem vollständigen Backup stammen, als abgelaufen kennzeichnen, weil die abhängigen Backup-Sätze ohne sie nicht funktionieren würden. Wenn Backup Exec abhängige Backup-Sätze erkennt, können Sie diese und alle von ihnen abhängigen Backup-Sätze als abgelaufen kennzeichnen.

Wenn Sie einen Backup-Satz auf einem eigenständigen Backup Exec-Server manuell als abgelaufen kennzeichnen, wird DLM sofort auf dem Speichergerät ausgeführt, auf dem sich der Backup-Satz befindet. Wenn Sie in einer Central Admin Server Feature(CAS)-Umgebung einen Backup-Satz über den zentralen Administrationsserver als abgelaufen kennzeichnen, wird DLM sofort auf dem Server ausgeführt, auf dem der Backup-Satz erstellt wurde. Bei diesem Server kann es sich um einen zentralen Administrationsserver oder den verwalteten Backup Exec-Server handeln. DLM wird nur auf dem Speichergerät ausgeführt, auf dem der Backup-Satz manuell als abgelaufen gekennzeichnet wurde. Wenn Sie einen Backup-Satz manuell von einem verwalteten Backup Exec-Server aus als abgelaufen kennzeichnen, wird DLM sofort auf dem Speichergerät ausgeführt, von dem aus der Backup-Satz manuell als abgelaufen gekennzeichnet wurde.

Siehe "[Löschen abgelaufener Backup-Sätze auf plattenbasiertem Speicher durch Data Lifecycle Management \(DLM\)](#)" auf Seite 393.

So ändern Sie das Ablaufdatum von Backup-Sätzen auf plattenbasierten Speichergeräten

- 1 Doppelklicken Sie auf der Registerkarte "Backup und Wiederherstellung" oder "Speicher" auf den Server bzw. das Speichergerät, der bzw. das mit den Backup-Sätzen verknüpft ist.
- 2 Klicken Sie im linken Teilfenster auf "Backup-Sätze".
- 3 Sie haben folgende Möglichkeiten:
 - Um das Ablaufdatum für einen einzelnen Backup-Satz zu ändern, klicken Sie mit der rechten Maustaste auf den Backup-Satz.
 - Um das Ablaufdatum für mehrere Backup-Sätze zu ändern, klicken Sie bei gedrückter Umschalt- bzw. Strg-Taste auf die Backup-Sätze, und dann mit der rechten Maustaste auf einen der ausgewählten Backup-Sätze.
- 4 Sie haben folgende Möglichkeiten:

So kennzeichnen Sie Backup-Sätze als ab sofort abgelaufen

- Klicken Sie auf "Ablauf". Backup Exec zeigt den Backup-Satz und alle abhängigen Backup-Sätze an.
- Um das ausgewählte einzelne Backup zusammen mit den abhängigen Backup-Sätzen ablaufen zu lassen, klicken Sie auf "Ablauf". Wenn Sie mehrere Backup-Sätze ausgewählt haben, klicken Sie auf "Ablauf" oder "Alle ablaufen lassen". Außerdem können Sie mit der Option "Überspringen" einen Backup-Satz zusammen mit den abhängigen Backup-Sätzen vom Löschen ausschließen.

So ändern Sie das Ablaufdatum von Backup-Sätzen

- Klicken Sie auf "Ablauf".
- Geben Sie im Feld "Ablauf" das neue Ablaufdatum ein.
- Klicken Sie auf "OK".

Siehe "[Backup-Sätze](#)" auf Seite 401.

Aufbewahren von Backup-Sätzen auf plattenbasierten Speichergeräten zum Vermeiden des Ablaufens

Sie können verhindern, dass Backup-Sätze auf plattenbasierten Speichergeräten automatisch als abgelaufen gekennzeichnet werden, indem Sie sie aufbewahren. Backup Exec bewahrt dann alle abhängigen Backup-Sätze auf. Wenn Sie beispielsweise einen inkrementellen Backup-Satz aufbewahren möchten, bewahrt Backup Exec alle Backup-Sätze bis zum letzten vollständigen Backup-Auftrag (einschließlich) auf. Möglicherweise müssen Sie Backup-Sätze aus rechtlichen Gründen beibehalten, zum Beispiel zur Einhaltung von Gesetzen zur Datenaufbewahrung.

Wenn Sie einen Backup-Satz beibehalten, verhindert Backup Exec auf unbegrenzte Zeit, dass der Backup-Satz abläuft. Wenn Sie entscheiden, dass Sie einen Backup-Satz nicht mehr brauchen, müssen Sie ihn veröffentlichen, damit er automatisch ablaufen kann. Data Lifecycle Management (DLM) löscht automatisch abgelaufene Backup-Sätze aus plattenbasierten Speichern.

Siehe "[Löschen abgelaufener Backup-Sätze auf plattenbasiertem Speicher durch Data Lifecycle Management \(DLM\)](#)" auf Seite 393.

So bewahren Sie Backup-Sätze auf plattenbasierten Speichergeräten auf, damit Sie nicht ablaufen

- 1 Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, das mit den beizubehaltenden Backup-Sätzen verbunden ist.
- 2 Klicken Sie im linken Teilfenster auf "Backup-Sätze".
- 3 Sie haben folgende Möglichkeiten:
 - Klicken Sie zum Beibehalten eines einzelnen Backup-Satzes mit der rechten Maustaste auf den Backup-Satz.
 - Um mehrere Backup-Sätze beizubehalten, klicken Sie bei gedrückter Umschalttaste oder Strg-Taste auf die Backup-Sätze und klicken Sie dann mit der rechten Maustaste auf einen der ausgewählten Backup-Sätze.
- 4 Klicken Sie auf "Beibehalten".
- 5 Wählen Sie im Feld "Grund für Aufbewahren der Backup-Sätze" den passenden Eintrag. Folgende Optionen sind verfügbar:

Rechtlich	Wählen Sie diese Option aus, wenn der Grund für das Aufbewahren der Backup-Sätze ein rechtlicher ist. Sie müssen Backup-Sätze möglicherweise aufgrund von Unternehmens- oder rechtlichen Richtlinien aufbewahren.
Benutzerdefiniert	Wählen Sie diese Option aus, wenn der Grund für das Aufbewahren nicht rechtlich ist.

- 6 Geben Sie im Feld "Erklärung" zusätzliche Informationen darüber an, warum Sie die Backup-Sätze aufbewahrt haben. Das Eingeben einer Erklärung in diesem Feld kann helfen, Sie daran zu erinnern, warum Sie die Backup-Sätze aufbewahrt haben oder wie lange diese erhalten bleiben sollen.
- 7 Klicken Sie auf "OK".

Siehe ["Backup-Sätze"](#) auf Seite 401.

Siehe ["Freigeben aufbewahrter Backup-Sätze auf plattenbasierten Speichergeräten"](#) auf Seite 407.

Freigeben aufbewahrter Backup-Sätze auf plattenbasierten Speichergeräten

Sie können die Aufbewahrungszeit für Backup-Sätze auf plattenbasierten Speichergeräten außer Kraft setzen, indem Sie sie manuell aufbewahren. Wenn

Sie festlegen, dass Backup-Sätze aufbewahrt werden sollen, verhindert Backup Exec, dass diese am Ende ihres Aufbewahrungszeitraums automatisch ablaufen. Sie können Backup-Sätze manuell für unbegrenzte Zeit beibehalten.

Wenn Sie die aufbewahrten Backup-Sätze nicht mehr benötigen, können Sie sie ablaufen lassen. Zuerst müssen Sie den Aufbewahrungstatus der Backup-Sätze aufheben. Dann lässt Backup Exec die Backup-Sätze automatisch entsprechend der Speichereinstellungen ablaufen. Data Lifecycle Management (DLM) löscht automatisch abgelaufene Backup-Sätze aus plattenbasierten Speichern.

So geben Sie aufbewahrte Backup-Sätze auf plattenbasierten Speichergeräten frei

- 1 Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, das mit den aufbewahrten Backup-Sätzen, die Sie freigeben möchten, verbunden ist.
- 2 Klicken Sie im linken Teilfenster auf "Backup-Sätze".
- 3 Sie haben folgende Möglichkeiten:
 - Um einen einzelnen Backup-Satz freizugeben, klicken Sie mit der rechten Maustaste auf den Backup-Satz.
 - Um mehrere Backup-Sätze freizugeben, klicken Sie bei gedrückter Umschalttaste oder Strg-Taste auf die Backup-Sätze und klicken Sie dann mit der rechten Maustaste auf einen der ausgewählten Backup-Sätze.
- 4 Klicken Sie auf "Beibehalten".
- 5 Wählen Sie "Nicht beibehalten" aus.
- 6 Klicken Sie auf "OK".

Siehe ["Backup-Sätze"](#) auf Seite 401.

Siehe ["Aufbewahren von Backup-Sätzen auf plattenbasierten Speichergeräten zum Vermeiden des Ablaufens"](#) auf Seite 406.

Siehe ["Löschen abgelaufener Backup-Sätze auf plattenbasiertem Speicher durch Data Lifecycle Management \(DLM\)"](#) auf Seite 393.

Anzeigen des Inhalts oder der Eigenschaften von Backup-Sätzen

Nachdem Sie einen Backup-Auftrag abgeschlossen haben, können Sie die in den erstellten Backup-Sätzen enthaltenen Daten anzeigen. Indem Sie den Inhalt der Backup-Sätze anzeigen, können Sie nachprüfen, welche Daten gesichert wurden. Sie sollten den Inhalt von Backup-Sätzen möglicherweise auch vor der Ausführung von Wiederherstellungsaufträgen anzeigen, um die enthaltenen Daten zu überprüfen.

Sie können auch die folgenden Backup-Satz-Eigenschaften:

- Backup-Quelle
- Backup-Datum
- Ablaufdatum
- Backup-Methode
- Größe
- Speicherort
- Beschreibung des Backup-Satzes
- Datenverschlüsselung
- True Image
- Servername
- Katalogdateiname
- Snapshot

So zeigen Sie den Inhalt oder die Eigenschaften von Backup-Sätzen an

- 1** Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, das mit den anzuzeigenden Backup-Sätzen verbunden ist.
- 2** Klicken Sie im linken Teilfenster auf "Backup-Sätze".
- 3** Doppelklicken Sie auf den Backup-Satz, den Sie anzeigen möchten.

Hinweis: Auf der Registerkarte "Backup und Wiederherstellung" müssen Sie die Backup-Quelle erweitern, um Backup-Sätze zu sehen.

- 4** Sie haben folgende Möglichkeiten:

So zeigen Sie den Inhalt von Backup-Sätzen an Klicken Sie im linken Teilfenster auf "Inhalt".

Der Inhalt des Backup-Satzes wird im linken Teilfenster in einer Strukturansicht angezeigt. Sie können Ordner und Laufwerke erweitern, um ihren Inhalt im rechten Teilfenster anzuzeigen.

So zeigen Sie die Eigenschaften der Backup-Sätze an

Klicken Sie im linken Teilfenster auf "Eigenschaften".

Siehe "[Backup-Sätze](#) " auf Seite 401.

Cloud-basierte Speichergeräte

In diesem Kapitel werden folgende Themen behandelt:

- [Info zu Cloud-basierten Speichergeräten](#)
- [Cloud-Speicher von Amazon S3](#)
- [Cloud-Speicher von Google](#)
- [Cloud-Speicher von Microsoft Azure](#)
- [Privater Cloud-Speicher](#)
- [Informationen zu S3-kompatiblen Cloud-Speicher](#)
- [Bearbeiten der Eigenschaften eines Cloud-basierten Speichergeräts](#)
- [Best Practices beim Einsatz von Cloud-basiertem Speicher](#)
- [Ändern der Standardeinstellungen für Cloud-Speicher](#)
- [Info zu Backup Exec™ CloudConnect Optimizer](#)

Info zu Cloud-basierten Speichergeräten

Backup Exec unterstützt das Sichern auf Cloud-basierten Speichergeräten. Sie können den Cloud Connector verwenden, um Daten aus dem Cloud-Speicher als Cloud-Storage as a Service-Anbieter (STaaS) zu sichern und wiederherzustellen. Der Cloud-basierte Speicher unterscheidet sich von herkömmlichen band- oder festplattenbasierten Datenträgern, die persistente Backup-Images nutzen. Normalerweise berechnen Anbieter einer öffentlichen Cloud die Speicherkosten pro gespeicherten und übertragenen Bytes.

Die unterstützten öffentlichen und privaten Cloud-Anbieter finden Sie in der Liste der mit Backup Exec kompatiblen Hardware unter folgender URL:

Hinweis: Ein Cloud-Speichergerät kann nicht zu Speicherpools gehören.

Informationen zu den Best Practices zum Verwalten von Backup Exec Cloud Connector finden Sie unter *Best Practices für Backup Exec*.

Die folgenden Hinweise gelten für Cloud-basierte Speichergeräte:

- Wenn Sie die Backup Exec Central Admin Server Option verwenden, können Sie ein öffentliches Cloud-Speichergerät auf mehreren verwalteten Backup Exec-Servern freigeben. Sie können die Freigabe aktivieren, wenn Sie ein öffentliches Cloud-Speichergerät hinzufügen. Sie können neue verwaltete Backup Exec-Server für die Freigabe eines öffentlichen Cloud-Speichergeräts auswählen. Sie können die Freigabe jederzeit für alle verwalteten Backup Exec-Server entfernen.
- Data Lifecycle Management lässt Backup-Sätze auf Cloud-Speichern automatisch ablaufen.
- Manche Cloud-Speicheranbieter erfordern Verschlüsselung.
Siehe ["Verwendung von Verschlüsselung mit Backup Exec"](#) auf Seite 727.

Cloud-Speicher von Amazon S3

Im Folgenden finden Sie Informationen zu den Anforderungen für die Konfiguration eines Amazon S3-Speichergeräts und des Amazon S3-Speichers in Backup Exec.

Siehe ["Anforderungen für die Konfiguration eines Cloud-basierten Speichers für Amazon S3"](#) auf Seite 411.

Siehe ["Konfigurieren des Amazon-Cloud-Speichers"](#) auf Seite 412.

Anforderungen für die Konfiguration eines Cloud-basierten Speichers für Amazon S3

Mit dem Backup Exec-Cloud Connector können Daten aus Amazon Simple Storage Service (S3) gesichert und wiederhergestellt werden.

Für die Konfiguration eines Cloud-basierten Speichers für Amazon S3 gelten folgende Anforderungen:

- Sie müssen ein Konto für Amazon Simple Storage Service (S3) mit Benutzernamen und Kennwort anlegen. Fordern Sie außerdem eine Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel für Amazon an.

- Vor der Konfiguration müssen Buckets erstellt werden. Buckets sind logische Speichereinheiten auf dem Cloud-basierten Speichergerät.

Hinweis: Als Best Practice sollten Sie bestimmte Buckets erstellen, die ausschließlich für Backup Exec verwendet werden.

Jedes Cloud-Speicher-Gerät muss einen anderen Bucket verwenden. Verwenden Sie nicht den gleichen Bucket für mehrere Cloud-Speicher-Geräte, selbst wenn diese Geräte auf verschiedenen Backup Exec-Servern konfiguriert sind.

- Stellen Sie sicher, dass die Bucket-Namen die folgenden Backup Exec-Anforderungen erfüllen:
 - Bucket-Namen dürfen Kleinbuchstaben, Ziffern und Gedanken- bzw. Bindestriche enthalten.
 - Sie dürfen nicht mit einem Gedanken- bzw. Bindestrich beginnen.Die Buckets sind nicht in Backup Exec verfügbar, wenn der Name dieser Namenskonvention nicht entspricht oder wenn die Buckets für eine Region erstellt wurden, die von Backup Exec nicht unterstützt wird. Die unterstützten Regionen finden Sie in der Liste der mit Backup Exec kompatiblen Hardware.

Siehe ["Konfigurieren des Amazon-Cloud-Speichers"](#) auf Seite 412.

Konfigurieren des Amazon-Cloud-Speichers

Sie können ein Cloud-basiertes Speichergerät für den Amazon-Cloud-Speicher konfigurieren und dann Daten darauf sichern.

Hinweis: Für Cloud-Speichergeräte ist jetzt standardmäßig die Option "Daten für diesen Auftrag nicht verifizieren" in den "Backup-Optionen" aktiviert. Einige Cloud-Anbieter berechnen Gebühren für Lese- und Schreibvorgänge in der Cloud. Diese Option ist standardmäßig aktiviert, um Belastungen beim Auslesen von Daten beim Verifizieren eines Backups oder Duplizierungsauftrags zu vermeiden.

Siehe ["Konfigurieren der automatischen Prüfung von Aufträgen"](#) auf Seite 655.

Siehe ["Hinzufügen einer Stufe zu einer Backup-Definition"](#) auf Seite 244.

Siehe ["Anforderungen für die Konfiguration eines Cloud-basierten Speichers für Amazon S3"](#) auf Seite 411.

So konfigurieren Sie den Speicher für den Amazon-Cloud-Speicher in Backup Exec:

- 1** Wählen Sie auf der Registerkarte "Backup und Wiederherstellung" die Option "Backup > In Cloud sichern" und klicken Sie auf "OK".

Oder klicken Sie auf der Registerkarte "Speicher" in der Gruppe "Speicher konfigurieren" auf "Cloud-Speicher" und dann auf "Weiter".

Alternativ können Sie auf der Registerkarte "Speicher" auf "Cloud-Speicher konfigurieren" klicken.
- 2** Geben Sie den Namen und die Beschreibung des Cloud-Speichergeräts ein und klicken Sie auf "Weiter".
- 3** Wählen Sie in der Liste der Cloud-Speicheranbieter die Option "S3" und klicken Sie auf "Weiter".
- 4** Wählen Sie im Feld "Cloud-Speicher" den Namen des Amazon-Servers aus der Dropdown-Liste.
- 5** Wählen Sie im Feld "Speicherebene" eine Ebene aus der Dropdown-Liste.

Sie können aus den beiden Optionen "Standard" (für häufig abgerufene Daten) oder "Standard_IA" (für selten abgerufene Daten) auswählen.
- 6** Wählen Sie im Feld "Login-Konto" ein Konto aus der Dropdown-Liste oder klicken Sie auf "Hinzufügen/Bearbeiten", um ein Konto hinzuzufügen.
- 7** Klicken Sie im Dialogfeld "Login-Konto auswählen" auf "Hinzufügen".
- 8** Führen Sie im Dialogfeld "Identifikationsdaten hinzufügen" folgende Schritte durch:
 - Geben Sie im Feld "Benutzername" die ID für den Amazon-Zugriffsschlüssel ein.
 - Geben Sie im Feld "Kennwort" den geheimen Amazon-Zugriffsschlüssel ein.
 - Geben Sie im Feld "Kennwort bestätigen" den geheimen Amazon-Zugriffsschlüssel erneut ein.
 - Geben Sie im Feld "Kontoname" einen Namen für das Login-Konto ein.
In Backup Exec wird dieser in allen Speichergerätelisten als Name des Cloud-Speichergeräts angezeigt.
- 9** Klicken Sie zweimal auf "OK".
- 10** Wählen Sie das in Schritt 7 erstellte Amazon-Login-Konto aus und klicken Sie dann auf "Weiter".

- 11 Wählen Sie ein Bucket aus der Liste der mit dem Servernamen verknüpften Buckets aus und klicken Sie auf "Weiter".
- 12 Geben Sie die Anzahl der gleichzeitig auf diesem Cloud-Speichergerät ausführbaren Schreibvorgänge ein und klicken Sie auf "Weiter".

Diese Einstellung legt die Anzahl von Aufträgen fest, die auf diesem Gerät gleichzeitig ausgeführt werden können. Der geeignete Wert für diese Einstellung hängt von Ihrer Umgebung und der Bandbreite des Cloud-Speichers ab. Sie können den Standardwert auswählen.
- 13 Überprüfen Sie die Konfiguration und klicken Sie auf "Fertigstellen".

Backup Exec erstellt ein Cloud-Speichergerät. Sie müssen die Backup Exec-Dienste neu starten, um das neue Gerät online zu schalten.
- 14 Klicken Sie im Fenster mit der Aufforderung "Backup Exec-Dienste neu starten" auf "Ja".

Nachdem die Dienste neu gestartet wurden, zeigt Backup Exec den neuen Cloud-Speicherort in der Liste "Gesamter Speicher" an.

Cloud-Speicher von Google

Im Folgenden finden Sie Informationen zu den Anforderungen für die Konfiguration eines Google-Speichergeräts und des Google-Speichers in Backup Exec.

Siehe ["Anforderungen für die Konfiguration von Cloud-basierten Google-Speichergeräten"](#) auf Seite 414.

Siehe ["Konfigurieren des Speichers für Google Cloud Storage"](#) auf Seite 415.

Anforderungen für die Konfiguration von Cloud-basierten Google-Speichergeräten

Mit dem Backup Exec-Cloud Connector können Daten aus Google Cloud Storage gesichert und wiederhergestellt werden.

Für die Konfiguration eines Cloud-basierten Google-Speichergeräts gelten folgende Anforderungen:

- Sie müssen ein Konto für die Google Cloud-Plattform mit Benutzernamen und Kennwort anlegen. Fordern Sie außerdem eine interoperable Zugriffsschlüssel-ID und einen interoperablen geheimen Zugriffsschlüssel für Google S3 an. Diese Schlüssel können in der Google Developers Console generiert werden.

-
- **Hinweis:** Als Best Practice sollten Sie bestimmte Buckets erstellen, die ausschließlich für Backup Exec verwendet werden.

Jedes Cloud-Speicher-Gerät muss einen anderen Bucket verwenden. Verwenden Sie nicht den gleichen Bucket für mehrere Cloud-Speicher-Geräte, selbst wenn diese Geräte auf verschiedenen Backup Exec-Servern konfiguriert sind.

Vor der Konfiguration müssen Buckets erstellt werden. Buckets sind logische Speichereinheiten auf dem Cloud-basierten Speichergerät.

- Stellen Sie sicher, dass die Bucket-Namen die folgenden Backup Exec-Anforderungen erfüllen:
 - Bucket-Namen dürfen Kleinbuchstaben, Ziffern und Gedanken- bzw. Bindestriche enthalten.
 - Sie dürfen nicht mit einem Gedanken- bzw. Bindestrich beginnen.Die Buckets sind nicht in Backup Exec verfügbar, wenn der Name dieser Namenskonvention nicht entspricht oder wenn die Buckets für eine Region erstellt wurden, die von Backup Exec nicht unterstützt wird. Die unterstützten Regionen finden Sie in der Liste der mit Backup Exec kompatiblen Hardware.

Siehe ["Konfigurieren des Speichers für Google Cloud Storage"](#) auf Seite 415.

Konfigurieren des Speichers für Google Cloud Storage

Sie können ein Cloud-basiertes Speichergerät für Google Cloud Storage konfigurieren und dann Daten darauf sichern.

Hinweis: Für Cloud-Speichergeräte ist jetzt standardmäßig die Option "Daten für diesen Auftrag nicht verifizieren" in den "Backup-Optionen" aktiviert. Einige Cloud-Anbieter berechnen Gebühren für Lese- und Schreibvorgänge in der Cloud. Diese Option ist standardmäßig aktiviert, um Belastungen beim Auslesen von Daten beim Verifizieren eines Backups oder Duplizierungsauftrags zu vermeiden.

Siehe ["Konfigurieren der automatischen Prüfung von Aufträgen"](#) auf Seite 655.

Siehe ["Hinzufügen einer Stufe zu einer Backup-Definition"](#) auf Seite 244.

Siehe ["Anforderungen für die Konfiguration von Cloud-basierten Google-Speichergeräten"](#) auf Seite 414.

So konfigurieren Sie den Speicher für Google Cloud Storage in Backup Exec

- 1** Wählen Sie auf der Registerkarte "Backup und Wiederherstellung" die Option "Backup > In Cloud sichern" und klicken Sie auf "OK".

Oder klicken Sie auf der Registerkarte "Speicher" in der Gruppe "Speicher konfigurieren" auf "Cloud-Speicher" und dann auf "Weiter".

Alternativ können Sie auf der Registerkarte "Speicher" auf "Cloud-Speicher konfigurieren" klicken.

- 2** Geben Sie den Namen und die Beschreibung des Cloud-Speichergeräts ein und klicken Sie auf "Weiter".
- 3** Wählen Sie in der Liste der Cloud-Speicheranbieter die Option "S3" und klicken Sie auf "Weiter".
- 4** Wählen Sie im Feld "Cloud-Speicher" den Namen des Google-Servers aus der Dropdown-Liste.
- 5** Wählen Sie im Feld "Login-Konto" ein Konto aus der Dropdown-Liste oder klicken Sie auf "Hinzufügen/Bearbeiten", um ein Konto hinzuzufügen.
- 6** Klicken Sie im Dialogfeld "Login-Konto auswählen" auf "Hinzufügen".
- 7** Führen Sie im Dialogfeld "Identifikationsdaten hinzufügen" folgende Schritte durch:
 - Geben Sie im Feld "Benutzername" die ID für den Google-Zugriffsschlüssel ein.
 - Geben Sie im Feld "Kennwort" den geheimen Google-Zugriffsschlüssel ein.
 - Geben Sie im Feld "Kennwort bestätigen" den geheimen Google-Zugriffsschlüssel erneut ein.
 - Geben Sie im Feld "Kontoname" einen Namen für das Login-Konto ein.

In Backup Exec wird dieser in allen Speichergerätelisten als Name des Cloud-Speichergeräts angezeigt.

- 8** Klicken Sie zweimal auf "OK".
- 9** Wählen Sie das Google-Login-Konto aus, das Sie in Schritt 7 erstellt haben, und klicken Sie dann auf "Weiter".
- 10** Wählen Sie ein Bucket aus der Liste der mit dem Servernamen verknüpften Buckets aus und klicken Sie auf "Weiter".

- 11** Geben Sie die Anzahl der gleichzeitig auf diesem Cloud-Speichergerät ausführbaren Schreibvorgänge ein und klicken Sie auf "Weiter".

Diese Einstellung legt die Anzahl von Aufträgen fest, die auf diesem Gerät gleichzeitig ausgeführt werden können. Der geeignete Wert für diese Einstellung hängt von Ihrer Umgebung und der Bandbreite des Cloud-Speichers ab. Sie können den Standardwert auswählen.

- 12** Überprüfen Sie die Konfiguration und klicken Sie auf "Fertigstellen".

Backup Exec erstellt ein Cloud-Speichergerät. Sie müssen die Backup Exec-Dienste neu starten, um das neue Gerät online zu schalten.

- 13** Klicken Sie im Fenster mit der Aufforderung "Backup Exec-Dienste neu starten" auf "Ja".

Nachdem die Dienste neu gestartet wurden, zeigt Backup Exec den neuen Cloud-Speicherort in der Liste "Gesamter Speicher" an.

Cloud-Speicher von Microsoft Azure

Im Folgenden finden Sie Informationen zu den Anforderungen für die Konfiguration eines Microsoft Azure-Speichergeräts und des Microsoft Azure-Speichers in Backup Exec.

Siehe ["Konfigurieren des Speichers für Microsoft Azure Cloud Storage"](#) auf Seite 418.

Anforderungen für die Konfiguration des Cloud-basierten Speichergeräts Microsoft Azure

Mit dem Backup Exec-Cloud Connector können Daten aus dem Cloud-basierten Speichergerät Microsoft Azure gesichert und wiederhergestellt werden.

Überprüfen Sie die folgenden Anforderungen vor der Konfiguration des Cloud-basierten Speichergeräts Microsoft Azure:

- Sie müssen ein Microsoft Azure-Speicherkonto anlegen und über mindestens einen Speicherzugriffsschlüssel verfügen (primärer oder sekundärer Zugriffsschlüssel).
- Zuvor müssen die Blob-Speichercontainer für das Speicherkonto erstellt werden. Blob-Speichercontainer sind logische Speichereinheiten auf dem Cloud-basierten Speichergerät.

Hinweis: Als Best Practice sollten Sie bestimmte Container erstellen, die ausschließlich für Backup Exec verwendet werden.

Jedes Cloud-Speichergerät muss einen anderen Container verwenden. Verwenden Sie nicht denselben Container für mehrere Cloud-Speichergeräte, selbst wenn diese Geräte auf verschiedenen Backup Exec-Servern konfiguriert sind.

- Stellen Sie sicher, dass die Containernamen die folgenden Backup Exec-Anforderungen erfüllen:
 - Containernamen dürfen Kleinbuchstaben, Ziffern und Gedanken- bzw. Bindestriche enthalten.
 - Sie dürfen nicht mit einem Gedanken- bzw. Bindestrich beginnen. Die Container sind nicht in Backup Exec verfügbar, wenn der Name diese Namenskonvention nicht erfüllt. Die unterstützten Regionen finden Sie in der Liste der mit Backup Exec kompatiblen Hardware.

Siehe ["Konfigurieren des Speichers für Microsoft Azure Cloud Storage"](#) auf Seite 418.

Konfigurieren des Speichers für Microsoft Azure Cloud Storage

Sie können ein Cloud-basiertes Speichergerät für den Cloud-Speicher "Microsoft Azure" konfigurieren und dann Daten darauf sichern.

Hinweis: Für Cloud-Speichergeräte ist jetzt standardmäßig die Option "Daten für diesen Auftrag nicht verifizieren" in den "Backup-Optionen" aktiviert. Einige Cloud-Anbieter berechnen Gebühren für Lese- und Schreibvorgänge in der Cloud. Diese Option ist standardmäßig aktiviert, um Belastungen beim Auslesen von Daten beim Verifizieren eines Backups oder Duplizierungsauftrags zu vermeiden.

Siehe ["Konfigurieren der automatischen Prüfung von Aufträgen"](#) auf Seite 655.

Siehe ["Anforderungen für die Konfiguration des Cloud-basierten Speichergeräts Microsoft Azure"](#) auf Seite 417.

So konfigurieren Sie den Cloud-Speicher für Microsoft Azure in Backup Exec

- 1** Wählen Sie auf der Registerkarte "Backup und Wiederherstellung" die Option "Backup > In Cloud sichern" und klicken Sie auf "OK".

Oder klicken Sie auf der Registerkarte "Speicher" in der Gruppe "Speicher konfigurieren" auf "Cloud-Speicher" und dann auf "Weiter".

Alternativ können Sie auf der Registerkarte "Speicher" auf "Cloud-Speicher konfigurieren" klicken.
- 2** Geben Sie den Namen und die Beschreibung des Cloud-Speichergeräts ein und klicken Sie auf "Weiter".
- 3** Wählen Sie in der Liste der Cloud-Speicheranbieter die Option "Azure" und klicken Sie auf "Weiter".
- 4** Wählen Sie im Feld "Cloud-Speicher" den Namen des Microsoft Azure-Servers aus der Dropdown-Liste.
- 5** Wählen Sie im Feld "Login-Konto" ein Konto aus der Dropdown-Liste oder klicken Sie auf "Hinzufügen/Bearbeiten", um ein Konto hinzuzufügen.
- 6** Klicken Sie im Dialogfeld "Login-Konto auswählen" auf "Hinzufügen".
- 7** Führen Sie im Dialogfeld "Identifikationsdaten hinzufügen" folgende Schritte durch:
 - Geben Sie im Feld "Benutzername" den Benutzernamen für den Microsoft Azure-Speicher ein.
 - Geben Sie im Feld "Kennwort" den Zugriffsschlüssel für den Microsoft Azure-Speicher ein. Sie können den primären oder sekundären Zugriffsschlüssel eingeben.
 - Geben Sie im Feld "Kennwort bestätigen" erneut den Zugriffsschlüssel für das Microsoft Azure-Speicherkonto ein.
 - Geben Sie im Feld "Kontoname" einen Namen für das Login-Konto ein. In Backup Exec wird dieser in allen Speichergerätelisten als Name des Cloud-Speichergeräts angezeigt.
- 8** Klicken Sie zweimal auf "OK".
- 9** Wählen Sie das Microsoft Azure-Login-Konto aus, das Sie in Schritt 7 erstellt haben, und klicken Sie auf "Weiter".
- 10** Wählen Sie einen Container aus der Liste der Container, die mit dem vorher angegebenen Servernamen und dem Login-Konto verknüpft sind, und klicken Sie auf "Weiter".

- 11** Geben Sie die Anzahl der gleichzeitig auf diesem Cloud-Speichergerät ausführbaren Schreibvorgänge ein und klicken Sie auf "Weiter".

Diese Einstellung legt die Anzahl von Aufträgen fest, die auf diesem Gerät gleichzeitig ausgeführt werden können. Der geeignete Wert für diese Einstellung hängt von Ihrer Umgebung und der Bandbreite des Cloud-Speichers ab. Sie können den Standardwert auswählen.

- 12** Überprüfen Sie die Konfiguration und klicken Sie auf "Fertigstellen".

Backup Exec erstellt ein Cloud-Speichergerät. Sie müssen die Backup Exec-Dienste neu starten, um das neue Gerät online zu schalten.

- 13** Klicken Sie im Fenster mit der Aufforderung "Backup Exec-Dienste neu starten" auf "Ja".

Nachdem die Dienste neu gestartet wurden, zeigt Backup Exec den neuen Cloud-Speicherort in der Liste "Gesamter Speicher" an.

Privater Cloud-Speicher

Im Folgenden finden Sie Informationen zu den Anforderungen für die Konfiguration eines privaten Speichergeräts und des privaten Speichers in Backup Exec. Außerdem sind Anweisungen zum Erstellen, Anzeigen, Bearbeiten und Löschen einer Cloud-Instanz für eine private Cloud enthalten.

Siehe ["Anforderungen für das Konfigurieren von privaten Cloud-basierten Speichergeräten"](#) auf Seite 420.

Siehe ["Konfigurieren des Speichers für ein privates Cloud-basiertes Speichergerät"](#) auf Seite 423.

Siehe ["Erstellen einer Cloud-Instanz für eine private Cloud"](#) auf Seite 422.

Siehe ["Anzeigen und Bearbeiten vorhandener Cloud-Instanzen für eine private Cloud"](#) auf Seite 424.

Siehe ["Löschen einer Cloud-Instanz für eine private Cloud"](#) auf Seite 425.

Anforderungen für das Konfigurieren von privaten Cloud-basierten Speichergeräten

Mit dem Backup Exec-Cloud Connector können Daten aus einem privaten Cloud-basierten Speichergerät gesichert und wiederhergestellt werden.

Für die Konfiguration eines privaten Cloud-basierten Speichergeräts gelten folgende Anforderungen:

- Konfigurieren Sie den privaten Cloud-basierten Speicher-Server in Ihrer Umgebung.
Erstellen Sie ein Konto für den Zugriff auf den privaten Cloud-basierten Speicherserver, bevor Sie ein Cloud-Speichergerät in Backup Exec konfigurieren. Fordern Sie außerdem die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel des Servers des privaten Cloud-basierten Speicherservers an.
- Stellen Sie sicher, dass der Bucket bereits auf dem privaten Cloud-Speicherserver erstellt wurde. Buckets sind logische Speichereinheiten auf dem Cloud-basierten Speichergerät.

Hinweis: Als Best Practice sollten Sie bestimmte Buckets erstellen, die ausschließlich für Backup Exec verwendet werden.

Jedes Cloud-Speicher-Gerät muss einen anderen Bucket verwenden. Verwenden Sie nicht den gleichen Bucket für mehrere Cloud-Speicher-Geräte, selbst wenn diese Geräte auf verschiedenen Backup Exec-Servern konfiguriert sind.

- Stellen Sie sicher, dass die Bucket-Namen die folgenden Backup Exec-Anforderungen erfüllen:
 - Bucket-Namen dürfen Kleinbuchstaben, Ziffern und Gedanken- bzw. Bindestriche enthalten.
 - Sie dürfen nicht mit einem Gedanken- bzw. Bindestrich beginnen.

Hinweis: Die Buckets sind nicht in Backup Exec verfügbar, wenn der Name diese Namenskonvention nicht erfüllt.

- Erstellen Sie eine Cloud-Instanz für den privaten Cloud-Speicherserver. Siehe ["Erstellen einer Cloud-Instanz für eine private Cloud"](#) auf Seite 422.
- Stellen Sie sicher, dass der private Cloud-basierte Speicherserver ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat enthält. Backup Exec unterstützt bei der Kommunikation mit Cloud-Speichern im SSL-Modus nur von der Zertifizierungsstelle (Certificate Authority, CA) signierte Zertifikate. Andernfalls kann die Datenübertragung zwischen Backup Exec und dem Anbieter der privaten Cloud im SSL-Modus fehlschlagen.
Beim Erstellen der Cloud-Instanz kann das SSL-Protokoll verwendet werden. Backup Exec unterstützt Backups auf einem privaten Cloud-Speicher auch dann, wenn Sie sich beim Erstellen der Cloud-Instanz gegen die Verwendung des SSL-Protokolls entscheiden.

Die unterstützten Regionen finden Sie in der Liste der mit Backup Exec kompatiblen Hardware.

Siehe ["Konfigurieren des Speichers für ein privates Cloud-basiertes Speichergerät"](#) auf Seite 423.

Erstellen einer Cloud-Instanz für eine private Cloud

Vor dem Konfigurieren eines Cloud-Speichergeräts für einen privaten Cloud-Anbieter müssen Sie eine benutzerdefinierte Cloud-Instanz für den privaten Cloud-Speicherserver erstellen.

Geben Sie zum Erstellen einer benutzerdefinierten Cloud-Instanz in BEMCLI folgenden Befehl ein:

```
New-BECloudInstance
```

Sie müssen diesen Befehl ausführen, bevor Sie ein Speichergerät für eine private Cloud erstellen.

Stellen Sie sicher, dass der Cloud-Instanz-Name die folgenden Backup Exec-Anforderungen erfüllt:

- Er darf Buchstaben, Ziffern und Gedanken- bzw. Bindestriche enthalten.
- Er darf nicht mit einem Gedanken- bzw. Bindestrich beginnen.

Hinweis: Sie dürfen nur eine Cloud-Instanz für einen privaten Cloud-Speicher-Server pro Backup Exec-Server erstellen. Sie können eine weitere Cloud-Instanz für denselben privaten Cloud-Speicher-Server auf einem anderen Backup Exec-Server erstellen.

Weitere Informationen zur Backup Exec-Befehlszeilenschnittstelle und den dazugehörigen Befehlen finden Sie in der Hilfedatei "BEMCLI" im Standard-Installationsverzeichnis:

```
C:<Backup Exec-Installationsordner>\Backup Exec
```

Siehe ["Konfigurieren des Speichers für ein privates Cloud-basiertes Speichergerät"](#) auf Seite 423.

Siehe ["Anforderungen für das Konfigurieren von privaten Cloud-basierten Speichergeräten"](#) auf Seite 420.

Konfigurieren des Speichers für ein privates Cloud-basiertes Speichergerät

Sie können ein privates Cloud-basiertes Speichergerät konfigurieren und anschließend Daten darauf sichern. Vor dem Konfigurieren eines Cloud-Speichergeräts für einen privaten Cloud-Speicherserver müssen Sie eine benutzerdefinierte Cloud-Instanz für den privaten Cloud-Speicherserver erstellen.

Hinweis: Für Cloud-Speichergeräte ist jetzt standardmäßig die Option "Daten für diesen Auftrag nicht verifizieren" in den "Backup-Optionen" aktiviert. Einige Cloud-Anbieter berechnen Gebühren für Lese- und Schreibvorgänge in der Cloud. Diese Option ist standardmäßig aktiviert, um Belastungen beim Auslesen von Daten beim Verifizieren eines Backups oder Duplizierungsauftrags zu vermeiden.

Siehe ["Konfigurieren der automatischen Prüfung von Aufträgen"](#) auf Seite 655.

Siehe ["Erstellen einer Cloud-Instanz für eine private Cloud"](#) auf Seite 422.

Siehe ["Hinzufügen einer Stufe zu einer Backup-Definition"](#) auf Seite 244.

Siehe ["Anforderungen für das Konfigurieren von privaten Cloud-basierten Speichergeräten"](#) auf Seite 420.

So konfigurieren Sie den Speicher für ein privates Cloud-basiertes Speichergerät

- 1 Wählen Sie auf der Registerkarte "Backup und Wiederherstellung" die Option "Backup > In Cloud sichern" und klicken Sie auf "OK".

Oder klicken Sie auf der Registerkarte "Speicher" in der Gruppe "Speicher konfigurieren" auf "Cloud-Speicher" und dann auf "Weiter".

Alternativ können Sie auf der Registerkarte "Speicher" auf "Cloud-Speicher konfigurieren" klicken.
- 2 Geben Sie den Namen und die Beschreibung des Cloud-Speichergeräts ein und klicken Sie auf "Weiter".
- 3 Wählen Sie in der Liste der Cloud-Speicheranbieter die Option "S3" und klicken Sie auf "Weiter".
- 4 Wählen Sie im Feld "Cloud-Speicher" den Namen des privaten Cloud-basierten Speicherservers aus der Dropdown-Liste.
- 5 Wählen Sie im Feld "Login-Konto" ein Konto aus der Dropdown-Liste oder klicken Sie auf "Hinzufügen/Bearbeiten", um ein Konto hinzuzufügen.
- 6 Klicken Sie im Dialogfeld "Login-Konto auswählen" auf "Hinzufügen".

- 7 Führen Sie im Dialogfeld "Identifikationsdaten hinzufügen" folgende Schritte durch:
 - Geben Sie im Feld "Benutzername" die ID für den Zugriffsschlüssel des privaten Cloud-basierten Speicherkontos ein.
 - Geben Sie im Feld "Kennwort" den geheimen Zugriffsschlüssel für das private Cloud-basierte Speichergerät ein.
 - Geben Sie im Feld "Kennwort bestätigen" den geheimen Zugriffsschlüssel erneut ein.
 - Geben Sie im Feld "Kontoname" einen Namen für das Login-Konto ein.

In Backup Exec wird dieser in allen Speichergerätelisten als Name des Cloud-Speichergeräts angezeigt.
- 8 Klicken Sie zweimal auf "OK".
- 9 Wählen Sie das Login-Konto aus, das Sie in Schritt 7 erstellt haben, und klicken Sie auf "Weiter".
- 10 Wählen Sie ein Bucket aus der Liste der mit dem Servernamen verknüpften Buckets aus und klicken Sie auf "Weiter".
- 11 Geben Sie die Anzahl der gleichzeitig auf diesem Cloud-Speichergerät ausführbaren Schreibvorgänge ein und klicken Sie auf "Weiter".

Diese Einstellung legt die Anzahl von Aufträgen fest, die auf diesem Gerät gleichzeitig ausgeführt werden können. Der geeignete Wert für diese Einstellung hängt von Ihrer Umgebung und der Bandbreite des Cloud-Speichers ab. Sie können den Standardwert auswählen.
- 12 Überprüfen Sie die Konfiguration und klicken Sie auf "Fertigstellen".

Backup Exec erstellt ein Cloud-Speichergerät. Sie müssen die Backup Exec-Dienste neu starten, um das neue Gerät online zu schalten.
- 13 Klicken Sie im Fenster mit der Aufforderung "Backup Exec-Dienste neu starten" auf "Ja".

Nachdem die Dienste neu gestartet wurden, zeigt Backup Exec den neuen Cloud-Speicherort in der Liste "Gesamter Speicher" an.

Anzeigen und Bearbeiten vorhandener Cloud-Instanzen für eine private Cloud

Geben Sie zum Anzeigen einer benutzerdefinierten Cloud-Instanz in BEMCLI folgenden Befehl ein:

```
Get-BECloudInstance
```

Geben Sie zum Bearbeiten einer benutzerdefinierten Cloud-Instanz in BEMCLI folgenden Befehl ein:

```
Set-BECloudInstance
```

Hinweis: Sie können Name und Anbieter einer benutzerdefinierten Cloud-Instanz nicht bearbeiten.

Sie dürfen nur eine Cloud-Instanz für einen privaten Cloud-Speicher-Server pro Backup Exec-Server erstellen. Sie können eine weitere Cloud-Instanz für denselben privaten Cloud-Speicher-Server auf einem anderen Backup Exec-Server erstellen.

Weitere Informationen zur Backup Exec-Befehlszeilenschnittstelle und den dazugehörigen Befehlen finden Sie in der Hilfedatei "BEMCLI" im Standard-Installationsverzeichnis:

```
C:<Backup Exec-Installationsordner>\Backup Exec
```

Siehe ["Erstellen einer Cloud-Instanz für eine private Cloud"](#) auf Seite 422.

Siehe ["Löschen einer Cloud-Instanz für eine private Cloud"](#) auf Seite 425.

Löschen einer Cloud-Instanz für eine private Cloud

Geben Sie zum Löschen einer benutzerdefinierten Cloud-Instanz in BEMCLI folgenden Befehl ein:

```
Remove-BECloudInstance
```

Hinweis: Löschen Sie vorher die entsprechenden Speichergeräte, die mit dieser Cloud-Instanz verbunden sind.

Siehe ["Löschen von Speichergeräten"](#) auf Seite 546.

Weitere Informationen zur Backup Exec-Befehlszeilenschnittstelle und den dazugehörigen Befehlen finden Sie in der Hilfedatei "BEMCLI" im Standard-Installationsverzeichnis:

```
C:<Backup Exec-Installationsordner>\Backup Exec
```

Siehe ["Erstellen einer Cloud-Instanz für eine private Cloud"](#) auf Seite 422.

Informationen zu S3-kompatiblen Cloud-Speicher

Backup Exec enthält die Funktion "S3-kompatibler Cloud-Speicher". Sie können den S3-Provider verwenden, um mit S3 kompatible Cloud-Speichergeräte mit Backup Exec zu konfigurieren.

Nach Abschluss der Konfiguration können Sie ein Speichergerät in der Backup Exec-Konsole erstellen, das auf die meisten mit S3 kompatiblen Cloud-Umgebungen zugreifen kann. Mit S3 kompatible Kommunikationen wurden nicht in allen Cloud-Umgebungen getestet und funktionieren eventuell in bestimmten Fällen nicht.

Mit S3 kompatible Umgebungen, die nicht ausdrücklich in der Liste der Hardwarekompatibilitätsliste von Backup Exec aufgeführt sind, werden als alternative Konfigurationen angesehen. Alternative Konfiguration werden folgendermaßen definiert:

Alternative Konfigurationen : Die lizenzierte Software ist auf die Zusammenarbeit mit vielen Typen von Computern, Anwendungen und Hardware ausgelegt. Gelegentlich kann ein Kunde die lizenzierte Software in einer "alternativen Konfiguration" ausführen, also einer Umgebung, die nicht für den Betrieb mit der lizenzierten Software validiert, genehmigt oder verifiziert wurde oder die die lizenzierte Software nicht oder nur teilweise unterstützt. In den meisten Fällen stellen wir keinen Support zur Verfügung, wenn die lizenzierte Software in einer alternativen Konfiguration ausgeführt wird. Es wird keine Garantie im Bezug auf den Einsatz der lizenzierten Software in einer anderen Konfiguration übernommen. Ein solcher Einsatz erfolgt auf Ihr eigenes Risiko. Eine "unterstützte Konfiguration" kann in eine alternative Konfiguration konvertiert werden, falls der Hersteller eine der Komponenten ändert. Die lizenzierte Software wird dann in einer alternativen Konfiguration ausgeführt. Sollten beim Ausführen der lizenzierten Software in einer anderen Konfiguration Probleme auftreten, oder ein Problem mit einem Skript auftreten, das nicht von einem beratenden Partner entwickelt wurde, bitten wir Sie eventuell, das Problem in einer unterstützten Konfiguration zu reproduzieren. Beachten Sie, dass wir nicht verpflichtet sind, Probleme, die in einer unterstützten Konfiguration nicht repliziert werden können, zu beheben. Ist dies jedoch möglich, werden wir das Problem untersuchen und versuchen, es zu beheben. Ist dies nicht möglich, werden wir das Problem eventuell nicht untersuchen.

Siehe ["Cloud-Speicher von Amazon S3"](#) auf Seite 411.

Siehe ["Cloud-Speicher von Google"](#) auf Seite 414.

Siehe ["Privater Cloud-Speicher"](#) auf Seite 420.

Siehe ["Konfigurieren des S3-kompatiblen Cloud-Speichers mit Backup Exec"](#) auf Seite 427.

Konfigurieren des S3-kompatiblen Cloud-Speichers mit Backup Exec

Sie können S3-kompatible Cloud-Speicher konfigurieren, auf die Backup Exec zugreifen kann.

So konfigurieren Sie einen S3-kompatiblen Cloud-Speicher mit Backup Exec

- 1 Konfigurieren Sie eine Cloud-Instanz mit der Backup Exec-Befehlszeilenschnittstelle (BEMCLI) und geben Sie die Cloud-Adresse und die Konfigurationsparameter für den Backup Exec-Server an.

Zum Konfigurieren einer Cloud-Instanz müssen Sie vorher ein Benutzerkonto und Buckets in der Cloud-Umgebung konfigurieren.

Beispiel für einen Befehl für S3:

```
New-BECloudInstance -Name "Cloud-Instanz0001" -Provider  
"compatible-with-s3" - ServiceHost "s3.endgerät.de" -SslMode  
"Disabled" -HttpPort 80 - HttpsPort 443
```

Dabei wird der Wert von "ServiceHost" durch die Adresse des Cloud-Server-Endgeräts ersetzt.

In diesem Beispiel ist der Wert für "SslMode" "Disabled" (deaktiviert). Backup Exec unterstützt das SSL-Protokoll. Beim Erstellen der Cloud-Instanz kann das SSL-Protokoll verwendet werden. Es wird empfohlen, SslMode auf Enabled zu setzen.

Stellen Sie sicher, dass der mit S3 kompatible Cloud-Speicherserver ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat enthält. Backup Exec unterstützt bei der Kommunikation mit mit S3 kompatiblen Cloud-Speichern im SSL-Modus nur von der Zertifizierungsstelle (Certificate Authority, CA) signierte Zertifikate. Andernfalls kann die Datenübertragung zwischen Backup Exec und dem S3-Cloud-Anbieter im SSL-Modus fehlschlagen.

- 2 Erstellen Sie ein Cloud-Speichergerät in Backup Exec mit dem Konfigurationsassistenten für Speichergeräte. Wählen Sie dann die neu erstellte Cloud-Instanz aus und geben Sie die Zugangsdaten für das S3-Konto für den Zugriff auf den mit S3 kompatiblen Cloud-Server an.

Siehe ["Cloud-Speicher von Amazon S3"](#) auf Seite 411.

Siehe ["Cloud-Speicher von Google"](#) auf Seite 414.

Siehe ["Privater Cloud-Speicher"](#) auf Seite 420.

Siehe ["Informationen zu S3-kompatiblen Cloud-Speicher"](#) auf Seite 426.

Bearbeiten der Eigenschaften eines Cloud-basierten Speichergeräts

Sie können alle Eigenschaften eines Cloud-Speichergeräts anzeigen und einige der Eigenschaften ändern.

So bearbeiten Sie die Eigenschaften eines Cloud-basierten Speichergeräts

- 1** Doppelklicken Sie auf der Registerkarte "Speicher" auf den Namen des Cloud-Speichergeräts.
- 2** Klicken Sie im linken Teilfenster auf "Eigenschaften".

3 Ändern Sie die Eigenschaften nach Bedarf:

Name	<p>Zeigt den benutzerdefinierten Namen für dieses Cloud-Speichergerät an.</p> <p>Sie können dieses Feld ändern.</p>
Beschreibung	<p>Zeigt die benutzerdefinierte Beschreibung dieses Cloud-Speichergeräts an.</p> <p>Sie können dieses Feld ändern.</p>
Status	<p>Zeigt den aktuellen Status des Geräts an.</p> <p>Sie können dieses Feld nicht ändern.</p>
Cloud-Speicher	<p>Gibt den vollqualifizierten Namen des Servers an, auf dem sich das Gerät befindet.</p> <p>Sie können dieses Feld nicht ändern.</p>
Speicherort	<p>Gibt den Namen des Servers an, auf dem sich das Gerät befindet.</p> <p>Sie können dieses Feld nicht ändern.</p>
Speichertyp	<p>Gibt den Typ des Cloud-Speichergeräts an.</p> <p>Sie können dieses Feld nicht ändern.</p>
Bucket-/Speichercontainer	<p>Zeigt den Namen des Speicherorts auf dem Cloud-Speichergerät an. Diese Speichereinheiten werden als "Buckets" bezeichnet.</p> <p>Sie können dieses Feld nicht ändern.</p>
Speicherebene	<p>Gibt den Namen der Speicherebene an.</p> <p>Sie können dieses Feld nicht ändern.</p> <p>Hinweis: In diesem Feld wird der Wert "N" angezeigt, wenn für ein Cloud-Speichergerät keine Speicherebenen unterstützt werden.</p>

Backup Exec-Server mit Gerätenäherung	<p>Zeigt den Backup Exec-Server an, der eine physische oder logische Nähe zum Speichergerät aufweist, um Vorgänge für das Gerät auszuführen.</p> <p>Verwenden Sie dieses Feld in einer CAS-Umgebung.</p>
Login-Konto	<p>Gibt den Namen des Login-Kontos an, das für den Zugriff auf das Gerät erforderlich ist.</p> <p>Sie können dieses Feld ändern.</p>
Gleichzeitige Vorgänge	<p>Gibt die maximale Zahl der Aufträge an, die Sie auf diesem Gerät gleichzeitig ausführen möchten.</p> <p>Sie können dieses Feld ändern.</p>
Geschriebene Backup-Daten	<p>Zeigt nur den Speicherplatz für die gesicherten Daten an.</p>
Verbindungstyp	<p>Zeigt den Typ der Verbindung zwischen dem Backup Exec-Server und dem Cloud-Speichergerät an. Die Verbindungsart ist "Netzwerk".</p> <p>Sie können dieses Feld nicht ändern.</p>
Neustart von Backup Exec-Dienst erforderlich	<p>Gibt an, ob die Backup Exec-Dienste neu gestartet werden müssen, um Änderungen, die an diesem Gerät vorgenommen werden, zu übernehmen.</p> <p>Sie können dieses Feld nicht ändern.</p>

- 4** Klicken Sie auf "Übernehmen", um die Änderungen zu speichern.

Best Practices beim Einsatz von Cloud-basiertem Speicher

Tabelle 9-1 Best Practices beim Einsatz von Cloud-basiertem Speicher

Element	Best Practice
Datenverschlüsselung beim Sichern von Daten auf einem öffentlichen Cloud-Speichergerät	<p>Bestimmte Anbieter von öffentlichen Cloud-Speicherdiensten verlangen, dass die Verschlüsselung aktiviert ist, wenn Backup-Aufträge oder doppelte Aufträge auf den Cloud-Speicher angewendet werden.</p> <p>Alle Daten sind unter Verwendung von SSL während der Datenübertragung aus Backup Exec auf ein öffentliches Cloud-Speichergerät geschützt. Allerdings muss für Backup Exec-Aufträge die Verschlüsselung aktiviert sein, um die Daten im Ruhezustand im öffentlichen Cloud-Speicher zu verschlüsseln.</p> <p>Siehe "Verwendung von Verschlüsselung mit Backup Exec" auf Seite 727.</p>
Netzwerknutzung und Backups auf einem Cloud-Speichergerät	<p>Während der Datenübertragung benötigen Cloud-basierte Speichergeräte eine hohe Bandbreite. Dies könnte dazu führen, dass andere kritische Anwendungen, die gleichzeitig ausgeführt werden, nicht mehr ordnungsgemäß funktionieren. Daher wird empfohlen, dass Sie Backup-Aufträge auf ein Cloud-Speichergerät zu einer Zeit planen, wenn andere Anwendungen nur eine geringe Bandbreite benötigen.</p>

Element	Best Practice
Backup Exec CloudConnect Optimizer	<p>Best Practices für Backup Exec CloudConnect Optimizer</p> <ul style="list-style-type: none"> ■ Wenn Sie mehrere Geräte für den gleichen Cloud-Anbieter haben, können Sie den CloudConnect-Optimizer-Auftrag für ein beliebiges Gerät ausführen, da der vorgeschlagene Schreibverbindungs Wert für alle Geräte dieses Cloud-Servertyps gilt. ■ Führen Sie den CloudConnect-Optimizer-Auftrag nahe des geplanten Zeitpunkts des Backup-Auftrags aus, damit der Berater- und Cloud-Backup-Auftrag in einer ähnlichen Netzwerkumgebung ausgeführt wird. Stellen Sie sicher, dass Zeit verfügbar ist, damit der CloudConnect-Optimizer-Auftrag abgeschlossen ist, bevor der Cloud-Backup-Auftrag gestartet wird. ■ Wenn der CloudConnect Optimizer-Auftrag ausgeführt wird, dürfen zur selben Zeit keine Cloud-Backups ausgeführt werden. Dadurch soll gewährleistet werden, dass keine anderen Backup-Aufträge die Netzwerkbandbreite gemeinsam mit Backup Exec CloudConnect Optimizer nutzen. ■ Es wird empfohlen, dass Sie den CloudConnect Optimizer-Auftrag ausführen, wenn Sie ein Cloud-Speichergerät konfigurieren, und zwar nachdem die Backup Exec-Dienste neu gestartet wurden. <p>Siehe "Info zu Backup Exec™ CloudConnect Optimizer" auf Seite 434.</p> <p>Siehe "Konfigurieren von Backup Exec™ CloudConnect Optimizer" auf Seite 435.</p> <p>Siehe "Bearbeiten des CloudConnect Optimizer-Auftrags" auf Seite 436.</p> <p>Siehe "Löschen des CloudConnect Optimizer-Auftrags" auf Seite 437.</p>

Ändern der Standardeinstellungen für Cloud-Speicher

Die Standardeinstellungen für Cloud-Speicher sind jetzt in Backup Exec aktiviert, um die Lese-/Schreibfehler zu verringern, die auftreten, wenn das Netzwerk nicht in der Lage ist, die Anzahl aller Verbindungen aus dem Backup Exec-Medienserver zum Cloud-Speicheranbieter zu bewältigen.

Diese Verbindungen zur Cloud werden zum Auslesen von Daten aus der Cloud und zum Speichern von Daten in der Cloud aufgebaut. Dies ist die maximale Anzahl Verbindungen, die Backup Exec öffnen kann.

Derzeit wird der maximale Wert für den Verbindungsbereich der Lese-/Schreibverbindungen automatisch eingestellt. Es wird empfohlen, die eingestellten Werte nur dann zu ändern, wenn aufgrund von Problemen mit dem Netzwerk oder der Bandbreite durch einen dieser Werte die Backup-Erstellung regelmäßig fehlschlägt. In diesem Fall führen Sie Backup Exec CloudConnect Optimizer aus. Dieser schlägt die Anzahl der Schreibverbindungen für einen Backup-Auftrag in Ihrer Umgebung vor.

Backup Exec CloudConnect Optimizer zeigt ein Auftragsprotokoll mit der vorgeschlagenen Anzahl Schreibverbindungen für den spezifischen Cloud-Servertyp an. Dieser Wert wird in den Backup Exec-Einstellungen aktualisiert, wenn Sie in Backup Exec CloudConnect Optimizer das Kontrollkästchen "Vorgeschlagene Anzahl Schreibverbindungen für anstehende Aufträge verwenden" aktivieren.

Siehe ["Konfigurieren von Backup Exec™ CloudConnect Optimizer"](#) auf Seite 435.

Sie können die Werte für die Lese-/Schreibverbindungen für jeden von Backup Exec unterstützten Cloud-Speicher-Servertyp ändern. Es wird empfohlen, die eingestellten Werte für die Lese-/Schreibverbindungen bei Backup- und Wiederherstellungsaufträgen nur dann zu ändern, wenn Probleme mit dem Netzwerk oder der Bandbreite auftreten. Weitere Informationen finden Sie im Best Practices-Dokument zu Backup Exec.

So ändern Sie die Speicher-Standard Einstellungen

- 1 Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie auf "Backup Exec-Einstellungen".
- 2 Klicken Sie auf der linken Seite auf "Cloud-Speicher".
- 3 Bearbeiten Sie eine der folgenden Optionen:

Cloud-Servertyp	Zeigt den Cloud-Servertyp an.
Verbindungsbereich	Zeigt den Verbindungsbereich für jeden Cloud-Servertyp an.
Leseverbindungen	<p>Hier können Sie die Anzahl der Leseverbindungen für jeden Cloud-Servertyp auswählen. Der automatisch eingestellte Wert für jeden Cloud-Server ist bereits ausgewählt.</p> <p>Die automatisch eingestellten Werte werden gemäß den Best Practices von Backup Exec ausgewählt.</p>
Schreibverbindungen	<p>Hier können Sie die Anzahl der Schreibverbindungen für jeden Cloud-Servertyp auswählen. Der automatisch eingestellte Wert für jeden Cloud-Server ist bereits ausgewählt.</p> <p>Die automatisch eingestellten Werte werden gemäß den Best Practices von Backup Exec ausgewählt.</p>

Info zu Backup Exec™ CloudConnect Optimizer

Führen Sie Backup Exec CloudConnect Optimizer aus, um eine vorgeschlagene Anzahl von Schreibverbindungen anzuzeigen, die die verfügbare Bandbreite nutzen. Nach Abschluss des CloudConnect Optimizer-Auftrags zeigt das Protokoll das Ergebnis und die vorgeschlagene Anzahl Schreibverbindungen an.

Siehe ["Ändern der Standardeinstellungen für Cloud-Speicher"](#) auf Seite 432.

Nachdem Sie CloudConnect Optimizer für ein beliebiges Cloud-Speichergerät ausgeführt haben, wird im Auftragsprotokoll die vorgeschlagene Anzahl Schreibverbindungen für den spezifischen Cloud-Servertyp angezeigt. Dieser Wert wird in den Backup Exec-Einstellungen aktualisiert, wenn Sie in CloudConnect Optimizer das Kontrollkästchen "Vorgeschlagene Anzahl Schreibverbindungen für anstehende Aufträge verwenden" aktivieren.

Dieser Wert ist spezifisch für den Cloud-Servertyp. Mehrere Cloud-Geräte können denselben Cloud-Servertyp haben. In diesem Fall ist der vorgeschlagene Wert für alle Cloud-Geräte dieses Typs identisch. Wenn Sie mehrere Geräte mit

unterschiedlichen Cloud-Anbietern auswählen, müssen Sie den CloudConnect Optimizer-Auftrag für jedes Gerät ausführen.

Es wird empfohlen, dass Sie den CloudConnect Optimizer-Auftrag nahe des geplanten Zeitpunkts des Backup-Auftrags und zur gleichen Zeit keine anderen Backup-Aufträge ausführen.

Siehe ["Konfigurieren von Backup Exec™ CloudConnect Optimizer"](#) auf Seite 435.

Siehe ["Bearbeiten des CloudConnect Optimizer-Auftrags"](#) auf Seite 436.

Siehe ["Löschen des CloudConnect Optimizer-Auftrags"](#) auf Seite 437.

Konfigurieren von Backup Exec™ CloudConnect Optimizer

Sie können den CloudConnect Optimizer-Auftrag konfigurieren und ausführen, um einen vorgeschlagenen Wert für die Anzahl Schreibverbindungen abzurufen.

So konfigurieren Sie den CloudConnect Optimizer-Auftrag

- 1** Klicken Sie auf der Registerkarte "Speicher" mit der rechten Maustaste auf ein Cloud-Speichergerät und wählen Sie die Option "CloudConnect Optimizer".
- 2** Bearbeiten Sie im Dialogfeld "Backup Exec CloudConnect Optimizer" auf der Registerkarte "Allgemein" beliebige der folgenden Optionen:

Auftragsname	Zeigt einen Namen für den CloudConnect Optimizer-Auftrag an. Sie können diesen bearbeiten.
Cloud-Servertyp	Zeigt den Cloud-Servertyp an.
Vorgeschlagene Anzahl Schreibverbindungen für anstehende Aufträge verwenden	Aktivieren Sie dieses Kontrollkästchen, um den vorgeschlagenen Wert in den Backup Exec-Einstellungen zu aktualisieren.

- 3** Klicken Sie auf die Registerkarte "Zeitplan".

- 4** Bearbeiten Sie in den Einstellungen für den Zeitplan beliebige der folgenden Optionen:

Jetzt ausführen	Führt den Auftrag sofort aus.
Ausführen am	Plant den Auftrag für ein bestimmtes Datum und eine bestimmte Uhrzeit.

- 5** Klicken Sie auf "OK".

Der CloudConnect Optimizer-Auftrag wird entsprechend der Einstellung entweder sofort oder nach Zeitplan ausgeführt.

Bei CAS-MMS können Sie auf dem Central Admin Server (CAS) einen CloudConnect Optimizer-Auftrag nur für die Geräte erstellen, die lokal auf dem CAS sind oder mit dem CAS gemeinsam genutzt werden. Für Geräte auf dem Managed Media Server (MMS) kann ein CloudConnect Optimizer-Auftrag nur auf diesem MMS erstellt werden. Wird ein Cloud-Speichergerät von einem CAS und MMS gemeinsam genutzt, und soll der Auftrag auf dem MMS ausgeführt werden, dürfen Sie ihn nur auf dem MMS erstellen. Der CloudConnect Optimizer-Auftrag wird auf dem Medienserver ausgeführt, auf dem er erstellt wurde.

Der Auftrag wird auf den Registerkarten "Auftragsüberwachung" und "Speicher" angezeigt. Wenn der Auftrag für einen späteren Zeitpunkt geplant ist, wird der Status "Geplant" angezeigt. Nach Abschluss des Auftrags werden in den Abschnitten "Auftragsüberwachung > Auftragsverläufe" und "Speicher > Auftragsverlauf" Details zum Auftrag und dessen Status angezeigt.

Nach Abschluss des CloudConnect Optimizer-Auftrags zeigt das Auftragsprotokoll den vorgeschlagenen Wert für die Anzahl Schreibverbindungen an. Wenn Sie das Kontrollkästchen zum Aktualisieren des vorgeschlagenen Werts in den Backup Exec-Einstellungen aktiviert haben, wird dieser Wert aktualisiert und für die anstehenden Aufträge verwendet. Eine Bestätigungsmeldung wird angezeigt, dass der Wert in den Backup Exec-Einstellungen aktualisiert wurde.

Siehe ["Ändern der Standardeinstellungen für Cloud-Speicher"](#) auf Seite 432.

Siehe ["Info zu Backup Exec™ CloudConnect Optimizer"](#) auf Seite 434.

Siehe ["Bearbeiten des CloudConnect Optimizer-Auftrags"](#) auf Seite 436.

Siehe ["Löschen des CloudConnect Optimizer-Auftrags"](#) auf Seite 437.

Bearbeiten des CloudConnect Optimizer-Auftrags

Sie können einen geplanten CloudConnect Optimizer-Auftrag bearbeiten.

So bearbeiten Sie den CloudConnect Optimizer-Auftrag

1 Sie haben folgende Möglichkeiten:

So bearbeiten Sie einen CloudConnect Optimizer-Auftrag auf der Registerkarte "Auftragsüberwachung"	Klicken Sie mit der rechten Maustaste auf der Registerkarte "Auftragsüberwachung" auf den geplanten CloudConnect Optimizer-Auftrag und dann auf "Bearbeiten".
So bearbeiten Sie einen CloudConnect Optimizer-Auftrag auf der Registerkarte "Speicher"	Klicken Sie mit der rechten Maustaste auf der Registerkarte "Speicher" auf den geplanten CloudConnect Optimizer-Auftrag und dann auf "Bearbeiten".

2 Nehmen Sie im Dialogfeld "CloudConnect Optimizer" die gewünschten Änderungen vor.

3 Klicken Sie auf "OK".

Siehe ["Info zu Backup Exec™ CloudConnect Optimizer"](#) auf Seite 434.

Siehe ["Konfigurieren von Backup Exec™ CloudConnect Optimizer"](#) auf Seite 435.

Siehe ["Löschen des CloudConnect Optimizer-Auftrags"](#) auf Seite 437.

Löschen des CloudConnect Optimizer-Auftrags

Sie können einen geplanten CloudConnect Optimizer-Auftrag bearbeiten.

So löschen Sie einen CloudConnect Optimizer-Auftrag

1 Sie haben folgende Möglichkeiten:

So löschen Sie einen CloudConnect Optimizer-Auftrag auf der Registerkarte "Auftragsüberwachung"	Suchen Sie auf der Registerkarte "Auftragsüberwachung" den zu löschenden geplanten CloudConnect Optimizer-Auftrag.
So löschen Sie einen CloudConnect Optimizer-Auftrag auf der Registerkarte "Speicher"	Suchen Sie auf der Registerkarte "Speicher" den zu löschenden geplanten CloudConnect Optimizer-Auftrag.

2 Klicken Sie mit der rechten Maustaste auf den geplanten Auftrag und klicken Sie dann auf "Löschen".

3 Klicken Sie auf "Ja".

Siehe ["Info zu Backup Exec™ CloudConnect Optimizer"](#) auf Seite 434.

Siehe ["Konfigurieren von Backup Exec™ CloudConnect Optimizer"](#) auf Seite 435.

Siehe ["Bearbeiten des CloudConnect Optimizer-Auftrags"](#) auf Seite 436.

Veraltete Backup-to-Disk-Ordner

In diesem Kapitel werden folgende Themen behandelt:

- [Veraltete Backup-to-Disk-Ordner](#)

Veraltete Backup-to-Disk-Ordner

In den vorherigen Versionen von Backup Exec konnten Sie mithilfe der Backup-to-Disk-Funktion Daten in einem Ordner auf einer Festplatte sichern. Diese älteren Backup-to-Disk-Ordner sind jetzt schreibgeschützt. Sie können weiter Daten aus einem Backup-to-Disk-Ordner inventarisieren, katalogisieren und wiederherstellen. Sie können standortfernes Simplified Disaster Recovery verwenden, um eine Notfallwiederherstellung von Backup-to-Disk-Ordnern durchzuführen.

Im Windows Explorer werden die Backup-to-Disk-Ordner in dem Pfad angezeigt, den Sie beim Hinzufügen der Ordner angegeben haben. Die Backup-to-Disk-Dateien haben die Dateierweiterung "BKF". Jeder Backup-to-Disk-Ordner enthält die Dateien "changer.cfg" und "folder.cfg", in denen Informationen zu den Backup-to-Disk-Dateien gespeichert werden.

Hinweis: Die Dateien "changer.cfg" und "folder.cfg" dürfen nicht gelöscht oder geändert werden.

Unter einem Backup-to-Disk-Ordner wird ein Unterordner angezeigt, dessen Name mit "IMG" beginnt.

In älteren Versionen erstellte Backup Exec diesen Unterordner, wenn die folgenden Bedingungen in einem Backup-Auftrag erfüllt waren:

- Die Option zum Aktivieren der Granular Recovery Technology (GRT) war ausgewählt.
- Ein Backup-to-Disk-Ordner war als Speicher für die Backup-Daten ausgewählt.

Sie können Backup-Daten nicht an einen Backup-to-Disk-Ordner senden. Es wird empfohlen, Daten auf einem plattenbasierten Speichergerät zu sichern.

Siehe ["Funktionen und Typen des plattenbasierten und netzwerkbasieren Speichers"](#) auf Seite 367.

Siehe ["Wiederherstellen von Daten aus einem veralteten Backup-to-Disk-Ordner"](#) auf Seite 443.

Siehe ["Ändern des Speicherorts eines älteren Backup-to-Disk-Ordners"](#) auf Seite 441.

Siehe ["Erneutes Erstellen eines veralteten Backup-to-Disk-Ordners einschließlich des Inhalts"](#) auf Seite 442.

Den Namen oder die Beschreibung eines veralteten Backup-to-Disk-Ordners ändern

Sie können den Namen und die Beschreibung von Backup-to-Disk-Ordnern bearbeiten.

Siehe ["Veraltete Backup-to-Disk-Ordner"](#) auf Seite 439.

Den Namen oder die Beschreibung eines veralteten Backup-to-Disk-Ordners ändern

- 1 Doppelklicken Sie auf der Registerkarte "Speicher" auf den Backup-to-Disk-Ordner, dessen Namen oder Beschreibung Sie bearbeiten möchten.
- 2 Klicken Sie im linken Teilfenster auf "Eigenschaften".
- 3 Ändern Sie eine der folgenden Eigenschaften:

"Name"

Zeigt den Namen des Backup-to-Disk-Ordners an. Namen von Backup-to-Disk-Ordnern können höchstens 128 Zeichen enthalten.

Beschreibung

Zeigt die Beschreibung des Backup-to-Disk-Ordners an.

- 4 Klicken Sie auf "Übernehmen".

Ändern der Einstellung für gepufferte Lesevorgänge für einen veralteten Backup-to-Disk-Ordner

Sie können die Einstellung für gepufferte Lesevorgänge einen veralteten Backup-to-Disk-Ordner ändern (aktivieren oder deaktivieren).

So ändern Sie die Einstellung für gepufferte Lesevorgänge für einen veralteten Backup-to-Disk-Ordner

- 1 Doppelklicken Sie auf der Registerkarte "Speicher" auf den Backup-to-Disk-Ordner, dessen Eigenschaften Sie bearbeiten möchten.
- 2 Klicken Sie im linken Teilfenster auf "Eigenschaften".
- 3 Ändern Sie eine der folgenden Eigenschaften:

Puffer automatisch erkennen

Gibt an, ob Backup Exec automatisch die bevorzugten Einstellungen für Lesepuffer für den Backup-to-Disk-Ordner erkennt.

Lesevorgänge puffern

Wenn diese Einstellung auf Aktiviert gesetzt ist, gilt:

- Backup Exec soll die Einstellungen für diesen Backup-to-Disk-Ordner nicht automatisch erkennen.
- Dieser Backup-to-Disk-Ordner soll gepufferte Lesevorgänge (das Lesen großer Datenblöcke) zulassen.

Das Aktivieren dieser Option kann zu einer höheren Leistung führen.

- 4 Klicken Sie auf "Übernehmen".

Ändern des Speicherorts eines älteren Backup-to-Disk-Ordnern

Sie können den Speicherort eines älteren Backup-to-Disk-Ordnern ändern.

Siehe "[Veraltete Backup-to-Disk-Ordner](#) " auf Seite 439.

So ändern Sie den Speicherort eines älteren Backup-to-Disk-Ordnern

- 1 Klicken Sie auf der Registerkarte "Speicher" mit der rechten Maustaste auf den ursprünglichen veralteten Backup-to-Disk-Ordner und klicken Sie dann auf "Löschen".
- 2 Erstellen Sie einen Ordner, dessen Name und Speicherort sich von den entsprechenden Daten für den älteren Backup-to-Disk-Ordner unterscheiden.

- 3 Kopieren Sie im Windows-Explorer alle folgenden Dateien und Ordner und fügen Sie sie in den neuen Ordner ein:
 - . Bkf-Dateien
 - . Cfg-Dateien
 - Alle Unterordner mit dem Präfix "IMG" im Namen
- 4 Löschen Sie im Windows-Explorer alle Dateien aus dem ursprünglichen Backup-to-Disk-Ordner.
- 5 Klicken Sie in der Backup Exec-Administratorkonsole auf der Registerkarte "Speicher" in der Gruppe "Konfigurieren" auf "Speicher konfigurieren".
- 6 Folgen Sie den Anweisungen, um den älteren Backup-to-Disk-Ordner vom neuen Speicherort zu importieren.

Siehe ["Wiederherstellen von Daten aus einem veralteten Backup-to-Disk-Ordner"](#) auf Seite 443.
- 7 Klicken Sie mit der rechten Maustaste auf den Backup-to-Disk-Ordner und klicken Sie dann auf "Inventar und Katalog".

Erneutes Erstellen eines veralteten Backup-to-Disk-Ordners einschließlich des Inhalts

Wenn Sie einen Backup-to-Disk-Ordner zwar aus Backup Exec entfernt, ihn jedoch nicht von der Festplatte gelöscht haben, können Sie den Backup-to-Disk-Ordner und die enthaltenen Dateien erneut erstellen. Sie müssen den Namen und den Pfad des ursprünglichen Backup-to-Disk-Ordners kennen, um ihn abzurufen. Wenn Sie einen Backup-to-Disk-Ordner vom Datenträger gelöscht haben, können Sie ihn nicht wieder erstellen.

Siehe ["Veraltete Backup-to-Disk-Ordner"](#) auf Seite 439.

So erstellen Sie einen veralteten Backup-to-Disk-Ordner einschließlich des Inhalts neu

- 1 Klicken Sie auf der Registerkarte "Speicher" unter "Konfigurieren" auf "Speicher konfigurieren".
- 2 Folgen Sie den Eingabeaufforderungen, um den älteren Backup-to-Disk-Ordner zu importieren, den Sie neu erstellen möchten.

Siehe ["Wiederherstellen von Daten aus einem veralteten Backup-to-Disk-Ordner"](#) auf Seite 443.

- 3 Klicken Sie mit der rechten Maustaste auf den Backup-to-Disk-Ordner, und klicken Sie dann auf "Inventar und Katalog".

Siehe ["Inventarisieren und Katalogisieren von Speichergeräten"](#) auf Seite 552.

Wiederherstellen von Daten aus einem veralteten Backup-to-Disk-Ordner

Sie müssen einen existierenden Backup-to-Disk-Ordner in Backup Exec importieren, um darin enthaltene Daten wiederherstellen zu können. Wenn Sie einen Backup-to-Disk-Ordner importieren, können Sie das Stammverzeichnis eines Datenträgers oder einen Administrator-UNC-Freigabe nicht als Pfad verwenden. Die administrativen Freigaben sind ADMIN\$ und IPC\$ sowie je eine für jeden Laufwerksbuchstaben, zum Beispiel C\$ für den lokalen Datenträger C, D\$, usw.

Hinweis: Wenn Sie einen veralteten Backup-to-Disk-Ordner importieren, werden alle Backup-Daten auf diesem Ordner so eingestellt, dass Sie ein Jahr nach dem Importdatum des Ordners ablaufen. Sie können die Daten länger oder kürzer aufbewahren.

Siehe ["Ändern des Ablaufdatums von Backup-Sätzen auf plattenbasierten Speichergeräten"](#) auf Seite 404.

Siehe ["Aufbewahren von Backup-Sätzen auf plattenbasierten Speichergeräten zum Vermeiden des Ablaufens"](#) auf Seite 406.

So stellen Sie Daten aus einem veralteten Backup-to-Disk-Ordner wieder her

- 1 Klicken Sie auf der Registerkarte "Speicher" in der Gruppe "Konfigurieren" auf "Speicher konfigurieren".
- 2 Sie haben folgende Möglichkeiten:

Wenn Central Admin Server Feature nicht installiert ist Klicken Sie auf "Plattenbasierter Speicher" und dann auf "Weiter".

Wenn Central Admin Server Feature installiert ist

Gehen Sie dazu nach folgender Reihenfolge vor:

- Wählen Sie den Backup Exec-Server aus, auf den Sie einen veralteten Backup-to-Disk-Ordner importieren möchten und klicken Sie dann auf "Weiter".
- Klicken Sie auf "Plattenbasierter Speicher" und dann auf "Weiter".

- 3 Wählen Sie "Alte Backup-to-Disk-Ordner importieren" und klicken Sie dann auf "Weiter".
- 4 Geben Sie einen Namen und eine Beschreibung für den veralteten Backup-to-Disk-Ordner ein und klicken Sie dann auf "Weiter".
- 5 Geben Sie den Pfad zum vorhandenen veralteten Backup-to-Disk-Ordner ein und klicken Sie dann auf "Weiter".
- 6 Lesen Sie die Übersicht und führen einen der folgenden Schritte aus:

So ändern Sie die Konfiguration

Gehen Sie dazu in folgender Reihenfolge vor:

- Klicken Sie auf die Überschrift, die die Elemente enthält, die Sie ändern möchten.
- Nehmen Sie alle Änderungen, vor und klicken Sie dann auf "Weiter", bis die Übersicht angezeigt wird.
- Klicken Sie auf "Fertigstellen".

So importieren Sie den veralteten Backup-to-Disk-Ordner

Klicken Sie auf "Fertigstellen".

- 7 Wenn der veraltete Backup-to-Disk-Ordner in der Ansicht "Speicher" angezeigt wird, klicken Sie mit der rechten Maustaste auf den Ordner und klicken Sie dann auf "Inventar und Katalog".

Hinweis: Abhängig von der Anzahl der betroffenen Backup-Sätze kann dieser Vorgang sehr lange dauern. Sie sollten diesen Vorgang daher nicht während der normalen Geschäftsstunden ausführen.

- 8 Wählen Sie auf der Registerkarte "Speicher" in der Ansicht "Gesamter Speicher" den veralteten Backup-to-Disk-Ordner aus, aus dem Sie wiederherstellen möchten.
- 9 Klicken Sie mit der rechten Maustaste auf den veralteten Backup-to-Disk-Ordner und klicken Sie dann auf "Wiederherstellen".

Bandspeicher

In diesem Kapitel werden folgende Themen behandelt:

- Support für Bandlaufwerke und Wechsler
- Hinzufügen oder Ersetzen von Geräten durch den Assistent für Hot Swap-Geräte
- Installieren von Bandgerätetreibern
- Bearbeiten von Bandlaufwerkeigenschaften
- Anzeigen von Statistiken zu Bandlaufwerken
- Wechsler in Backup Exec
- Erstellen von Wechslerpartitionen
- Verwalten von Bändern
- Kennzeichnen von Bandmedien
- So werden WORM-Medien in Backup Exec verwendet
- Standardmedienspeicher
- Ausrangieren beschädigter Bandmedien
- Löschen von Bandmedien
- Band- oder Datenträgermedien löschen
- Info zum Katalogisieren von Band- oder Plattenspeichermedien, die verschlüsselte Backup-Sätze enthalten
- Verknüpfen von Bandmedien mit einem Mediensatz
- Bearbeiten von Bandmedieneigenschaften

- [Rotationsstrategien für Bandmedien](#)

Support für Bandlaufwerke und Wechsler

Wenn Sie Backup Exec installieren, erkennt es automatisch alle Bandspeicher, die mit dem Backup Exec-Server verknüpft sind.

Die Unterstützung für Bandlaufwerke und -bibliotheken ist von der jeweiligen Backup Exec-Edition abhängig. Weitere Informationen finden Sie in den Lizenzinformationen zur installierten Edition.

Sie können den Assistenten "Speicher konfigurieren" verwenden, um die folgenden Aktionen für Bandspeicher durchzuführen:

- Partitionieren Sie Wechsler-Schächte.
- Installieren von Bandgerätetreibern

Hinweis: Sie müssen keine Bandgerätetreiber installieren, wenn Backup Exec unter Windows Server 2012 oder höher ausgeführt wird. Kernelmodustreiber und tapeinst.exe werden nicht mehr installiert, wenn Backup Exec unter Windows Server 2012 oder höher ausgeführt wird.

Siehe "[Installieren von Bandgerätetreibern](#)" auf Seite 449.

- Ersetzen Sie Hot Swap-Speicher auf einem Backup Exec-Server oder fügen Sie sie hinzu, ohne den Server neu starten zu müssen.
- Erstellen Sie Mediensätze, um die Backup-Daten auf Bändern zu verwalten.

Siehe "[Standard-Mediansätze](#)" auf Seite 473.

Siehe "[Anzeigen von Aufträgen, Auftragsverläufen, Backup-Sätzen und aktiven Warnmeldungen für Speichergeräte](#)" auf Seite 548.

Hinzufügen oder Ersetzend von Geräten durch den Assistent für Hot Swap-Geräte

Verwenden Sie den Assistenten für Hot Swap-Geräte, um Hot Swap-Speicher auf einem Backup Exec-Server zu ersetzen oder hinzuzufügen, ohne den Server neu starten zu müssen.

Wenn Sie USB-Bandgeräte (Universal Serial Bus) von einem USB-Port trennen und anschließend wieder damit verbinden, müssen Sie den Assistenten für Hot Swap-Geräte ausführen, damit Backup Exec die Geräte erneut erkennen kann.

Bei über iSCSI angeschlossenen Geräten müssen Sie das Gerät als "Dauerhaftes Ziel" im iSCSI-Systemsteuerungs-Applet auflisten und anschließend den Assistenten für Hot Swap-Geräte ausführen. Das Auflisten des Geräts als "Dauerhaftes Ziel" lässt Backup Exec das Gerät wieder erkennen, wann immer Sie den Backup Exec-Server neu starten.

Nach dem Start des "Assistenten für Hot Swap-Geräte" werden Sie aufgefordert, die Backup Exec-Administratorkonsole zu schließen. Der "Assistent für Hot Swap-Geräte" wartet, bis alle Aufträge, die bearbeitet werden, abgeschlossen sind. Der Assistent hält den Backup Exec-Server an und beendet die Backup Exec-Dienste. Sie können dann beliebige Speichergeräte hinzufügen oder austauschen. Der Assistent erkennt die neuen und ersetzten Geräte und speichert neue Informationen über das jeweilige Gerät in der Backup Exec-Datenbank. Dann wird der Assistent beendet und Sie können die Backup Exec-Administratorkonsole wieder öffnen.

Jeder neue Speicher wird auf der Registerkarte "Speicher" angezeigt, zusammen mit Verwendungsstatistiken für den angesammelten Speicher. Sie können den neuen Speicher in einem Speichergerätpool aktivieren.

Jeder ausgetauschte Speicher wird auf der Registerkarte "Speicher" angezeigt, und zwar in der Ansicht "Gesamter Speicher" mit dem Status "Offline".

Hinweis: Starten Sie den Assistenten für Hot Swap-Geräte, bevor Sie Speicher hinzufügen oder ersetzen.

So fügen Sie Geräte mit dem Assistenten für Hot Swap-Geräte hinzu oder ersetzen sie

1 Sie haben folgende Möglichkeiten:

Für über iSCSI verknüpften Speicher:	Fügen Sie im iSCSI-Systemsteuerungs-Applet den Speicher zur Liste "Dauerhafte Ziele" hinzu. Fahren Sie mit dem nächsten Schritt fort.
Für alle anderen Hot Swap-fähigen Speicher:	Fahren Sie mit dem nächsten Schritt fort.

2 Klicken Sie auf der Registerkarte "Speicher" in der Gruppe "Konfigurieren" auf "Speicher konfigurieren".

- 3 Wenn Sie nach dem Typ des Speichers gefragt werden, den Sie konfigurieren möchten, wählen Sie "Bandspeicher" und klicken Sie auf "Weiter".
- 4 Wählen Sie "Assistent für Hot Swap-Geräte ausführen", klicken Sie auf "Weiter" und folgen Sie dann den Bildschirmanweisungen.

Installieren von Bandgerätetreibern

Sie können den Assistenten "Speicher konfigurieren" verwenden, um Bandgerätgerätetreiber zu installieren und Einträge für Bandgeräte zu löschen, die nicht verfügbar, entfernt oder ausgeschaltet sind.

Dieses Thema enthält folgende Informationen:

[Kernelmodus-Bandtreiber und tapeinst.exe](#)

Führen Sie vor dem Installieren der Bandgerätetreiber folgende Schritte aus:

- Stellen Sie sicher, dass Backup Exec das Bandgerät unterstützt.
Die unterstützten Speichertypen finden Sie in der Liste der mit Backup Exec kompatiblen Hardware.
- Führen Sie den Windows-Geräte-Manager aus, um sicherzustellen, dass er das Bandgerät auflistet.
- Rufen Sie die neuesten Backup Exec-Gerätetreiber auf.

So installieren Sie die neuesten Gerätetreiber in den Installationsordner "Backup Exec"n den

- 1 Klicken Sie auf die Schaltfläche "Backup Exec", wählen Sie "Technischer Support" und klicken Sie dann auf "Aktuelle Backup Exec-Gerätetreiber".
- 2 Führen Sie den Assistenten für die Installation der Gerätetreiber aus (siehe unten).

So installieren Sie die Bandgerätgerätetreiber mit dem Assistenten "Speicher konfigurieren"

- 1 Klicken Sie auf der Registerkarte "Speicher" in der Gruppe "Konfigurieren" auf "Speicher konfigurieren".
- 2 Wählen Sie im Fenster des Assistenten "Bandspeicher" und klicken Sie anschließend auf "Weiter".
- 3 Wählen Sie "Bandgerätetreiber installieren" und klicken Sie anschließend auf "Weiter".
- 4 Folgen Sie den Anweisungen im Assistenten für die Installation der Gerätetreiber.

Kernelmodus-Bandtreiber und tapeinst.exe

Kernelmodustreiber und tapeinst.exe werden nicht mehr installiert, wenn Backup Exec unter Windows Server 2012 oder höher ausgeführt wird. Wird der Backup Exec-Server unter Windows Server 2012 oder höher ausgeführt, ist im Assistenten "Speicher konfigurieren" die Option "Bandgerätetreiber installieren" nicht verfügbar, und tapeinst.exe ist im Installationsordner von Backup Exec nicht verfügbar. tapeinst.exe ist ein Programm, das Kernelmodus Bandtreiber installiert. Wird der Backup Exec-Server unter Windows Server 2008 R2 oder niedriger ausgeführt, können Sie tapeinst.exe manuell oder über den Assistenten "Speicher konfigurieren" ausführen.

Wenn Sie ältere oder nicht unterstützte Bandgeräte nutzen, testen Sie diese, bevor Sie Windows Server 2012 und höher verwenden, um die Funktionstüchtigkeit zu bestimmen, falls Kernelmodustreiber benötigt werden.

Benutzermodustreiber greifen jetzt auf alle unterstützten Bandgeräte zu. Benutzermodustreiber konnten bisher unter mehreren Versionen von Backup Exec auf die meisten Bandgeräte zugreifen.

Benutzermodustreiber sind nicht im Windows-Geräte-Manager sichtbar. Wenn keine Kernelmodustreiber installiert sind, kennzeichnet der Windows-Geräte-Manager möglicherweise das Bandlaufwerk mit einem gelben Ausrufezeichen. Dies ist akzeptabel und verhindert nicht den Einsatz des Geräts mit Backup Exec und den Benutzermodustreibern. Kernelmodustreiber von Microsoft oder vom Hersteller der Band-Hardware sind im Allgemeinen für die Installation akzeptabel. Backup Exec greift weiterhin über die Benutzermodustreiber auf die Bandgeräte zu.

So installieren Sie Bandgerätetreiber auf einem Backup Exec-Server unter Windows Server 2008 R2 oder niedriger durch Ausführen von tapeinst.exe

- 1 Doppelklicken Sie im Backup Exec-Installationsverzeichnis auf die Datei "tapeinst.exe".

Der Standardinstallationsordner ist "C:<Backup Exec-Installationsordner>\Backup Exec".

- 2 Folgen Sie den Anweisungen im Assistenten für die Installation der Gerätetreiber.

Bearbeiten von Bandlaufwerkseigenschaften

Sie können die folgenden Eigenschaften von Bandlaufwerken bearbeiten:

Siehe ["Support für Bandlaufwerke und Wechsler"](#) auf Seite 447.

So bearbeiten Sie Bandlaufwerkseigenschaften

- 1** Doppelklicken Sie auf der Registerkarte "Speicher" auf das Bandlaufwerk, dessen Eigenschaften Sie Statistiken bearbeiten möchten.
- 2** Klicken Sie im linken Teilfenster auf "Eigenschaften".

3 Bearbeiten Sie eine der folgenden Optionen:

Name	Zeigt den Namen des Bandlaufwerks an. Sie können dieses Feld bearbeiten.
Beschreibung	Zeigt die Beschreibung des Bandlaufwerks an. Sie können dieses Feld bearbeiten.
Hardwarekomprimierung	Gibt an, ob die Hardwarekomprimierung aktiviert ist. Wenn diese Option zur Verfügung steht, unterstützt dieses Laufwerk die Hardwarekomprimierung. Wenn Sie einen Auftrag dafür konfigurieren, Hardwarekomprimierung zu verwenden und Hardwarekomprimierung auf dem Gerät deaktiviert ist, dann ist die Hardwarekomprimierung nicht verfügbar und wird nicht verwendet.

Blockgröße

Zeigt die Größe der Datenblöcke an, die auf die neuen Medien in diesem Bandlaufwerk geschrieben werden. Standardeinstellung ist die bevorzugte Blockgröße.

Einige Geräte (z. B. LTO-Geräte) erzielen eine bessere Verarbeitungsleistung, wenn größere Blockgrößen verwendet werden. Die bevorzugte Blockgröße kann zwischen 512 Byte und 64 Kilobyte oder mehr liegen. Wenn Sie ein Bandlaufwerk verwenden, das größere Blockgrößen unterstützt, können Sie die Blockgröße des Bandlaufwerks ändern. Wenn jedoch das Bandlaufwerk keine so große Blockgröße wie die von Ihnen benötigte ermöglicht, konfigurieren Sie den Host-Bus-Adapter oder das Bandlaufwerk erneut. Nachdem Sie die Hardware erneut konfiguriert und die Backup Exec-Dienste neu gestartet haben, prüfen Sie, ob die von Ihnen gewünschte Blockgröße verfügbar ist.

Lesen Sie die Dokumentation des Bandlaufwerkherstellers, um Hilfe beim Konfigurieren des Geräts zu erhalten.

Backup Exec kann nicht gewährleisten, dass die angeforderte Blockgröße von diesem Bandlaufwerk unterstützt wird. Überprüfen Sie daher anhand der Spezifikationen des Bandlaufwerks, ob die Blockgröße unterstützt wird. Wenn das Bandlaufwerk eine Blockgröße nicht unterstützt, verwendet es die Standard-Blockgröße.

Wenn das Bandlaufwerk das Konfigurieren der Blockgröße nicht unterstützt, ist diese Option nicht verfügbar.

Puffergröße

Zeigt die Datenmenge an, die bei jeder Lese- oder Schreibanfrage an das Bandlaufwerk gesendet wird. Die Puffergröße muss der Blockgröße oder sogar einem geraden Vielfachen der Blockgröße entsprechen.

Je nach Größe des Speichers in Ihrem System können Sie durch Erhöhen dieses Werts die Leistung des Bandlaufwerks verbessern. Jeder Bandlaufwerkstyp erfordert eine andere Puffergröße, um optimale Leistungswerte zu erzielen.

Pufferzahl

Zeigt die Anzahl von Puffern an, die für dieses Bandlaufwerk zugeordnet werden.

Je nach Größe des Speichers in Ihrem System können Sie durch Erhöhen dieses Werts die Leistung des Geräts verbessern. Jeder Bandlaufwerkstyp erfordert eine andere Anzahl von Puffern, um optimale Leistungswerte zu erzielen.

Wenn Sie die Pufferzahl ändern, müssen Sie möglicherweise den oberen Schwellenwert entsprechend anpassen.

Oberer Schwellenwert

Zeigt die Anzahl der Puffer an, die gefüllt werden müssen, bevor Daten erstmals an das Bandlaufwerk geschickt werden, und bei geringer Auslastung des Bandlaufwerks.

Der obere Schwellenwert darf die Pufferzahl nicht überschreiten. Der Wert 0 deaktiviert die Schwellenwertsteuerung, d. h. jeder Puffer wird zum Gerät gesendet, sobald er gefüllt ist.

Die Standardeinstellung erzielt in den meisten Fällen ausreichende Leistungswerte, in einigen Konfigurationen kann der Datendurchsatz jedoch durch Angabe anderer Werte in diesem Feld verbessert werden. Wenn Sie die Pufferzahl ändern, sollten Sie den oberen Schwellenwert entsprechend anpassen. Wenn ein Gerät in der Standardeinstellung einen oberen Schwellenwert von 0 hat, sollte er auf 0 belassen werden.

Auf Standardeinstellungen zurücksetzen

Setzt alle bevorzugten Konfigurationseinstellungen auf die Standardeinstellung zurück.

Einzelblockmodus lesen

Gibt an, ob dieses Bandlaufwerk nur einen Datenblock zur gleichen Zeit liest, unabhängig von der Größe des Pufferblocks.

Diese Option ist standardmäßig deaktiviert.

Einzelblockmodus schreiben

Gibt an, ob dieses Bandlaufwerk nur einen Datenblock zur gleichen Zeit schreibt. Diese Option bietet mehr Kontrolle beim Umgang mit Fehlern beim Schreiben von Daten.

Es wird empfohlen, dass Sie diese Option aktivieren, wenn das Bandlaufwerk gemeinsam genutzt wird.

Diese Option ist standardmäßig aktiviert.

SCSI-Pass-Through-Modus lesen	<p>Gibt an, ob dieses Bandlaufwerk Daten liest, ohne dabei eine Microsoft-Bandlaufwerk-API zu verwenden. Bei Aktivierung dieser Option werden die Daten direkt über das Bandlaufwerk übermittelt. Dadurch stehen bei Gerätefehlern genauere Informationen zur Verfügung.</p> <p>Diese Option ist standardmäßig deaktiviert.</p>
SCSI-Pass-Through-Modus schreiben	<p>Gibt an, ob dieses Bandlaufwerk Daten schreibt, ohne dabei eine Microsoft-Bandlaufwerk-API zu verwenden. Durch Aktivierung dieser Option werden die Daten direkt über den Gerätetreiber übermittelt. Dadurch stehen bei Gerätefehlern genauere Informationen zur Verfügung.</p> <p>Es wird empfohlen, dass Sie diese Option aktivieren, wenn das Bandlaufwerk gemeinsam genutzt wird.</p> <p>Diese Option ist standardmäßig aktiviert.</p>
Server, die dieses Gerät gemeinsam nutzen	<p>Zeigt die Server an, die dieses Gerät auch verwenden können.</p> <p>Siehe "Freigeben von Speichergeräten" auf Seite 544.</p>
Medientyp	<p>Gibt an, ob Barcoderegeln für den Wechsler aktiviert sind, der an dieses Bandlaufwerk angeschlossen ist. Wenn Barcoderegeln aktiviert sind, werden die Medientypen aufgelistet, von denen dieses Bandlaufwerk lesen und auf die es schreiben kann. Backup Exec verwendet die Barcoderegeln zum Identifizieren des Medientyps, der für ein Laufwerk verwendet werden soll.</p> <p>Sie können Barcoderegeln konfigurieren und für einen Wechsler aktivieren oder deaktivieren.</p> <p>Siehe "Barcoderegeln für einen Wechsler konfigurieren" auf Seite 459.</p>

Kann lesen aus

Gibt an, ob dieses Bandlaufwerk aus dem Medientyp lesen kann.

Siehe ["Barcoderegeln für einen Wechsler konfigurieren"](#) auf Seite 459.

Kann schreiben in

Gibt an, ob dieses Bandlaufwerk im Medientyp schreiben kann.

Siehe ["Barcoderegeln für einen Wechsler konfigurieren"](#) auf Seite 459.

- 4 Klicken Sie auf "Übernehmen".

Anzeigen von Statistiken zu Bandlaufwerken

Sie können Statistiken über Bandlaufwerke anzeigen.

Siehe ["Support für Bandlaufwerke und Wechsler"](#) auf Seite 447.

So zeigen Sie Bandlaufwerksstatistiken an

- 1 Doppelklicken Sie auf der Registerkarte "Speicher" auf das Bandlaufwerk, für das Sie Statistiken anzeigen möchten.
- 2 Im linken Teilfenster klicken Sie auf "Statistische Daten".

Wechsler in Backup Exec

Die ADAMM-Funktion (Advanced Device and Media Management) in Backup Exec löst die Probleme, die mit typischen Wechslermodulen im Zusammenhang stehen. Backup Exec greift auf alle Medien im Wechsler zu und verwendet die Medien, die zum angegebenen Mediensatz gehören. Wenn der Backup-Auftrag die Kapazität des Mediums überschreitet, durchsucht Backup Exec alle Medien, die im Wechsler enthalten sind, und findet die zur Verwendung geeigneten Medien.

Beispiel: Ein Operator hat einen Wechsler mit sechs Schächten. Er legt sechs leere Bänder ein und leitet Backup-Aufträge an verschiedene Mediensätze im Wechsler. Backup Exec ordnet automatisch verfügbare Bänder im Wechsler zu. Wenn ein Auftrag die Kapazität eines Bands übersteigt und sich noch ein anderes überschreibbares Band im Wechsler befindet, wird der Auftrag automatisch auf diesem Band fortgesetzt. Wenn Backup Exec keine verfügbaren Bänder mehr findet, wird der Operator aufgefordert, überschreibbare Medien einzulegen.

In einem Wechsler wählt Backup Exec zuerst das älteste wiederverwendbare Medium zur Verwendung aus. Wenn mehrere Medien gefunden werden, die die

Bedingungen erfüllen, wählt Backup Exec die Medien im Schacht mit der niedrigsten Nummer aus. Beispielsweise wählt Backup Exec Medien in Schacht 2 aus, bevor er gleichwertige Medien in Schacht 4. auswählt.

Für Wiederherstellungsaufträge, die Wechsler verwenden, greift Backup Exec auf die Quellmedien zu, unabhängig von ihrer sequenziellen Platzierung im Magazin. Wenn sich die Daten für einen Wiederherstellungsauftrag z. B. auf zwei Medien im Magazin befinden, müssen sich die beiden Medien nicht in benachbarten Schächten befinden, damit die Daten in Backup Exec wiederhergestellt werden können. Wenn Backup Exec die Medien nicht findet, die für den Wiederherstellungsauftrag im Wechsler erforderlich sind, wird eine Warnmeldung generiert, die die Medien anfordert, die zum Abschließen des Auftrags erforderlich sind.

Siehe ["Anforderungen zum Einrichten der Wechsler-Hardware"](#) auf Seite 458.

Siehe ["Erstellen von Wechslerpartitionen"](#) auf Seite 466.

Anforderungen zum Einrichten der Wechsler-Hardware

Sie können Backup Exec für die Verwendung von Wechslerlaufwerken konfigurieren, indem Sie Verknüpfungen zwischen den Laufwerken des Wechslers, dem Transportarm und Backup Exec herstellen. Backup Exec unterstützt serialisierte Laufwerke. Eine manuelle Konfiguration der serialisierten Laufwerke ist nicht erforderlich.

Die unterstützten Speichertypen finden Sie in der Liste der mit Backup Exec kompatiblen Hardware.

Stellen Sie sicher, dass die Wechsler-Hardware wie folgt konfiguriert wird:

- Stellen Sie sicher, dass der Transportarm auf den Zufallsmodus eingestellt ist. Weitere Informationen finden Sie in der Dokumentation zum Wechsler.
- Stellen Sie für einen Wechsler mit mehreren logischen Geräteummern (multi-LUN) Folgendes sicher:
 - Die Controller-Karte wird so eingestellt, dass sie mehrere logische Geräteummern (LUNs) unterstützt (wenn diese unterstützt werden).
 - Das Ziel-LUN für das Bandlaufwerk ist niedriger als das Ziel-LUN für den Wechsler.
- Legen Sie fest, welches Laufwerk das erste Laufwerk im Wechsler ist, und richten Sie die SCSI-IDs dann so ein, dass sie der Folge der Laufwerkelementadressen entsprechen. Weitere Informationen zum Festlegen der Laufwerkelementadresse für jedes Speichergerät finden Sie in der Dokumentation zum Wechsler.

- Stellen Sie sicher, dass die SCSI-ID des Transportarms den SCSI-IDs der Laufwerke im Wechsler vorausgeht. Verwenden Sie nicht 0 oder 1, da diese SCSI-IDs normalerweise für Boot-Geräte reserviert sind.

Wenn der Wechsler im folgenden Beispiel zwei Laufwerke hat, sollte dem Laufwerk mit der niedrigeren Laufwerkelementadresse die niedrigere SCSI-ID zugeordnet werden.

Tabelle 11-1 Beispielkonfiguration für einen Wechsler mit mehreren Laufwerken

Datentransferelement (Speichergeräte)	SCSI-ID	Laufwerkelementadresse
Transportarm	4	N/A
Speichergerät 0	5	00008000
Speichergerät 1	6	00008001

Siehe ["Wechsler in Backup Exec"](#) auf Seite 457.

Inventarisieren von Wechslern beim Starten der Backup Exec-Dienste

Sie können einen Standard festlegen, damit alle Wechsler im Inventarauftrag enthalten sind, wann immer Backup Exec Services gestartet wird. Es wird empfohlen, dass Sie diesen Standard aktivieren, wenn Medien häufig zwischen Wechslern verschoben werden. Backup Exec kann für den Start länger benötigen.

So inventarisieren Sie Wechsler beim Starten der Backup Exec-Dienste

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Backup Exec-Einstellungen".
- 2 Klicken Sie im linken Teilfenster auf "Speicher".
- 3 Klicken Sie auf "Inventarisieren von Wechslern beim Starten der Backup Exec-Dienste".
- 4 Klicken Sie auf "OK".

Siehe ["Inventarisieren eines Speichergeräts"](#) auf Seite 550.

Barcoderegeln für einen Wechsler konfigurieren

Wenn Sie einen Wechsler mit Barcodeunterstützung verwenden, der mit verschiedenen Arten von Laufwerken arbeitet, können Sie eine Barcoderegel verwenden. Backup Exec verwendet die Barcoderegeln zum Identifizieren des Medientyps, der für ein Laufwerk verwendet werden soll. Wenn Backup Exec diese Barcoderegel liest, wird nach dem Medientyp gesucht, der diesem Präfix bzw. Suffix

entspricht. Backup Exec lädt dann das Medium in ein für dieses Medium geeignetes Laufwerk.

Die Barcoderegeln gelten für alle Wechsler, für die Barcoderegeln aktiviert sind. Standardmäßig werden Barcoderegeln deaktiviert.

Sie können den Assistenten "Speicher konfigurieren" verwenden, um Barcoderegeln zu konfigurieren, oder Sie können Barcoderegeln in den Backup Exec-globalen Einstellungen hinzufügen, bearbeiten und löschen. Sie können Barcoderegeln auch in den Wechslereigenschaften aktivieren oder deaktivieren.

Siehe „[Barcoderegeln für einen Wechsler mithilfe des Assistenten "Speicher konfigurieren" konfigurieren](#)“ auf Seite 460.

Siehe „[Barcoderegeln mithilfe der globalen Einstellungen von Backup Exec hinzufügen, bearbeiten und löschen](#)“ auf Seite 462.

Siehe „[Aktivieren oder Deaktivieren der Barcoderegeln mithilfe der Wechslereigenschaften](#)“ auf Seite 462.

Barcoderegeln für einen Wechsler mithilfe des Assistenten "Speicher konfigurieren" konfigurieren

Barcoderegeln für einen Wechsler konfigurieren

1 Klicken Sie auf der Registerkarte "Speicher" in der Gruppe "Konfigurieren" auf "Speicher konfigurieren".

2 Sie haben folgende Möglichkeiten:

Wenn Central Admin Server Feature nicht installiert ist	Klicken Sie auf "Plattenbasierter Speicher" und dann auf "Weiter".
---	--

Wenn Central Admin Server Feature installiert ist	Gehen Sie dazu in folgender Reihenfolge vor:
---	--

- Wählen Sie den Backup Exec-Server aus, auf dem Sie Speicher konfigurieren wollen, und klicken Sie dann auf "Weiter".
- Klicken Sie auf "Plattenbasierter Speicher" und dann auf "Weiter".

3 Klicken Sie auf "Barcoderegeln für einen Wechsler konfigurieren" und klicken Sie dann auf "Weiter".

4 Wählen Sie den Wechsler aus, für den Sie Speicher konfigurieren möchten, und klicken Sie dann auf "Weiter".

- 5** Um die verfügbaren Barcoderegeln in der Liste zu ändern, klicken Sie auf eine der folgenden Optionen:

So fügen Sie eine neue Barcoderegeln hinzu Gehen Sie dazu wie folgt vor:

- Klicken Sie auf "Neu".
- Klicken Sie auf das Dropdown-Menü und wählen Sie dann einen Medientyp aus
- Geben Sie den Händlernamen und das Barcodepräfix und/oder -suffix ein.
- Klicken Sie auf "OK".

So bearbeiten Sie eine vorhandene Barcoderegeln

Gehen Sie dazu nach folgender Reihenfolge vor:

- Wählen Sie die Barcoderegeln aus, die Sie bearbeiten möchten, und klicken Sie dann auf "Bearbeiten".
- Nehmen Sie alle Änderungen, vor und klicken Sie dann auf "OK".

So löschen Sie eine Barcoderegeln

Wählen Sie eine Barcoderegeln aus, klicken Sie auf "Löschen" und klicken Sie dann auf "Ja", um den Löschvorgang zu bestätigen.

- 6** Klicken Sie auf "Weiter".
- 7** Wählen Sie ein Bandlaufwerk aus und geben dann mithilfe des Kontrollkästchens für die aufgeführten Medientypen an, ob das Bandlaufwerk auf den Medientyp lesen und schreiben kann.

Klicken Sie auf "Weiter".

- 8** Lesen Sie die Übersicht und führen einen der folgenden Schritte aus:

So ändern Sie die Barcodekonfiguration Gehen Sie dazu nach folgender Reihenfolge vor:

- Klicken Sie auf die Überschrift, die die zu ändernden Elemente enthält.
- Nehmen Sie alle Änderungen vor und klicken Sie dann auf "Weiter".
- Klicken Sie auf "Fertigstellen".

So schließen Sie die Barcodekonfiguration ab. Klicken Sie auf "Fertigstellen".

- 9 Stellen Sie sicher, dass Barcoderegeln für den entsprechenden Wechsler aktiviert sind.

Aktivieren oder Deaktivieren der Barcoderegeln mithilfe der Wechslereigenschaften

Sie können Barcoderegeln für einen Wechsler aktivieren oder deaktivieren. Standardmäßig sind Barcoderegeln für Wechsler deaktiviert.

Aktivieren oder Deaktivieren der Barcoderegeln mithilfe der Wechslereigenschaften

- 1 Doppelklicken Sie auf der Registerkarte "Speicher" auf den Wechsler, dessen Barcoderegeln Sie aktivieren möchten.
- 2 Klicken Sie im linken Teilfenster auf "Eigenschaften".
- 3 Im Feld "Barcoderegeln" im Dropdown-Menü haben Sie folgende Möglichkeiten:

Alle Barcoderegeln für diesen Wechsler konfigurieren Klicken Sie auf "Aktiviert".

Alle Barcoderegeln für diesen Wechsler deaktivieren Klicken Sie auf "Deaktiviert".

- 4 Klicken Sie auf "OK".

Barcoderegeln mithilfe der globalen Einstellungen von Backup Exec hinzufügen, bearbeiten und löschen

Sie können die Barcoderegeln für einen Wechsler in den globalen Einstellungen für Backup Exec hinzufügen, bearbeiten oder löschen. Die Barcoderegeln gelten für alle Wechsler, für die Barcoderegeln aktiviert sind.

Barcoderegeln mithilfe der globalen Einstellungen von Backup Exec hinzufügen, bearbeiten und löschen

- 1 Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Backup Exec-Einstellungen".
- 2 Klicken Sie im linken Teilfenster auf "Barcoderegeln".
- 3 Sie haben folgende Möglichkeiten:

So fügen Sie eine neue Barcoderegeln hinzu: Klicken Sie auf "Neu" und fahren Sie dann mit dem nächsten Schritt fort.

So bearbeiten Sie eine vorhandene Barcoderegel

Wählen Sie die Barcoderegel aus, die Sie bearbeiten möchten, klicken Sie dann auf "Bearbeiten" und fahren mit dem nächsten Schritt fort.

So löschen Sie eine vorhandene Barcoderegel

Gehen Sie dazu nach folgender Reihenfolge vor:

- Wählen Sie die Barcoderegel aus, die Sie löschen möchten, und klicken Sie dann auf "Löschen".
- Klicken Sie auf "Ja" und dann auf "OK", um den Löschvorgang zu bestätigen.

Die Barcoderegel wird gelöscht.

4 Hinzufügen oder Ändern einer der folgenden Informationen:

Medientyp	Klicken Sie auf das Dropdown-Menü und wählen Sie dann einen Medientyp aus
Hersteller	<p>Den Namen des Wechslerherstellers eingeben oder ändern.</p> <p>Ein bewährtes Verfahren ist es, nur dann einen Händlernamen zu verwenden, wenn es unbedingt notwendig ist und Sie mehrere verfügbare Marken des Bandlaufwerks haben</p> <p>Dieses Feld ist auf 16 Zeichen begrenzt.</p>
Barcode-Präfix	<p>Das Vorzeichen eines Barcodes eingeben oder ändern, auf den Sie diese Barcoderegeln anwenden möchten.</p> <p>Ein gängiges Verfahren ist es, ein Präfix zu verwenden, um eine Richtlinie zur Bearbeitung von Medien anzugeben, z.B. "CLN" für das Bereinigen von Medien oder "I" für die interne Verwendung oder "O" für Kassetten, die extern verwendet werden sollen.</p> <p>Dieses Feld ist auf 16 Zeichen begrenzt.</p>
Barcode-Präfix	<p>Das Vorzeichen eines Barcodes eingeben oder ändern, auf den Sie diese Barcoderegeln anwenden möchten.</p> <p>Ein gängiges Verfahren ist es, ein Suffix zu verwenden, um die Generation der Medien anzugeben, z.B. L1, L2, usw.</p> <p>Dieses Feld ist auf 16 Zeichen begrenzt.</p>

5 Klicken Sie auf "OK".

Initialisieren eines Wechslers beim Starten des Backup Exec-Dienstes

Sie können bei jedem Start der Backup Exec-Dienste einen Wechsler initialisieren. Befinden sich beim Starten Medien in den Laufwerken im Wechsler, versucht Backup Exec, die Medien an das ursprüngliche Laufwerk zurückzugeben. Falls die Medien

nicht an das Laufwerk zurückgegeben werden können, wird eine Fehlermeldung angezeigt, in der Sie aufgefordert werden, die Medien im Laufwerk auszuwerfen.

Sie können außerdem einen Auftrag zur Initialisierung eines Wechslers erstellen.

Siehe ["Initialisieren eines Wechslers"](#) auf Seite 553.

Siehe ["Wechsler in Backup Exec"](#) auf Seite 457.

So initialisieren Sie einen Wechsler beim Starten der Backup Exec-Dienste

- 1 Doppelklicken Sie auf der Registerkarte "Speicher" auf den Wechsler, den Sie initialisieren möchten.
- 2 Im linken Teilfenster klicken Sie auf "Eigenschaften".
- 3 Klicken Sie im Feld "Startinitialisierung" in der Dropdown-Liste auf "Aktiviert".
- 4 Klicken Sie auf "Übernehmen".

Festlegen eines Reinigungsschachts

Bevor Sie einen Reinigungsauftrag senden, müssen Sie einen Reinigungsschacht definieren, der das Reinigungsmedium enthält.

Stellen Sie sicher, dass der als Reinigungsslot festgelegte Schacht ein Reinigungsband enthält. Nachdem Sie den Reinigungsslot festgelegt haben, können Sie einen Reinigungsauftrag für das Wechslerlaufwerk einrichten.

Siehe ["Reinigen eines Wechslerlaufwerks"](#) auf Seite 556.

Hinweis: Festgelegte Reinigungsslots werden nicht inventarisiert, wenn ein Inventarisierungsauftrag läuft.

So legen Sie einen Reinigungsslot fest:

- 1 Erweitern Sie auf der Registerkarte "Speicher" den Wechsler und doppelklicken Sie dann auf "Schächte".
- 2 Doppelklicken Sie auf den Schacht, der das Reinigungsmedium enthält.
- 3 Klicken Sie im Feld "Reinigungsschacht" auf das Dropdown-Menü und dann auf "Ja".
- 4 Klicken Sie auf "Übernehmen".

Wechslereigenschaften bearbeiten

Sie können Eigenschaften von Wechslern anzeigen.

Siehe ["Wechsler in Backup Exec"](#) auf Seite 457.

So zeigen Sie Eigenschaften von Wechslern an

- 1 Doppelklicken Sie auf der Registerkarte "Speicher" auf den Wechsler, dessen Eigenschaften Sie anzeigen möchten.
- 2 Klicken Sie im linken Teilfenster auf "Eigenschaften".
- 3 Bearbeiten Sie die folgenden Optionen dementsprechend:

Name	Zeigt den Namen des Wechslers an. Sie können dieses Feld bearbeiten.
Beschreibung	<p>Zeigt die Beschreibung des Wechslers an. Sie können dieses Feld bearbeiten.</p> <p>Standardmäßig zeigt Backup Exec die Anfragenzeichenkette des Geräts an, die aus dem Herstellernamen und der Produkt-ID besteht.</p>
Erste Schachtnummer	<p>Zeigt den Start-Schacht für diesen Wechsler an. Backup Exec legt fest, welcher der Start-Schacht für diesen Bibliothekstyp sein sollte. Einige Wechsler haben Schächte, die mit 0 beginnen. Andere Bibliotheken beginnen mit 1. Sie können den Start-Schacht bei Bedarf ändern.</p>

- 4 Klicken Sie auf "OK".

Erstellen von Wechslerpartitionen

Sie können einen oder mehrere Wechslerlots in Partitionen zusammenfassen. Mithilfe der Partitionierung von Wechsler­schächten können Sie steuern, welches Band für Backup-Aufträge verwendet wird. Beim Erstellen von Wechslerpartitionen erstellt Backup Exec einen Speichergerätepool für jede Partition. Aufträge, die Sie an den Speichergerätepool einer Partition senden, werden auf den Medien in den Schächten der Partition ausgeführt. Wenn Sie beispielsweise eine Partition einrichten, die über die Schächte 1 und 2 verfügt und wöchentliche Backups nur an die in diesen Schächten befindlichen Medien gesendet werden sollen, senden Sie den Auftrag an den Gerätepool der Partition, in der sich die Schächte 1 und 2 befinden. Die Speichergerätepools für Wechslerpartitionen werden im Dropdown-Menü unter dem Feld "Speicher" angezeigt, wenn Sie den Backup-Auftrag bearbeiten. Alle Speichergerätepools eines Wechslers haben den gleichen Namen und zeigen in Klammern die in den Partitionen enthaltenen Schächte an.

Partitionen können eine beliebige Anzahl Wechsler­schächte enthalten.

Der erste Schacht kann je nach Wechslerkonfiguration mit 1 oder 0 nummeriert werden. Wenn der Wechsler eine null-basierte Schachtkonfiguration verwendet, verwendet der Assistent "Speicher konfigurieren" den Schacht "0" als ersten Schacht für die Partition "1" und passt den Start-Schacht für alle anderen Partition entsprechend an.

Siehe ["Erneute Zuweisung einer Schacht-Basisnummer für Wechsler"](#) auf Seite 469.

Wenn der Wechsler partitioniert wurde, sucht Backup Exec nur in der zugewiesenen Partition nach dem ältesten wiederverwendbaren Medium. Wird mehr als ein Medium gefunden, das die Bedingungen erfüllt, wählt Backup Exec die Medien im Schacht mit der niedrigsten Nummer aus; beispielsweise werden Medien in Schacht 2 vor gleichwertigen Medien in Schacht 4 ausgewählt.

Sie können ein Partitionsschema erstellen, das sich am besten für Ihre Umgebung eignet. Beispielsweise erstellen einige Administratoren Partitionen möglicherweise nach Benutzern und Gruppen; andere hingegen erstellen Partitionen entsprechend den Vorgangstypen.

So erstellen Sie Wechslerpartitionen

1 Sie haben folgende Möglichkeiten:

So zeigen Sie alle Wechsler an, für die Sie Partitionen konfigurieren können

Gehen Sie dazu in folgender Reihenfolge vor:

- Klicken Sie auf der Registerkarte "Speicher" in der Gruppe "Konfigurieren" auf "Speicher konfigurieren".
- Wählen Sie "Bandspeicher" aus, und klicken Sie dann auf "Weiter".
- Wählen Sie "Wechslerpartitionen konfigurieren" und klicken Sie anschließend auf "Weiter".
- Wählen Sie den Wechsler aus, für den die Partitionen konfiguriert werden sollen und klicken Sie dann auf "Weiter".

So konfigurieren Sie Partitionen für einen bestimmten Wechsler

Gehen Sie dazu in folgender Reihenfolge vor:

- Klicken Sie auf der Registerkarte "Speicher" mit der rechten Maustaste auf den Wechsler, für den Sie Partitionen konfigurieren möchten.
- Klicken Sie auf "Partitionen konfigurieren".

- 2** Geben Sie die Anzahl zu erstellender Partitionen an, geben Sie die Anzahl von Schächten für jede Partition an und klicken Sie dann auf "Weiter".
- 3** Überprüfen Sie die Speicherkonfigurationsübersicht und führen Sie anschließend eine der folgenden Aktionen aus:

So ändern Sie die Konfiguration

Gehen Sie dazu in folgender Reihenfolge vor:

- Klicken Sie auf die Überschrift, die die Elemente enthält, die Sie ändern möchten.
- Nehmen Sie alle Änderungen, vor und klicken Sie dann auf "Weiter", bis die Übersicht angezeigt wird.
- Klicken Sie auf "Fertigstellen".

So konfigurieren Sie die Partitionen

Klicken Sie auf "Fertigstellen".

Bandlaufwerke in einer Wechslerpartition hinzufügen oder entfernen

Sie können Bandlaufwerke in einer Wechslerpartition hinzufügen oder entfernen.

Siehe ["Erstellen von Wechslerpartitionen"](#) auf Seite 466.

Bandlaufwerke in einer Wechslerpartition hinzufügen oder entfernen

- 1** Auf der Registerkarte "Speicher" doppelklicken Sie auf die Wechslerpartition.
- 2** Klicken Sie im linken Teilfenster auf "Eigenschaften".
- 3** Sie haben folgende Möglichkeiten:

So fügen Sie ein Bandlaufwerk der Wechslerpartition hinzu

Gehen Sie dazu wie folgt vor:

- Klicken Sie auf "Hinzufügen".
- In der Geräteliste, die angezeigt wird, wählen Sie das Bandlaufwerk, das Sie hinzufügen möchten, aus und klicken Sie dann auf "OK".

So entfernen Sie ein Bandlaufwerk von der Wechslerpartition

Wählen Sie das zu entfernende Bandlaufwerk aus und klicken Sie dann auf "Entfernen".

- 4 Klicken Sie auf "Übernehmen".

Erneute Zuweisung einer Schacht-Basisnummer für Wechsler

Backup Exec weist Wechslern automatisch Schachtbasisnummern zu. Sie können ggf. die Art und Weise, in der Wechslerschächte in Backup Exec angezeigt werden, neu zuweisen. Die Schachtbasisnummern einiger Wechsler beginnen bei 0, während Schächte in anderem Wechslern bei 1 beginnen. Wenn der Wechsler eine null-basierte Schachtkonfiguration verwendet, können Sie die Anzeige von Schächten erneut festlegen.

Siehe ["Wechsler in Backup Exec"](#) auf Seite 457.

So weisen Sie eine Schachtbasisnummer für Wechsler neu zu

- 1 Doppelklicken Sie auf der Registerkarte "Speicher" auf den Wechsler, für den Sie eine neue Schachtbasisnummer zuweisen möchten.
- 2 Klicken Sie im Feld "Erste Schachtnummer" auf das Dropdown-Menü, um die Basisnummer zu ändern.
- 3 Klicken Sie auf "Übernehmen".

Bearbeiten der Eigenschaften von Wechslerschächten

Sie können die Eigenschaften eines Wechslerschachts bearbeiten.

Siehe ["Wechsler in Backup Exec"](#) auf Seite 457.

So bearbeiten Sie Eigenschaften von Wechslerschächten

- 1 Doppelklicken Sie auf der Registerkarte "Speicher" auf den Wechsler.
- 2 Klicken Sie im linken Teilfenster auf "Schächte".
- 3 Doppelklicken Sie auf den Schacht, für den Sie Eigenschaften anzeigen möchten, und wählen Sie "Eigenschaften".

- 4 Um die Eigenschaften eines anderen Schachts anzuzeigen, klicken Sie auf das Dropdown-Menü oben in der Mitte des Fensters, und klicken Sie dann auf eine Schachtnummer.
- 5 Bearbeiten Sie eine der folgenden Optionen.

Reinigungsschacht

Zeigt an, ob der Schacht als Reinigungsschacht definiert wurde. Wenn "Ja" angezeigt wird, ist dieser Schacht als Reinigungsschacht definiert worden.

Bevor Sie einen Reinigungsauftrag senden, müssen Sie einen Reinigungsschacht definieren, der das Reinigungsmedium enthält.

Stellen Sie sicher, dass der als Reinigungsslot festgelegte Schacht ein Reinigungsband enthält. Nachdem Sie den Reinigungsslot festgelegt haben, können Sie einen Reinigungsauftrag für das Wechslerlaufwerk einrichten.

Hinweis: Festgelegte Reinigungsschächte werden nicht inventarisiert, wenn ein Inventarisierungsauftrag läuft.

Siehe ["Reinigen eines Wechslerlaufwerks"](#) auf Seite 556.

Beschreibung beibehalten

Behält die Medienbeschreibung bei, wenn Sie im Dropdown-Menü die Option "Ja" wählen. Die Medienbeschreibung wird beibehalten, bis ein überschreibender Backup-Auftrag bzw. ein Lösch- oder Bezeichnungsspeichervorgang ausgeführt wird.

Standardmäßig wird die Medienbeschreibung nicht beibehalten. Der Standardwert dieser Option ist "Nein".

- 6 Klicken Sie auf "Übernehmen".

Entfernen oder erneutes Konfigurieren von Wechslerpartitionen

Sie können Wechslerpartitionen entfernen oder neu konfigurieren.

So entfernen Sie Wechslerpartitionen

- 1 Auf der Registerkarte "Speicher" klicken Sie mit der rechten Maustaste auf den Wechsler, der die Partitionen enthält, die Sie entfernen oder neu konfigurieren möchten.
- 2 Klicken Sie auf "Partitionen konfigurieren".
- 3 Klicken Sie auf "Alle Wechslerpartitionen entfernen" und dann auf "Weiter".
- 4 Lesen Sie die Übersicht und führen einen der folgenden Schritte aus:

So ändern Sie die Konfiguration

Gehen Sie dazu nach folgender Reihenfolge vor:

- Klicken Sie auf die Überschrift, die die zu ändernden Elemente enthält.
- Nehmen Sie die Änderungen vor und klicken Sie dann auf "Weiter", bis die Übersicht angezeigt wird.
- Klicken Sie auf "Fertigstellen".

So entfernen Sie Partitionen

Klicken Sie auf "Fertigstellen".

So konfigurieren Sie Wechslerpartitionen neu

- 1 Auf der Registerkarte "Speicher" klicken Sie mit der rechten Maustaste auf den Wechsler, der die Partitionen enthält, die Sie entfernen oder neu konfigurieren möchten.
- 2 Klicken Sie auf "Partitionen konfigurieren".
- 3 Klicken Sie auf "Wechslerpartitionen neu konfigurieren" und dann auf "Weiter".
- 4 Geben Sie die Anzahl der zu erstellenden Partitionen und der Schächte für jede Partition ein und klicken Sie dann auf "Weiter".
- 5 Lesen Sie die Übersicht und führen einen der folgenden Schritte aus:

So ändern Sie die Konfiguration

Gehen Sie dazu nach folgender Reihenfolge vor:

- Klicken Sie auf die Überschrift, die die zu ändernden Elemente enthält.
- Nehmen Sie die Änderungen vor und klicken Sie dann auf "Weiter", bis die Übersicht angezeigt wird.
- Klicken Sie auf "Fertigstellen".

So konfigurieren Sie die Partitionen

Klicken Sie auf "Fertigstellen".

Siehe ["Erneute Zuweisung einer Schacht-Basisnummer für Wechsler"](#) auf Seite 469.

Verwalten von Bändern

Für Bandmedien können Sie die folgenden Aktionen durchführen:

- Schutz der Daten vor Überschreibung
- Einrichten von Medienrotationsstrategien
- Überwachen der Medienspeicherorte
- Automatisches Kennzeichnen der Medien
- Lesen und Verfolgen der Medienkennungen, die Barcodes haben
- Erstellen und Zusammenfassen von statistischen Daten zu Medien

Die Funktion "Advanced Device and Media Management" (ADAMM) in Backup Exec wählt automatisch die Bandmedien für Aufträge aus. Backup Exec verfolgt alle Bandmedien, die in den verbundenen Speicher geladen werden. Außerdem verfolgt Backup Exec alle Medien, die offline sind, sowie die in Medienspeichern abgelegten Medien.

Bei Daten, die auf Bändern gespeichert werden, verwendet Backup Exec Mediensätze, für die Überschreibschutzzeiträume und Anhängezeiträume gelten, um das Ablaufen von Backup-Sätzen zu verwalten.

Ein Mediensatz besteht aus den folgenden Regeln, die auf Bandmedien zutreffen:

- Dauer des Schutzes der Daten auf einem Medium vor dem Überschreiben. Dies wird der Überschreibschutzzeitraum genannt.
- Dauer des Anhängens von Daten an ein Medium. Dies wird der Anhängezeitraum genannt.
- Zeitpunkt und Ziel zum Senden der Daten an Speicher.

Medien, die zu einem Mediensatz gehören, werden als zugewiesene Medien bezeichnet. Bei zugewiesenen Medien sind aktuelle Anhänge- und Überschreibschutzzeiträume vorhanden. Medien, die zu einem Mediensatz gehören, deren Überschreibschutzzeitraum aber abgelaufen ist, werden wiederverwendbare Medien genannt.

Informationen zu den Best Practices zum Verwalten von Bändern in Backup Exec finden Sie unter *Best Practices für Backup Exec*.

Siehe ["Standard-Mediensätze"](#) auf Seite 473.

Siehe ["Rotationsstrategien für Bandmedien"](#) auf Seite 508.

Siehe ["Erstellen von Mediensätzen für Bänder"](#) auf Seite 480.

Standard-Mediansätze

Wenn Sie Backup Exec installieren, werden automatisch Standard-Systemmediensätze und Standard-Benutzermediensätze erstellt. Wenn Sie Backup Exec Bänder hinzufügen, indem Sie Medien importieren, verknüpft Backup Exec die Bänder mit einem der Systemmediensätze.

Hinweis: Sie sollten temporäre Medien nicht mit einem von Ihnen erstellten Mediansatz verknüpfen. Wenn ein Backup-Auftrag ausgeführt wird, verschiebt Backup Exec automatisch die Medien aus dem temporären Mediansatz, in den erforderlichen Mediansatz.

Siehe ["Importieren von Medien in Backup Exec"](#) auf Seite 558.

Sie können die Eigenschaften von Systemmediensätzen nicht ändern. Systemmediensätze werden in der folgenden Tabelle beschrieben:

Tabelle 11-2 Standard-Systemmediensätze

Name	Beschreibung
Backup Exec- und Windows NT-Backup-Medien	Listet alle Medien auf, die aus einer anderen Installation von Backup Exec importiert werden. Siehe "Katalogisieren eines Speichergeräts" auf Seite 548.
Reinigungsmedien	Zeigt alle Reinigungsmedien an. Siehe "Reinigen eines Wechslerlaufwerks" auf Seite 556.
Fremde Medien	Listet alle Medien auf, die von anderen Produkten als Backup Exec importiert werden. Siehe "Info zur Wiederherstellung von NetWare SMS-Datenträger-Backups auf andere als SMS-Datenträger mit Backup Exec" auf Seite 277. Siehe "Katalogisieren eines Speichergeräts" auf Seite 548.

Name	Beschreibung
Ausrangierte Medien	<p>Liste aller Medien, die nicht mehr genutzt werden, meistens weil die Anzahl der aufgetretenen Fehler nicht mehr akzeptabel ist: Nachdem Sie Medien mit dem ausrangierten Mediensatz verbinden, wählt Backup Exec ihn nicht für Backup-Aufträge aus. Sie stehen jedoch nach wie vor für Wiederherstellungsaufträge zur Verfügung, sofern sie nicht beschädigt sind. "Ausrangierte Medien" werden nicht mehr weiterverwendet (überschrieben).</p> <p>Wenn Backup Exec Daten auf einem Band nicht erkennen kann, dann verschiebt es das Band in "Ausrangierte Medien". Wenn Sie das Band wiederverwenden möchten, löschen oder kennzeichnen Sie es. Diese Vorgänge schreiben eine neue Kopfzeile auf das Band, die von Backup Exec gelesen werden kann. Nachdem das Band gelöscht oder gekennzeichnet wurde, verschiebt Backup Exec es auf das festgelegte temporäre Medium.</p> <p>Sie können Medien aus "Ausrangierte Medien" löschen, um sie aus Backup Exec zu entfernen. Sie sollten Medien löschen, wenn viele externe Medien vorhanden sind, die Sie nicht wiederverwenden möchten. Sie können Medien auch löschen, wenn Sie die Medien wegwerfen.</p> <p>Siehe "Band- oder Datenträgermedien löschen" auf Seite 502.</p> <p>Siehe "Ausrangieren beschädigter Bandmedien" auf Seite 501.</p>
Temporäre Medien	<p>Zeigt alle überschreibbaren Medien an. Neue und leere Medien sowie Medien, deren Daten gelöscht wurden, werden automatisch mit dem Satz "Temporäre Medien" verknüpft.</p> <p>Siehe "Überschreibschutzzeiträume und Anhängenzeiträume in Mediensätzen" auf Seite 476.</p>

Backup Exec erstellt die folgenden Standardbenutzermediensätze:

Tabelle 11-3 Standardbenutzermediensätze

Name	Beschreibung
Daten für 4 Wochen aufbewahren	<p>Zeigt alle Bandmedien an, die mit diesem Mediensatz verknüpft sind. Wenn Sie die standardmäßigen Backup-Aufträge verwenden, die bei der Installation von Backup Exec festgelegt wurden, ist der Mediensatz "Daten für 4 Wochen aufbewahren" der Standardmediensatz für alle Backup-Aufträge, die an den Bandspeicher gesendet werden. Dieser Mediensatz schützt Daten für vier Wochen vor dem Überschreiben und ermöglicht es, dass die Medien sechs Tage lang angehängt werden können.</p> <p>Sie können die Option "Daten für 4 Wochen aufbewahren" nach der Installation bearbeiten und umbenennen. Deshalb wird sie möglicherweise in der Ansicht "Medien" oder in den Backup-Auftragsstandards nicht mehr mit dem Namen "Daten für 4 Wochen aufbewahren" angezeigt.</p>
Daten unbegrenzt beibehalten – kein Überschreiben zulassen	<p>Zeigt alle Bandmedien an, die mit diesem Mediensatz verknüpft sind.</p> <p>Wenn Sie Medien diesem Mediensatz zuordnen, werden Daten nicht überschrieben, es sei denn, Sie führen auf den Medien eine der folgenden Aktionen durch:</p> <ul style="list-style-type: none">■ Löschen■ Kennzeichnen■ Formatieren■ Zuordnen der Medien zum temporären Mediensatz <p>Sie können diesen Medien Daten während eines unbegrenzten Zeitraums (bis die Medien voll sind) anhängen.</p> <p>Sie können die Option "Daten unbegrenzt beibehalten – kein Überschreiben zulassen" nach der Installation bearbeiten und umbenennen. Daher wird sie in der Ansicht "Medien" oder in den Backup-Auftragsstandards möglicherweise nicht mehr als "Daten unbegrenzt beibehalten – kein Überschreiben zulassen" angezeigt.</p>

Sie können den Standardmediensatz für Backup-Aufträge ändern. Hierfür haben Sie folgende Möglichkeiten:

- Erstellen Sie neue Mediensätze und legen Sie deren Anhänge- und Überschreibschutzzeiträume auf die Zeitintervalle fest, die Ihrer Datenaufbewahrungsstrategie entsprechen. Dann geben Sie den Mediensatz an, der am angebrachtesten ist, wenn Sie einen Backup-Auftrag erstellen.

Beispielsweise können Sie einen Mediensatz, der Daten für 60 Tage beibehält, und einen Mediensatz erstellen, der Daten für 90 Tage beibehält.

- Wählen Sie den anderen Standardmediensatz "Daten unbegrenzt beibehalten - kein Überschreiben zulassen" aus, wenn Sie einen Backup-Auftrag erstellen. Das Risiko, das mit dem Mediensatz "Daten unbegrenzt beibehalten - kein Überschreiben zulassen" zusammenhängt, besteht darin, dass Sie alle Ihre temporären Medien verwenden können. Sie müssen Backup Exec laufend neue Band- oder Plattenkassettenmedien hinzufügen.

Hinweis: Es wird empfohlen, wenn Sie Daten länger als vier Wochen aufbewahren müssen, diese zu duplizieren. Sie können die Backup-Daten aus dem ursprünglichen Speichergerät auf Band duplizieren, das Sie dann zur langfristigen oder externe Off-Site-Aufbewahrung senden können.

So zeigen Sie alle Mediensätze an

- ◆ Klicken Sie auf der Registerkarte "Speicher" auf "Alle Mediensätze".

Siehe ["Überschreibschutzzeiträume und Anhängezeiträume in Mediensätzen"](#) auf Seite 476.

Siehe ["Erstellen von Mediensätzen für Bänder"](#) auf Seite 480.

Siehe ["Erstellen von Medienspeicherregeln zum Verschieben von Speichermedien in und aus Medienspeichern"](#) auf Seite 499.

Siehe ["Manuelles Duplizieren von Backup-Sätzen bzw. Auftragsverläufen"](#) auf Seite 246.

Siehe ["Verknüpfen von Bandmedien mit einem Mediensatz"](#) auf Seite 505.

Überschreibschutzzeiträume und Anhängezeiträume in Mediensätzen

Jedes Bandmedium ist mit einem Mediensatz verbunden, der Regeln zum Verwalten der Medien enthält.

Diese Regeln umfassen Überschreibschutz- und Anhängezeiträume.

Tabelle 11-4 Überschreibschutz- und Anhängezeiträume

Regel	Beschreibung
Anhängezeitraum	Der Zeitraum, in dem einem Medium Daten hinzugefügt (angehängt) werden können. Er wird von dem Zeitpunkt an gemessen, zu dem das Medium zugewiesen wurde. Der Zeitraum kann in Stunden, Tagen, Wochen oder Jahren angegeben werden.

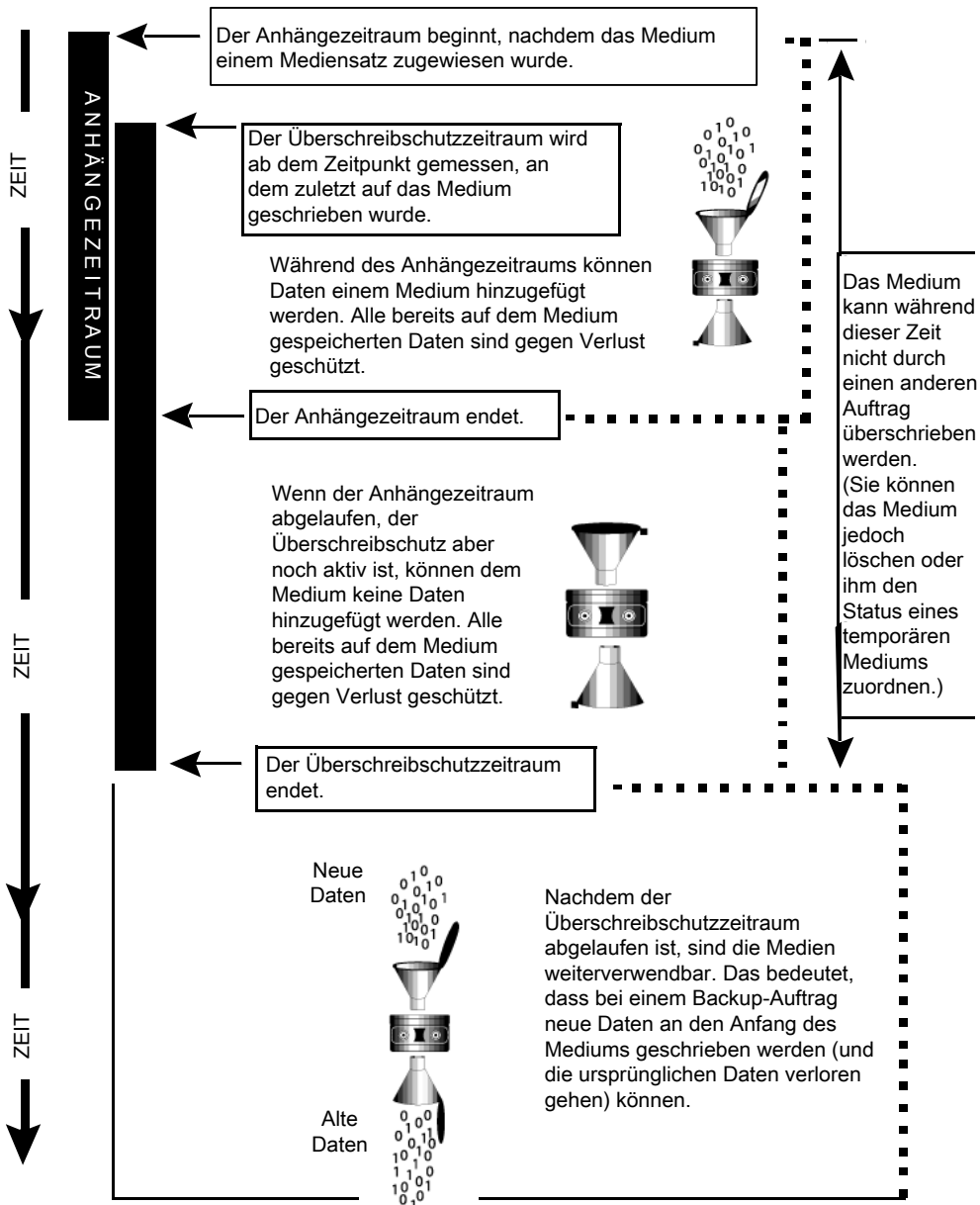
Regel	Beschreibung
Überschreibschutzzeitraum	<p>Der Zeitraum, in dem Bandmedien vor Überschreibung geschützt sind. Dieser Zeitraum wird von dem Zeitpunkt an berechnet, zu dem zuletzt auf den Datenträger geschrieben wurde, d. h., er beginnt mit dem Ende des letzten Anhäng- oder Überschreibungsauftrags. Der Zeitraum kann in Stunden, Tagen, Wochen oder Jahren angegeben werden. Nachdem der Überschreibschutzzeitraum abgelaufen ist, ist das Medium weiterverwendbar und kann überschrieben werden.</p> <p>Der Überschreibschutzzeitraum beginnt, nachdem der Backup-Auftrag beendet wurde. Wenn ein Anhängezeitraum eingestellt wurde, beginnt der Überschreibschutzzeitraum jedes Mal nach Beenden eines Anhängauftrags. Da der Überschreibschutzzeitraum erst nach Abschluss des Auftrags beginnt, wirkt sich die Dauer des Auftrags darauf aus, wann die Medien überschrieben werden können. Sie können den Überschreibschutzzeitraum verkürzen, um die zur Ausführung des Auftrags benötigte Zeit einzurechnen.</p> <p>So könnten Sie z. B. einen Überschreibschutzzeitraum von sieben Tagen festlegen. Außerdem legen Sie den Anhängezeitraum auf vier Tage fest, um sicherzustellen, dass Daten mindestens sieben Tage lang nicht überschrieben werden. Auf den Datenträgern können damit innerhalb der folgenden vier Tage Daten hinzugefügt werden. Die letzten auf diesem Datenträger angehängten Daten werden mindestens sieben Tage lang gespeichert.</p> <p>Hinweis: Wenn als Überschreibschutzstufe "Keine" festgelegt wird, können Medien grundsätzlich überschrieben werden.</p> <p>Siehe "Medienüberschreibschutzstufen für Bandmedien" auf Seite 487.</p>

Bei der Wahl Ihrer Medienrotationsstrategie müssen Sie einerseits berücksichtigen, dass Daten so lange wie möglich aufbewahrt werden sollen, andererseits, dass nur in begrenztem Umfang Bandmedien verfügbar sind. Anhand der Mediensatzregeln kann Backup Exec feststellen, auf welche Bandmedien geschrieben werden kann und bei welchen Überschreibschutz besteht. Sie sollten den Gebrauch von Plattenspeichern für Backup-Daten erwägen.

Siehe "[Konfigurieren von Festplattenspeicher](#)" auf Seite 372.

Die folgende Grafik zeigt das Verhältnis zwischen dem Anhängezeitraum und dem Überschreibschutzzeitraum an.

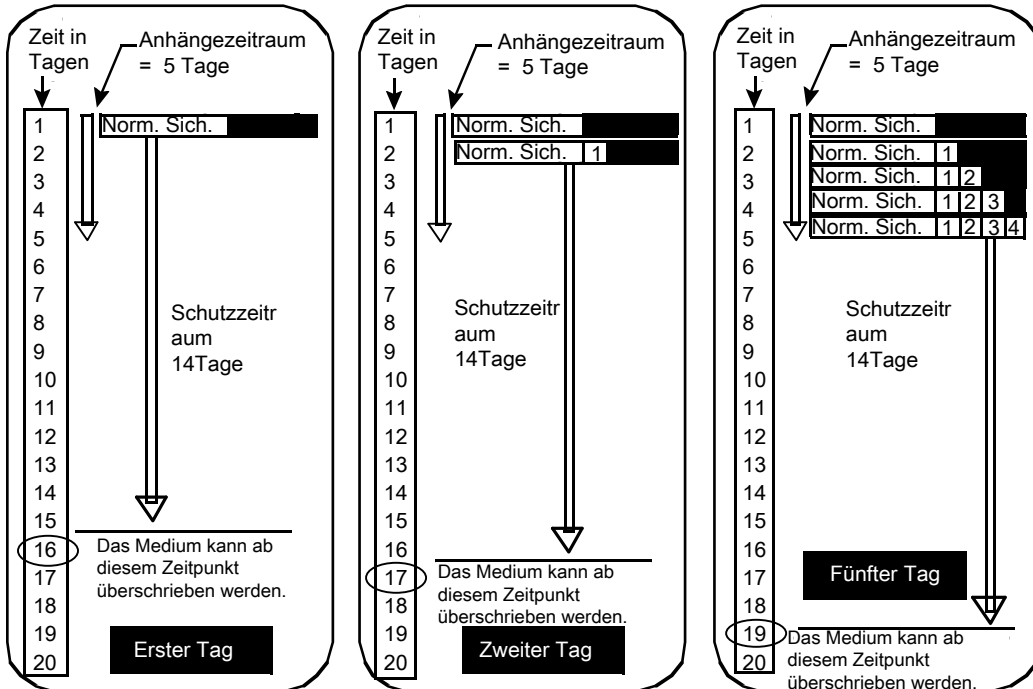
Abbildung 11-1 Anhängezeiträume und Überschreibschutzzeiträume



Die Einstellungen für den Anhänge- und Überschreibschutzzeitraum gelten für alle Daten auf dem Medium.

Daher wird beim Schreiben von Daten auf Medien die für den Überschreibschutzzeitraum verbleibende Zeit zurückgesetzt und neu mit der Zählung begonnen.

Abbildung 11-2 Zurücksetzen von Überschreibschutzzeiträumen



Der für den Abschluss des Auftrags erforderliche Zeitraum wirkt sich darauf aus, wann die Medien überschrieben werden können.

Angenommen, Sie erstellen einen Mediensatz mit dem Namen "Wöchentlich", für den ein Überschreibschutzzeitraum von sieben Tagen gilt. Sie geben außerdem einen Anhängenzeitraum von null Tagen an und Sie planen einen vollständigen Backup-Auftrag, der jeden Freitag um 20:00 Uhr ausgeführt werden soll. Der vollständige Backup-Auftrag am folgenden Freitag um 20:00 kann jedoch nicht ausgeführt werden. Der erste Backup-Auftrag, der am vorherigen Freitag ausgeführt wurde, war erst um 21:10 Uhr abgeschlossen. Damit verbleiben 70 Minuten des Überschreibschutzzeitraums für den Mediensatz "Wöchentlich".

Um derartige Situationen zu vermeiden, können Sie den Überschreibschutzzeitraum so verkürzen, dass die für die Auftragsausführung erforderliche Zeit eingerechnet wird. In diesem Beispiel kann der geplante wiederkehrende Auftrag um 20:00 Uhr

ausgeführt werden, wenn für den Überschreibschutzzeitraum nicht sieben, sondern sechs Tage festgelegt werden.

Erstellen von Mediensätzen für Bänder

Ein Mediensatz besteht aus den Regeln, die Folgendes angeben:

- Anhängezeiträume
- Überschreibschutzzeiträume
- Medienspeicher
- Zeitraum für die Verschiebung von Medien in den und aus dem Medienspeicher

Die Mediensatzregeln treffen auf alle Medien zu, die Sie mit dem Mediensatz verbinden.

Hinweis: Sie müssen bereits einen Medienspeicher erstellt haben, bevor Sie aufgefördert werden, Medienspeicherregeln in einem Mediensatz hinzuzufügen.

Siehe "[Standard-Mediansätze](#)" auf Seite 473.

So erstellen Sie einen Mediensatz für Bänder

- 1 Auf der Registerkarte "Speicher" erweitern Sie "Band- und Plattenspeichermedien".
- 2 Doppelklicken Sie auf "Alle Mediansätze".
- 3 Klicken Sie unter "Benutzer-Mediansätze" mit der rechten Maustaste auf einen Mediansatz und klicken Sie dann auf "Mediansatz erstellen".
- 4 Geben Sie einen Namen und eine Beschreibung für den Mediansatz ein und klicken Sie dann auf "Weiter".
- 5 Geben Sie an, wie lange Sie Daten in diesem Mediansatz vor dem Überschreiben schützen möchten und klicken Sie dann auf "Weiter".
- 6 Geben Sie an, wie lange Daten an Medien in diesem Mediansatz angehängt werden dürfen und klicken Sie dann auf "Weiter".
- 7 Überprüfen Sie die Übersicht und führen Sie anschließend eine der folgenden Aktionen aus:

So ändern Sie die Konfiguration

Gehen Sie dazu in folgender Reihenfolge vor:

- Klicken Sie auf die Überschrift, die die Elemente enthält, die Sie ändern möchten.
- Nehmen Sie alle Änderungen, vor und klicken Sie dann auf "Weiter", bis die Übersicht angezeigt wird.
- Klicken Sie auf "Fertigstellen".

So erstellen Sie den Mediensatz

Klicken Sie auf "Fertigstellen".

Bearbeiten der Eigenschaften von Mediensätzen

Sie können die folgenden Eigenschaften für Mediensätze bearbeiten:

- Name des Mediensatzes.
- Überschreibschutz- und Anhängezeiträume für einen Mediensatz.
- Medienspeicher und Speicherzeiträume, die einem Mediensatz zugeordnet sind.

Siehe "[Standard-Mediansätze](#)" auf Seite 473.

So bearbeiten Sie Eigenschaften von Mediensätzen

- 1 Erweitern Sie auf der Registerkarte "Speicher" den Eintrag "Band- und Plattenspeichermedien".
- 2 Doppelklicken Sie auf "Alle Mediansätze".
- 3 Doppelklicken Sie auf den Mediansatz, für den Sie Eigenschaften bearbeiten möchten.
- 4 Klicken Sie im linken Teilfenster auf "Eigenschaften".
- 5 Ändern Sie eine der folgenden Informationen:

Name

Zeigt den Namen des Mediansatzes an.

Beschreibung

Zeigt die Beschreibung des Mediansatzes an.

Überschreibschutzzeitraum

Zeigt den Zeitraum in Stunden, Tagen, Wochen oder Jahre an, in dem die Daten auf den Medien beibehalten werden, bevor sie überschrieben werden können.

Mit den folgenden Vorgängen können Medien unabhängig vom festgelegten Überschreibschutzzeitraum überschrieben werden:

- Löschen
- Kennzeichnen
- Verknüpfen mit dem Satz temporärer Medien
- Festlegen von "Medienüberschreibschutzstufe" auf "Keine"
- Formatieren

Aufgrund der Methode, mit der Backup Exec die Zeit berechnet, wird die von Ihnen eingegebene Zeiteinheit eventuell konvertiert. Wenn Sie z. B. 14 Tage eingeben, kann der Eintrag bei der nächsten Ansicht als zwei Wochen angezeigt sein.

Der Standardzeitraum ist "Unbegrenzt - Überschreiben nicht ermöglichen", der die Medien für 1.000 Jahre vor dem Überschreiben schützt.

Siehe ["Überschreibschutzzeiträume und Anhängezeiträume in Mediensätzen"](#) auf Seite 476.

Anhängezeitraum

Gibt den Zeitraum in Stunden, Tagen oder Wochen an, in dem den Medien Daten hinzugefügt werden können. Aufgrund der Methode, mit der Backup Exec die Zeit berechnet, wird die von Ihnen eingegebene Zeiteinheit eventuell konvertiert. Wenn Sie z. B. 14 Tage eingeben, kann der Eintrag bei der nächsten Ansicht als zwei Wochen angezeigt sein.

Der Anhangzeitraum beginnt, wenn der erste Backup-Auftrag auf das Medium geschrieben wird.

Der Standardzeitraum ist "Unbegrenzt – Anhängen ermöglichen", bei der Daten so lange angehängt werden können, bis die Kapazität des Mediums erschöpft ist.

Für diesen Mediensatz zu verwendender Medienspeicher

Zeigt den Medienspeicher an, in dem die mit diesem Mediensatz verbundenen Medien gespeichert werden.

Siehe "[Standardmedienspeicher](#)" auf Seite 496.

Medien in diesen Speicher verschieben nach

Gibt den Zeitraum an, nach dem gemeldet wird, dass das Medium in diesen Speicher verschoben werden kann.

Medien aus diesem Speicher zurückholen nach

Gibt den Zeitraum an, nach dem gemeldet wird, dass das Medium aus diesem Speicher zurückgeholt werden kann.

6 Klicken Sie auf "Übernehmen".

Ändern des Überschreibschutz- oder Anhangzeitraums für einen Mediensatz

Sie können die Länge des Zeitraums ändern, für den Medien, die zu einem Mediensatz gehören, aufbewahrt werden. Sie können auch die Länge des Zeitraums ändern, für den Daten zu Medien, die zu einem Mediensatz gehören, hinzugefügt werden können.

Siehe "[Überschreibschutzzeiträume und Anhangzeiträume in Mediensätzen](#)" auf Seite 476.

So ändern Sie den Überschreibschutz- oder Anhängezeitraum für einen Mediensatz

- 1 Erweitern Sie auf der Registerkarte "Speicher" den Eintrag "Band- und Plattenspeichermedien".
- 2 Doppelklicken Sie auf "Alle Mediensätze".
- 3 Doppelklicken Sie auf den Mediensatz, für den Sie den Überschreibschutz- oder Anhängezeitraum ändern möchten.
- 4 Klicken Sie im linken Teilfenster auf "Eigenschaften".
- 5 Ändern Sie die folgenden Informationen je nach Bedarf:

Überschreibschutzzeitraum

Zeigt den Zeitraum in Stunden, Tagen, Wochen oder Jahre an, in dem die Daten auf den Medien beibehalten werden, bevor sie überschrieben werden können.

Mit den folgenden Vorgängen können Medien unabhängig vom festgelegten Überschreibschutzzeitraum überschrieben werden:

- Löschen
- Kennzeichnen
- Verknüpfen mit dem Satz temporärer Medien
- Festlegen von "Medienüberschreibschutzstufe" auf "Keine"
- Formatieren

Aufgrund der Methode, mit der Backup Exec die Zeit berechnet, wird die von Ihnen eingegebene Zeiteinheit eventuell konvertiert. Wenn Sie z. B. 14 Tage eingeben, kann der Eintrag bei der nächsten Ansicht als zwei Wochen angezeigt sein.

Der Standardzeitraum ist "Unbegrenzt - Überschreiben nicht ermöglichen", der die Medien für 1.000 Jahre vor dem Überschreiben schützt.

Anhängezeitraum

Gibt den Zeitraum in Stunden, Tagen oder Wochen an, in dem den Medien Daten hinzugefügt werden können.

Aufgrund der Methode, mit der Backup Exec die Zeit berechnet, wird die von Ihnen eingegebene Zeiteinheit eventuell konvertiert. Wenn Sie z. B. 14 Tage eingeben, kann der Eintrag bei der nächsten Ansicht als zwei Wochen angezeigt sein.

Der Anhängezeitraum beginnt, wenn der erste Backup-Auftrag auf das Medium geschrieben wird.

Der Standardzeitraum ist "Unbegrenzt – Anhängen ermöglichen", bei der Daten so lange angehängt werden können, bis die Kapazität des Mediums erschöpft ist.

- 6 Klicken Sie auf "Übernehmen".

Ändern des Namens und der Beschreibung eines Mediensatzes

Sie können den Namen und die Beschreibung eines Mediensatzes ändern.

So ändern Sie den Namen und die Beschreibung eines Mediensatzes

- 1 Erweitern Sie auf der Registerkarte "Speicher" den Eintrag "Band- und Plattenspeichermedien".
- 2 Doppelklicken Sie auf "Alle Mediensätze".
- 3 Doppelklicken Sie auf den Mediensatz, dessen Namen bzw. Beschreibung Sie ändern möchten.
- 4 Klicken Sie im linken Teilfenster auf "Eigenschaften".
- 5 Ändern Sie den Namen bzw. die Beschreibung des Mediensatzes und klicken Sie dann auf "Übernehmen".

Ändern des Medienspeicher oder der Vaulting-Zeiträume für einen Mediensatz

Sie können den Medienspeicher ändern, in dem dieser Mediensatz gespeichert wird, und Sie können die Zeiträume ändern, in denen Medien in einen Speicher verschoben oder von einem Speicher abrufen möchten.

Siehe ["Standardmedienspeicher"](#) auf Seite 496.

So ändern Sie den Medienspeicher oder die Vaulting-Zeiträume für einen Mediensatz

- 1 Erweitern Sie auf der Registerkarte "Speicher" den Eintrag "Band- und Plattenspeichermedien".
- 2 Doppelklicken Sie auf "Alle Mediensätze".
- 3 Doppelklicken Sie auf den Mediensatz, für den Sie den Medienspeicher oder die Vaulting-Zeiträume ändern möchten.
- 4 Klicken Sie im linken Teilfenster auf "Eigenschaften".
- 5 Ändern Sie die folgenden Informationen entsprechend:

Für diesen Mediensatz zu verwendender Medienspeicher	Zeigt den Medienspeicher an, in dem die mit diesem Mediensatz verbundenen Medien gespeichert werden.
Medien in diesen Speicher verschieben nach	Gibt den Zeitraum an, nach dem gemeldet wird, dass das Medium in diesen Speicher verschoben werden kann.
Medien aus diesem Speicher zurückholen nach	Gibt den Zeitraum an, nach dem gemeldet wird, dass das Medium aus diesem Speicher zurückgeholt werden kann.

- 6 Klicken Sie auf "Übernehmen".

Löschen eines Mediensatzes

Wenn Sie einen Mediensatz löschen, mit dem geplante Aufträge verbunden sind, werden Sie aufgefordert, die Aufträge mit einem anderen Mediensatz zu verbinden.

Vorsicht: Stellen Sie sicher, dass für den Mediensatz, mit dem Sie die Aufträge verbinden, angemessene Überschreibschutz- und Anhängenzeiträume festgelegt wurden.

Siehe ["Standard-Mediansätze"](#) auf Seite 473.

So löschen Sie einen Mediensatz

- 1 Auf der Registerkarte "Speicher" erweitern Sie "Band- und Plattenspeichermedien".
- 2 Doppelklicken Sie auf "Alle Mediansätze".

- 3 Klicken Sie mit der rechten Maustaste auf den Mediensatz, den Sie löschen möchten, und klicken Sie dann auf "Löschen".
- 4 Wenn Sie aufgefordert werden, den Mediensatz zu löschen, klicken Sie auf "OK".

Umbenennen eines Mediensatzes

Wenn Sie einen Mediensatz umbenennen, werden alle Aufträge, die diesen Mediensatz verwenden, mit dem neuen Mediensatznamen angezeigt.

Siehe ["Standard-Mediensätze"](#) auf Seite 473.

So benennen Sie einen Mediensatz um

- 1 Auf der Registerkarte "Speicher" erweitern Sie "Band- und Plattenspeichermedien".
- 2 Doppelklicken Sie auf "Alle Mediensätze".
- 3 Klicken Sie mit der rechten Maustaste auf den Mediensatz, den Sie umbenennen möchten, und klicken Sie dann auf "Details".
- 4 Im linken Teilfenster klicken Sie auf "Eigenschaften".
- 5 Geben Sie im Feld "Name" den neuen Namen ein, den Sie dem Mediensatz zuweisen möchten. Klicken Sie anschließend auf "Übernehmen".

Medienüberschreibschutzstufen für Bandmedien

Die Medienüberschreibschutzstufe ist eine globale Einstellung, die den Überschreibschutzzeitraum des Mediensatzes außer Kraft setzt. Obwohl sich die Medienüberschreibschutzstufen und der Überschreibschutzzeitraum ähnlich anhören, handelt es sich um zwei verschiedene Dinge. Der Überschreibschutzzeitraum von Medien ist ein Zeitraum, der für jeden Mediensatz einzeln festgelegt wird und bei verschiedenen Mediensätzen unterschiedliche Werte haben kann. Die Medienüberschreibschutzstufe gibt an, ob temporäre, importierte oder zugewiesene Medien überschrieben werden können, wobei der Überschreibschutzzeitraum nicht berücksichtigt wird.

Verwenden Sie die Medienüberschreibschutzstufe, um den Typ der Medien anzugeben, die zum Überschreiben von Backups verfügbar sein sollen.

Siehe ["Überschreibschutzzeiträume und Anhängenzeiträume in Mediensätzen"](#) auf Seite 476.

Überschreiben der zugeordneten oder importierten Bandmedien

Medien, die zu einem Mediensatz gehören, sind sogenannte zugewiesene Medien. Medien, die aus einer anderen Installation von Backup Exec oder aus einem anderen Produkt importiert werden, werden als importierte Medien bezeichnet. Backup Exec schützt zugewiesene und importierte Medien vor dem Überschreiben, wenn vollständiger oder teilweiser Überschreibschutz verwendet wird. Sie können Backup Exec jedoch anweisen, dass zugewiesene und importierte Medien vor Ablauf des Überschreibschutzzeitraums für die Daten überschrieben werden sollen. Dazu ist es nicht erforderlich, als Überschreibschutzstufe "Kein" festzulegen.

Folgende Methoden sind verfügbar:

- Verbinden Sie die Medien mit dem Satz temporärer Medien. Das Medium wird überschrieben, wenn es für einen Überschreibauftrag ausgewählt wird.
- Löschen Sie das Medium. Gelöschte Medien werden automatisch als temporäre Medien erkannt und werden sofort überschrieben.
- Kennzeichnen Sie das Medium. Bei der Medienbezeichnung wird automatisch eine neue Medienkennung auf das Medium geschrieben, wodurch alle darauf enthaltenen Daten zerstört werden.
- Formatieren Sie das Medium. Die Formatierung zerstört alle Daten, die auf den Medien enthalten wird.
- Ändern Sie den Überschreibschutzzeitraum für den Mediensatz, sodass dieser abgelaufen ist.

Siehe ["Verwalten von Bändern"](#) auf Seite 472.

Siehe ["Löschen von Bandmedien"](#) auf Seite 502.

Siehe ["Bearbeiten globaler Einstellungen für Speicher"](#) auf Seite 535.

So sucht Backup Exec nach überschreibbaren Medien in Bandlaufwerken

Die Überschreiboptionen für Medien legen die Reihenfolge fest, in der Backup Exec Bandlaufwerke und Plattenkassetten nach überschreibbaren Medien durchsucht. Bei der Suche nach überschreibbaren Medien für einen Backup-Auftrag sucht Backup Exec entweder nach temporären Medien oder Medien, deren Überschreibschutzzeitraum abgelaufen ist.

Sie werden gefragt, welche Optionen Backup Exec zuerst verwenden soll:

- Temporäre Medien überschreiben, bevor wiederverwendbare Medien des Zielmediensatzes überschrieben werden.

Wenn Sie festlegen, dass temporäre Medien vor wiederverwendbaren Medien überschrieben werden sollen, werden evtl. mehr Medien für dieselbe Anzahl an

Aufträgen benötigt. Jedoch werden die wiederverwendbaren Medien evtl. länger für eine mögliche Wiederherstellung beibehalten.

- Wiederverwendbare Medien des Zielmediensatzes überschreiben, bevor temporäre Medien überschrieben werden.
Wenn Sie festlegen, dass wiederverwendbare Medien vor temporären Medien überschrieben werden sollen, werden dieselben Medien häufiger wiederverwendet, als wenn Sie temporäre Medien vor wiederverwendbaren Medien überschreiben.

In einem Speichergerätepool für Bandlaufwerke wählt Backup Exec zuerst die ältesten wiederverwendbaren Medien im Speichergerätepool für die Verwendung aus.

In einem Wechsler wählt Backup Exec zuerst das älteste wiederverwendbare Medium zur Verwendung aus. Falls der Wechsler partitioniert wurde, sucht Backup Exec nur in der angegebenen Partition nach dem ältesten wiederverwendbaren Medium.

Vorsicht: Es wird empfohlen, für Medien, die kritische Daten enthalten, einen physischen Schreibschutz zu verwenden. Verwenden Sie den Schreibschutz der Medienkassette zum Schutz der Daten gegen unbeabsichtigtes Verschieben oder Löschen oder ablaufende Überschreibschutzzeiträume.

Die folgende Tabelle beschreibt die Reihenfolge, in der Backup Exec nach Medien für einen Überschreibungsauftrag sucht.

Tabelle 11-5 So sucht Backup Exec nach überschreibbaren Medien in Bandlaufwerken

Überschreibschutzstufe und Überschreiboption:	Medien werden im Bandlaufwerk in dieser Reihenfolge überschrieben:
Vollständig + Temporäre Medien zuerst überschreiben Hinweis: Diese Kombination gewährleistet den bestmöglichen Überschreibschutz.	1 Temporäre Medien 2 Wiederverwendbare Medien im Zielmediensatz 3 Wiederverwendbare Medien in einem beliebigen Mediensatz
Vollständig + Wiederverwendbare Medien zuerst überschreiben	1 Wiederverwendbare Medien im Zielmediensatz 2 Temporäre Medien 3 Wiederverwendbare Medien in einem beliebigen Mediensatz

Überschreibschutzstufe und Überschreiboption:	Medien werden im Bandlaufwerk in dieser Reihenfolge überschrieben:
Teilweise + Temporäre Medien zuerst überschreiben	<ol style="list-style-type: none"> 1 Temporäre Medien 2 Wiederverwendbare Medien im Zielmediensatz 3 Wiederverwendbare Medien in einem beliebigen Mediensatz 4 Medien, die aus einer anderen Installation von Backup Exec oder aus einem anderen Produkt importiert wurden
Teilweise + wiederverwendbare Medien zuerst überschreiben	<ol style="list-style-type: none"> 1 Wiederverwendbare Medien im Zielmediensatz 2 Temporäre Medien 3 Wiederverwendbare Medien in einem beliebigen Mediensatz 4 Medien, die aus einer anderen Installation von Backup Exec oder aus einem anderen Produkt importiert wurden
Kein – Kein Überschreibschutz + Temporäre Medien zuerst überschreiben Warnung: Die Auswahl dieser Option wird nicht empfohlen, da hierdurch Daten nicht vor dem Überschreiben geschützt werden.	<ol style="list-style-type: none"> 1 Temporäre Medien 2 Wiederverwendbare Medien im Zielmediensatz 3 Wiederverwendbare Medien in einem beliebigen Mediensatz 4 Medien, die aus einer anderen Installation von Backup Exec oder aus einem anderen Produkt importiert wurden 5 Zugewiesene Medien in einem beliebigen Mediensatz
Kein – Kein Überschreibschutz + Wiederverwendbare Medien zuerst überschreiben Warnung: Die Auswahl dieser Option wird nicht empfohlen, da hierdurch Daten nicht vor dem Überschreiben geschützt werden.	<ol style="list-style-type: none"> 1 Wiederverwendbare Medien im Zielmediensatz 2 Temporäre Medien 3 Wiederverwendbare Medien in einem beliebigen Mediensatz 4 Medien, die aus einer anderen Installation von Backup Exec oder aus einem anderen Produkt importiert wurden 5 Zugewiesene Medien in einem beliebigen Mediensatz

Neben dem Einstellen der Überschreibschutzstufen müssen Sie in den Überschreiboptionen auch eine Reihenfolge angeben, in der Backup Exec nach wiederbeschreibbaren Medien sucht.

Die offensichtlichsten Kandidaten für Backup-Aufträge, die überschreibbare Medien erfordern, sind temporäre Medien und wiederverwendbare Medien. Wiederverwendbare Medien haben abgelaufene Überschreibschutzzeiträume. Backup Exec sucht zuerst nach diesen Medientypen, wenn für ein Backup Bandmedien überschrieben werden müssen. Das Suchmuster ist davon abhängig, welche der Optionen "Vollständig", "Teilweise" oder "Kein" Sie ausgewählt haben. Das Medium zeigt an, dass ein Typ von Mediensätzen auf Verfügbarkeit überprüft wird.

Siehe ["Bearbeiten globaler Einstellungen für Speicher"](#) auf Seite 535.

Siehe ["Standardmedienspeicher"](#) auf Seite 496.

Anzeigen von Bändern, die von einem Auftrag genutzt werden

Wenn Sie wissen möchten, welche Bänder für einen Auftrag genutzt werden, lesen Sie den Abschnitt "Gerät- und Medieninformationen" im Auftragsprotokoll.

Siehe ["Verwalten von Bändern"](#) auf Seite 472.

So zeigen Sie die Bänder an, die von einem Auftrag genutzt werden

1 Sie haben folgende Möglichkeiten:

So zeigen Sie das Auftragsprotokoll auf der Registerkarte "Auftragsüberwachung" an

Klicken Sie auf die Registerkarte "Auftragsüberwachung".

So zeigen Sie das Auftragsprotokoll auf der Registerkarte "Backup und Wiederherstellung" oder "Speicher" an

Gehen Sie dazu nach folgender Reihenfolge vor:

- Doppelklicken Sie auf einer der Registerkarten "Backup und Wiederherstellung" oder "Speicher" auf den Server oder das Speichergerät, auf dem der Auftrag ausgeführt wurde.
- Im linken Teilfenster klicken Sie auf "Auftragsverlauf".

2 Klicken Sie mit der rechten Maustaste auf den Auftrag und wählen Sie "Auftragsprotokoll anzeigen".

3 Überprüfen Sie die Informationen im Abschnitt Gerät- und Medieninformationen.

Kennzeichen von Bandmedien

Medienkennungen identifizieren die Bänder, die Sie in Backup Exec verwenden. Wenn neue, leere oder nicht gekennzeichnete Bänder während eines Backup-Vorgangs verwendet werden, kennzeichnet Backup Exec die Medien automatisch. Diese Kennzeichnung besteht aus einem Präfix für den Medientyp und einer laufenden Nummer. So werden z. B. für ein 4-mm-Band das Präfix "4M" und die Nummer "000001" festgelegt. Für das nächste unbenannte 4-mm-Band wird die Kennung "4M000002" generiert usw.

Ein weiterer von Backup Exec verwendeter Medienkennungstyp ist die Medien-ID. Die Medien-ID ist eine eindeutige Kennung, die von Backup Exec für einzelne in Backup Exec verwendete Bandmedien vergeben wird. Die Medien-ID wird von Backup Exec intern verwendet, um statistische Daten für jedes Medium aufzuzeichnen. Weil die Medien- oder Barcodeerkennung für Medien geändert werden kann, benötigt Backup Exec die Medien-ID, um Kontinuität Bestandsführung für einzelne Bandmedien zu gewährleisten. Sie können die Medien-ID nicht ändern oder löschen. Die Medien-ID hat keine Auswirkungen auf die Medienkennung bzw. auf die Möglichkeiten zum Umbenennen, Kennzeichnen oder Löschen von Bandmedien.

In manchen Fällen benötigen Sie die Medien-ID eventuell zur Unterscheidung von Bandmedien mit identischen Medienkennungen. Doppelte Kennungen können automatisch bei einer erneuten Installation von Backup Exec oder bei der Verwendung von Medien einer anderen Backup Exec-Installation erzeugt werden. Sie können die Medien-ID auf der Eigenschaftenseite des Mediums anzeigen lassen.

SchreibenBeschriften Sie das Etikett auf dem physischen Bandmedien mit der Medienkennung. Sie sollten bei jeder Änderung der Medienkennung auch das Etikett auf dem physischen Medium entsprechend ändern.

Folgende Methoden stehen in Backup Exec zum Ändern einer Medienkennung zur Verfügung:

- Schreiben Sie eine neue Medienkennung auf das Bandmedium. Der Vorgang "Kennung" zerstört alle Daten auf den Medien.
- Benennen Sie die Medien um. Durch Umbenennen ändern Sie zwar den Namen des Mediums in der Anzeige, die neue Kennung wird jedoch erst bei einem Überschreibvorgang auf das Medium geschrieben. Die Daten auf dem Medium stehen so lange zur Verfügung, bis das Medium überschrieben wird.
- Bearbeiten Sie die Bezeichnung. Durch das Bearbeiten ändern Sie zwar den Namen des Bandmediums in der Anzeige, doch wird die neue Kennung erst bei einem Überschreibvorgang auf das Medium geschrieben. Die Daten auf

dem Medium stehen so lange zur Verfügung, bis das Medium überschrieben wird.

Hinweis: Medien, die Barcodekennungen verwenden, können nicht umbenannt werden. Wenn Sie versuchen, Medien zu kennzeichnen, die Barcodekennungen verwenden, werden erfolgreiche Aufträge in den Auftragsprotokollen aufgezeichnet. Die Namen der Medienkennungen ändern sich jedoch nicht.

So kennzeichnen Sie ein Medium

- 1** Führen Sie auf der Registerkarte "Speicher" einen der folgenden Schritte aus:
 - Klicken Sie mit der rechten Maustaste auf das Laufwerk, das das zu kennzeichnende Band enthält.
 - Doppelklicken Sie auf "Schächte" und klicken Sie anschließend mit der rechten Maustaste auf den Schacht, der das zu kennzeichnende Band enthält.
- 2** Klicken Sie auf "Kennzeichnen".

Die folgende Warnung wird angezeigt:

Dieser Vorgang wird an dem aktuellen Medium im Laufwerk oder Schacht vorgenommen. Wenn das Medium seit der letzten Inventarisierung geändert wurde, stimmt die Medienkennung im folgenden Dialogfeld eventuell nicht mit dem Medium im ausgewählten Gerät überein.

- 3** Klicken Sie auf "OK".
- 4** Geben Sie den Namen ein, der als Medienkennung für dieses Medium verwendet werden soll.
- 5** Um alle Daten auf den Medien zu löschen und die Medien neu zu bezeichnen, klicken Sie auf "OK".
- 6** Beschriften Sie das Etikett auf dem Medium mit dieser neuen Medienkennung.
- 7** (Optional) Zeigen Sie den Auftragsverlauf für Details zum Auftrag an.

Siehe ["Anzeigen von Aufträgen, Auftragsverläufen, Backup-Sätzen und aktiven Warnmeldungen für Speichergeräte"](#) auf Seite 548.

Siehe ["Umbenennen einer Bandmedienkennung "](#) auf Seite 495.

Siehe ["So werden Barcodebezeichnungen Medienkennungen für Bänder"](#) auf Seite 494.

Info zum Kennzeichnen von importierten Bandmedien

Bandmedien, die aus einer anderen Installation von Backup Exec oder aus einem anderen Produkt importiert werden, werden als importierte Medien bezeichnet. Importierte Medien werden von Backup Exec nicht automatisch neu gekennzeichnet.

Backup Exec liest die vorhandene Kennung der importierten Bandmedien und zeigt die Kennung entweder im Mediensatz "Backup Exec- und Windows NT-Backup-Medien" oder "Fremde Medien" an. Wenn die Überschreibschutzstufen "Teilweise" oder "Kein" aktiviert sind, können importierte Medien jedoch für Backup-Aufträge ausgewählt und überschrieben werden. Importierte Medien werden, wenn sie während eines Auftrags überschrieben werden, automatisch gekennzeichnet. Wenn Sie ein bestimmtes importiertes Medium kennzeichnen möchten, ohne dabei die Überschreibschutzstufe "Vollständig" für alle anderen importierten Medien zu deaktivieren, löschen Sie das betreffende Medium und kennzeichnen Sie es anschließend.

Die ursprüngliche Medienkennung der importierten Bandmedien wird in den Eigenschaften der Medien angezeigt. Sie können die Medienbeschreibung in der Eigenschaftenseite des Mediums bearbeiten und aussagekräftiger gestalten.

Siehe ["Band- oder Datenträgermedien löschen"](#) auf Seite 502.

So werden Barcodebezeichnungen Medienkennungen für Bänder

Wenn auf der physischen Kassette eine Barcodekennung vorhanden ist und der Wechsler über einen Barcodeleser verfügt, wird die Barcodekennung automatisch als Medienkennung verwendet.

Beispiel: Wechsler 1 bietet Unterstützung für Barcodes. Während eines Backup-Vorgangs fordert Backup Exec ein neues oder überschreibbares Medium an. Ein neues Medium mit der Barcodekennung "ABCD" wird in das Wechslermagazin eingelegt und der Barcodeleser scannt die Barcode-ID. Backup Exec wählt dieses Medium für den Auftrag aus und stellt fest, dass dem Medium eine Barcodekennung zugewiesen wurde. Backup Exec verwendet automatisch die Barcodekennung und setzt den Vorgang fort.

Wenn es sich bei der Medienkennung um einen Barcode handelt, können Sie die Medienkennung nicht in Backup Exec ändern. Um eine Barcode-Kennung zu ändern und eine Medienkennung zu verwenden, müssen Sie die physische Barcode-Kennung aus der Medienkassette entfernen. Sie können die Medien auch in einem Gerät verwenden, das keinen Barcodeleser hat.

Wenn Sie das Magazin austauschen oder neue Medien in das Magazin einlegen, können Sie die Schacht-Informationen mithilfe des Vorgangs "Einlesen" schnell aktualisieren.

Siehe ["Kennzeichen von Bandmedien"](#) auf Seite 492.

Siehe ["Scannen eines Speichergeräts"](#) auf Seite 549.

Umbenennen einer Bandmedienkennung

Sie können die Bezeichnung und die Kennung von Bandmedien umbenennen. Die neue Bezeichnung wird erst auf das Bandmedium geschrieben, wenn ein Überschreibvorgang stattfindet. Alle Daten auf den Medien bleiben bis zum nächsten Überschreibungsauftrag erhalten. Die neue Medienkennung wird jedoch in der Datenbank gespeichert und für das Medium angezeigt. Um sofort eine neue Medienkennung auf die Medien zu schreiben, verwenden Sie die Funktion "Kennung". Die Inhalte der Medien werden gelöscht.

Wenn Sie Bandmedien umbenennen und anschließend in einer anderen Installation von Backup Exec verwenden, werden diese Medien in den Mediensatz für Backup Exec und Windows NT importiert. Die ursprüngliche Medienkennung der Medien wird angezeigt. Die umbenannte Bezeichnung wird nicht in andere Installationen von Backup Exec übertragen.

Hinweis: Wenn es sich bei der Medienkennung um einen Barcode handelt, können Sie die Medienkennung nicht in Backup Exec ändern.

Siehe ["Kennzeichen von Bandmedien"](#) auf Seite 492.

So benennen Sie eine Bandmedienkennung um

- 1 Klicken Sie auf der Registerkarte "Speicher" mit der rechten Maustaste auf das Bandlaufwerk oder den Schacht mit dem Medium, dessen Bezeichnung Sie ändern möchten, und klicken Sie dann auf "Details".
- 2 Klicken Sie im linken Teilfenster auf "Medieneigenschaften".
- 3 Geben Sie im Feld "Medienkennung" die neue Bezeichnung ein.
- 4 Um die Beschreibung zu ändern, geben Sie eine neue Beschreibung im Feld "Medienbeschreibung" ein.
- 5 Klicken Sie auf "Übernehmen".

So werden WORM-Medien in Backup Exec verwendet

WORM-Datenspeicher (Write Once, Read Many) wird zum Speichern von Daten mit langer Aufbewahrungsdauer verwendet. Auf WORM-Medien können Daten nur einmal geschrieben werden. Nachdem einmal auf diese Medien geschrieben wurde,

können weitere Daten angefügt werden, das Überschreiben, Löschen oder Neuformatieren ist jedoch nicht möglich.

Werden WORM-Medien in einem Mediensatz verwendet, wird der Überschreibschutzzeitraum nicht darauf angewendet, der Anhängezeitraum hingegen schon.

Neue WORM-Medien sind WORM-Medien, auf die noch nicht geschrieben wurde. Wenn neue WORM-Medien in Backup Exec eingeführt werden, werden sie dem Mediensatz "Temporäre Medien" hinzugefügt. Nach einmaligem Beschreiben können WORM-Medien dem temporären Mediensatz nicht mehr zugeordnet werden. Sie können WORM-Medien in den Mediensatz "Ausrangierte Medien" verschieben, um sie aus Backup Exec zu löschen, es ist jedoch nicht möglich, sie zu löschen oder neu zu formatieren.

Sie können ein Band als WORM-Band formatieren, wenn das Bandlaufwerk den Vorgang unterstützt.

Siehe ["Formatieren eines Bands als WORM-Band"](#) auf Seite 553.

Wenn Sie die Option zur Verwendung von WORM-Medien wählen, überprüft Backup Exec, dass das Zielgerät ein WORM-kompatibles Laufwerk ist oder enthält. Backup Exec überprüft auch, dass die WORM-Medien im Laufwerk verfügbar sind. Wenn WORM-Medien oder ein WORM-kompatibles Laufwerk nicht gefunden wird, wird eine Warnmeldung gesendet und der Backup-Auftrag fällt möglicherweise aus.

Siehe ["Konfigurieren von Speicheroptionen für Backup-Aufträge"](#) auf Seite 645.

Standardmedienspeicher

Ein Medienspeicher ist eine logische Darstellung des tatsächlichen physischen Speicherorts von angegebenen Bandmedien. Sie können Medienspeicher erstellen, um zu verfolgen, wo Medien physisch gespeichert werden, wie zum Beispiel in einem temporären Bin oder an einem externen Speicherort. Backup Exec erstellt Standardmedienspeicher, sodass Sie alle Medien, die sich online, offline oder in einem Medienspeicher befinden, anzeigen können.

Sie müssen den Assistenten "Speicher konfigurieren" ausführen, um den Speicherort von Bandmedien in Medienspeichern zu aktualisieren. Im Assistenten "Speicher konfigurieren" können Sie Berichte drucken, die angeben, welche Bandmedien zum Verschieben in den und aus dem Speicher bereit sind. Sie können außerdem den Speicherort der Medien aktualisieren, wenn Sie sie verschieben möchten. Die Bandmedien müssen jedoch physisch gesammelt und dem Speicher hinzugefügt bzw. entnommen werden. Der Speicherort der Bandmedien wird in der Backup Exec-Datenbank aktualisiert, aber die Medien werden nicht ausgeworfen oder exportiert. Wenn Backup Exec erkennt, dass sich die Medien in einem Wechsler befinden, werden Sie aufgefordert, Medien zu exportieren. Wenn Sie die Medien

exportieren möchten, wird der Auftrag "Medien exportieren" ausgeführt. Wenn Ihre Umgebung Remote-Standorte umfasst, sollten Sie separate Mediensätze für jeden Remote-Standort erstellen. Dann enthalten die Berichte Details dazu, welche Medien an einen bestimmten Standort verschoben werden können.

Tabelle 11-6 Standardmedienspeicher

Standardmedienspeicher	Beschreibung
Online-Bandmedien	Zeigt die Medien an, die in Bandlaufwerken oder in den Wechslern verfügbar sind. Sie können Medien nicht dem Online-Medienspeicher hinzufügen oder in diesen verschieben. Dies erfolgt in Backup Exec automatisch. Wenn Sie Medien vom Online-Medienspeicher in einen anderen Medienspeicher verschieben, bleiben der Überschreibschutzzeitraum und der Anhängenzeitraum der Medien erhalten.
Offline-Bandmedien	Zeigt die Medien an, die sich vor Ort aber nicht in Bandlaufwerken oder Wechslern befinden und die nicht in Medienspeichern liegen. Medien werden im Offline-Medienspeicher angezeigt, wenn Sie Backup Exec verwenden, um Medien aus einem Bandlaufwerk oder Wechsler zu entfernen. Sie können Medien dem Offline-Medienspeicher aus einem anderen Medienspeicher hinzufügen. Bei einer Inventarisierung oder einer Katalogisierung werden die Offline-Medien zurück in den Online-Medienspeicher verschoben. Sie können den Offline-Medienspeicher nicht löschen oder umbenennen.
Bandmedien im Speicher	Zeigt die Medien an, die sich nicht in Bandlaufwerken oder Wechslern befinden und die in einen Medienspeicher verschoben wurden. "Bandmedien im Speicher" wird unter "Alle Medienspeicher" erst angezeigt, nachdem Sie einen Medienspeicher erstellt haben.

Standardmedienspeicher	Beschreibung
Alle Medienspeicher	<p>Zeigt die Medien an, die sich in den Medienspeichern befinden, die Sie erstellen.</p> <p>"Alle Medienspeicher" wird auf der Registerkarte "Speicher" erst angezeigt, nachdem Sie einen Medienspeicher erstellt haben.</p> <p>Sie können Medienspeicher mit Mediensätzen verbinden, die Sie erstellen. Sie legen fest, wann die Medien aus einem Mediensatz in den Medienspeicher verschoben werden. Sie legen außerdem fest, wann die Medien in den Mediensatz aus dem Medienspeicher zurückgeholt werden.</p> <p>Siehe "Erstellen von Medienspeicherregeln zum Verschieben von Speichermedien in und aus Medienspeichern" auf Seite 499.</p>

Siehe ["Ändern des Namens oder der Beschreibung eines Medienspeichers"](#) auf Seite 498.

Ändern des Namens oder der Beschreibung eines Medienspeichers

Sie können den Namen und die Beschreibung eines Medienspeichers bearbeiten.

Siehe ["Standardmedienspeicher"](#) auf Seite 496.

Um Medienspeicher und Medienspeicherregeln zu ändern, bearbeiten Sie die Eigenschaften des zu dem Medienspeicher gehörigen Mediensatzes.

Siehe ["Bearbeiten der Eigenschaften von Mediensätzen"](#) auf Seite 481.

Ändern des Namens oder der Beschreibung eines Medienspeichers

- 1 Erweitern Sie auf der Registerkarte "Speicher" den Eintrag "Band/Plattenspeicher-Mediansätze und -speicher" und dann "Alle Medienspeicher".
- 2 Klicken Sie mit der rechten Maustaste auf den Medienspeicher, dessen Eigenschaften Sie anzeigen möchten, und wählen Sie "Details".
- 3 Im linken Teilfenster klicken Sie auf "Medienspeichereigenschaften".
- 4 Ändern Sie den Namen oder die Beschreibung des Medienspeichers.
- 5 Klicken Sie auf "Übernehmen".

Eigenschaften von Medienspeichern

Die Eigenschaften eines Medienspeichers umfassen den Namen und eine Beschreibung des Medienspeichers.

Siehe ["Ändern des Namens oder der Beschreibung eines Medienspeichers"](#) auf Seite 498.

Tabelle 11-7 Eigenschaften von Medienspeichern

Element	Beschreibung
Name	Zeigt den Namen des Medienspeichers an.
Beschreibung	Zeigt eine Beschreibung des Medienspeichers an.

Erstellen von Medienspeicherregeln zum Verschieben von Speichermedien in und aus Medienspeichern

Sie erstellen Medienspeicherregeln für die folgenden Vorgänge:

- Verbinden Sie einen Medienspeicher mit dem Mediensatz, an den Sie Medien schicken möchten.
- Die Wartezeit zwischen der Zuweisung der Medien und ihrer Weiterleitung an den Medienspeicher festlegen
- Die Wartezeit zwischen dem letzten Schreibvorgang auf dem Medium und dem Zurückholen aus dem Medienspeicher festlegen

Siehe ["Standardmedienspeicher"](#) auf Seite 496.

Backup Exec aktualisiert den Speicher nicht automatisch. Sie müssen den Assistenten "Speicher konfigurieren" verwenden, um den Speicherort der Medien zu aktualisieren. Sie können auch Berichte drucken oder anzeigen, die Details dazu enthalten, welche Medien zum Verschieben in den und aus dem Speicher bereit sind.

Siehe ["Aktualisieren des Bandmedienspeicherorts in Medienspeichern"](#) auf Seite 500.

So erstellen Sie Medienspeicherregeln, um Medien in und aus Medienspeicher zu verschieben

- 1 Erweitern Sie auf der Registerkarte "Speicher" den Eintrag "Alle Mediensätze".
- 2 Klicken Sie mit der rechten Maustaste auf "Daten für 4 Wochen aufbewahren", "Daten unbegrenzt beibehalten - kein Überschreiben zulassen" oder auf einen Mediensatz, den Sie erstellt haben, und klicken Sie auf "Details".
- 3 Im linken Teilfenster klicken Sie auf "Eigenschaften".

- 4 Wählen Sie den Medienspeicher aus, den Sie mit dem Mediensatz verwenden möchten.
- 5 Geben Sie an, wann die Medien in den Speicher verschoben und wann sie in den Mediensatz zurückgeholt werden.

Aktualisieren des Bandmedienspeicherorts in Medienspeichern

Sie können den Speicherort von in Speichern abgelegten Bandmedien aktualisieren. Sie können auch Berichte drucken, die angeben, welche Medien zum Verschieben in den und aus dem Speicher bereit sind. Die Medien müssen jedoch physisch eingesammelt und dem Speicher hinzugefügt bzw. entnommen werden.

Siehe "[Standardmedienspeicher](#)" auf Seite 496.

So aktualisieren Sie den Speicherort von Bandmedien in Medienspeichern

- 1 Erweitern Sie auf der Registerkarte "Speicher" den Eintrag "Band/Plattenspeicher-Mediensätze und -speicher" und doppelklicken Sie auf "Alle Medienspeicher".
- 2 Klicken Sie mit der rechten Maustaste auf den Medienspeicher, für den der Speicherort der Medien aktualisiert werden soll, und klicken Sie dann auf "Speicher aktualisieren mit Assistent".
- 3 Befolgen Sie die Anweisungen auf dem Bildschirm.

Löschen eines Medienspeichers

Sie können nur leere Medienspeicher löschen. Wenn sich Bandmedien im Speicher befinden, müssen Sie diese verschieben, bevor Sie den Speicher löschen können. Sie können die Online-Medienpeicher oder die Offline-Medienpeicher nicht löschen.

Siehe "[Standardmedienspeicher](#)" auf Seite 496.

So löschen Sie einen Medienspeicher

- 1 Erweitern Sie auf der Registerkarte "Speicher" den Eintrag "Alle Medienspeicher".
- 2 Klicken Sie mit der rechten Maustaste auf den Medienspeicher, den Sie löschen möchten, und klicken Sie dann auf "Löschen".
- 3 Klicken Sie auf "Ja", wenn Sie aufgefordert werden, den Medienspeicher zu löschen.

Verschieben von Bandmedien in einen Speicher

Sie können einen Barcode-Scanner verwenden, um die Medienkennungen von Bandmedien einzugeben, die Sie in einen Speicher verschieben möchten. Sie können auch eine Medienkennung in das Dialogfeld eingeben.

Siehe "[Standardmedienspeicher](#)" auf Seite 496.

So verschieben Sie Bandmedien in einen Speicher

- 1 Auf der Registerkarte "Speicher" erweitern Sie "Band- und Plattenspeichermedien" und doppelklicken Sie dann auf "Alle Medienspeicher".
- 2 Klicken Sie mit der rechten Maustaste auf den Medienspeicher, den Sie verschieben möchten, und klicken Sie dann auf "Medien zum Speicher verschieben".
- 3 Befolgen Sie die Anweisungen auf dem Bildschirm.

Ausrangieren beschädigter Bandmedien

Sie können beschädigte Bandmedien ausrangieren, damit Backup Exec sie nicht für Backup-Aufträge verwendet. Sie sollten Bandmedien verbinden, die die Schwellenwerte für Verwurfsprozesse einhalten oder überschreiten, die vom Medienhersteller mit dem Mediensatz "Ausrangierte Medien" festgelegt werden. Backup Exec verfolgt die behebbaren Fehler, die die Firmware des Speichergeräts generiert hat. Medien, die annehmbare Stufen dieser Fehler überschreiten, werden als Medien gemeldet, die verworfen werden können.

Um zu bestimmen, welche Bandmedien ausrangiert werden sollen, führen Sie den Bericht "Mediensätze" aus, um die Gesamtzahl der Fehler für Medien zu erhalten. Wahlweise können Sie sich die Eigenschaften eines bestimmten Mediums anzeigen lassen.

Verknüpfen Sie alle Medien mit nicht akzeptablen Fehlerzahlen mit "Ausrangierte Medien", sodass Sie sichergehen können, keine fehlerhaften Medien für Backup-Vorgänge zu verwenden. Nachdem Sie Medien mit dem Satz "Ausrangierte Medien" verbinden, wird es nicht von Backup Exec für zukünftige Backup-Aufträge verwendet. Die Medien stehen nach wie vor für Wiederherstellungen zur Verfügung, wenn sie nicht beschädigt sind.

So rangieren Sie beschädigte Bandmedien aus

- 1 Auf der Registerkarte "Speicher" erweitern Sie "Band- und Plattenspeichermedien".
- 2 Klicken Sie mit der rechten Maustaste auf "Online-Bandmedien" und klicken Sie auf "Details".

- 3 Klicken Sie mit der rechten Maustaste auf die Medien, die Sie ausrangieren möchten, und klicken Sie dann auf "Ausrangieren".
- 4 Klicken Sie auf "Ja", wenn Sie aufgefordert werden, die Medien auszurangieren.

Siehe ["Löschen von Bandmedien"](#) auf Seite 502.

Siehe ["Bericht "Medienfehler""](#) auf Seite 835.

Löschen von Bandmedien

Wenn Sie Bandmedien aus Backup Exec löschen, werden alle Datensätze der Medien aus der Backup Exec-Datenbank entfernt. Diese Datensätze umfassen Kataloginformationen, Mediumstatistiken und andere Informationen in Verbindung mit den Bandmedien. Sie können ein Medium nur löschen, wenn es zum Satz "Ausrangierte Medien" gehört.

Unter folgenden Umständen sollten Sie Bandmedien löschen:

- Wenn Sie viele Offsite-Medien haben, die Sie nicht weiterverwenden möchten.
- Wenn Sie beschädigte oder alte Medien entsorgen.

Wenn Sie gelöschte Medien wieder in Backup Exec importieren, wird es entweder zum Mediensatz "Backup Exec- und Windows NT-Backup-Medien" oder zum Mediensatz "Fremde Medien" hinzugefügt. Bevor Sie eine Wiederherstellung durchführen können, müssen die entsprechenden Medien katalogisiert werden.

So löschen Sie Bandmedien

- 1 Auf der Registerkarte "Speicher" erweitern Sie "Band- und Plattenspeichermedien".
- 2 Erweitern Sie "Alle Mediensätze", klicken Sie mit der rechten Maustaste auf "Ausrangierte Medien" und klicken Sie anschließend auf "Details".
- 3 Klicken Sie mit der rechten Maustaste auf das Medium, das Sie löschen möchten, und klicken Sie dann auf "Löschen".
- 4 Klicken Sie auf "Ja", wenn Sie aufgefordert werden, die Medien zu löschen.

Siehe ["Ausrangieren beschädigter Bandmedien"](#) auf Seite 501.

Band- oder Datenträgermedien löschen

Sie können Bandmedien oder Datenträgermedien sofort löschen oder Sie können den Löschenvorgang planen.

Warnung: Der Löschvorgang wird auf den Medien ausgeführt, die im Laufwerk oder im Schacht sind, wenn der Vorgang ausgeführt wird. Falls das Medium seit der letzten Inventarisierung geändert wurde, stimmt die Medienkennung auf der Backup Exec-Administratorkonsole evtl. nicht mit dem Medium im ausgewählten Laufwerk oder Schacht überein. Wenn Medien unerwartet verschoben werden, kann Datenverlust auftreten. Prüfen Sie alle geplanten Löschaufträge sorgfältig.

Tabelle 11-8 Löschvorgänge

Löschvorgang	Beschreibung
"Medium jetzt löschen"	<p>Schreibt eine Anzeige zu Beginn der Medien, die die Daten auf den Medien unzugänglich macht. Für die meisten Verwendungsarten ist der Vorgang "Medium jetzt löschen" ausreichend.</p> <p>Dies ist der einzige Löschvorgang, der für Plattenkassettenmedien verfügbar ist.</p>
"Medium jetzt gründlich löschen"	<p>Weist das Laufwerk an, sämtliche Medien physisch zu löschen. Wenn sich auf den Medien vertrauliche Information befinden, die Sie entfernen möchten, verwenden Sie den Vorgang "Medium jetzt gründlich löschen". Eine langsame Löschung auf Medien dauert einige Stunden bis zum Abschluss, abhängig von dem Laufwerk und der Mediumkapazität.</p> <p>Einige Geräte unterstützen keine langsame Löschung.</p>
Planen	<p>Hiermit können Sie eine Löschung oder langsame Löschung planen und Benachrichtigungsoptionen auswählen.</p>

Der Löschvorgang ändert nicht die Medienkennung. Um eine Medienkennung zu ändern, führen Sie einen Kennungsvorgang aus oder benennen Sie die Medien um, bevor Sie einen Löschvorgang ausführen.

Sie können einen Löschvorgang nicht abbrechen, nachdem er begonnen hat. Sie können einen Löschvorgang abbrechen, der geplant oder in der Warteschlange ist.

Wenn Sie einen Löschauftrag planen, können Sie die Zeit und die Häufigkeit für die Ausführung des Auftrags konfigurieren.

So löschen Sie Band- oder Datenträgermedien jetzt

- 1** Klicken Sie auf der Registerkarte "Speicher" auf das Laufwerk oder den Wechslerlot, der die Medien enthält, die Sie löschen möchten.
- 2** Klicken Sie auf "Medium jetzt löschen" und führen Sie einen der folgenden Schritte aus:

So führen Sie einen Löschenvorgang sofort aus Klicken Sie auf "Medium jetzt löschen".

So führen Sie einen langsamen Löschvorgang sofort aus Klicken Sie auf "Medium jetzt löschen (lang)".

- 3** Klicken Sie auf "Ja", wenn Sie aufgefordert werden, das Medium zu löschen.

So planen Sie einen Löschvorgang für Band- oder Plattenkassettenmedien

- 1** Klicken Sie auf der Registerkarte "Speicher" auf das Laufwerk oder den Wechslerlot, der die Medien enthält, die Sie löschen möchten.
- 2** Klicken Sie auf "Medium jetzt löschen" und führen Sie einen der folgenden Schritte aus:

So planen Sie einen Löschenvorgang Klicken Sie auf "Löschen planen".

So planen Sie einen langsamen Löschvorgang Klicken Sie auf "Langsames Löschen planen".

- 3** Klicken Sie auf "Ja", wenn Sie aufgefordert werden, das Medium zu löschen.
- 4** Um nach Abschluss des Auftrags eine Benachrichtigung zu senden, klicken Sie im linken Teilfenster auf "Benachrichtigung" und wählen Sie die entsprechenden Optionen aus.

- 5** Um den Auftrag zu planen, klicken Sie im linken Teilfenster auf "Planen" und wählen Sie die entsprechenden Optionen aus.

Siehe ["Einen Speicherauftrag planen"](#) auf Seite 527.

- 6** Klicken Sie auf "OK".

Info zum Katalogisieren von Band- oder Plattenspeichermedien, die verschlüsselte Backup-Sätze enthalten

Beim Katalogisieren von Band- oder Plattenspeichermedien, die verschlüsselte Backup-Sätze verwenden, sucht Backup Exec in der Backup Exec-Datenbank nach gültigen Verschlüsselungsschlüsseln für die Sätze. Wird kein gültiger Schlüssel gefunden, gibt Backup Exec eine Warnmeldung aus, in der Sie angewiesen werden, einen Schlüssel zu erstellen. Nachdem Sie einen gültigen Schlüssel erstellt haben, können Sie so auf die Warnmeldung reagieren, dass die Katalogisierung des verschlüsselten Satzes erneut versucht wird. Alternativ können Sie den verschlüsselten Satz auch überspringen und mit dem Katalogisieren der restlichen Medien fortfahren oder den Katalogisierungsauftrag abbrechen.

Siehe "[Verwaltung von Verschlüsselungscodes](#)" auf Seite 731.

Verknüpfen von Bandmedien mit einem Mediensatz

Wenn Sie einen Backup-Auftrag für Bandmedien erstellen, wird der Standard-Mediensatz, den Backup Exec für Sie auswählt, "Daten für 4 Wochen aufbewahren" benannt. Sie können andere Mediensätze auswählen, wenn Sie den Backup-Auftrag erstellen, oder Sie können die Bandmedien mit einem anderen Mediensatz später verbinden.

Wenn Sie Bandmedien mit einem Mediensatz verbinden, verwendet das Band die folgenden Eigenschaften dieses Mediensatzes:

- Anhängezeiträume
- Überschreibschutzzeiträume
- Medienspeicher
- Zeitraum für die Verschiebung von Medien in den und aus dem Medienspeicher

Hinweis: Sie sollten temporäre oder importierte Medien mit einem Mediensatz nicht verbinden. Backup Exec verknüpft temporäre oder importierte Medien automatisch mit einem Mediensatz, wenn dies für einen Backup-Auftrag erforderlich ist.

Siehe "[Erstellen von Mediensätzen für Bänder](#)" auf Seite 480.

So verknüpfen Sie Bandmedien mit einem Mediensatz

- 1** Auf der Registerkarte "Speicher" erweitern Sie "Band- und Plattenspeichermedien".
- 2** Doppelklicken Sie auf "Alle Bandmedien", um eine Liste der Medien anzuzeigen.
- 3** Klicken Sie mit der rechten Maustaste auf das Bandmedium, das Sie mit einem Mediensatz verbinden möchten, und klicken Sie dann auf "Mit Mediensatz verknüpfen".
- 4** Wählen Sie aus der Dropdown-Liste einen Mediensatz und klicken Sie anschließend auf "OK".

Siehe "[Standard-Mediensätze](#)" auf Seite 473.

Bearbeiten von Bandmedieneigenschaften

Sie können Bandmedieneigenschaften anzeigen und einige davon bearbeiten.

Siehe "[Verwalten von Bändern](#)" auf Seite 472.

So bearbeiten Sie Bandmedieneigenschaften

- 1** Doppelklicken Sie auf der Registerkarte "Speicher" auf das Laufwerk mit den Medien.
- 2** Klicken Sie im linken Teilfenster auf "Medieneigenschaften".

3 Ändern Sie eine der folgenden Optionen:

Medienkennung

Zeigt die Medienkennung an, die Backup Exec automatisch zuweist, die der Administrator zugewiesen hat oder bei der es sich um eine zuvor zugewiesene Barcodekennung handelt.

Sie können die Medienkennung bearbeiten, die aus maximal 32 Zeichen bestehen kann. Durch das Bearbeiten ändern Sie zwar den Namen des Mediums in der Anzeige, doch wird die neue Kennung erst bei einem Überschreibvorgang auf das Medium geschrieben. Beim Bearbeiten einer Medienkennung sollten Sie versuchen, eine aussagekräftige Identifizierungsmöglichkeit zu erstellen, die auch bei Wiederverwendung des Mediums erhalten bleibt. Schreiben Sie diese Medienkennung auf ein an der Außenseite des Mediums angebrachtes Etikett.

Unter Umständen können duplizierte Kennungen automatisch erzeugt werden. Wenn Backup Exec beispielsweise erneut installiert wird oder Medien einer anderen Backup Exec-Installation eingeführt werden, kann es zu doppelten Kennungen kommen. Doppelte Kennungen sind zwar zulässig, werden jedoch nicht empfohlen.

Wenn ein Barcode verfügbar ist und ein mit einem Barcode versehenes Gerät verwendet wird, wird standardmäßig als Medienkennung automatisch dieser Barcode verwendet.

Medienbeschreibung

Zeigt die ursprüngliche Medienkennung an, wenn das Medium importiert ist.

Die Zeichenbeschränkung beträgt 128 Zeichen, um Beschreibungen in der Kennung zu ermöglichen.

Beschreibung beibehalten

Behält die Medienbeschreibung bei, wenn Sie im Drop-Down-Feld "Ja" auswählen. Die Medienbeschreibung wird beibehalten, bis ein Auftrag zum Überschreiben oder Löschen des Backups oder ein Speicherauftrag für die Kennung ausgeführt wird.

Standardmäßig wird die Medienbeschreibung nicht behalten. Diese Option ist standardmäßig auf "Nein" eingestellt.

4 Klicken Sie auf "Übernehmen".

Rotationsstrategien für Bandmedien

Es gibt viele Medienrotationsstrategien, die Sie verwenden können, um Ihre Daten zu sichern.

Zu den am häufigsten eingesetzten Medienrotationsstrategien gehören folgende:

- **Sohn:** Verwendet jeden Tag das gleiche Band, um ein vollständiges Backup auszuführen.
- **Vater/Sohn:** Verwendet mehrere Bänder und ist eine Kombination aus wöchentlichen vollständigen Backups und täglichen Differenzial- bzw. inkrementellen Backups über einen Zeitraum von zwei Wochen. Diese Strategie bietet Backups bei externer Speicherung.
- **Großvater:** Verwendet mehrere Bänder und ist eine Kombination aus wöchentlichen und monatlichen vollständigen Backups und täglichen Differenzial- bzw. inkrementellen Backups. Diese Strategie bietet auch Backups bei externer Speicherung.

Medienrotationsstrategie "Sohn"

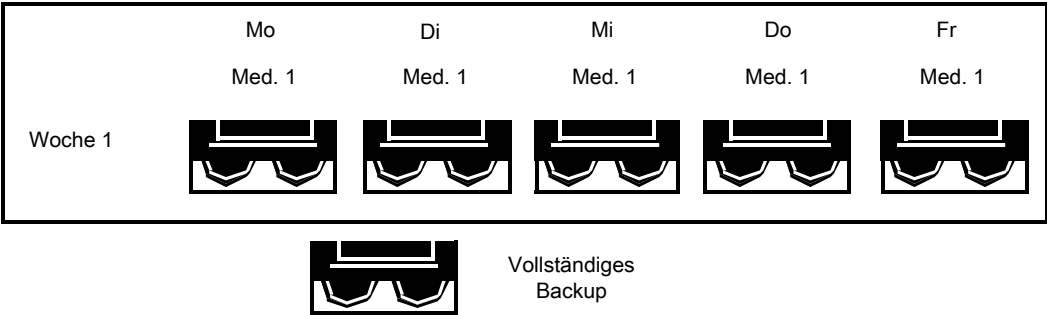
Die Medienrotationsstrategie Sohn erfordert Folgendes:

Tabelle 11-9 Medienrotationsstrategie Sohn

Element	Beschreibung
Anzahl erforderlicher Medien	1 (mindestens)
Überschreibeschutzzeitraum	Letztes Backup

Bei der Strategie "Sohn" wird jeden Tag ein vollständiges Backup durchgeführt.

Abbildung 11-3 Backup-Strategie "Sohn"



Obwohl diese Strategie einfach zu verwalten ist, ist das Sichern mit nur einem Medium kein effektives Backup-Verfahren. Magnetische Medien nutzen sich durch häufige Verwendung ab, und es können nur die Daten wiederhergestellt werden, die seit dem letzten Backup gesichert wurden.

Medienrotationsstrategie "Vater/Sohn"

Die Medienrotationsstrategie "Vater/Sohn" erfordert Folgendes:

Tabelle 11-10 Medienrotationsstrategie "Vater/Sohn"

Element	Beschreibung
Anzahl erforderlicher Medien	6 (mindestens)
Überschreibschutzzeitraum	Zwei Wochen

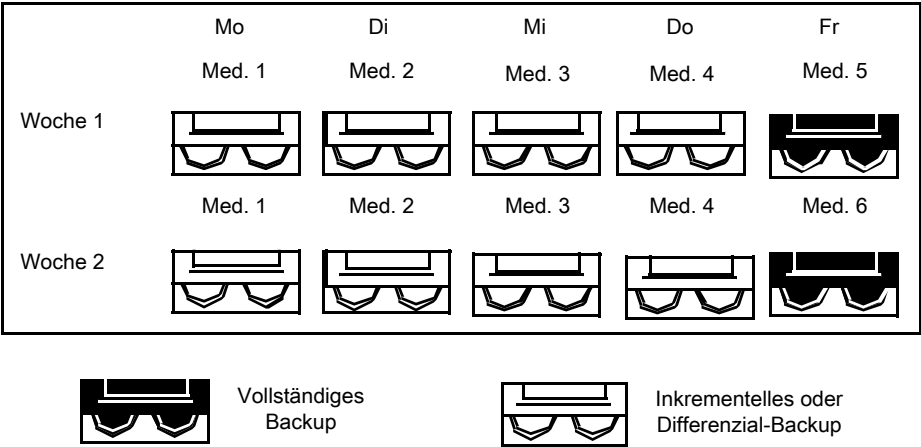
Die Medienrotationsstrategie Vater/Sohn ist eine Kombination aus vollständigen Backups und Differenzial- bzw. inkrementellen Backups über einen Zeitraum von zwei Wochen.

Bei dieser Strategie werden vier Medien für Differenzial- oder inkrementelle Backups von Montag bis Donnerstag benötigt. Die beiden anderen Medien enthalten vollständige Backups und werden jeden Freitag aus der Rotation entnommen und außerhalb des Unternehmens aufbewahrt.

Die Strategie "Vater/Sohn" ist einfach zu verwalten und ermöglicht es, Daten länger als bei der Strategie "Sohn" aufzubewahren. Diese Strategie eignet sich nicht für die strengen Datenschutzanforderungen der meisten Netzwerkumgebungen.

Wenn Sie diese Backup-Strategie erstmals einsetzen, müssen Sie zuerst ein vollständiges Backup durchführen.

Abbildung 11-4 Backup-Strategie "Vater/Sohn"



Medienrotationsstrategie "Großvater"

Die Medienrotationsstrategie Großvater erfordert Folgendes:

Tabelle 11-11 Medienrotationsstrategie Großvater

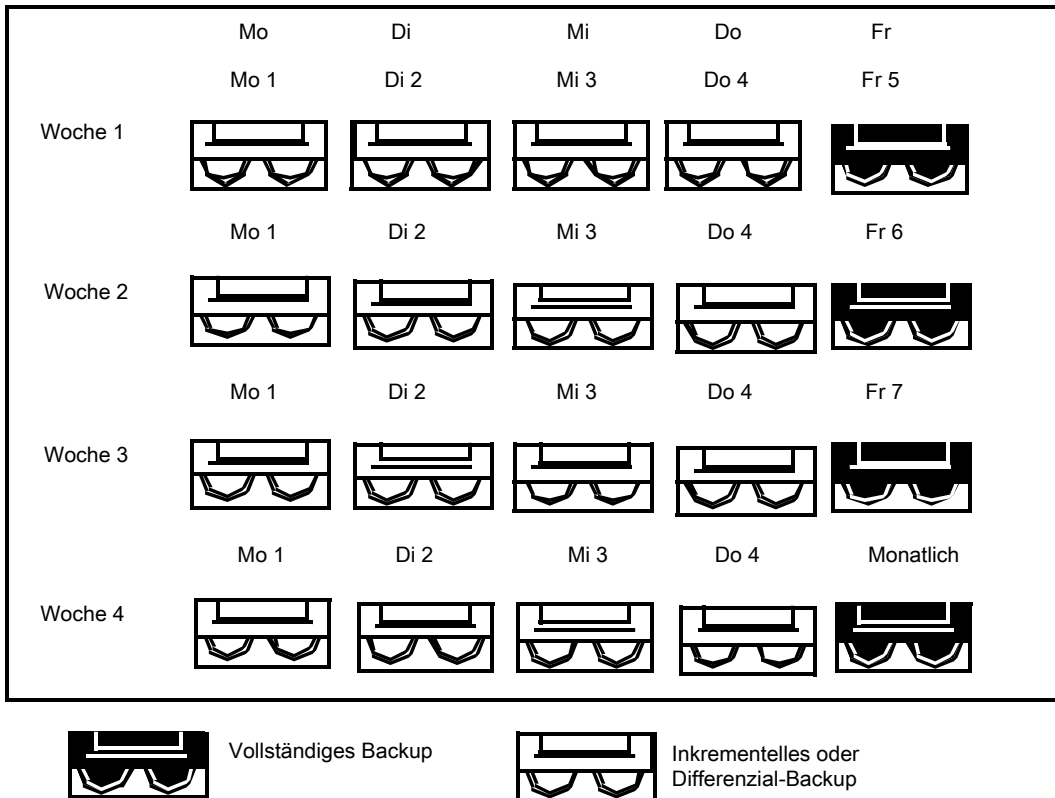
Element	Beschreibung
Anzahl erforderlicher Medien	19 (mindestens)
Überschreibschutzzeitraum	Ein Jahr

Das Großvater-Schema ist eine der am häufigsten verwendeten Medienrotationsstrategien. Sie ist einfach zu verwalten und umfassend genug, um Dateien leicht zu finden, wenn sie wiederhergestellt werden müssen.

Bei dieser Backup-Strategie werden vier Bänder benötigt, um von Montag bis Donnerstag inkrementelle bzw. Differenzial-Backups durchzuführen. Drei weitere Bänder werden für vollständige Backups am Freitag verwendet.

Die übrigen zwölf Medien sind für monatliche vollständige Backups gedacht und werden extern aufbewahrt.

Abbildung 11-5 Backup-Strategie "Großvater"



Die Strategie "Großvater" wird empfohlen, da das Verhältnis der Anzahl der Medien zur Aufbewahrungszeit der Daten günstig ist (19 Medien/1 Jahr). Sie können leicht mehr Medien mit einbeziehen. So könnten Sie zum Beispiel an jedem letzten Samstag des Monats ein vollständiges Backup für eine dauerhafte Aufbewahrung durchführen.

Speichergerätepools

In diesem Kapitel werden folgende Themen behandelt:

- Erstellen von Speichergerätepools
- Festlegen einer Standard-Auswahlmethode für ein Gerät in einem Speichergerätepool
- Anzeigen von Aufträgen, Auftragsverläufen und aktiven Warnmeldungen für einen Speichergerätepool
- Hinzufügen und Entfernen von Geräten in einem Speichergerätepool

Erstellen von Speichergerätepools

Ein Speichergerätepool ist eine Gruppe von Speichergeräten ähnlichen Typs, die die Lastverteilung für Backup Exec-Aufträge ermöglicht. Das Arbeitslast auf die Geräte im Speichergerätepool verteilt. Sie können Backup-Aufträge an bestimmte Speichergeräte oder einen Speichergerätepool schicken. Wenn ein bestimmtes Speichergerät ausgelastet ist, muss der Auftrag warten, bis das Speichergerät verfügbar wird.

Wenn Sie einen Auftrag an ein bestimmtes Speichergerät schicken, kann Backup Exec den Auftrag nicht automatisch zum nächsten verfügbaren Speichergerät weiterleiten. Wenn Sie einen Backup-Auftrag an einen Speichergerätepool senden, wird der Auftrag standardmäßig an das erste verfügbare Gerät in diesem Pool geschickt. Weitere Aufträge, die in der Zwischenzeit erstellt und gestartet werden, können parallel auf anderen Speichergeräten im gleichen Speichergerätepool ausgeführt werden. Durch dynamisches Zuweisen von Speichergeräten für neu hinzukommende Aufträge gewährleistet Backup Exec eine schnelle und effiziente Auftragsverarbeitung. Speichergerätepools ermöglichen Fehlertoleranz: Sie können Fehlerbehandlungsregeln konfigurieren, um Aufträge, die wegen Fehlern an Speichergeräten fehlschlagen, erneut zu senden.

Sie können die Standard-Auswahlmethode für ein Gerät in einem Speichergerätepool ändern, damit Aufträge zuerst an eines der folgenden Geräte im Speichergerätepool gesendet werden:

- Ein Speichergerät mit dem geringsten freien Speicherplatz. Diese Einstellung ist für manuelle externe Rotationsstrategien geeignet, da der Auftrag auf demselben Gerät ausgeführt wird, bis es voll ist.
- Ein Speichergerät mit dem größten freien Speicherplatz. Diese Einstellung ist für ein Backup geeignet, für das die Granular Recovery Technology (GRT) aktiviert ist und an einen Datenträgerspeichergerätepool gesendet wird. GRT-Aufträge, die an Datenträgerspeichergeräte gesendet werden, können nicht übergreifen.

Hinweis: Sie müssen die Backup Exec-Befehlszeilenschnittstelle verwenden, um den Standard zu ändern, um anzugeben, ob Aufträge an ein Gerät, das den meisten oder den wenigsten freien Speicherplatz hat, gesendet werden sollen.

Siehe ["Festlegen einer Standard-Auswahlmethode für ein Gerät in einem Speichergerätepool"](#) auf Seite 515.

Backup Exec erstellt und verwaltet vom System definierte Speichergerätepools für Festplatten, Bandlaufwerke, Plattenkassetten und virtuelle Datenträger. Alle Speichergeräte, die Sie konfigurieren oder anschließen, werden automatisch dem entsprechenden vom System definierten Speichergerätepool hinzugefügt. Sie können diese Speichergerätepools auswählen, wenn Sie den Speicher für einen Backup-Auftrag auswählen. Sie können einen vom System definierten Speichergerätepool nicht bearbeiten. Bevor Sie die Standard-Speichergerätepools auf der Registerkarte "Speicher" unter "Alle Speicherpools" anzeigen können, müssen Sie einen Speichergerätepool erstellen. Wenn Sie Central Admin Server Feature installiert haben, können Sie verwaltete Backup Exec-Server-Pools erstellen.

Tabelle 12-1 Von Backup-Exec verwaltete, vom System definierte Speichergerätepools

Von Backup-Exec verwaltete, vom System definierte Speichergerätepools	Beschreibung
Beliebiger Festplattenspeicher	Enthält den Festplattenspeicher.

Von Backup-Exec verwaltete, vom System definierte Speichergerätepools	Beschreibung
Beliebiges Bandlaufwerk	Enthält das Bandlaufwerk. Backup Exec erstellt diesen Pool, wenn ein verbundenes Bandlaufwerk oder ein Wechsler erkannt wird. In einem Bandlaufwerk-Speicherpool verwendet Backup Exec die ältesten wiederverwendbaren Medien zuerst.
Beliebiger Festplattenkassettenspeicher	Enthält die Festplattenkassetten, die Sie zur Verwendung als Speicher konfiguriert haben. Backup Exec erstellt diesen Pool, wenn Sie zum ersten Mal einen Festplattenkassettenspeicher konfigurieren.

Für Speichergerätepools, die Sie erstellen, müssen Sie die Eigenschaften des Pools bearbeiten und das Kontrollkästchen neben dem Gerät aktivieren, bevor Aufträge dieses Gerät im Pool verwenden können.

Verwenden Sie den Speicher konfigurieren -Assistenten, um Speichergeräte-Pools zu erstellen.

Erstellen eines Speichergeräte-Pools

- 1 Klicken Sie auf der Registerkarte "Speicher" unter "Konfigurieren" auf "Speicher konfigurieren".
- 2 Sie haben folgende Möglichkeiten:

Wenn Central Admin Server Feature nicht installiert ist	Wählen Sie Speicherpools und klicken Sie anschließend auf Weiter.
Wenn Central Admin Server Feature installiert ist	Gehen Sie dazu in folgender Reihenfolge vor: <ul style="list-style-type: none"> ■ Wählen Sie den Backup Exec-Server aus, für den Sie Speicher konfigurieren möchten, und klicken Sie dann auf "Weiter". ■ Wählen Sie Speicherpools und klicken Sie anschließend auf Weiter.
- 3 Wählen Sie "Speichergerätepool" und klicken Sie dann auf "Weiter".
- 4 Geben Sie einen Namen und eine Beschreibung für den Pool ein und klicken Sie dann auf "Weiter".

- 5 Klicken Sie auf den Nach-unten-Pfeil, wählen Sie den Typ des Speichergerätepools, den Sie konfigurieren möchten, aus und klicken Sie dann auf "Weiter".
- 6 Wählen Sie alle Speichergeräte, die Sie in den Pool einschließen möchten, aus und klicken Sie dann auf "Weiter".
- 7 Überprüfen Sie die Speicherkonfigurationsübersicht und führen Sie einen der folgenden Schritte aus:

So ändern Sie die Konfiguration

Gehen Sie dazu in folgender Reihenfolge vor:

- Klicken Sie auf die Überschrift, die die Elemente enthält, die Sie ändern möchten.
- Nehmen Sie alle Änderungen, vor und klicken Sie dann auf "Weiter", bis die Übersicht angezeigt wird.
- Klicken Sie auf "Fertigstellen".

So konfigurieren Sie den Speichergerätepool

Klicken Sie auf "Fertigstellen".

Siehe ["Hinzufügen und Entfernen von Geräten in einem Speichergerätepool"](#) auf Seite 517.

Siehe ["Verwenden von Backup Exec-Server-Pools in CAS"](#) auf Seite 1498.

Siehe ["Hinzufügen und Entfernen von Geräten in einem Speichergerätepool"](#) auf Seite 517.

Siehe ["Fehlerbehandlungsregeln für fehlgeschlagene oder abgebrochene Aufträge"](#) auf Seite 316.

Festlegen einer Standard-Auswahlmethode für ein Gerät in einem Speichergerätepool

Die Standard-Auswahlmethode für ein Gerät in einem Speichergerätepool ist das erste verfügbare Speichergerät in einem Pool. Sie können die Backup Exec-Befehlszeilenschnittstelle verwenden, um eine andere Auswahlmethode für einen Pool mit plattenbasierten Speichergeräten festzulegen. Sie können die Standardeinstellungen eines vorhandenen Speichergerätepools oder eines von Backup Exec erstellten Speichergerätepools ändern.

Sie können die Standardvorgabe so ändern, dass Aufträge zuerst an eines der folgenden Geräte gesendet werden:

- Ein Speichergerät mit dem geringsten freien Speicherplatz. Diese Einstellung ist für manuelle externe Rotationsstrategien geeignet, da der Auftrag auf demselben Gerät ausgeführt wird, bis es voll ist.
- Ein Speichergerät mit dem meisten freien Speicherplatz. Diese Einstellung ist für einen Backup-Auftrag geeignet, für den die Granular Recovery Technology (GRT) aktiviert ist und der an einen Pool mit plattenbasierten Speichergeräten gesendet wird. Ein GRT-Auftrag kann nicht datenträgerübergreifend sein, wenn er an ein Plattenspeichergerät gesendet wird.

Die Befehle der Backup Exec-Befehlszeilenschnittstelle lauten wie folgt:

- "New-BEStorageDevicePool" legt die Geräteauswahlmethode für einen neuen Pool mit plattenbasierten Speichergeräten bei dessen Erstellung fest.
- "Set-BEStorageDevicePool" legt die Geräteauswahlmethode für einen vorhandenen Pool mit plattenbasierten Speichergeräten fest.

Informationen zur Verwendungsweise der Backup Exec-Befehlszeilenschnittstelle und den zugehörigen Befehlen finden Sie in der Hilfedatei mit dem Namen "BEMCLI" im standardmäßigen Installationsverzeichnis:

C:<Backup Exec-Installationsordner>\Backup Exec

Siehe ["Erstellen von Speichergerätepools"](#) auf Seite 512.

Anzeigen von Aufträgen, Auftragsverläufen und aktiven Warnmeldungen für einen Speichergerätepool

Sie können die Aufträge, die zu einem Speichergerätepool geschickt werden, die Auftragsverläufe sowie alle aktiven Warnmeldungen anzeigen. Sie müssen einen Speicherpool erstellen, damit "Alle Speicherpools" auf der Registerkarte "Speicher" angezeigt wird.

Siehe ["So überwachen und verwalten Sie Aufträge in Backup Exec"](#) auf Seite 286.

Siehe ["Warnmeldungen und Benachrichtigungen in Backup Exec"](#) auf Seite 334.

So zeigen Sie Aufträge, Auftragsverläufe und aktive Warnmeldungen für Speichergerätepools an

- 1 Erweitern Sie auf der Registerkarte "Speicher" den Eintrag "Alle Speicherpools".
- 2 Klicken Sie mit der rechten Maustaste auf den Speichergerätepool, dessen Aufträge Sie anzeigen möchten, und wählen Sie "Details".
- 3 Im linken Teilfenster klicken Sie auf "Aufträge", "Auftragsverlauf" oder "Aktive Warnmeldungen".

Hinzufügen und Entfernen von Geräten in einem Speichergerätepool

Sie können Geräte in einem Speichergerätepool hinzufügen oder entfernen. Nur Speichergeräte ähnlichen Typs können zum selben Speichergerätepool gehören. Sie können einen vom System festgelegten Speichergerätepool nicht bearbeiten. Beispiel: Beliebiger Festplattenspeicher oder Beliebiger Plattenkassettenpeicher.

Sie müssen einen Speichergerätepool erstellen, bevor "Alle Speicherpools" auf der Registerkarte "Speicher" angezeigt wird.

Siehe ["Erstellen von Speichergerätepools"](#) auf Seite 512.

Hinweis: Um die Standardmethode zum Auswählen eines Speichergerätepools anzuzeigen oder zu ändern, müssen Sie die Backup Exec Management-Befehlszeilenschnittstelle verwenden.

Siehe ["Festlegen einer Standard-Auswahlmethode für ein Gerät in einem Speichergerätepool"](#) auf Seite 515.

So entfernen Sie Geräte aus einem Speichergerätepool oder fügen welche hinzu

- 1 Erweitern Sie auf der Registerkarte "Speicher" den Eintrag "Alle Speicherpools".
- 2 Doppelklicken Sie auf den Speicherpool, für den Sie Geräte hinzufügen und entfernen möchten.
- 3 Klicken Sie im linken Teilfenster auf "Eigenschaften".
- 4 Führen Sie einen oder beide der folgenden Schritte aus:

So fügen Sie dem Pool ein Speichergerät hinzu	Gehen Sie dazu wie folgt vor:
---	-------------------------------

- Klicken Sie auf "Hinzufügen".
- Wählen Sie die Geräte, die Sie hinzufügen möchten, aus und klicken Sie dann auf "OK".

So entfernen Sie ein Speichergerät aus einem Pool	Wählen Sie das zu entfernende Gerät aus, und klicken Sie dann auf "Entfernen".
---	--

- 5 Klicken Sie auf "Übernehmen".

Speichervorgänge

In diesem Kapitel werden folgende Themen behandelt:

- Info zu Speicheraufträgen
- Übersicht über die Registerkarte "Speicher" in Backup Exec
- Verwenden des Assistenten "Speicher konfigurieren"
- Anzeigen von Details für mehrere Speichergeräte
- Senden einer Benachrichtigung beim Abschließen eines geplanten Speicherauftrags
- Einen Speicherauftrag planen
- Bearbeiten globaler Einstellungen für Speicher
- Freigeben von Speichergeräten
- Löschen von Speichergeräten
- Ändern des Status eines Speichergeräts in "Online"
- Umbenennen von Speichergeräten
- Anzeigen von Aufträgen, Auftragsverläufen, Backup-Sätzen und aktiven Warnmeldungen für Speichergeräte
- Katalogisieren eines Speichergeräts
- Scannen eines Speichergeräts
- Inventarisieren eines Speichergeräts
- Inventarisieren und Katalogisieren von Speichergeräten
- Ein Speichergerät anhalten und wieder starten

- [Deaktivieren und Aktivieren eines Speichergeräts](#)
- [Initialisieren eines Wechslers](#)
- [Formatieren eines Bands als WORM-Band](#)
- [Spannen eines Bands](#)
- [Formatierung eines Bandes in einem Bandlaufwerk](#)
- [Auswerfen von Medien aus einer Plattenkassette oder einem Bandlaufwerk](#)
- [Reinigen eines Wechslerlaufwerks](#)
- [Importieren von Medien in Backup Exec](#)
- [Exportieren von Medien und abgelaufenen Medien](#)
- [Sperren und Freigen des vorderen Ladeschachts](#)
- [Status von Backup Exec-Servern und Speichergeräten](#)
- [So sehen Sie den Status des Sperrmodus für die Datenträgerspeicherung](#)

Info zu Speicheraufträgen

Backup Exec liefert die Speichervorgänge, die Ihnen helfen, Speichergeräte und Medien zu verwalten. Sie können die meisten Speichervorgänge durchführen, indem Sie mit der rechten Maustaste auf das Speichergerät klicken und dann den Vorgang auswählen. Nur die Speichervorgänge, die für dieses Speichergerät oder diese Medien unterstützt werden, sind im Kontextmenü enthalten. Nicht alle Speichervorgänge sind für alle Geräte verfügbar.

Backup Exec behandelt virtuelle Bandbibliotheken und simulierte Bandbibliotheken als physische Wechsler. Sie können virtuelle Bandbibliotheken anhand der Bezeichnung VTL identifizieren, die auf den Eigenschaftenseiten der Bibliothek angezeigt wird. Sie können simulierte Bandbibliotheken durch die Bezeichnung TLS (Tape Library Simulator Utility) identifizieren. Die virtuellen Bandbibliotheken und die simulierten Bandbibliotheken unterstützen nicht alle Speichervorgänge, die für physische Wechsler verfügbar sind.

Sie können einige Speichervorgänge als wiederkehrende Aufträge planen. Sie können einen Zeitplan angeben und festlegen, wer bei Ausführung dieser Aufträge benachrichtigt werden soll.

Sie können alle aktiven und geplanten Speichervorgänge und Verläufe von Speichervorgängen auf der Registerkarte "Auftragsüberwachung" anzeigen.

Siehe ["Einen Speicherauftrag planen"](#) auf Seite 527.

Siehe ["Senden einer Benachrichtigung beim Abschließen eines geplanten Speicherauftrags"](#) auf Seite 526.

Übersicht über die Registerkarte "Speicher" in Backup Exec

Backup Exec zeigt auf der Registerkarte "Speicher" ein Übersicht über die konfigurierten Speichergeräte an. Sie können Details für jedes Speichergerät anzeigen. Wenn Sie Details für alle Speichergeräte auf einem Server anzeigen möchten, können Sie mehrere Speichergeräte auswählen.

Siehe ["Anzeigen von Details für mehrere Speichergeräte"](#) auf Seite 526.

Sie können die Spalten anpassen, die in der Ansicht "Gesamter Speicher" angezeigt werden. Verschiedene Spalten sind in der Struktur- und der Listenansicht verfügbar. Abhängig von der aktiven Ansicht und den verfügbaren Speichergeräten werden eventuell nur einige der Spalten, die in der folgenden Tabelle beschrieben werden, angezeigt.

Siehe ["Sortieren, Filtern und Kopieren von Informationen in der Backup Exec-Administratorkonsole"](#) auf Seite 135.

Tabelle 13-1 Übersicht "Gesamter Speicher"

Element	Beschreibung
Name	<p>Gibt den Namen des Speichergeräts an.</p> <p>Standardmäßig gibt Backup Exec einen Namen für das Speichergerät an, der aus dem Typ des Speichergeräts und einer Nummer besteht, die sich jeweils um 1 erhöht, z. B. "Festplattenspeicher 001". Sie können den Namen des Speichergeräts in den Speichereigenschaften ändern.</p> <p>Siehe "Umbenennen von Speichergeräten" auf Seite 547.</p>
Status	<p>Gibt den Zustand des Speichergeräts an, z. B. ob es online, offline oder deaktiviert ist oder ob Dienste neu gestartet werden müssen.</p> <p>Siehe "Status von Backup Exec-Servern und Speichergeräten" auf Seite 576.</p>

Element	Beschreibung
Übergeordnetes Gerät	<p>Identifiziert das übergeordnete Gerät, wenn es ein Verhältnis zwischen Geräten gibt. Beispiele: Ein Verhältnis zwischen einer Bandbibliothek und einem Bandlaufwerk oder zwischen einer Speichergruppe und einem virtuellen Datenträger.</p> <p>Diese Spalte wird nur angezeigt, wenn Sie die Listenansicht aus der Gruppe "Ansichten" oben im Dialogfeld auswählen.</p>
Backup Exec-Server	<p>Der Name des Backup Exec-Servers, auf dem das Speichergerät konfiguriert ist. Wenn Sie das Gerät auf mehreren Backup Exec-Servern gemeinsam nutzen, wird es für jeden Backup Exec-Server angezeigt.</p> <p>Diese Spalte wird nur angezeigt, wenn Sie die Listenansicht aus der Gruppe "Ansichten" oben im Dialogfeld auswählen.</p>
Speichertyp	<p>Der Typ des mit dem Gerät verknüpften Speichers. Der Speichertyp kann Bandlaufwerke, Wechsler, Festplattenspeicher, Mediensätze, Medienspeicher, Cloud-Speicher usw. enthalten.</p> <p>Diese Spalte wird nur angezeigt, wenn Sie die Listenansicht aus der Gruppe "Ansichten" oben im Dialogfeld auswählen.</p>
Aktive Warnmeldungen	<p>Weist darauf hin, dass ein Ereignis oder eine Bedingung in Backup Exec aufgetreten ist, für die eine Meldung angezeigt wird oder eine Reaktion erforderlich ist.</p> <p>Siehe "Warnmeldungen und Benachrichtigungen in Backup Exec" auf Seite 334.</p>
Speichertrends	<p>Gibt einen Schätzwert (in Tagen) dafür an, wie lange der Speicherplatz auf den Festplatten und virtuellen Datenträgern noch ausreicht.</p> <p>Siehe "Speichertrendanalysestatus für Plattenspeicher und virtuelle Datenträger" auf Seite 369.</p>

Element	Beschreibung
Kapazität	<p>Zeigt die Speicherkapazität an. Backup Exec liefert Überblicksinformationen zur verwendeten und freien Speicherkapazität sowie Kapazitätsdetails für jeden von Ihnen konfigurierten Speicher. Speicherkapazitätsinformationen werden für alle unter einem Speichertyp (z. B. Wechsler) zusammengefassten Elemente kumuliert. Die in der Spalte "Kapazität" angezeigten Informationen geben die Gesamtspeicherkapazität sämtlicher zusammengefasster Elemente an. Wenn Sie die Elemente erweitern, werden Speicherkapazitätsinformationen für jedes Element angezeigt.</p> <p>Bevor Kapazitätsinformationen für den Speicher angezeigt werden können, müssen Sie den Speicher inventarisieren und Katalogisieren.</p> <p>Sie können Speicherkapazität wie folgt anzeigen:</p> <ul style="list-style-type: none"> ■ Auf der Registerkarte "Speicher" in der Spalte "Kapazität". Wenn Sie den Mauszeiger auf die Kapazitätsleiste setzen, werden in der QuickInfo weitere Details angezeigt. ■ Auf der Registerkarte "Backup und Wiederherstellung", wenn Sie den Speicher für einen Backup-Auftrag angeben. ■ Auf der Registerkarte "Startseite" unter "Speicherstatus". ■ Auf der Registerkarte "Speicher", wenn Sie Eigenschaften für Speichergeräte anzeigen. <p>Für Plattenspeicher und Plattenkassettenspeicher können Sie die Schwellenwerte für niedrigen Speicherplatz in den Geräteeigenschaften festlegen.</p> <p>Siehe "Bearbeiten der Eigenschaften von Festplattenspeichern" auf Seite 376.</p> <p>Siehe "Bearbeiten der Eigenschaften von Festplattenkassetten" auf Seite 385.</p> <p>Siehe "Funktionsweise der Backup Exec-Kataloge" auf Seite 277.</p> <p>Siehe "Inventarisieren eines Speichergeräts" auf Seite 550.</p>

Element	Beschreibung
Gesamtkapazität	<p>Zeigt den gesamten Speicherplatz an, der auf dem Gerät verfügbar ist.</p> <p>Für Plattenspeicher wird hier die Größe des Datenträgers angezeigt, auf dem sich der Speicher befindet.</p> <p>Für Plattenkassettenspeicher wird hier die Größe der Kassette angezeigt.</p> <p>Für Bänder wird hier die genutzte native Kapazität und die native Gesamtkapazität des Mediums angezeigt.</p>
Belegter Speicher	Zeigt den genutzten Speicherplatz nach Ausführung aller Komprimierungs- oder Deduplizierungsvorgänge an.
Geschriebene Backup-Daten:	Zeigt an, wie viele rohe Backup-Daten gesichert wurden, bevor Komprimierung oder Deduplizierung ausgeführt wurden. Beispiel: Wenn Sie 100 MB Daten zehnmal in einem Deduplizierungsordner sichern, ist der genutzte Speicherplatz 100 MB, aber die geschriebene Größe der Backup-Daten ist 1 GB.
Verfügbarer Speicherplatz	Zeigt die Differenz zwischen "Gesamtkapazität" und "Genutzter Speicherplatz" an.
Verfügbarer Speicherplatz in %	Zeigt den Unterschied als Prozentsatz zwischen "Gesamtkapazität" und "Genutzter Speicherplatz" an.
Aktive und geplante Aufträge	Zeigt die Anzahl von Speicher-, Backup- und Wiederherstellungsaufträgen an, die auf diesem Gerät aktiv sind. Klicken Sie auf den Text in dieser Spalte, um weitere Informationen zu allen aktiven oder geplanten Aufträgen anzuzeigen.
Komprimierungsgrad	Zeigt das Verhältnis der unkomprimierten zur komprimierten Größe einer Datei an.
Durchschnittliche Auftragsrate	Zeigt die Durchschnittsgeschwindigkeit der Aufträge an, die auf diesem Gerät ausgeführt werden.

Verwenden des Assistenten "Speicher konfigurieren"

Verwenden Sie den Assistenten "Speicher konfigurieren", um verschiedene Speichertypen einzurichten, in denen Sie Daten sichern können. Der Assistent "Speicher konfigurieren" erstellt den Speicher, der die optimalen

Standardeinstellungen für Ihre Umgebung verwendet. Sie können jedoch auch alle Geräteeinstellungen in den Geräteeigenschaften anpassen.

Die unterstützten Speichergeräte finden in der Liste der mit Backup Exec kompatiblen Hardware.

Klicken Sie "Speicher konfigurieren" auf der Registerkarte "Speicher", um den Assistenten "Speicher konfigurieren" zu starten.

Nachdem Backup Exec installiert ist und die Backup Exec-Dienste gestartet wurden, wird jeder Speicher, der mit dem Backup Exec-Server verknüpft ist, automatisch erkannt. Jedoch müssen Sie den Assistenten "Speicher konfigurieren" verwenden, um den Speicher für Backups zu konfigurieren.

Tabelle 13-2 Speicher, den Sie im Assistenten "Speicher konfigurieren" konfigurieren können

Typ des Speichers	Beschreibung
Plattenbasierter Speicher	<p>Speicher, der mit dem Server verknüpft bleibt.</p> <p>Es gibt folgende Typen von plattenbasiertem Speicher:</p> <ul style="list-style-type: none">■ Datenträgerspeicher Ein Speicherort auf einer lokal angehängten internen Festplatte, einem USB-Gerät, einem FireWire-Gerät oder einem NAS-Gerät (Network Attached Storage). Siehe "Konfigurieren von Festplattenspeicher" auf Seite 372.■ Festplattenkassettenspeicher Speicher, der normalerweise mit dem Server verknüpft bleibt, während Sie die Medien entfernen. Plattenkassetten verwenden Medien wie zum Beispiel ein RDX-Gerät oder Geräte, die in Windows als entfernbarer Speicher angezeigt werden. Siehe "Konfigurieren des Plattenkassettenspeichers" auf Seite 384.■ Deduplizierungsspeicher Ein Speicherort auf einer Festplatte, der die Größe von Backups reduziert, indem er nur eindeutige Daten speichert. Siehe "Erstellen oder Importieren des Deduplizierungsspeichers" auf Seite 1064.

Typ des Speichers	Beschreibung
Netzwerkspeicher	<p>Der Netzwerkspeicher umfasst Folgendes:</p> <ul style="list-style-type: none"> ■ NDMP-Server Mit dem Netzwerk verknüpfter Speicher (NAS), der das NDMP (Network Data Management Protocol)unterstützt, um die Verwendung von Geräten zu ermöglichen, die mit den Servern verknüpft sind. Siehe "Funktionen von NDMP Feature" auf Seite 1539. ■ OpenStorage-Geräte NAS-Speicher, der Veritas OpenStorage unterstützt. Siehe "Konfigurieren eines OpenStorage-Geräts" auf Seite 1058. ■ Cloud-Speichergeräte Cloud-Speichergeräte sind die in der Cloud konfigurierten und durch den Service-Provider des Cloud-Speichers gehosteten Speichergeräte. Die unterstützten Cloud-Anbieter finden Sie in der Liste der mit Backup Exec kompatiblen Hardware. ■ Remote Media Agent for Linux Ermöglicht es, Daten von den Remote-Computern auf den Speichergeräten zu sichern, die direkt mit einem Linux-Server verknüpft sind. Sie können Daten auch auf einer simulierten Bandbibliothek auf einem Linux-Server sichern. Siehe "Info zu Remote Media Agent for Linux " auf Seite 1598.
Bandspeicher	<p>Der Bandspeicher umfasst Folgendes:</p> <ul style="list-style-type: none"> ■ Eigenständige Bandlaufwerke Speicher, der eine Bandkassette für das Lesen und das Schreiben von Daten verwendet. Siehe "Support für Bandlaufwerke und Wechsler" auf Seite 447. ■ Wechsler Speicher, der Bandlaufwerke, Schächte und eine automatisierte Methode für das Laden von Bändern enthält. Siehe "Wechsler in Backup Exec" auf Seite 457. ■ Barcoderegeln Siehe "Barcoderegeln für einen Wechsler konfigurieren " auf Seite 459.
Speicherpools	<p>Speicherpools umfassen Folgendes:</p> <ul style="list-style-type: none"> ■ Speichergerätepools ■ Verwaltete Backup Exec-Server-Pools <p>Siehe "Erstellen von Speichergerätepools" auf Seite 512.</p>

Typ des Speichers	Beschreibung
Mediensätze und Speicher	<p>Mediensätze und Speicher sind für nur Bandmedien und enthalten Folgendes:</p> <ul style="list-style-type: none"> ■ Anhängezeitraum ■ Überschreibschutzzeitraum ■ Vaulting-Regeln <p>Sie können auch Assistenten ausführen, um Medienspeicher zu aktualisieren.</p> <p>Siehe "Verwalten von Bändern" auf Seite 472.</p>

Siehe ["Info zu Speicheraufträgen"](#) auf Seite 519.

Anzeigen von Details für mehrere Speichergeräte

Sie können mehrere Speichergeräte auswählen, für die Sie alle Aufträge, Auftragsverläufe und aktiven Warnmeldungen anzeigen möchten. Sie können alle Aktivitäten für einen bestimmten Backup Exec-Server anzeigen.

Siehe ["Übersicht über die Registerkarte "Speicher" in Backup Exec"](#) auf Seite 520.

So zeigen Sie Details für mehrere Speichergeräte an

- 1 Auf der Registerkarte "Speicher" halten Sie die Umschalt- oder Strg-Taste gedrückt und klicken Sie auf die Speichergeräte. Klicken Sie dann mit der rechten Maustaste auf eins der ausgewählten Speichergeräte.
- 2 Klicken Sie auf "Details".
- 3 Im linken Teilfenster klicken Sie auf "Aufträge", "Auftragsverlauf" oder "Aktive Warnmeldungen".

Senden einer Benachrichtigung beim Abschließen eines geplanten Speicherauftrags

Sie können die Empfänger angeben, die beim Abschluss eines geplanten Speicherauftrags benachrichtigt werden sollen. Die Empfänger müssen festgelegt sein, bevor Sie die Benachrichtigung einrichten können.

Siehe ["Info zu Speicheraufträgen"](#) auf Seite 519.

Senden einer Benachrichtigung nach Abschluss eines geplanten Speicherauftrags

- 1** Erstellen Sie einen neuen Speicherauftrag oder bearbeiten Sie einen vorhandenen Auftrag.

Siehe ["Info zu Speicheraufträgen"](#) auf Seite 519.
- 2** Klicken Sie im linken Teilfenster des Speicherauftrags-Dialogfelds auf Benachrichtigung.
- 3** Wählen Sie das Kontrollkästchen für jeden Empfänger, der nach Abschluss eines jeden Speicherauftrags benachrichtigt werden soll.
- 4** Sie können fortfahren, indem Sie andere Optionen auswählen oder auf OK klicken.

Siehe ["Einen Speicherauftrag planen"](#) auf Seite 527.

Einen Speicherauftrag planen

Wenn Sie einen Speicherauftrag planen, können Sie die Zeit und die Häufigkeit für die Ausführung des Auftrags konfigurieren.

Siehe ["Info zu Speicheraufträgen"](#) auf Seite 519.

So planen Sie einen Speicherauftrag

- 1** Klicken Sie auf der Registerkarte "Speicher" mit der rechten Maustaste auf den zu planenden Speicherauftrag.

Wenn der Speichervorgang geplant werden kann, wird neben dem Vorgangsnamen ein kleiner Pfeil angezeigt.
- 2** Klicken Sie auf den Speichervorgang und klicken Sie dann auf "Zeitplan".
- 3** Klicken Sie im linken Teilfenster des Dialogfelds "Speicherauftrag" auf "Zeiplan".
- 4** Wählen Sie eine der folgenden Optionen:

Wiederkehrend

Ermöglicht das Erstellen eines wiederkehrenden Zeitplans für den Auftrag.

Stunden

Hiermit können Sie ein Wiederholungsmuster erstellen, das in Stunden oder Minuten gemessen wird.

Wenn Sie "Stunden" auswählen, können Sie folgende Optionen konfigurieren:

- Alle X Stunden/Minuten
Gibt die Anzahl von Stunden oder Minuten zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz an.
- Von
Gibt die Startzeit eines Auftrags an.
- Zwischen
Schränkt den Auftrag auf bestimmte Stunden und Tage ein. Wenn der Auftrag beispielsweise nur während Geschäftszeiten ausgeführt werden soll, können Sie 9:00 bis 17:00 Uhr am Montag, Dienstag, Mittwoch, Donnerstag und Freitag auswählen. Die Start- und Endzeit können maximal 24 Stunden auseinander liegen, doch sie können sich über Mitternacht in den folgenden Tag hinein überschneiden.

Tage

Hiermit können Sie ein Wiederholungsmuster erstellen, das in Tagen gemessen wird.

Wenn Sie "Tage" auswählen, müssen Sie zwischen den folgenden Optionen auswählen:

- Alle X Tage
Gibt die Anzahl von Tagen zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz an.
- Jeden Wochentag
Gibt an, dass der Auftrag Montag, Dienstag, Mittwoch, Donnerstag und Freitag ausgeführt werden soll.

Wochen

Hiermit können Sie ein Wiederholungsmuster erstellen, das in Wochen gemessen wird.

Wenn Sie ein Wiederholungsmuster erstellen, das in Wochen gemessen wird, müssen Sie das Feld "Alle X Wochen am" konfigurieren. Das Feld "Alle X Wochen am" gibt die Anzahl von Wochen zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz an. Es gibt außerdem die Wochentage an, an denen der Auftrag ausgeführt werden soll.

Monate

Hiermit können Sie ein Wiederholungsmuster erstellen, das in Monaten gemessen wird.

Wenn Sie "Monate" auswählen, müssen Sie zwischen den folgenden Optionen auswählen:

- Tag X jedes X. Monats
Gibt den Tag an, an dem der Auftrag aufgeführt werden soll. Gibt außerdem die Anzahl von Monaten zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz an.
- Jeden X X jedes X. Monats
Gibt den Tag an, an dem der Auftrag aufgeführt werden soll. Gibt außerdem die Anzahl von Monaten zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz an.
- Ausgewählte Monatstage
Gibt die bestimmten Tage des Monats an, an denen Backup Exec den Auftrag ausführt. Sie wählen die Tage und die Wochen auf einem Raster aus. Das ausgewählte Wiederholungsmuster wird jeden Monat wiederholt.
Standardmäßig wird der Auftrag jeden Monat ausführt und beginnt in der aktuellen Woche und am aktuellen Tag des Monats. Wenn Sie beispielsweise den Auftrag am dritten Montag im Monat erstellen, wird der Auftrag standardmäßig am dritten Montag jedes Monats ausgeführt.
Sie können den Standard ändern oder zusätzliche Tage auswählen, auf denen der Auftrag ausführen sollte. Alle zusätzlich ausgewählten Tage werden dem monatlichen Wiederholungsmuster hinzugefügt.
- Ausgewählte Monatstage
Gibt die Tage des Monats an, an denen Backup Exec den Auftrag ausführt. Das ausgewählte Wiederholungsmuster

wird jeden Monat wiederholt.

Standardmäßig wird der Auftrag jeden Monat ausgeführt und beginnt am aktuellen Tag des Monats. Wenn Sie den Auftrag beispielsweise am 15. April erstellen, wird der Auftrag standardmäßig am 15. jedes Monats ausgeführt.

Sie können den Standard ändern oder zusätzliche Tage auswählen, auf denen der Auftrag ausführen sollte. Alle zusätzlich ausgewählten Tage werden dem monatlichen Wiederholungsmuster hinzugefügt.

Wenn Sie den 31. auswählen, wird der Auftrag in Monaten, die keine 31 Tage haben, am letzten Tag des Monats ausgeführt. Wenn Sie den Auftrag beispielsweise so konfigurieren, dass er am 31. ausgeführt wird, wird er im September stattdessen am 30. ausgeführt.

Jahre

Hiermit können Sie ein Wiederholungsmuster erstellen, das in Jahren gemessen wird.

Wenn Sie "Jahre" auswählen, können Sie die folgenden Optionen konfigurieren:

- Alle X Jahre
Gibt die Anzahl von Jahren zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz an.
- "Am X"
Gibt das Datum an, an dem Backup Exec den Auftrag ausführt. Das in diesem Feld ausgewählte Datum entspricht der Anzahl von Jahren, die Sie im Feld "Alle X Jahre" ausgewählt haben. Wenn Sie festgelegt haben, dass der Auftrag alle zwei Jahre ausgeführt werden soll, und Sie in diesem Feld 28. Juni ausgewählt haben, wird der Auftrag alle zwei Jahre jeweils am 28. Juni ausgeführt.
- "Am X. X"
Gibt den Tag und den Monat an, an dem Backup Exec den Auftrag ausführt. Das in diesem Feld ausgewählte Datum entspricht der Anzahl von Jahren, die Sie im Feld "Alle X Jahre" ausgewählt haben. Wenn Sie festgelegt haben, dass der Auftrag alle zwei Jahre ausgeführt werden soll, und Sie in diesem Feld den vierten Donnerstag im Juni ausgewählt haben, wird der Auftrag alle zwei Jahre jeweils am vierten Donnerstag im Juni ausgeführt.

um

Gibt die Startzeit des ersten Auftrags im Wiederholungsmuster an.

Kalender

Ermöglicht die Anzeige aller geplanten Aufträge in einem Kalender, um Konflikte bei der Planung zu vermeiden.

Auftrag neu planen, falls er X Stunden nach geplanter Startzeit noch immer nicht ausgeführt wird	Gibt den Zeitraum nach der geplanten Startzeit des Auftrags an, nach dessen Ablauf Backup Exec den Auftragsabschlussstatus in "Verpasst" ändert. Der Auftrag wird erneut geplant, um gemäß des von Ihnen festgelegten Zeitfensters ausgeführt zu werden.
Abbrechen des Auftrags, falls er X Stunden nach der ursprünglich festgelegten Startzeit noch immer ausgeführt wird	Gibt den Zeitraum nach der geplanten Startzeit des Auftrags an, nach dessen Ablauf der Auftrag abgebrochen wird, wenn er noch ausgeführt wird. Backup Exec ändert den Auftragsabschlussstatus in "Abgebrochen, Zeitüberschreitung".
"Daten mit dem Zeitplan dieses Auftrags einschließen"	Geben Sie Daten an, die in den Auftragszeitplan eingeschlossen werden sollen. Der Auftrag wird an allen mit dieser Option ausgewählten Tagen ausgeführt, zusätzlich zu den Tagen, die Teil des normalen Zeitplans sind. Der Auftrag wird am nächsten im normalen Zeitplan festgelegten Tag nach dem eingeschlossenen Datum fortgesetzt.
"Daten vom Zeitplan des Auftrags ausschließen"	Geben Sie Daten an, die aus dem Auftragszeitplan ausgeschlossen werden sollen. Der Auftrag wird an diesen Tagen nicht ausgeführt. Er wird am nächsten im normalen Zeitplan festgelegten Tag nach dem ausgeschlossenen Datum fortgesetzt.
Jetzt ohne regelmäßigen Zeitplan ausführen	Führt den Auftrag sofort aus, ohne weitere Instanzen für die Zukunft zu planen.
Ausführen am	Führt den den Auftrag am angegebenen Datum zur angegebenen Zeit aus.

Ohne Zeitplan erstellen

Erstellt einen Auftrag ohne Zeitplan. Wenn Sie diese Option verwenden, wird der Auftrag nicht zur Zeit der Erstellung ausgeführt und hat keinen wiederkehrenden Zeitplan. Der Auftrag verbleibt ungeplant, bis Sie beschließen, ihn auszuführen. Sie können ein Drittanbieter-Tool zur automatischen Auftragsausführung oder -planung verwenden, um den Auftrag später auszuführen.

Wenn Sie diese Option zum Erstellen eines Auftrags verwenden, können Sie den Auftrag nicht anhalten. Sie können Aufträge nicht anhalten, es sei denn, dass sie geplant werden.

5 Klicken Sie auf "OK".

Bearbeiten globaler Einstellungen für Speicher

Sie können die globalen Einstellungen für die Wechsler, die Bandmedien und den plattenbasierten Speicher in Ihrer Umgebung bearbeiten.

So bearbeiten Sie globale Einstellungen für Speicher

- 1** Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Backup Exec-Einstellungen".
- 2** Klicken Sie im linken Teilfenster auf "Speicher".
- 3** Wählen Sie die entsprechenden Optionen aus.

Inventarisieren von Wechslern beim
Starten der Backup Exec-Dienste

Mit dieser Option kann Backup Exec alle Schächte in einem Wechsler inventarisieren, wenn die Backup Exec-Dienste gestartet werden. Je nach Anzahl von Schächten und Wechslern kann dieser Prozess einige Minuten in Anspruch nehmen.

Diese Option ist standardmäßig deaktiviert.

Vollständig – Zugewiesene und importierte Medien schützen

Wählen Sie diese Option aus, um zu verhindern, dass Backup Exec Bänder überschreibt, die sich in Mediensätzen befinden, und solche, die aus einer anderen Installation von Backup Exec oder aus einem anderen Produkt importiert wurden.

Siehe "[Überschreibschutzzeiträume und Anhängezeiträume in Mediensätzen](#)" auf Seite 476.

Diese Option bietet die größte Sicherheit, da geschützte Bandmedien erst in den folgenden Fällen überschrieben werden können:

- Der Überschreibschutzzeitraum für das Medium ist abgelaufen.
- Sie verschieben ein Medium, das zu einem aktiven Mediensatz gehört, in die temporären Medien.
- Sie löschen, formatieren oder kennzeichnen das Medium.
- Sie verschieben importierte Medien in "Temporäre Medien".

Teilweise – Nur zugewiesene Medien schützen

Wählen Sie diese Option, wenn Backup Exec Bänder überschreiben soll, die aus einer anderen Installation von Backup Exec oder aus einem anderen Produkt importiert wurden, oder temporäre Medien. Medien in einem Mediensatz, dessen Überschreibschutz noch nicht abgelaufen ist (zugewiesene Medien) können nicht überschrieben werden.

Verwenden Sie diese Option, wenn Sie Medien aus einer anderen Installation von Backup Exec oder aus einem anderen Produkt verwenden möchten.

Diese Option ist standardmäßig aktiviert.

Aufforderung vor Überschreiben
importierter Medien

Wählen Sie diese Option aus, wenn Sie aufgefordert werden wollen, bevor Backup Exec Bänder überschreibt, die aus einer anderen Installation von Backup Exec oder aus einem anderen Produkt importiert wurden. Sie müssen die Option "Teilweise – Nur zugewiesene Medien schützen" wählen.

Der Auftrag kann erst ausgeführt werden, wenn Sie auf diese Eingabeaufforderung reagieren.

Keine

Wählen Sie diese Option, um den Medienüberschreibschutz für Bandlaufwerke zu deaktivieren. Mit dieser Option müssen Sie selbst sicherstellen, dass die Medien in Bandlaufwerken nicht versehentlich überschrieben werden.

Wenn ein Überschreibauftrag für ein Bandlaufwerk eingegeben wird und die Medienüberschreibschutzstufe "Keine" festgelegt ist, wird das Medium überschrieben.

Hinweis: Die Auswahl dieser Option wird nicht empfohlen, da hierdurch Daten nicht vor dem Überschreiben geschützt werden.

Aufforderung vor Überschreiben
zugewiesener oder importierter Medien

Wählen Sie diese Option, wenn Sie aufgefordert werden wollen, bevor Backup Exec die zugeordneten oder importierten Medien in Bandlaufwerken überschreibt. Wenn Sie zuvor "Keine" ausgewählt haben, wird empfohlen, diese Option zu wählen, damit Sie vor dem Überschreiben zugewiesener oder importierter Medien zur Bestätigung des Vorgangs aufgefordert werden.

Der Auftrag kann erst ausgeführt werden, wenn Sie auf diese Eingabeaufforderung reagieren.

Temporäre Medien überschreiben, bevor
wiederverwendbare Medien des
Zielmediensatzes überschrieben werden

Wählen Sie diese Option, wenn temporäre
Backup Exec-Medien zuerst in einem
Bandlaufwerk überschrieben werden
sollen, wenn ein Überschreibungsauftrag
auftritt.

Siehe "[So sucht Backup Exec nach
überschreibbaren Medien in
Bandlaufwerken](#) " auf Seite 488.

Wenn keine temporären Medien in den
Bandlaufwerken gefunden werden,
überschreibt Backup Exec
wiederverwendbare Medien im
ausgewählten Mediensatz.

Wenn keine wiederverwendbaren Medien
im ausgewählten Mediensatz gefunden
werden, sucht Backup Exec nach
wiederverwendbaren Medien in allen
Mediensätzen.

Wenn keine wiederverwendbare Medien
gefunden werden, sucht Backup Exec
automatisch nach anderen Medien zum
Überschreiben. Welche Medien
überschrieben werden, ist von der von
Ihnen festgelegten Überschreibschutzstufe
abhängig. Wenn Sie diese Option
aktivieren, werden eventuell mehr Medien
für die gleiche Anzahl an Aufträgen
benötigt, als wenn zuerst die
wiederverwendbaren Medien
überschrieben werden.

Diese Option wirkt sich auf die Reihenfolge
aus, in der Backup Exec Medien
überschreibt. Wenn Sie festlegen, dass
temporäre Medien zuerst überschrieben
werden sollen, werden die
wiederverwendbaren Medien
möglicherweise länger für eine mögliche
Wiederherstellung beibehalten.

Diese Option ist standardmäßig aktiviert.

Wiederverwendbare Medien des
Zielmediensatzes überschreiben, bevor
temporäre Medien überschrieben werden

Wählen Sie diese Option, wenn Backup
Exec wiederverwendbare Medien in einem
Bandlaufwerk zuerst im ausgewählten
Mediensatz überschreiben soll, wenn ein
Überschreibungsauftrag auftritt.

Wenn sich keine wiederverwendbaren
Medien in den Bandlaufwerken befinden,
überschreibt Backup Exec die temporären
Medien.

Wenn weder wiederverwendbare noch
temporäre Medien gefunden werden, sucht
Backup Exec nach Medien zum
Überschreiben. Welche Medien
überschrieben werden, ist von der von
Ihnen festgelegten Überschreibschutzstufe
abhängig.

Siehe "[So sucht Backup Exec nach
überschreibbaren Medien in
Bandlaufwerken](#)" auf Seite 488.

Wenn Sie festlegen, dass zuerst
wiederverwendbare Medien im
ausgewählten Mediensatz überschrieben
werden sollen, werden dieselben Medien
häufiger wiederverwendet, als wenn zuerst
temporäre Medien überschrieben werden.

Backup Exec auf schreibgeschützte Vorgänge auf einem plattenbasierten Speichergerät begrenzen, wenn es für entfernt worden ist

Wählen Sie diese Option aus, um zu verhindern, dass Backup Exec Speicherplatz aus abgelaufenen Backup-Sätzen auf einem beliebigen plattenbasierten Speichergerät freigibt, das nach einer mehrtägigen Pause wieder angeschlossen wird. Backup-Aufträge, die Sie an dieses Gerät senden, schlagen fehl. Sie können diese Einstellung pro plattenbasiertes Speichergerät in den Eigenschaften des Geräts ändern.

Bevor Sie diese Einstellung deaktivieren, sollten Sie die Ablaufdaten der Backup-Sätze anzeigen und entscheiden, ob Sie einige Backup-Sätze länger behalten möchten. Sie können das Ablaufdatum eines Backup-Satzes ändern, oder Sie können einen Backup-Satz unbestimmt behalten.

Siehe ["Bearbeiten der Eigenschaften von Festplattenspeichern"](#) auf Seite 376.

Siehe ["Backup-Sätze "](#) auf Seite 401.

Siehe ["Wiederherstellen von Daten von einem erneut verbundenen oder eingelegten, plattenbasierten Speichergerät"](#) auf Seite 383.

Siehe ["Löschen abgelaufener Backup-Sätze auf plattenbasiertem Speicher durch Data Lifecycle Management \(DLM\)"](#) auf Seite 393.

Anzahl der Tage

Gibt an, wie lange Backup Exec auf schreibgeschützte Vorgängen auf einem plattenbasierten Speichergerät beschränkt ist, wenn Sie es wieder anschließen.

Die Standardeinstellung ist 14 Tage.

Backup Exec auf schreibgeschützte Vorgänge auf einer Datenträgerkassette begrenzen, wenn sie nicht für eingelegt worden ist

Verhindert, dass Backup Exec Speicherplatz von abgelaufenen Backup-Sätzen auf Plattenspeichergeräten zurückfordert, nachdem das Gerät eine angegebenen Anzahl an Tagen abwesend war. Backup-Aufträge, die Sie an dieses Gerät senden, schlagen fehl. Sie können diese Einstellung pro Datenträgerkassette in den Eigenschaften des Geräts ändern.

Bevor Sie diese Einstellung deaktivieren, sollten Sie die Ablaufdaten der Backup-Sätze anzeigen und entscheiden, ob Sie einige Backup-Sätze länger behalten möchten. Sie können das Ablaufdatum eines Backup-Satzes ändern, oder Sie können einen Backup-Satz unbestimmt behalten.

Siehe ["Bearbeiten der Eigenschaften von Festplattenkassetten"](#) auf Seite 385.

Siehe ["Backup-Sätze"](#) auf Seite 401.

Siehe ["Wiederherstellen von Daten von einem erneut verbundenen oder eingelegten, plattenbasierten Speichergerät"](#) auf Seite 383.

Siehe ["Löschen abgelaufener Backup-Sätze auf plattenbasiertem Speicher durch Data Lifecycle Management \(DLM\)"](#) auf Seite 393.

Anzahl der Tage

Gibt den Zeitraum in Tagen an, für den ein Gerät vom Backup Exec-Server getrennt sein muss, nach dem Backup Exec auf schreibgeschützte Vorgänge auf dem Gerät begrenzt wird, wenn Sie es erneut anschließen.

Die Standardeinstellung ist 30 Tage.

Zulassen, dass Backup Exec alle
abgelaufenen Backup-Sätze löscht

Wählen Sie diese Option, um Backup Exec die letzten vollen, inkrementellen und differenziellen Backup-Sätze löschen zu lassen, die notwendig sind, um einen Server wiederherzustellen, wenn die Backup-Sätze abgelaufen sind. Standardmäßig behält Backup Exec die aktuellen Backup-Sätze, die notwendig sind, um einen Server wiederherzustellen, selbst wenn die Backup-Sätze ablaufen. Wenn Sie zulassen, dass Backup Exec alle abgelaufenen Backup-Sätze für einen Server löscht, sind Sie möglicherweise nicht in der Lage, diesen Server wiederherzustellen.

Diese Option ist sinnvoll, wenn Sie Daten nach einem bestimmten Zeitraum (z. B. mehrere Jahre) nicht mehr behalten möchten.

Wenn Sie diese Option jedoch aktivieren, können Sie Backup-Sätze unter den folgenden Bedingungen verlieren:

- Wenn der Zeitraum, für den die Backup-Daten oder die Backup-Sätze behalten werden, kleiner ist als die Häufigkeit des Backups. Das heißt, laufen die Backup-Sätze vom letzten vollständigen Backup-Auftrag laufen ab, bevor das nächste vollständige Backup ausgeführt wird. Stellen Sie sicher, dass, wenn Sie Aufträge erstellen, die Backup-Daten länger aufbewahrt werden als der bestimmte Zeitraum zwischen vollständigen Backups.
- Wenn der Backup-Auftrag ausfällt oder verpasst wird und nicht erneut ausgeführt wird, bevor die Backup-Sätze ablaufen. Überwachen Sie fehlgeschlagene oder übersprungene Aufträge, und stellen Sie sicher, dass Sie sie erneut ausführen, bevor die Backup-Sätze vom vorherigen vollständigen Backup ablaufen.

Diese Option ist standardmäßig nicht ausgewählt.

Hinweis: In einer CAS-Umgebung (Central Admin Server Feature) ist diese Option nur auf dem zentralen Administrationsserver verfügbar. Wenn Sie diese Option auf dem zentralen Administrationsserver aktivieren, löscht DLM alle abgelaufenen Backup-Sätze auf dem zentralen Administrationsserver sowie auf allen verwalteten Backup Exec-Servern. Diese Option löscht alle abgelaufenen Backup-Sätze auf zentral und lokal verwalteten Backup Exec-Servern in einer CAS-Umgebung.

Siehe "[Backup-Sätze](#) " auf Seite 401.

Siehe "[Löschen abgelaufener Backup-Sätze auf plattenbasiertem Speicher durch Data Lifecycle Management \(DLM\)](#)" auf Seite 393.

4 Klicken Sie auf "OK".

Freigeben von Speichergeräten

In Umgebungen, in denen es mehr als einen Backup Exec-Server gibt, können Backup Exec-Server Speichergeräte gemeinsam nutzen. Beispielsweise können mehrere Backup Exec-Server in einer CAS-Umgebung Speichergeräte gemeinsam nutzen. In diesen Umgebungen verwaltet Backup Exec eine Datenbank des gemeinsam genutzten Speichergeräts. Andernfalls können die Backup-Daten, die ein Server an das Speichergerät sendet, die Daten überschreiben, die ein anderer Server sendet.

Hinweis: Die Enterprise Server Feature muss installiert sein, damit Sie die Speichergeräte zwischen den Backup Exec-Servern freigeben können.

Backup Exec-Server können die folgenden Speichertypen gemeinsam nutzen:

- Speicher, der mit einem NDMP-Server verknüpft ist
- Deduplizierungdatenträgerspeicher
- OpenStorage-Geräte

- Cloud-Speichergeräte
- Virtuelle Datenträger
- Datenträgerspeicher
- Remote Media Agents
- Die Backup Exec-Agents, die konfiguriert werden, Daten direkt in den Speicher zu senden

Bei Speichergeräten und virtuellen Datenträgern müssen Sie einen UNC-Pfad angeben, über den die Backup Exec-Server auf das Speichergerät zugreifen können. Plattenkassetten können nicht freigegeben werden.

Wenn Sie ein Speichergerät gemeinsam nutzen, können Sie auswählen, welche Backup Exec-Server auf das Speichergerät zugreifen können. Der Backup Exec-Server, von dem aus Sie das Speichergerät hinzugefügt haben, wird automatisch aktiviert, um das Speichergerät gemeinsam zu nutzen. Sie können die Funktion für die gemeinsame Nutzung jedoch jederzeit von diesem Backup Exec-Server entfernen. Wenn Sie z. B. ein Speichergerät zu einem zentralen Administrationsserver hinzufügen, kann dieser Server das Speichergerät verwenden. Wenn der zentrale Administrationsserver jedoch in Ihrer Umgebung nicht als verwalteter Backup Exec-Server fungieren kann, können Sie die Funktion für die gemeinsame Nutzung vom zentralen Administrationsserver entfernen.

Wenn Sie mehrere Backup Exec-Server und mehrere Speichertypen in Ihrer Umgebung haben, können Sie einen Backup Exec-Server auswählen und den Speicher für ihn verwalten.

So geben Sie ein Speichergerät frei

- 1 Klicken Sie auf der Registerkarte "Speicher" mit der rechten Maustaste auf das Speichergerät, das Sie freigeben möchten.
- 2 Klicken Sie auf "Freigeben".
- 3 Um ein Speichergerät oder einen virtuellen Datenträger freizugeben, geben Sie einen UNC-Pfad ein, über den die Server auf das Speichergerät zugreifen können, das Sie freigeben möchten.
- 4 Prüfen Sie die Backup Exec-Server oder die verwalteten Backup Exec-Server, die dieses Speichergerät gemeinsam nutzen sollen.
- 5 Klicken Sie auf "OK".

Löschen von Speichergeräten

Speichergeräte können aus der Backup Exec-Datenbank gelöscht werden. Wenn das Speichergerät ein veralteter Backup-to-Disk-Ordner, ein Datenträgerspeichergerät, ein Deduplizierungsspeichergerät oder ein Cloud-basiertes Speichergerät ist, fordert Backup Exec Sie auf, die Backup-Sätze aus der Administratorkonsolenansicht zu löschen. Sie können diese Backup-Sätze nicht mehr über die Administratorkonsole anzeigen oder auswählen. Die Backup-Sätze verbleiben jedoch auf dem Speichergerät. Sie müssen Inventar- und Katalogvorgänge auf dem Speichergerät ausführen, bevor Sie von ihm wiederherstellen können.

Sie sollten die Backup-Sätze aus der Administratorkonsole löschen, wenn Sie ein Speichergerät auf eine andere Backup Exec-Installation verschieben. Wenn das jedoch Verschieben nur vorübergehend ist, werden Sie die Backup-Sätze vermutlich nicht löschen wollen. Wenn Sie die Backup-Sätze behalten, vermeiden Sie es, Inventar- und Katalogvorgänge auf dem Gerät ausführen zu müssen, wenn Sie sie zurückverschieben. Sie sollten die Backup-Sätze auch behalten, wenn Sie planen, das Speichergerät neu zu erstellen.

Sie können auch Windows-Explorer verwenden, um zum älteren Backup-to-Disk-Ordner oder zum Datenträgerspeicher zu navigieren und ihn dann zu löschen. Wenn Sie diese Methode verwenden, können Sie den Speicher in Backup Exec nicht neu erstellen.

Löschen eines Speichergeräts.

- 1** Klicken Sie mit der rechten Maustaste auf der Registerkarte "Speicher" auf das Speichergerät, das Sie löschen möchten, und dann auf "Deaktivieren".
- 2** Klicken Sie mit der rechten Maustaste auf das Gerät und dann auf "Löschen".
- 3** Wenn Sie aufgefordert werden, das Speichergerät zu löschen, klicken Sie auf "Ja".

Siehe ["Deaktivieren und Aktivieren eines Speichergeräts"](#) auf Seite 553.

Siehe ["Erneutes Erstellen eines veralteten Backup-to-Disk-Ordners einschließlich des Inhalts"](#) auf Seite 442.

Siehe ["Backup-Sätze "](#) auf Seite 401.

Ändern des Status eines Speichergeräts in "Online"

Normalerweise wird eine Warnmeldung angezeigt, wenn ein Gerät zu Offline wechselt. Die Warnmeldung enthält einen bestimmten Grund, warum das Gerät offline ist.

Außerdem kann ein Link zur Supportdatenbank enthalten sein.

Korrigieren Sie das Problem, durch das das Gerät offline geschaltet wurde. Für Bandlaufwerke, Wechsler und einige andere Gerätetypen, müssen Sie den Zustand des Geräts manuell zu online ändern.

Backup Exec erkennt bei Datenträgerspeichern, Plattenkassetten, Speichergruppen und virtuellen Datenträgergeräten innerhalb von fünf Minuten, dass das Gerät online ist, und ändert automatisch den Zustand zu online.

Siehe ["Fehlerbehebung von Hardware-bezogenen Problemen"](#) auf Seite 880.

So ändern Sie den Status eines Speichergeräts in "Online"

- 1 Klicken Sie auf der Registerkarte "Speicher" auf das Speichergerät, das Sie online schalten möchten.
- 2 Klicken Sie auf "Offline", um das Häkchen zu löschen.

Umbenennen von Speichergeräten

Sie können ein Speichergerät umbenennen, das sich in Ihrer Umgebung befindet.

Sie können vom System festgelegte Speichergerätpools nicht umbenennen, aber Sie können alle Speichergerätpools umbenennen, die Sie erstellen.

Siehe ["Info zu Speicheraufträgen"](#) auf Seite 519.

So benennen Sie ein Speichergerät um

- 1 Doppelklicken Sie auf der Registerkarte "Speicher" auf das Speichergerät, das Sie umbenennen möchten.
- 2 Geben Sie in den Eigenschaften des Speichergeräts den neuen Namen in das Namensfeld ein.
- 3 Klicken Sie auf "Übernehmen".

Anzeigen von Aufträgen, Auftragsverläufen, Backup-Sätzen und aktiven Warnmeldungen für Speichergeräte

Sie können Informationen zu einem Speichergerät anzeigen.

Siehe ["Info zu Speicheraufträgen"](#) auf Seite 519.

So zeigen Sie Aufträge, Auftragsverläufe, Backup-Sätze und aktive Warnmeldungen für Speichergeräte an

- 1 Doppelklicken Sie auf der Registerkarte "Speicher" auf das Speichergerät, für das Sie den Auftragsverlauf, die Backup-Sätze oder die aktiven Warnmeldungen anzeigen möchten.
- 2 Klicken Sie im linken Teilfenster auf "Aufträge", "Auftragsverlauf", "Backup-Sätze" oder "Aktive Warnmeldungen".

Siehe ["Informationen zum Auftragsverlauf"](#) auf Seite 302.

Siehe ["So überwachen und verwalten Sie Aufträge in Backup Exec"](#) auf Seite 286.

Siehe ["Informationen zur Auftragsüberwachung"](#) auf Seite 289.

Siehe ["Warnmeldungen und Benachrichtigungen in Backup Exec"](#) auf Seite 334.

Siehe ["Backup-Sätze"](#) auf Seite 401.

Katalogisieren eines Speichergeräts

Eine Katalogisierung ermöglicht Folgendes:

- Protokollieren des Inhalts von Medien, die von einer anderen Installation von Backup Exec erstellt wurden.
- Erstellen eines neuen Katalogs auf der lokalen Festplatte, wenn der Katalog für das Medium nicht mehr vorhanden ist.

Bevor Sie Daten auf einem Speichergerät wiederherstellen oder überprüfen können, muss ein Katalog für dieses Gerät existieren. Wenn Backup Exec dieses Speichergerät zuvor nicht verwendet hat, müssen Sie zuerst einen "Inventar und Katalog" -Speichervorgang auf dem Gerät ausführen.

Hinweis: Wenn ein Medienkennwort aus einer niedrigeren Version von Backup Exec verwendet wurde, katalogisiert Backup Exec das Medium, als ob es nicht kennwortgeschützt wäre. Verschlüsseln Sie stattdessen die Daten.

Siehe ["Verwendung von Verschlüsselung mit Backup Exec"](#) auf Seite 727.

Siehe ["Inventarisieren und Katalogisieren von Speichergeräten"](#) auf Seite 552.

Siehe ["Funktionsweise der Backup Exec-Kataloge"](#) auf Seite 277.

So katalogisieren Sie Speicher

- 1 Klicken Sie auf der Registerkarte "Speicher" mit der rechten Maustaste auf das zu katalogisierende Speichergerät.
- 2 Klicken Sie auf "Katalogisieren".
- 3 Klicken Sie im Katalogdialogfeld auf "Allgemein" und geben Sie einen Namen für den Auftrag ein.
- 4 Klicken Sie auf "OK".
- 5 (Optional) zeigen Sie das Auftragsprotokoll an oder klicken Sie auf die Registerkarte "Auftragsüberwachung", um Details über den Auftrag anzuzeigen.

Siehe ["Anzeigen von Aufträgen, Auftragsverläufen, Backup-Sätzen und aktiven Warnmeldungen für Speichergeräte"](#) auf Seite 548.

Scannen eines Speichergeräts

Beim Scannen werden Informationen über die Medien in den Schächten gesammelt, einschließlich Barcode-Informationen, sofern verfügbar. Anschließend wird die Backup Exec-Datenbank mit den neuesten Informationen darüber aktualisiert, wo sich die Medien befinden. Wenn Sie Magazine austauschen oder neue Medien in ein Magazin in einem Wechsler einlegen, aktualisieren Sie mithilfe eines Scan-Vorgangs die Daten zu diesem Schacht.

Das Scan-Auftragsprotokoll berichtet die mit Barcode versehenen Medien in den Laufwerken und Portalen. Wenn der Wechsler ausgelastet ist, kann das Scan-Auftragsprotokoll den Laufwerks- und Portalstatus möglicherweise nicht erkennen. Wenn die Laufwerke und Portale nicht gelesen werden können, werden sie im Auftragsprotokoll nicht angezeigt. Beste Ergebnisse erhalten Sie, wenn Sie den Scanvorgang ausführen, während der Wechsler inaktiv ist.

Siehe ["Info zu Speicheraufträgen"](#) auf Seite 519.

So scannen Sie ein Speichergerät sofort

- 1 Klicken Sie auf der Registerkarte "Speicher" mit der rechten Maustaste auf den zu scannenden Wechsler oder Schacht.
- 2 Klicken Sie auf "Scan" und dann auf "Jetzt scannen".
- 3 (Optional) zeigen Sie den Auftragsverlauf an oder klicken Sie auf die Registerkarte "Auftragsüberwachung", um Details zum Auftrag anzuzeigen.

So planen Sie einen Scanvorgang für ein Speichergerät

- 1 Klicken Sie auf der Registerkarte "Speicher" mit der rechten Maustaste auf den zu scannenden Wechsler oder Schacht.
- 2 Klicken Sie auf "Scan" und dann auf "Planen".
- 3 Um nach Abschluss des Auftrags eine Benachrichtigung zu senden, klicken Sie im linken Teilfenster auf "Benachrichtigung" und wählen Sie die entsprechenden Optionen aus.
- 4 Um den Auftrag zu planen, klicken Sie im linken Teilfenster auf "Planen" und wählen Sie die entsprechenden Optionen aus.

Siehe ["Einen Speicherauftrag planen"](#) auf Seite 527.

- 5 (Optional) Zeigen Sie das Scan-Auftragsprotokoll an, um zu sehen, welche mit Barcode versehenen Medien sich in den Schächten, Laufwerken und Portalen eines Wechslers befinden, oder klicken Sie auf die Registerkarte "Auftragsüberwachung", um Details zum Auftrag anzuzeigen.

Siehe ["Anzeigen von Aufträgen, Auftragsverläufen, Backup-Sätzen und aktiven Warnmeldungen für Speichergeräte"](#) auf Seite 548.

Inventarisieren eines Speichergeräts

Sie können eine Inventarisierung so ausführen, dass Backup Exec ein Speichergerät liest und die Backup Exec-Datenbank mit Informationen über die Medien auf diesem Gerät aktualisiert.

Bei Wechslern können Sie alle Schächte inventarisieren, wenn Sie Bänder wechseln. Sie können auch bestimmte Schächte für die Inventarisierung auswählen. Sie müssen Schächte nicht erneut inventarisieren, wenn Sie die Bänder hinzufügen, die Backup Exec anfordert. Wenn beispielsweise die Daten, die Sie wiederherstellen möchten, auf einem Band sind, das nicht im Wechsler ist, werden Sie aufgefordert, das richtige Band für den Wiederherstellungsvorgang einzufügen. In diesem Fall müssen Sie den Schacht, in den das Band eingefügt wird, nicht neu inventarisieren. Wenn Sie ein Band dass Backup Exec nicht anfordert, hinzufügen oder entfernen, sollten Sie eine Inventarisierung der geänderten Schächte ausführen. Sie können

bestimmte Schächte für die Inventarisierung auswählen. Wenn Sie Bänder häufig austauschen, sollten Sie bei jedem Neustart der Backup Exec-Dienste eine Inventarisierung des Wechslermagazins ausführen.

Für Bandlaufwerke können Sie eine Inventarisierung ausführen, um die enthaltenen Medien bereitzustellen und die Medienkennungen zu lesen. Wenn Sie die Medien in einem Laufwerk ändern, führen Sie eine Inventarisierung aus, damit die Kennung der aktuellen Medien in den Eigenschaften angezeigt werden. Andernfalls werden die vorherigen Medien weiterhin in den Eigenschaften angezeigt. Es kommt möglicherweise zu einer Verzögerung, während die Medien in einem Wechsler bereitgestellt und inventarisiert werden.

So inventarisieren Sie ein Speichergerät jetzt

- 1** Klicken Sie auf der Registerkarte "Speicher" mit der rechten Maustaste auf das Speichergerät, das Sie inventarisieren möchten.
- 2** Klicken Sie auf "Inventarisieren" und klicken Sie dann auf "Jetzt inventarisieren".
Die Inventarisierung wird ausgeführt. Sie können das Auftragsprotokoll anzeigen oder auf die Registerkarte "Auftragsüberwachung" für Details über den Auftrag klicken.

So planen Sie einen Inventarisierungsauftrag für ein Speichergerät

- 1** Klicken Sie auf der Registerkarte "Speicher" mit der rechten Maustaste auf das Speichergerät, das Sie inventarisieren möchten.
- 2** Klicken Sie auf "Inventarisieren" und klicken Sie dann auf "Planen".
- 3** Um nach Abschluss des Auftrags eine Benachrichtigung zu senden, klicken Sie im linken Teilfenster auf "Benachrichtigung" und wählen Sie die entsprechenden Optionen aus.
- 4** Um den Auftrag zu planen, klicken Sie im linken Teilfenster auf "Planen" und wählen Sie die entsprechenden Optionen aus.

Siehe ["Einen Speicherauftrag planen"](#) auf Seite 527.

- 5** Klicken Sie auf "OK".
- 6** (Optional) zeigen Sie den Auftragsverlauf an oder klicken Sie auf die Registerkarte "Auftragsüberwachung" für Details über den Auftrag.
Siehe ["Anzeigen von Aufträgen, Auftragsverläufen, Backup-Sätzen und aktiven Warnmeldungen für Speichergeräte"](#) auf Seite 548.

Siehe ["Inventarisieren von Wechslern beim Starten der Backup Exec-Dienste"](#) auf Seite 459.

Inventarisieren und Katalogisieren von Speichergeräten

Sie können die Inventarisierung und die Katalogisierung zusammen auf einem Speichergerät ausführen, sofern das Gerät beide Vorgänge unterstützt.

Siehe ["Info zu Speicheraufträgen"](#) auf Seite 519.

Ein Speichergerät inventarisieren und katalogisieren

- 1 Klicken Sie auf der Registerkarte Speicher mit der rechten Maustaste auf das Speichergerät, das Sie inventarisieren und katalogisieren möchten.
- 2 Klicken Sie auf Inventar und Katalog.
- 3 (Optional) Zeigen Sie den Auftragsverlauf an oder klicken Sie auf die Registerkarte "Auftragsüberwachung", um Details zum Auftrag anzuzeigen.

Siehe ["Anzeigen von Aufträgen, Auftragsverläufen, Backup-Sätzen und aktiven Warnmeldungen für Speichergeräte"](#) auf Seite 548.

Ein Speichergerät anhalten und wieder starten

Sie können ein Speichergerät anhalten, um zu verhindern, dass die geplanten und neuen Aufträge auf dem Speicher ausgeführt werden, während Sie Wartungsarbeiten ausführen. Aktive Aufträge sind nicht davon betroffen, wenn sie gestartet wurden, bevor das Speichergerät angehalten wird.

Siehe ["Info zu Speicheraufträgen"](#) auf Seite 519.

So halten Sie ein Speichergerät an und starten es wieder

- 1 Klicken Sie auf der Registerkarte "Speicher" mit der rechten Maustaste auf das Speichergerät, das Sie anhalten bei dem Sie das Anhalten aufheben möchten.
- 2 Sie haben folgende Möglichkeiten:
 - Um das Speichergerät anzuhalten, klicken Sie auf "Anhalten".
 - Um das Speichergerät wieder zu starten, klicken Sie mit der rechten Maustaste darauf und anschließend auf "Anhalten", um das Häkchen zu entfernen.

Deaktivieren und Aktivieren eines Speichergeräts

Sie können ein Speichergerät deaktivieren, um die Ausführung neuer Aufträge darauf zu verhindern. Backup Exec erkennt deaktivierte NDMP-Speichergeräte beim Starten der Backup Exec-Dienste nicht.

So deaktivieren und aktivieren Sie ein Speichergerät

- 1 Klicken Sie auf der Registerkarte "Speicher" mit der rechten Maustaste auf das Speichergerät, das Sie deaktivieren oder aktivieren möchten.
- 2 Sie haben folgende Möglichkeiten:
 - Klicken Sie zum Deaktivieren des Speichergeräts auf "Deaktivieren".
 - Um das Speichergerät zu aktivieren, klicken Sie mit der rechten Maustaste darauf und klicken Sie dann auf "Deaktivieren", um das Häkchen zu entfernen.

Initialisieren eines Wechslers

Sie können den Wechsler initialisieren, der einen Startbefehl an die Bibliothek schickt.

So initialisieren Sie einen Wechsler

- 1 Klicken Sie auf der Registerkarte "Speicher" mit der rechten Maustaste auf den Wechsler, den Sie initialisieren möchten.
- 2 Klicken Sie auf "Initialisieren".
- 3 (Optional) zeigen Sie den Auftragsverlauf an oder klicken Sie auf die Registerkarte "Auftragsüberwachung" für Details über den Auftrag.

Siehe ["Anzeigen von Aufträgen, Auftragsverläufen, Backup-Sätzen und aktiven Warnmeldungen für Speichergeräte"](#) auf Seite 548.

Formatieren eines Bands als WORM-Band

Sie können ein Band in ein WORM-Band (write once, read many) konvertieren, wenn das Bandlaufwerk den Vorgang unterstützt. DLT-Bandlaufwerke unterstützen den Vorgang "WORM formatieren".

So formatieren Sie ein Band als WORM-Band

- 1 Auf der Registerkarte "Speicher" klicken Sie mit der rechten Maustaste auf das Bandlaufwerk, das das zu konvertierende Band enthält.
- 2 Klicken Sie auf "WORM formatieren".
- 3 (Optional) zeigen Sie den Auftragsverlauf an oder klicken Sie auf die Registerkarte "Auftragsüberwachung", um Details zum Auftrag anzuzeigen.

Siehe ["So werden WORM-Medien in Backup Exec verwendet"](#) auf Seite 495.

Spannen eines Bands

Bevor Sie einen Backup-Auftrag auf einem Band ausführen, können Sie das Band im Bandlaufwerk schnell von Anfang bis Ende laufen lassen. Durch Spannen wird das Band gleichmäßig aufgewickelt und kommt somit auch gleichmäßig mit den Abtastköpfen des Bandlaufwerks in Kontakt. Informationen darüber, wie häufig dieser Vorgang auszuführen ist, finden Sie in der Dokumentation zum Bandlaufwerk.

Dieser Vorgang ist nur verfügbar, wenn das Bandlaufwerk das Spannen unterstützt.

Siehe ["Info zu Speicheraufträgen"](#) auf Seite 519.

So spannen Sie ein Band

- 1 Führen Sie auf der Registerkarte "Speicher" einen der folgenden Schritte aus:
 - Klicken Sie mit der rechten Maustaste auf das Laufwerk, das das zu spannende Band enthält.
 - Doppelklicken Sie auf "Schächte" und klicken Sie anschließend mit der rechten Maustaste auf den Schacht, der das zu spannende Band enthält.
- 2 Klicken Sie auf "Spannen".
- 3 (Optional) Zeigen Sie das Auftragsprotokoll an oder klicken Sie für Details zum Auftrag auf die Registerkarte "Auftragsüberwachung".

Siehe ["Anzeigen von Aufträgen, Auftragsverläufen, Backup-Sätzen und aktiven Warnmeldungen für Speichergeräte"](#) auf Seite 548.

Formatierung eines Bandes in einem Bandlaufwerk

Backup Exec kann das Band in einem Laufwerk formatieren, sofern das Laufwerk das Formatieren unterstützt. Die Formatierung eines Bandes kann mehrere Stunden

in Anspruch nehmen. Die meisten Bandlaufwerke unterstützen das Formatieren nicht.

Vorsicht: Beim Formatieren wird das Band vollständig gelöscht. Dabei werden alle auf dem Band befindlichen Daten zerstört.

Die angezeigte Medienkennung wurde während des letzten Inventarisierungsvorgangs gelesen. Die Medienkennung ändert sich erst beim Durchführen der nächsten Inventarisierung. Wenn Sie die Bänder in einem Gerät ändern, das Gerät dabei jedoch nicht inventarisieren, entspricht die angezeigte Medienkennung möglicherweise nicht den tatsächlichen Medien im Gerät.

Siehe ["Info zu Speicheraufträgen"](#) auf Seite 519.

So formatieren Sie ein Band in einem Bandlaufwerk

- 1 Führen Sie auf der Registerkarte "Speicher" einen der folgenden Schritte aus:
 - Klicken Sie mit der rechten Maustaste auf das Bandlaufwerk, das das zu formatierende Band enthält.
 - Doppelklicken Sie auf "Schächte" und klicken Sie anschließend mit der rechten Maustaste auf den Schacht, der das zu formatierende Band enthält.
- 2 Klicken Sie auf "Formatieren".
- 3 Wenn Sie das angezeigte Band formatieren möchten, klicken Sie auf "Ja".
- 4 (Optional) Zeigen Sie das Auftragsprotokoll an oder klicken Sie für Details zum Auftrag auf die Registerkarte "Auftragsüberwachung".

Siehe ["Anzeigen von Aufträgen, Auftragsverläufen, Backup-Sätzen und aktiven Warnmeldungen für Speichergeräte"](#) auf Seite 548.

Auswerfen von Medien aus einer Plattenkassette oder einem Bandlaufwerk

Backup Exec kann die Medien in einer Plattenkassette oder einem Bandlaufwerk auswerfen. Einige Geräte unterstützen das Auswerfen von Medien über eine Software nicht. Wenn es sich bei dem Medium um ein Band handelt, wird es zurückgespult, und Sie müssen es eventuell manuell aus dem Laufwerk entfernen.

Siehe ["Info zu Speicheraufträgen"](#) auf Seite 519.

So werfen Sie Medien aus einer Plattenkassette oder einem Bandlaufwerk aus

- 1 Klicken Sie auf der Registerkarte "Speicher" mit der rechten Maustaste auf die Plattenkassette oder das Bandlaufwerk, aus der bzw. aus dem Sie die Medien auswerfen möchten.
- 2 Klicken Sie auf "Auswerfen" und klicken Sie dann auf "Jetzt auswerfen".
- 3 (Optional) zeigen Sie den Auftragsverlauf an oder klicken Sie auf die Registerkarte "Auftragsüberwachung" für Details über den Auftrag.

So planen Sie einen Auswerfenvorgang für eine Datenträgerkassette oder ein Bandlaufwerk

- 1 Klicken Sie auf der Registerkarte "Speicher" mit der rechten Maustaste auf die Plattenkassette oder das Bandlaufwerk, aus der bzw. aus dem Sie die Medien auswerfen möchten.
- 2 Klicken Sie auf "Auswerfen" und klicken Sie dann auf "Planen".
- 3 Um nach Abschluss des Auftrags eine Benachrichtigung zu senden, klicken Sie im linken Teilfenster auf "Benachrichtigung" und wählen Sie die entsprechenden Optionen aus.
- 4 Um den Auftrag zu planen, klicken Sie im linken Teilfenster auf "Planen" und wählen Sie die entsprechenden Optionen aus.
Siehe ["Einen Speicherauftrag planen"](#) auf Seite 527.
- 5 Klicken Sie auf "OK".
- 6 (Optional) zeigen Sie den Auftragsverlauf an oder klicken Sie auf die Registerkarte "Auftragsüberwachung" für Details über den Auftrag.

Siehe ["Anzeigen von Aufträgen, Auftragsverläufen, Backup-Sätzen und aktiven Warnmeldungen für Speichergeräte"](#) auf Seite 548.

Reinigen eines Wechslerlaufwerks

Sie können einen Reinigungsauftrag für ein Wechslerlaufwerk erstellen und planen.

Siehe ["Info zu Speicheraufträgen"](#) auf Seite 519.

So erstellen Sie jetzt einen Reinigungsauftrag

- 1 Stellen Sie sicher, dass Sie den Schacht angeben, der das Reinigungsband enthält.
Siehe ["Festlegen eines Reinigungsschachts"](#) auf Seite 465.
- 2 Stellen Sie sicher, dass das Reinigungsband im definierten Reinigungsslot ist und in der gleichen Bibliothek ist, die das Laufwerk enthält, das Sie bereinigen möchten.
- 3 Klicken Sie auf der Registerkarte "Speicher" mit der rechten Maustaste auf das Laufwerk, das Sie reinigen möchten und klicken Sie dann auf "Reinigen" und anschließend auf "Jetzt reinigen".
- 4 (Optional) zeigen Sie den Auftragsverlauf an oder klicken Sie auf die Registerkarte "Auftragsüberwachung" für Details über den Auftrag.

So planen Sie einen Reinigungsauftrag

- 1 Stellen Sie sicher, dass Sie den Schacht angeben, der das Reinigungsband enthält.
- 2 Stellen Sie sicher, dass das Reinigungsband im definierten Reinigungsslot ist und in der gleichen Bibliothek ist, die das Laufwerk enthält, das Sie bereinigen möchten.
- 3 Klicken Sie auf der Registerkarte "Speicher" mit der rechten Maustaste auf das Laufwerk, das Sie reinigen möchten und klicken Sie dann auf "Jetzt reinigen" und anschließend auf "Planen".
- 4 Um nach Abschluss des Auftrags eine Benachrichtigung zu senden, klicken Sie im linken Teilfenster auf "Benachrichtigung" und wählen Sie die entsprechenden Optionen aus.
- 5 Um den Auftrag zu planen, klicken Sie im linken Teilfenster auf "Planen" und wählen Sie die entsprechenden Optionen aus.
Siehe ["Einen Speicherauftrag planen"](#) auf Seite 527.
- 6 Klicken Sie auf "OK".
- 7 (Optional) zeigen Sie den Auftragsverlauf an oder klicken Sie auf die Registerkarte "Auftragsüberwachung" für Details über den Auftrag.
Siehe ["Anzeigen von Aufträgen, Auftragsverläufen, Backup-Sätzen und aktiven Warnmeldungen für Speichergeräte"](#) auf Seite 548.

Importieren von Medien in Backup Exec

Sie können Medien in einen Wechsler importieren, um Backup Exec Bänder hinzuzufügen oder Medien zu importieren, die für einen Wiederherstellungsauftrag erforderlich sind. Beim Einfügen von Medien in einen Wechsler müssen Sie einen Auftrag zum Importieren von Speicher erstellen. Dieser Vorgang aktualisiert die Backup Exec-Datenbank mit den Informationen zu den Medien. Backup Exec verknüpft die Medien, die Sie importieren, mit einem Systemmediensatz.

Siehe ["Standard-Mediensätze"](#) auf Seite 473.

Hinweis: Sie sollten temporäre Medien nicht mit einem Mediensatz verknüpfen, den Sie erstellen. Backup Exec verschiebt die Medien bei Bedarf automatisch auf den erforderlichen Mediensatz.

Beachten Sie vor dem Importieren von Medien Folgendes:

- Falls die Medien über keinen Barcode verfügen, müssen Sie den Speichervorgang "Nach Import inventarisieren" auswählen, damit die Medienkennung in den Eigenschaften angezeigt wird. Sie können diesen Vorgang nur auswählen, nachdem Sie "Medium jetzt importieren" ausgewählt haben.
- Verwendet der Wechsler ein Medienmagazin, stellen Sie sicher, dass derzeit keine Aufträge ausgeführt werden. Vergewissern Sie sich vor dem Austausch des Magazins, dass alle Medien vom Laufwerk ausgeworfen worden sind und sich wieder in den Magazinschächten befinden.

Sie können eine beliebige Anzahl von Schächten auswählen, in die Medien importiert werden sollen.

Der Speichervorgang zum Importieren unterstützt Wechsler mit Ladeschächten. Wird dieser Speichervorgangsauftrag ausgeführt, prüft Backup Exec die ausgewählten Schächte auf Medien. Falls Medien gefunden werden, werden sie zu den Ladeschächten exportiert. Nach dem Export der Medien werden Sie aufgefordert, das neue Medium in den Ladeschacht einzulegen, damit es importiert werden kann. Dieser Vorgang wiederholt sich, bis alle angeforderten Medien in den Wechsler importiert wurden.

Sie können einen Scanvorgang auch ausführen, um die Schachtinformationen zu aktualisieren, wenn Sie neue Medien in einen Wechsler einlegen. Das Scanauftragsprotokoll berichtet über die Medien mit Barcode, die sich in den Laufwerken und Schächten befinden.

Siehe ["Scannen eines Speichergeräts"](#) auf Seite 549.

So importieren Sie Medien jetzt

- 1** Führen Sie auf der Registerkarte "Speicher" einen der folgenden Schritte aus.
 - Erweitern Sie den Wechsler, klicken Sie mit der rechten Maustaste auf "Schächte" und klicken Sie anschließend auf "Medium jetzt importieren".
 - Klicken Sie mit der rechten Maustaste auf den Wechsler und klicken Sie dann auf "Medium jetzt importieren".
- 2** (Optional) zeigen Sie den Auftragsverlauf an oder klicken Sie auf die Registerkarte "Auftragsüberwachung" für Details über den Auftrag.

So planen Sie einen Auftrag zum Importieren von Medien

- 1** Führen Sie auf der Registerkarte "Speicher" einen der folgenden Schritte aus:
 - Erweitern Sie den Wechsler, klicken Sie mit der rechten Maustaste auf "Schächte" und klicken Sie anschließend auf "Medium jetzt importieren".
 - Klicken Sie mit der rechten Maustaste auf den Wechsler, klicken Sie dann auf "Medium jetzt importieren" und anschließend auf "Planen".
- 2** Im linken Teilfenster klicken Sie auf "Speicher".
- 3** Klicken Sie auf das Dropdown-Menü und wählen Sie Speichervorgang aus, den Sie planen möchten:

Importieren

Aktualisiert die Backup Exec-Datenbank mit Informationen über die Medien.

Nach Import inventarisieren

Installiert die Medien in Laufwerken, liest die Medienkennung und aktualisiert die Backup Exec-Datenbank. Dieser Vorgang ist für Medien notwendig, die keine Barcodes haben.

- 4** Um nach Abschluss des Auftrags eine Benachrichtigung zu senden, klicken Sie im linken Teilfenster auf "Benachrichtigung" und wählen Sie die entsprechenden Optionen aus.

Empfängername	Zeigt die Namen der Empfänger (Einzelpersonen und Gruppen) an.
Empfängertyp	Zeigt "Empfänger" für eine Einzelperson oder "Gruppe" für einen Gruppe an.
Empfänger verwalten	Empfänger hinzufügen, bearbeiten oder löschen.
Eigenschaften	Anzeigen oder Ändern der Eigenschaften eines ausgewählten Empfängers.

- 5** Um den Auftrag zu planen, klicken Sie im linken Teilfenster auf "Planen" und wählen Sie die entsprechenden Optionen aus.

Wiederkehrend	Ermöglicht das Erstellen eines wiederkehrenden Zeitplans für den Auftrag.
Stunden	<p>Hiermit können Sie ein Wiederholungsmuster erstellen, das in Stunden oder Minuten gemessen wird.</p> <p>Wenn Sie "Stunden" auswählen, können Sie folgende Optionen konfigurieren:</p> <ul style="list-style-type: none"> ■ Alle X Stunden/Minuten Gibt die Anzahl von Stunden oder Minuten zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz an. ■ Von Gibt die Startzeit eines Auftrags an. ■ Zwischen Schränkt den Auftrag auf bestimmte Stunden und Tage ein. Wenn der Auftrag beispielsweise nur während Geschäftszeiten ausgeführt werden soll, können Sie 9:00 bis 17:00 Uhr am Montag, Dienstag, Mittwoch, Donnerstag und Freitag auswählen. Die Start- und Endzeit können maximal 24 Stunden auseinander liegen, doch sie können sich über Mitternacht in den folgenden Tag hinein überschneiden.

Tage

Hiermit können Sie ein Wiederholungsmuster erstellen, das in Tagen gemessen wird.

Wenn Sie "Tage" auswählen, müssen Sie zwischen den folgenden Optionen auswählen:

- **Alle X Tage**
Gibt die Anzahl von Tagen zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz an.
- **Jeden Wochentag**
Gibt an, dass der Auftrag Montag, Dienstag, Mittwoch, Donnerstag und Freitag ausgeführt werden soll.

Wochen

Hiermit können Sie ein Wiederholungsmuster erstellen, das in Wochen gemessen wird.

Wenn Sie ein Wiederholungsmuster erstellen, das in Wochen gemessen wird, müssen Sie das Feld "Alle X Wochen am" konfigurieren. Das Feld "Alle X Wochen am" gibt die Anzahl von Wochen zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz an. Es gibt außerdem die Wochentage an, an denen der Auftrag ausgeführt werden soll.

Monate

Hiermit können Sie ein Wiederholungsmuster erstellen, das in Monaten gemessen wird.

Wenn Sie "Monate" auswählen, müssen Sie zwischen den folgenden Optionen auswählen:

- **Tag X jedes X. Monats**
 Gibt den Tag an, an dem der Auftrag aufgeführt werden soll. Gibt außerdem die Anzahl von Monaten zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz an.
- **Jeden X X jedes X. Monats**
 Gibt den Tag an, an dem der Auftrag aufgeführt werden soll. Gibt außerdem die Anzahl von Monaten zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz an.
- **Ausgewählte Monatstage**
 Gibt die bestimmten Tage des Monats an, an denen Backup Exec den Auftrag ausführt. Sie wählen die Tage und die Wochen auf einem Raster aus. Das ausgewählte Wiederholungsmuster wird jeden Monat wiederholt.
 Standardmäßig wird der Auftrag jeden Monat ausführt und beginnt in der aktuellen Woche und am aktuellen Tag des Monats. Wenn Sie beispielsweise den Auftrag am dritten Montag im Monat erstellen, wird der Auftrag standardmäßig am dritten Montag jedes Monats ausgeführt.
 Sie können den Standard ändern oder zusätzliche Tage auswählen, auf denen der Auftrag ausführen sollte. Alle zusätzlich ausgewählten Tage werden dem monatlichen Wiederholungsmuster hinzugefügt.
- **Ausgewählte Monatstage**
 Gibt die Tage des Monats an, an denen Backup Exec den Auftrag ausführt. Das ausgewählte Wiederholungsmuster wird jeden Monat wiederholt.
 Standardmäßig wird der Auftrag jeden Monat ausgeführt und beginnt am aktuellen Tag des Monats. Wenn Sie den Auftrag beispielsweise am 15. April erstellen, wird der Auftrag standardmäßig am 15. jedes Monats

ausgeführt.

Sie können den Standard ändern oder zusätzliche Tage auswählen, auf denen der Auftrag ausführen sollte. Alle zusätzlich ausgewählten Tage werden dem monatlichen Wiederholungsmuster hinzugefügt.

Wenn Sie den 31. auswählen, wird der Auftrag in Monaten, die keine 31 Tage haben, am letzten Tag des Monats ausgeführt. Wenn Sie den Auftrag beispielsweise so konfigurieren, dass er am 31. ausgeführt wird, wird er im September stattdessen am 30. ausgeführt.

Jahre

Hiermit können Sie ein Wiederholungsmuster erstellen, das in Jahren gemessen wird.

Wenn Sie "Jahre" auswählen, können Sie die folgenden Optionen konfigurieren:

- **Alle X Jahre**
Gibt die Anzahl von Jahren zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz an.
- **"Am X"**
Gibt das Datum an, an dem Backup Exec den Auftrag ausführt. Das in diesem Feld ausgewählte Datum entspricht der Anzahl von Jahren, die Sie im Feld "Alle X Jahre" ausgewählt haben. Wenn Sie festgelegt haben, dass der Auftrag alle zwei Jahre ausgeführt werden soll, und Sie in diesem Feld 28. Juni ausgewählt haben, wird der Auftrag alle zwei Jahre jeweils am 28. Juni ausgeführt.
- **"Am X. X"**
Gibt den Tag und den Monat an, an dem Backup Exec den Auftrag ausführt. Das in diesem Feld ausgewählte Datum entspricht der Anzahl von Jahren, die Sie im Feld "Alle X Jahre" ausgewählt haben. Wenn Sie festgelegt haben, dass der Auftrag alle zwei Jahre ausgeführt werden soll, und Sie in diesem Feld den vierten Donnerstag im Juni ausgewählt haben, wird der Auftrag alle zwei Jahre jeweils am vierten Donnerstag im Juni ausgeführt.

um	Gibt die Startzeit des ersten Auftrags im Wiederholungsmuster an.
Kalender	Ermöglicht die Anzeige aller geplanten Aufträge in einem Kalender, um Konflikte bei der Planung zu vermeiden.
Auftrag neu planen, falls er X Stunden nach geplanter Startzeit noch immer nicht ausgeführt wird	Gibt den Zeitraum nach der geplanten Startzeit des Auftrags an, nach dessen Ablauf Backup Exec den Auftragsabschlussstatus in "Verpasst" ändert. Der Auftrag wird erneut geplant, um gemäß des von Ihnen festgelegten Zeitfensters ausgeführt zu werden.
Abbrechen des Auftrags, falls er X Stunden nach der ursprünglich festgelegten Startzeit noch immer ausgeführt wird	Gibt den Zeitraum nach der geplanten Startzeit des Auftrags an, nach dessen Ablauf der Auftrag abgebrochen wird, wenn er noch ausgeführt wird. Backup Exec ändert den Auftragsabschlussstatus in "Abgebrochen, Zeitüberschreitung".
"Daten mit dem Zeitplan dieses Auftrags einschließen"	Geben Sie Daten an, die in den Auftragszeitplan eingeschlossen werden sollen. Der Auftrag wird an allen mit dieser Option ausgewählten Tagen ausgeführt, zusätzlich zu den Tagen, die Teil des normalen Zeitplans sind. Der Auftrag wird am nächsten im normalen Zeitplan festgelegten Tag nach dem eingeschlossenen Datum fortgesetzt.
"Daten vom Zeitplan des Auftrags ausschließen"	Geben Sie Daten an, die aus dem Auftragszeitplan ausgeschlossen werden sollen. Der Auftrag wird an diesen Tagen nicht ausgeführt. Er wird am nächsten im normalen Zeitplan festgelegten Tag nach dem ausgeschlossenen Datum fortgesetzt.
Jetzt ohne regelmäßigen Zeitplan ausführen	Führt den Auftrag sofort aus, ohne weitere Instanzen für die Zukunft zu planen.
Ausführen am	Führt den den Auftrag am angegebenen Datum zur angegebenen Zeit aus.

Ohne Zeitplan erstellen

Erstellt einen Auftrag ohne Zeitplan. Wenn Sie diese Option verwenden, wird der Auftrag nicht zur Zeit der Erstellung ausgeführt und hat keinen wiederkehrenden Zeitplan. Der Auftrag verbleibt ungeplant, bis Sie beschließen, ihn auszuführen. Sie können ein Drittanbieter-Tool zur automatischen Auftragsausführung oder -planung verwenden, um den Auftrag später auszuführen.

Wenn Sie diese Option zum Erstellen eines Auftrags verwenden, können Sie den Auftrag nicht anhalten. Sie können Aufträge nicht anhalten, es sei denn, dass sie geplant werden.

6 Klicken Sie auf "OK".

7 (Optional) zeigen Sie den Auftragsverlauf an oder klicken Sie auf die Registerkarte "Auftragsüberwachung" für Details über den Auftrag.

Siehe ["Anzeigen von Aufträgen, Auftragsverläufen, Backup-Sätzen und aktiven Warnmeldungen für Speichergeräte"](#) auf Seite 548.

Exportieren von Medien und abgelaufenen Medien

Der Vorgang "Medium exportieren" unterstützt Wechsler mit Schächten. Wenn dieser Vorgang für einen oder mehrere Wechsler-Schächte ausgeführt wird, werden die exportierten Medien in den Ladeschächten abgelegt. Falls Sie mehr Medien auswählen, als Ladeschächte vorhanden sind, füllt der Wechsler so viele Schächte wie möglich. Daraufhin werden Sie aufgefordert, die Medien aus dem Ladeschacht zu entfernen. Dieser Vorgang wiederholt sich, bis alle ausgewählten Medien aus dem Wechsler entfernt wurden. Sie können auch abgelaufene Medien von einem Wechsler exportieren.

Mit dem Vorgang "Abgelaufene Medien exportieren" können Sie die Behandlung von Medien in Wechslern automatisieren. Hiermit werden die Medien entfernt, auf die Backup Exec nicht schreiben kann. Sie können zur Vorbereitung auf das nächste Backup dem Wechsler mithilfe des Vorgangs "Nach dem Export importieren" temporäre Medien hinzufügen.

Nachdem Sie die abgelaufenen Medien vom Wechsler exportieren, werden die abgelaufenen Medien unter "Offline-Bandmedien" angezeigt. Falls die Medien sich in einem Mediensatz mit einer anwendbaren Speichermedienregel befinden, werden die Medien im Speicherort angezeigt.

Sie können Reinigungsmedien mithilfe des Speichervorgangs "Abgelaufene Medien exportieren" exportieren. Sie können sämtliche Reinigungsmedien oder nur die Medien mit der maximalen Anzahl von Reinigungsvorgängen auswählen.

Siehe ["Importieren von Medien in Backup Exec"](#) auf Seite 558.

Hinweis: Nicht alle Speichervorgänge sind für alle Geräte verfügbar.

So exportieren Sie Medien oder abgelaufene Medien

1 Führen Sie auf der Registerkarte "Speicher" einen der folgenden Schritte aus:

- Erweitern Sie den Wechsler, klicken Sie mit der rechten Maustaste auf "Schächte" und klicken Sie anschließend auf "Medien exportieren".
- Klicken Sie mit der rechten Maustaste auf den Wechsler und klicken Sie dann auf "Export".

2 Sie haben folgende Möglichkeiten:

So exportieren Sie nur die Medien sofort, die Backup Exec nicht auf den Ladeschacht schreiben oder dort ablegen kann	<p>Klicken Sie auf "Abgelaufene Medien exportieren".</p> <p>Der Vorgang wird ausgeführt. Im Auftragsverlauf können Sie Details über den Auftrag anzeigen.</p>
So exportieren Sie die Medien sofort in den Ladeschacht	<p>Klicken Sie auf "Medium jetzt exportieren".</p> <p>Der Vorgang wird ausgeführt. Im Auftragsverlauf können Sie Details über den Auftrag anzeigen.</p>
So importieren Sie Medien sofort nach dem Export	<p>Klicken Sie auf "Nach dem Export importieren".</p> <p>Der Vorgang wird ausgeführt. Im Auftragsverlauf können Sie Details über den Auftrag anzeigen.</p>

3 (Optional) zeigen Sie den Auftragsverlauf an oder klicken Sie auf die Registerkarte "Auftragsüberwachung" für Details über den Auftrag.

Siehe ["Anzeigen von Aufträgen, Auftragsverläufen, Backup-Sätzen und aktiven Warnmeldungen für Speichergeräte"](#) auf Seite 548.

So planen Sie den Export von Medien oder abgelaufenen Medien

1 Führen Sie auf der Registerkarte "Speicher" einen der folgenden Schritte aus:

- Erweitern Sie den Wechsler, klicken Sie mit der rechten Maustaste auf "Schächte" und klicken Sie anschließend auf "Medien exportieren".
 - Klicken Sie mit der rechten Maustaste auf den Wechsler und klicken Sie dann auf "Export".
- 2 Klicken Sie auf "Planen".
 - 3 Im linken Teilfenster klicken Sie auf "Speicher".
 - 4 Klicken Sie auf das Dropdown-Menü und wählen Sie einen der folgenden Speichervorgänge aus, die Sie planen möchten:

Export	<p>Legt die Medien in die Schächte des Wechslers ab.</p> <p>Falls Sie mehr Medien auswählen, als Schächte vorhanden sind, füllt der Wechsler so viele Schächte wie möglich. Daraufhin werden Sie aufgefordert, die Medien aus dem Schacht zu entfernen. Dieser Vorgang wiederholt sich, bis alle ausgewählten Medien aus dem Wechsler entfernt wurden.</p>
Medium nach Export importieren	<p>Fügt die temporären Medien dem Wechsler hinzu, um sich für das nächste Backup vorzubereiten.</p>
Abgelaufene Medien exportieren	<p>Legt die abgelaufenen Medien in die Schächte des Wechslers ab.</p> <p>Mit diesem Vorgang können Sie die Medienbehandlung in den Wechslern automatisieren, indem sie die Medien entfernen, auf denen Backup Exec nicht schreiben kann. Nachdem Sie die abgelaufenen Medien vom Wechsler exportieren, werden die abgelaufenen Medien unter "Offline-Bandmedien" angezeigt. Falls die Medien sich in einem Mediensatz mit einer anwendbaren Speichermedienregel befinden, werden die Medien im Speicherort angezeigt.</p>

- 5 Um nach Abschluss des Auftrags eine Benachrichtigung zu senden, klicken Sie im linken Teilfenster auf "Benachrichtigung" und wählen Sie die entsprechenden Optionen aus.

- 6 Um den Auftrag zu planen, klicken Sie im linken Teilfenster auf "Planen" und wählen Sie die entsprechenden Optionen aus.
- 7 Klicken Sie auf "OK".
- 8 (Optional) zeigen Sie den Auftragsverlauf an oder klicken Sie auf die Registerkarte "Auftragsüberwachung" für Details über den Auftrag.

Sperren und Freigen des vorderen Ladeschachts

Standardmäßig wird der Ladeschacht des Wechslers nicht gesperrt, selbst wenn Sie den Sperrvorgang ausführen. Die Backup Exec-Medienserver sperren keine Wechsler beim Ausführen von Backup-Aufträgen oder eines Sperrauftrags.

Wenn Sie die Wechsler freigeben möchten, wenden Sie sich an den technischer Support.

Sie müssen einen Auftrag zur Freigabe des vorderen Ladeschachts des Wechslers erstellen.

So geben Sie den vorderen Ladeschacht des Wechslers frei

- 1 Klicken Sie auf der Registerkarte "Speicher" mit der rechten Maustaste auf den Wechsler mit dem freizugebenden vorderen Ladeschacht.
- 2 Klicken Sie auf "Sperrung aufheben" und klicken Sie dann auf "Jetzt freigeben".
- 3 (Optional) zeigen Sie den Auftragsverlauf an oder klicken Sie auf die Registerkarte "Auftragsüberwachung" für Details über den Auftrag.

So planen Sie einen Auftrag zur Freigabe des vorderen Ladeschachts des Wechslers

- 1 Klicken Sie auf der Registerkarte "Speicher" mit der rechten Maustaste auf den Wechsler mit dem freizugebenden vorderen Ladeschacht.
- 2 Klicken Sie auf "Sperrung aufheben".
- 3 Klicken Sie auf "Planen".

- 4** Um nach Abschluss des Auftrags eine Benachrichtigung zu senden, klicken Sie im linken Teilfenster auf "Benachrichtigung" und wählen Sie eine der folgenden Optionen aus:

Empfängername	Zeigt die Namen der Empfänger (Einzelpersonen und Gruppen) an.
Empfängertyp	Zeigt "Empfänger" für eine Einzelperson oder "Gruppe" für einen Gruppe an.
Empfänger verwalten	Empfänger hinzufügen, bearbeiten oder löschen.
Eigenschaften	Anzeigen oder Ändern der Eigenschaften eines ausgewählten Empfängers.

- 5** Um den Auftrag zu planen, klicken Sie im linken Teilfenster auf "Planen" und wählen Sie die entsprechenden Optionen aus.

Wiederkehrend	Ermöglicht das Erstellen eines wiederkehrenden Zeitplans für den Auftrag.
Stunden	<p>Hiermit können Sie ein Wiederholungsmuster erstellen, das in Stunden oder Minuten gemessen wird.</p> <p>Wenn Sie "Stunden" auswählen, können Sie folgende Optionen konfigurieren:</p> <ul style="list-style-type: none"> ■ Alle X Stunden/Minuten Gibt die Anzahl von Stunden oder Minuten zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz an. ■ Von Gibt die Startzeit eines Auftrags an. ■ Zwischen Schränkt den Auftrag auf bestimmte Stunden und Tage ein. Wenn der Auftrag beispielsweise nur während Geschäftszeiten ausgeführt werden soll, können Sie 9:00 bis 17:00 Uhr am Montag, Dienstag, Mittwoch, Donnerstag und Freitag auswählen. Die Start- und Endzeit können maximal 24 Stunden auseinander liegen, doch sie können sich über Mitternacht in den folgenden Tag hinein überschneiden.

Tage

Hiermit können Sie ein Wiederholungsmuster erstellen, das in Tagen gemessen wird.

Wenn Sie "Tage" auswählen, müssen Sie zwischen den folgenden Optionen auswählen:

- Alle X Tage
Gibt die Anzahl von Tagen zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz an.
- Jeden Wochentag
Gibt an, dass der Auftrag Montag, Dienstag, Mittwoch, Donnerstag und Freitag ausgeführt werden soll.

Wochen

Hiermit können Sie ein Wiederholungsmuster erstellen, das in Wochen gemessen wird.

Wenn Sie ein Wiederholungsmuster erstellen, das in Wochen gemessen wird, müssen Sie das Feld "Alle X Wochen am" konfigurieren. Das Feld "Alle X Wochen am" gibt die Anzahl von Wochen zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz an. Es gibt außerdem die Wochentage an, an denen der Auftrag ausgeführt werden soll.

Monate

Hiermit können Sie ein Wiederholungsmuster erstellen, das in Monaten gemessen wird.

Wenn Sie "Monate" auswählen, müssen Sie zwischen den folgenden Optionen auswählen:

- Tag X jedes X. Monats
Gibt den Tag an, an dem der Auftrag aufgeführt werden soll. Gibt außerdem die Anzahl von Monaten zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz an.
- Jeden X X jedes X. Monats
Gibt den Tag an, an dem der Auftrag aufgeführt werden soll. Gibt außerdem die Anzahl von Monaten zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz an.
- Ausgewählte Monatstage
Gibt die bestimmten Tage des Monats an, an denen Backup Exec den Auftrag ausführt. Sie wählen die Tage und die Wochen auf einem Raster aus. Das ausgewählte Wiederholungsmuster wird jeden Monat wiederholt.

Standardmäßig wird der Auftrag jeden Monat ausführt und beginnt in der aktuellen Woche und am aktuellen Tag des Monats. Wenn Sie beispielsweise den Auftrag am dritten Montag im Monat erstellen, wird der Auftrag standardmäßig am dritten Montag jedes Monats ausgeführt.

Sie können den Standard ändern oder zusätzliche Tage auswählen, auf denen der Auftrag ausführen sollte. Alle zusätzlich ausgewählten Tage werden dem monatlichen Wiederholungsmuster hinzugefügt.
- Ausgewählte Monatstage
Gibt die Tage des Monats an, an denen Backup Exec den Auftrag ausführt. Das ausgewählte Wiederholungsmuster wird jeden Monat wiederholt.

Standardmäßig wird der Auftrag jeden Monat ausgeführt und beginnt am aktuellen Tag des Monats. Wenn Sie den Auftrag beispielsweise am 15. April erstellen, wird der Auftrag standardmäßig am 15. jedes Monats

ausgeführt.

Sie können den Standard ändern oder zusätzliche Tage auswählen, auf denen der Auftrag ausführen sollte. Alle zusätzlich ausgewählten Tage werden dem monatlichen Wiederholungsmuster hinzugefügt.

Wenn Sie den 31. auswählen, wird der Auftrag in Monaten, die keine 31 Tage haben, am letzten Tag des Monats ausgeführt. Wenn Sie den Auftrag beispielsweise so konfigurieren, dass er am 31. ausgeführt wird, wird er im September stattdessen am 30. ausgeführt.

Jahre

Hiermit können Sie ein Wiederholungsmuster erstellen, das in Jahren gemessen wird.

Wenn Sie "Jahre" auswählen, können Sie die folgenden Optionen konfigurieren:

- **Alle X Jahre**
Gibt die Anzahl von Jahren zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz an.
- **"Am X"**
Gibt das Datum an, an dem Backup Exec den Auftrag ausführt. Das in diesem Feld ausgewählte Datum entspricht der Anzahl von Jahren, die Sie im Feld "Alle X Jahre" ausgewählt haben. Wenn Sie festgelegt haben, dass der Auftrag alle zwei Jahre ausgeführt werden soll, und Sie in diesem Feld 28. Juni ausgewählt haben, wird der Auftrag alle zwei Jahre jeweils am 28. Juni ausgeführt.
- **"Am X. X"**
Gibt den Tag und den Monat an, an dem Backup Exec den Auftrag ausführt. Das in diesem Feld ausgewählte Datum entspricht der Anzahl von Jahren, die Sie im Feld "Alle X Jahre" ausgewählt haben. Wenn Sie festgelegt haben, dass der Auftrag alle zwei Jahre ausgeführt werden soll, und Sie in diesem Feld den vierten Donnerstag im Juni ausgewählt haben, wird der Auftrag alle zwei Jahre jeweils am vierten Donnerstag im Juni ausgeführt.

um	Gibt die Startzeit des ersten Auftrags im Wiederholungsmuster an.
Kalender	Ermöglicht die Anzeige aller geplanten Aufträge in einem Kalender, um Konflikte bei der Planung zu vermeiden.
Auftrag neu planen, falls er X Stunden nach geplanter Startzeit noch immer nicht ausgeführt wird	Gibt den Zeitraum nach der geplanten Startzeit des Auftrags an, nach dessen Ablauf Backup Exec den Auftragsabschlussstatus in "Verpasst" ändert. Der Auftrag wird erneut geplant, um gemäß des von Ihnen festgelegten Zeitfensters ausgeführt zu werden.
Abbrechen des Auftrags, falls er X Stunden nach der ursprünglich festgelegten Startzeit noch immer ausgeführt wird	Gibt den Zeitraum nach der geplanten Startzeit des Auftrags an, nach dessen Ablauf der Auftrag abgebrochen wird, wenn er noch ausgeführt wird. Backup Exec ändert den Auftragsabschlussstatus in "Abgebrochen, Zeitüberschreitung".
"Daten mit dem Zeitplan dieses Auftrags einschließen"	Geben Sie Daten an, die in den Auftragszeitplan eingeschlossen werden sollen. Der Auftrag wird an allen mit dieser Option ausgewählten Tagen ausgeführt, zusätzlich zu den Tagen, die Teil des normalen Zeitplans sind. Der Auftrag wird am nächsten im normalen Zeitplan festgelegten Tag nach dem eingeschlossenen Datum fortgesetzt.
"Daten vom Zeitplan des Auftrags ausschließen"	Geben Sie Daten an, die aus dem Auftragszeitplan ausgeschlossen werden sollen. Der Auftrag wird an diesen Tagen nicht ausgeführt. Er wird am nächsten im normalen Zeitplan festgelegten Tag nach dem ausgeschlossenen Datum fortgesetzt.
Jetzt ohne regelmäßigen Zeitplan ausführen	Führt den Auftrag sofort aus, ohne weitere Instanzen für die Zukunft zu planen.
Ausführen am	Führt den den Auftrag am angegebenen Datum zur angegebenen Zeit aus.

Ohne Zeitplan erstellen

Erstellt einen Auftrag ohne Zeitplan. Wenn Sie diese Option verwenden, wird der Auftrag nicht zur Zeit der Erstellung ausgeführt und hat keinen wiederkehrenden Zeitplan. Der Auftrag bleibt ungeplant, bis Sie ihn ausführen. Sie können ein Drittanbieter-Tool zur automatischen Auftragsausführung oder -planung verwenden, um den Auftrag später auszuführen.

Wenn Sie diese Option zum Erstellen eines Auftrags verwenden, können Sie den Auftrag nicht anhalten. Sie können Aufträge nicht anhalten, es sei denn, dass sie geplant werden.

6 Klicken Sie auf "OK".

Siehe ["Anzeigen von Aufträgen, Auftragsverläufen, Backup-Sätzen und aktiven Warnmeldungen für Speichergeräte"](#) auf Seite 548.

Status von Backup Exec-Servern und Speichergeräten

Für Backup Exec-Server und Speichergeräte wird ein Status angezeigt, der ihren aktuellen Zustand angibt.

Tabelle 13-3 Mögliche Status für Backup Exec-Server und Speichergeräte

Status	Beschreibung
Alle Backup Exec-Dienste auf < Backup Exec-Server> müssen neu gestartet werden.	Die Backup Exec-Dienste und die Backup Exec-Deduplizierungsdienste müssen neu gestartet werden. Siehe "Starten und Anhalten von Backup Exec-Diensten" auf Seite 776.
Beim Erkennen dieses Geräts ist ein Fehler aufgetreten. Führen Sie die Dienste auf < Backup Exec-Server> aus, um die Geräteerkennung zu wiederholen.	Die Backup Exec-Dienste müssen neu gestartet werden. Siehe "Starten und Anhalten von Backup Exec-Diensten" auf Seite 776.
Aktiv	Das Speichergerät wird für einen Auftrag verwendet.

Status	Beschreibung
Konfiguration fehlgeschlagen	Die Konfiguration ist für ein lokales Speichergerät oder einen lokalen virtuellen Datenträger fehlgeschlagen.
Konfigurieren	Ein lokales Speichergerät oder ein lokaler virtueller Datenträger wird gerade konfiguriert.
Deaktiviert	Das Speichergerät ist deaktiviert und Backup Exec kann es nicht verwenden. Das Gerät steht anderen Anwendungen zur Verfügung.
Deaktiviert; aktiv	Der Status des Speichergeräts wurde in Deaktiviert geändert, während ein Auftrag auf dem Gerät lief.
Geringer Speicherplatz; aktiv	Auf dem Speichergerät ist nur noch wenig Speicherplatz vorhanden, es wird jedoch derzeit von einem Auftrag verwendet.
Geringer Speicherplatz	Auf dem Speichergerät ist nur wenig Speicherplatz vorhanden.
Keine Verbindung	<p>Die Kommunikation zwischen einem verwalteten Backup Exec-Server und einem zentralen Administrationsserver in einer Central Admin Server Feature-Umgebung wurde beendet.</p> <p>Siehe "Erreichen der CAS-Kommunikationsschwellenwerte" auf Seite 1491.</p>
Nicht konfigurierbar	Der Datenträger kann nicht konfiguriert werden, weil er in einem schlechten Zustand oder fehlgeschlagen ist.
Nicht konfiguriert	Der Datenträger ist für die Konfiguration verfügbar, wurde jedoch noch nicht konfiguriert.

Status	Beschreibung
Offline	<p>Das Speichergerät ist offline.</p> <p>Ein Speichergerät kann offline angezeigt werden, wenn eine der folgenden Aktionen auftritt:</p> <ul style="list-style-type: none"> ■ Das Gerät wurde nach dem Starten von Backup Exec ausgeschaltet. ■ Das Gerät wurde durch eine andere Anwendung verwendet, als Backup Exec gestartet wurde. ■ Das Gerät wurde vom Computer getrennt. ■ Am Gerät wurde ein schwerer Fehler gemeldet. ■ Die Firmware des Geräts wurde aktualisiert. <p>Normalerweise wird eine Warnmeldung angezeigt, wenn ein Gerät zu Offline wechselt. Die Warnmeldung enthält einen bestimmten Grund, warum das Gerät offline ist.</p> <p>Außerdem kann ein Link zur Supportdatenbank enthalten sein.</p> <p>Korrigieren Sie das Problem, durch das das Gerät offline geschaltet wurde. Für Bandlaufwerke, Wechsler und einige andere Gerätetypen, müssen Sie den Zustand des Geräts manuell zu online ändern. Backup Exec erkennt bei Datenträgerspeicher, Datenträgerkassette, Speichergruppen und virtuellen Datenträgergeräte, dass das Gerät innerhalb von fünf Minuten online ist und ändert automatisch den Zustand zu online</p> <p>Siehe "Ändern des Status eines Speichergeräts in "Online"" auf Seite 547.</p>
Online	Das Speichergerät ist online.
Angehalten	<p>Das Speichergerät wurde angehalten.</p> <p>Siehe "Ein Speichergerät anhalten und wieder starten" auf Seite 552.</p>
Angehalten; Aktiv	Das Speichergerät wurde angehalten, wird jedoch derzeit für einen Auftrag verwendet.

Status	Beschreibung
Verzögert	<p>Es ist zu einer Verzögerung der laufenden Kommunikation zwischen einem verwalteten Backup Exec-Server und einem zentralen Administrationsserver in einer Central Admin Server Feature-Umgebung gekommen.</p> <p>Siehe "Erreichen der CAS-Kommunikationsschwellenwerte" auf Seite 1491.</p>
Die Backup Exec-Deduplizierungsdienste auf <Backup Exec-Server> müssen neu gestartet werden.	<p>Die Backup Exec-Deduplizierungsdienste müssen neu gestartet werden. Die Deduplizierungsdienste sind von den Backup Exec-Diensten getrennt; die Backup Exec-Dienste sind somit nicht betroffen.</p> <p>Siehe "Starten und Anhalten von Backup Exec-Diensten" auf Seite 776.</p>
Die Backup Exec-Dienste auf < Backup Exec-Server> müssen neu gestartet werden.	<p>Die Backup Exec-Dienste müssen neu gestartet werden.</p> <p>Siehe "Starten und Anhalten von Backup Exec-Diensten" auf Seite 776.</p>
Dieses Gerät wurde nicht richtig erkannt. Führen Sie die Dienste auf < Backup Exec-Server> aus, um die Geräteerkennung zu wiederholen.	<p>Dieser Status kann auftreten, nachdem Sie Backup Exec ein neues Speichergerät hinzufügen. Sie müssen die Backup Exec-Dienste neu starten, damit die Geräteerkennung wiederholt werden kann.</p>
Nicht initialisiert	Das Gerät wurde nicht initialisiert.

So sehen Sie den Status des Sperrmodus für die Datenträgerspeicherung

Das Einstellen des Sperrmodus für die Datenträgerspeicherung schützt die plattenbasierte Sicherung, die mit Backup Exec konfiguriert wurde. Der Zugang zur Datenträgerspeicherung ist auf zugelassene Verfahren, wie Backup Exec-Dienste, beschränkt. Demnach darf nur Backup Exec auf den Datenträgerspeicher schreiben. Der Status des Sperrmodus für die Datenträgerspeicherung zeigt den Status des plattenbasierten Backup an, das mit Backup Exec konfiguriert wurde.

Diese Einstellung ist standardmäßig aktiviert und ist die empfohlene Einstellung zum Schutz Ihrer Backup-Daten. Sie können die Einstellung durch Eingabe der

So sehen Sie den Status des Sperrmodus für die Datenträgerspeicherung

Zugangsdaten für die Systemanmeldung deaktivieren. Klicken Sie zum Deaktivieren des Sperrmodus auf, Backup Exec-Einstellungen > Netzwerk und Sicherheit > Einstellungen Sperrmodus für Datenträgerspeicherung > Deaktivieren und geben Sie die Zugangsdaten für die Systemanmeldung ein.

So können Sie den Status des Sperrmodus für die Datenträgerspeicherung einsehen

- 1 Doppelklicken Sie in der Statusleiste von Backup Exec auf "Status Sperrmodus für Datenträgerspeicherung"

Das Dialogfeld "Details Status Sperrmodus" wird angezeigt. Der "Status des Sperrmodus für die Datenträgerspeicherung" zeigt den Status für die Einstellung des Sperrmodus für die Datenträgerspeicherung an. Der Sperrmodus kann vier verschiedene Status annehmen.

Aktiviert	Der Sperrmodus für die Datenträgerspeicherung ist aktiviert und die plattenbasierte Backup-Speicherung wird durch Backup Exec geschützt.
Deaktiviert	Die Einstellung des Sperrmodus für die Datenträgerspeicherung ist deaktiviert.
Mit Ausnahme aktiviert	Die Einstellung für die Datenträgerspeicherung ist aktiviert, es sind jedoch Datenträger vorhanden, für die der Sperrmodus nicht aktiviert werden kann.
Nicht verfügbar	Backup Exec kann den Status für die Einstellungen des Sperrmodus nicht abrufen.

- 2 Klicken Sie auf "OK".

Siehe ["Netzwerk- und Sicherheitsoptionen für Backup Exec ändern"](#) auf Seite 713.

Konvertierung in virtuelle Computer

In diesem Kapitel werden folgende Themen behandelt:

- Funktionsweise der Konvertierung eines physischen Computers in einen virtuellen in Backup Exec
- Anforderungen für die Konvertierung in Aufträge für virtuelle Computer
- Gleichzeitig mit Backup-Auftrag in virtuellen Computer konvertieren
- Konvertierung in virtuellen Computer nach Backup-Auftrag
- Hinzufügen einer Konvertierung in eine virtuelle Computer-Phase zu einem Backup-Auftrag
- Konvertieren in einen virtuellen Computer von einem Zeitpunkt
- Erstellen einer einmaligen Konvertierung in einen virtuellen Computer
- Einstellungsstandardoptionen für die Konvertierung in Aufträge für virtuelle Computer

Funktionsweise der Konvertierung eines physischen Computers in einen virtuellen in Backup Exec

Mit Backup Exec können Sie einen physischen Computer in einen virtuellen konvertieren:

- Sichern Sie einen physischen Computer und konvertieren Sie ihn gleichzeitig in einen virtuellen Computer.

- Sichern Sie einen physischen Computer und planen Sie eine Konvertierung in einen virtuellen Computer nach Abschluss des Backups.
- Konvertieren Sie vorhandene Backup-Sätze in einen virtuellen Computer.
- Konvertiert einen laufenden physischen Computer in einen virtuellen Computer, ohne einen Backup-Auftrag auszuführen.

Hinweis: Die Konvertierung eines physischen Hyper-V-Hosts in eine virtuelle Maschine wird nicht unterstützt. Darüber hinaus wird in VMware-Umgebungen die Konvertierung von physischen Servern mit Windows Server 2012 und 4K-Datenträgern nicht unterstützt.

Der neu erstellte virtuelle Computer ist startfähig und identisch mit dem physischen Computer, aus dem der virtuelle Computer konvertiert wurde, mit Ausnahme der Netzwerkkarten und Einstellungen. Die Konvertierung in einen virtuellen Computer ermöglicht die Gewährleistung der geschäftlichen Verfügbarkeit für Hyper-V- und VMware-Umgebungen.

Dieses Thema umfasst die folgenden Informationen:

[Optionen für die Konvertierung in virtuelle Computer](#)

[Verarbeiten der Backup-Auswahl beim Konvertieren in virtuelle Computer](#)

[Funktionsweise von vollständigen, inkrementellen und Differenzial-Backups bei der Konvertierung in virtuelle Computer](#)

[Konvertieren von Datenträgern, die größer als 2 Terabyte sind](#)

[Hinweise zur Konvertierung in einen virtuellen Computer, der auf einem Hyper-V-Host mit Windows Server 2012 oder höher ausgeführt wird](#)

[Hinweise zum Konvertieren von Exchange-Servern](#)

Optionen für die Konvertierung in virtuelle Computer

Sie verwenden eine der folgenden Optionen auf der Registerkarte "Backup und Wiederherstellung", um eine Konvertierung in einen virtuellen Computer einzurichten:

Tabelle 14-1 Optionen für die Konvertierung in virtuelle Computer

Name der Option	Beschreibung
Auf Datenträger sichern und gleichzeitig in virtuellen Computer konvertieren	Diese Optionen führen die Konvertierung gleichzeitig mit dem Backup-Auftrag aus. Weil zwei Vorgänge gleichzeitig durchgeführt werden, dauert möglicherweise dieser Auftrag länger als ein normaler Backup-Auftrag. Für diese Backup-Option wird die Einplanung eines großen Zeitfensters empfohlen.
Auf Deduplizierungsdatenträger sichern und gleichzeitig in virtuellen Computer konvertieren	<p>Eine Konvertierung aus einem vollständigen Backup erstellt den neuen virtuellen Computer. Inkrementelle und Differenzial-Backups aktualisieren den virtuellen Computer, der aus dem vollständigen Backup erstellt wurde.</p> <p>Hinweis: Inkrementelle werden gegenüber Differenzial-Backups bevorzugt, da Differenzial-Backups für die Konvertierung weniger effektiv sind.</p> <p>Obwohl das Backup gleichzeitig mit der Konvertierung ausgeführt wird, ist das Backup der Hauptauftrag. Daher findet bei Ausfall des Backups auch die Konvertierung nicht statt. Allerdings wird bei einem Fehlschlag des Konvertierung das Backup weiter ausgeführt. Bei einem Konvertierungsausfall wird der Auftrag als Erfolg mit Ausnahmen markiert. Bei einem Konvertierungsausfall wird der Konvertierungsprozess während des nächsten vollständigen Backups erneut ausgeführt.</p> <p>Siehe "Gleichzeitig mit Backup-Auftrag in virtuellen Computer konvertieren" auf Seite 592.</p>

Name der Option	Beschreibung
<p>Auf Datenträger sichern und dann in virtuellen Computer konvertieren</p> <p>Auf Deduplizierungsdatenträger sichern und gleichzeitig in virtuellen Computer konvertieren</p>	<p>Mit diesen Optionen können Sie die Konvertierung nach dem Backup-Auftrag planen. Diese Optionen erfordern ein geringeres Backup-Zeitfenster als die Optionen für die gleichzeitige Konvertierung.</p> <p>Eine Konvertierung aus einem vollständigen Backup erstellt den neuen virtuellen Computer. Inkrementelle und Differenzial-Backups aktualisieren den virtuellen Computer, der aus dem vollständigen Backup erstellt wurde.</p> <p>Hinweis: Inkrementelle werden gegenüber Differenzial-Backups bevorzugt, da Differenzial-Backups für die Konvertierung weniger effektiv sind.</p> <p>Siehe "Konvertierung in virtuellen Computer nach Backup-Auftrag" auf Seite 599.</p>

Name der Option	Beschreibung
Von Zeitpunkt in virtuelle Einheit konvertieren	<p>Bei der Konvertierung in einen virtuellen Computer von einem Zeitpunkt an werden vorhandene Backup-Sätze aus einem Backup-Auftrag konvertiert, bei dem alle für einen virtuellen Computer erforderlichen Komponenten ausgewählt waren. Wenn alle notwendigen Komponenten für einen Backup-Auftrag ausgewählt sind, identifiziert Backup Exec den Auftrag als "Vollständig ausgewählt" und die Option "Simplified Disaster Recovery" hat den Status "Ein". Die Option zur Konvertierung aus einem Zeitpunkt in einen virtuellen Computer ist bei der Notfallwiederherstellung nützlich, wenn ein ausgefallener Server schnell wiederhergestellt werden muss. Die Backup-Sätze enthalten alle wichtigen Komponenten des Servers. Zusätzlich können Sie Anwendungsdaten oder Benutzerdaten auswählen, um in die Konvertierung einzuschließen.</p> <p>Hinweis: Die Option "Von Zeitpunkt in virtuelle Einheit konvertieren" steht erst dann zur Verfügung, wenn Sie mindestens ein vollständiges Backup ausgeführt haben, das alle kritischen Systemkomponenten umfasst.</p> <p>Siehe "Konvertieren in einen virtuellen Computer von einem Zeitpunkt" auf Seite 614.</p>

Name der Option	Beschreibung
Einmalig in virtuellen Computer konvertieren	<p>Diese Option konvertiert einen laufenden physischen Computer in einen virtuellen ohne einen separaten Backup-Auftrag. Ein einmaliger Konvertierungsauftrag kann für einen späteren Zeitpunkt geplant, aber nur einmal ausgeführt werden.</p> <p>Bei diesem Konvertierungstyp werden nur vollständige Backups unterstützt. Inkrementelle und Differenzial-Backups werden bei der einmaligen Konvertierung nicht unterstützt.</p> <p>Hinweis: Kopier-Backups werden unter Hyper-V 2008 oder 2008 R2 nicht unterstützt. Stattdessen wird eine absturzkonsistente Konvertierung erstellt.</p> <p>Siehe "Erstellen einer einmaligen Konvertierung in einen virtuellen Computer" auf Seite 616.</p>
Stufe hinzufügen	<p>Außerdem können Sie beim Konvertieren in einen virtuellen Computer einem Backup-Auftrag eine Stufe hinzufügen. Es stehen zwei Stufen zur Verfügung: "Nach Backup in virtuellen Computer konvertieren" und "In virtuellen Computer konvertieren und gleichzeitig sichern".</p> <p>Siehe "Hinzufügen einer Konvertierung in eine virtuelle Computer-Phase zu einem Backup-Auftrag" auf Seite 607.</p>

Hinweis: Unabhängig von der Option, mit der die Konvertierung initiiert wurde, schaltet Backup Exec den virtuellen Computer nicht ein, nachdem es ihn erstellt hat.

Backup Exec erstellt am Ende der Konvertierung einen Snapshot des virtuellen Computers. Der Snapshot wird entfernt, bevor der nächste Auftrag ausgeführt, solange der virtuelle Computer nicht angeschaltet wird und der von Backup Exec erstellte Snapshot der einzige Snapshot auf dem virtuellen Computer ist. Wenn Sie beginnen möchten, den virtuellen Computer zu verwenden, müssen Sie den Snapshot manuell entfernen.

Wenn der Host des konvertierten virtuellen Computers ausfällt und Sie den virtuellen Computer online schalten, wird der vorhandene Konvertierungsauftrag weiter ausgeführt und schlägt schließlich fehl. In diesem Fall müssen Sie einen neuen Konvertierungsauftrag erstellen.

Verarbeiten der Backup-Auswahl beim Konvertieren in virtuelle Computer

Wenn Sie einen Auftrag zum Konvertieren in einem virtuellen Computer einrichten, wählen Sie die zu Elemente aus, die vor oder während der Konvertierung gesichert werden sollen. Backup Exec kann automatisch Daten in bestimmten Situationen aus- oder einschließen. Das Auftragsprotokoll enthält die Elemente, die in die Konvertierung ein- bzw. daraus ausgeschlossen wurden.

Die Auswahl wird wie folgt verarbeitet:

- Wenn Sie einen Datenträger aus dem Backup-Auftrag ausschließen, wird dieser Datenträger automatisch aus dem entsprechenden Konvertierungsauftrag ausgeschlossen.
- Wenn Sie eine Anwendung in den Backup-Auftrag einschließen, wird der Datenträger, auf dem sich diese Anwendung befindet, automatisch in den Konvertierungsauftrag eingeschlossen.
- Wenn Sie einen Datenträger aus dem Backup ausschließen, wird ein Datenträger, der Teil des ersten Datenträgers ist, automatisch ausgeschlossen, wenn der Datenträger der einzige auf dem anderen Datenträger ist.

Funktionsweise von vollständigen, inkrementellen und Differenzial-Backups bei der Konvertierung in virtuelle Computer

Aufträge zum Konvertieren in einen virtuellen Computer erstellen einen virtuellen Computer aus einem vollständigen Backup. Spätere inkrementelle und Differenzial-Backup-Aufträge aktualisieren den virtuellen Computer, der aus dem vollständigen Backup erstellt wurde. Obgleich Differenzial-Backups für Konvertierungsaufträge unterstützt werden, sind inkrementelle Backups die bevorzugte Methode für das Aktualisieren von virtuellen Computern. Differenzial-Backups sind im Vergleich zu inkrementellen Backups für die Konvertierung weniger geeignet.

Wenn Sie ein inkrementelles Backup für die Konvertierung in virtuelle Computer verwenden, beachten Sie die folgenden Punkte:

- Daten aus Datenträgern werden auf Datei-\Ordner Ebene gesichert. Selbst wenn sich nur ein Teil der Datei geändert hat, wird die gesamte Datei gesichert.

- Der gesamte Systemstatus wird gesichert. Inkrementelle Backups werden nur für die Systemdateikomponenten des Systemstatus unterstützt. Die anderen Systemstatuskomponenten werden als vollständiges Backup gesichert.
- Für SQL müssen Backup-Methoden auf Blockebene ausgewählt werden. Nachdem das erste inkrementelle Backup für SQL ausgeführt wurde, werden Backups auf Blockebene für alle folgenden vollständigen oder inkrementellen Backups ausgeführt, für die die Option "Simplified Disaster Recovery" auf "Ein" steht. Die Konvertierung wird nicht durchgeführt, wenn keine Backup-Methode auf Blockebene ausgewählt ist.
- Vollständige Backups werden immer für Active Directory durchgeführt. Weder inkrementelle noch Differenzial-Backups werden für Active Directory unterstützt.

Konvertieren von Datenträgern, die größer als 2 Terabyte sind

Backup Exec unterstützt die Konvertierung von Datenträgern, die größer als 2 Terabyte (TB) sind, für Hosts von VMware und Hyper-V 2012 oder höher.

Hinweis: Wenn der Start- oder Systemdatenträger auf dem physischen Quellcomputer größer als 2 TB ist und in einen virtuellen VMware- oder Hyper-V 2008 R2-Computer konvertiert werden soll, ist die Konvertierung nicht möglich. Ein Startdatenträger kann nicht als dynamischer übergreifender Datenträger aufgeteilt oder erstellt werden. Diese Beschränkung trifft auch zu, wenn der Startdatenträger auf der Quelle größer als die maximal unterstützte Datenträgergröße des Zieldatenspeichers ist.

Backup Exec konvertiert alle Datenträger auf dem Ziel in einfache oder übergreifende dynamische Datenträger. Auch wenn die Quelle ein Basisdatenträger ist, sind die konvertierten Datenträger auf dem Ziel dynamisch. Da Backup Exec nur einfache und übergreifende dynamische Datenträger unterstützt, wenn der Quelldatenträgertyp Stripeset, Spiegel, oder Raid5 ist, konvertiert Backup Exec diesen Datenträger entweder einfach oder übergreifend auf dem Ziel.

Die folgende zusätzliche Information gilt nur für VMware:

- Die Konvertierung eines Datenträgers, der größer als 2 TB ist, wird in den folgenden Situationen unterstützt:
 - Wenn der Datenträger kein Start- oder Systemdatenträger ist
 - Wenn der Datenträger auf einem dynamischen Datenträger erstellt wurde
 - Wenn der Datenträger ein MBR-Datenträger ist

- Das Konvertieren von GPT-Datenträgern wird nicht unterstützt, unabhängig von der Größe des Datenträgers. Konvertierungen von GPT-Datenträgern schlagen fehl.
- In Situationen, in denen der VMware-Quelldatenträger größer als die maximal unterstützte Größe des Zieldatenspeichers ist, wird der Quelldatenträger in mehrere Datenträger aufgeteilt. Backup Exec teilt den Datenträger basierend auf der maximalen Größe des Zieldatenspeichers.

Hinweise zur Konvertierung in einen virtuellen Computer, der auf einem Hyper-V-Host mit Windows Server 2012 oder höher ausgeführt wird

Bevor Sie einen Auftrag erstellen, um einen physischen Computer in einen mit Windows Server 2012 und anschließend in einem Hyper-V-Host zu konvertieren, gewährleisten Sie Folgendes:

- Datenträgerdaten werden in VHDX-Dateien gespeichert. Die VHDX-Dateien haben eine maximale Kapazität von 64 TB. Die Festplattensektorgröße des physischen Computers wird während der Konvertierung aufrechterhalten.
- Die Konvertierung von physischen Computern, die einfache GPT-Datenträger haben, wird unterstützt.
- Die Konvertierung von physischen Computern, die dynamische Datenträger haben, wird nicht unterstützt.
- Speicherplätze und Speicherpools werden nicht unterstützt.
- Da die Konvertierung in vorherige Versionen eines Windows-Hyper-V-Hosts nicht unterstützt wird, schlagen diese Aufträge fehl. Beispiel: Wenn der physische Computer Windows Server 2012 mit einem ReFS-Datenträger ausführt, wird die Konvertierung in einen Windows Server 2012-Hyper-V-Host unterstützt.
- Wenn der physische Computer Windows Server 2012 mit einem oder mehreren Windows-Deduplizierungsdatenträgern ausführt, ist die Konvertierung in einen Hyper-V-Host möglich, aber sie schlägt möglicherweise fehl. Die konvertierten Datenträgerdaten werden nicht dedupliziert. Es wird also eine nicht optimierte Datenübertragung durchgeführt. Aus diesem Grund schlägt möglicherweise die Konvertierung fehl, wenn die Menge nicht optimierter Daten größer als die Kapazität des Zieldatenträgers ist.

Hinweise zum Konvertieren von Exchange-Servern

Backup Exec deaktiviert Exchange-Dienste auf einem neu erstellten virtuellen Computer nach einem Auftrag in einen virtuellen Computer. Befinden sich Exchange-Datenbanken auf einem konvertierten Server, nachdem ein Auftrag zum Konvertieren in einen virtuellen Computer ausgeführt wurde, müssen Sie Microsoft

Services Control Manager öffnen und folgende Exchange-Dienste manuell neu starten:

- MExchangeDagMgmt
- MExchangeADTopology
- MExchangeAntispamUpdate
- MExchangeDiagnostics
- MExchangeEdgeSync
- MExchangeFrontEndTransport
- MExchangeHM
- MExchangeMailboxAssistants
- MExchangeDelivery
- MExchangeSubmission
- MExchangeMigrationWorkflow
- MExchangeMailboxReplication
- MExchangeRPC
- MExchangeFastSearch
- HostControllerService
- MExchangeServiceHost
- MExchangeThrottling
- MExchangeTransport
- MExchangeTransportLogSearch
- MExchangeUM
- MExchangeUMCR

Siehe ["Anforderungen für die Konvertierung in Aufträge für virtuelle Computer"](#) auf Seite 590.

Anforderungen für die Konvertierung in Aufträge für virtuelle Computer

Stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind, bevor Sie die Konvertierungsfunktion verwenden.

- Die Option "Simplified Disaster Recovery" muss den Status "EIN" auf der Registerkarte "Durchsuchen" im Dialogfeld "Backup-Auswahl" haben.

Hinweis: Der Agent for VMware und Hyper-V ist für die Konvertierung in virtuelle Computer nicht erforderlich.

- Nur Windows-Server werden unterstützt.
- Die Konvertierung aus einem doppelten Backup-Satz wird nicht unterstützt.
- Wenn Sie in einer VMware-Umgebung einen physischen in einen virtuellen Server konvertieren und dann den konvertierten Server sichern möchten, müssen Sie eine Push-Installation des Agent for Windows auf dem konvertierten Server ausführen. Dabei wird der VSS-Anbieter von Backup Exec installiert. Beachten Sie, dass Sie den Agent for Windows auf dem konvertierten Server installieren müssen, selbst wenn er bereits auf dem physischen Server installiert war, bevor Sie ihn in einen virtuellen konvertierten.
- Für die Konvertierung in einer Hyper-V-Umgebung gelten folgende zusätzliche Anforderungen:
 - Agent for Windows muss auf dem Hyper-V-Host installiert sein, an den die Konvertierung gesendet wird.
 - Die maximale Datenträgergröße ist 2 TB für Hyper-V 2008/2008 R2 und frühere Versionen. Datenträger, die eine Größe von mehr als 2 TB haben, werden für Hyper-V 2012 oder höher unterstützt.
 - Nur Basisdatenträger werden unterstützt. Dynamische Datenträger werden für Hyper-V-Konvertierungen nicht unterstützt.
 - Bevor Sie einen Konvertierungsauftrag für einen Hyper-V-Host ausführen, deaktivieren Sie den Ressourcen-Manager für Dateiserver (FSRM). Wenn Sie FSRM nicht deaktivieren, kann der Auftrag mit dem Fehler "Nicht genügend Speicherplatz." fehlschlagen.

Hinweis: Die Konvertierung eines physischen Hyper-V-Hosts in eine virtuelle Maschine wird nicht unterstützt.

- Informationen zu den spezifischen Betriebssystemanforderungen für die Konvertierung in virtuelle Computer finden Sie in der Liste der mit Backup Exec kompatiblen Software.

Siehe ["Funktionsweise der Konvertierung eines physischen Computers in einen virtuellen in Backup Exec"](#) auf Seite 581.

Gleichzeitig mit Backup-Auftrag in virtuellen Computer konvertieren

Bei diesem Konvertierungstyp werden das Backup und die Konvertierung gleichzeitig ausgeführt.

Hinweis: Bei Ausfall des Backups findet auch die Konvertierung nicht statt. Allerdings wird bei einem Fehlschlag der Konvertierung das Backup weiter ausgeführt. Bei einem Konvertierungsausfall wird der Auftrag als Erfolg mit Ausnahmen markiert und die Konvertierung wird während des vollständigen Backups erneut ausgeführt.

Gleichzeitige Ausführung des Backups und der Konvertierung in virtuellen Computer

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" mit der rechten Maustaste auf den Server, der die Daten enthält, die Sie sichern und konvertieren möchten.
- 2 Wählen Sie "Backup" und dann "Auf Datenträger sichern und gleichzeitig in virtuellen Computer konvertieren" oder "Auf Deduplizierungsdatenträger sichern und gleichzeitig in virtuellen Computer konvertieren", je nach Typ des Speichergeräts, das Sie verwenden möchten.
- 3 Führen Sie einen der folgenden Schritte aus:

Ändern der Backup-Auswahl

Gehen Sie wie folgt vor:

- Im <Servername>-Feld klicken Sie auf Bearbeiten und wählen Sie dann die Elemente aus, die Sie sichern möchten.

Hinweis: Die Option "Simplified Disaster Recovery" muss den Status "EIN" haben.

- Klicken Sie auf "OK".

Ändern der Backup-Optionen

Gehen Sie wie folgt vor:

- Im Backup -Feld klicken Sie auf Bearbeiten und ändern Sie dann die Backup-Optionen wie gewünscht.
- Klicken Sie auf "OK".

- 4** Klicken Sie im Feld "Konvertierung in virtuellen Computer" auf "Bearbeiten", um die Optionen für die Konvertierung festzulegen.
- 5** Wählen Sie im Feld "Konvertieren für" entweder "Hyper-V" oder "VMware ESX/vCenter-Server" aus.
- 6** Konfigurieren Sie die Konvertierungsoptionen:

Wenn Sie in Schritt 5 "Hyper-V"
ausgewählt haben

So konfigurieren Sie die Konvertierungsoptionen

- Klicken Sie im Feld "Hyper-V-Servername", wählen Sie den Namen des Servers, in dem Sie den virtuellen Computer erstellen möchten, aus und klicken Sie dann auf "Hinzufügen".
- Geben Sie im Feld "Ziellaufwerk oder Pfad" den Speicherort auf dem physischen Computer ein, in dem die virtuellen Datenträger erstellt werden sollen. Geben Sie einen Laufwerksbuchstaben und einen Pfad ein.
- Wenn Sie den Standardnamen des virtuellen Computers ändern möchten, geben Sie den neuen Namen im Feld "Name des virtuellen Computers" ein.
- Soll Backup Exec einen virtuellen Computer überschreiben können, wenn bereits ein virtueller Computer mit dem gleichen Namen existiert, stellen Sie sicher, dass die Option "Virtuellen Computer überschreiben, wenn bereits vorhanden" ausgewählt ist. Falls diese Option nicht aktiviert ist und der Name des virtuellen Computers bereits vorhanden ist, schlägt der Auftrag fehl.
- Geben Sie im Feld "Vollständiger Pfad des ISO-Image von Hyper-V Integration Components" den Speicherort ein. Das ISO-Image ist erforderlich, um den virtuellen Computer startfähig zu machen.

Hinweis: Diese Option ist nicht für Hyper-V-Server mit Windows Server 2016 oder höher verfügbar. Solche Hyper-V-Server installieren Integrationsdienste direkt auf dem virtuellen Computer entweder über ein Windows-Update oder durch Herunterladen durch den Benutzer.

- Wenn Sie die Anzahl der CPUs oder die Größe des RAM für den virtuellen

Zielcomputer ändern möchten, geben Sie auf der Registerkarte

"Serverkonfiguration" unter "Virtueller Zielcomputer" die neuen Werte ein.

- Wenn Sie den Typ, den Controller oder den Speicherort eines virtuellen Datenträgers ändern möchten, klicken Sie auf der Registerkarte "Datenträgerkonfiguration" auf "Datenträgerkonfiguration bearbeiten" und geben dann die neuen Werte ein.

Wenn Sie in Schritt 5 "VMware
ESX/vCenter-Server" ausgewählt haben

So konfigurieren Sie die Konvertierungsoptionen

- Klicken Sie im Feld "ESX/vCenter-Servername" auf den Pfeil und dann auf den Namen des Servers, auf dem der virtuelle Computer erstellt werden soll.
- Klicken Sie auf den Pfeil im Feld "Login-Konto" und wählen Sie dann das entsprechende Login-Konto für den ausgewählten Server aus.
- Klicken Sie neben dem Feld "ESX-/vCenter-Servername" auf "Auswählen". Backup Exec füllt die restlichen Informationen über den Server aus.
- Wählen Sie den Ordner für den virtuellen Computer und den Ressourcenpool aus, die mit dem ausgewählten Server verknüpft sind.

Hinweis: Wenn Sie einen ESX-Server als Ziel auswählen und einen Ressourcenpool auswählen, wird der neu erstellte virtuelle Computer nicht automatisch dem Ressourcenpool hinzugefügt. Sie können nach der Konvertierung den virtuellen Computer manuell in den geeigneten Ressourcenpool verschieben.

- Wenn Sie den Standardnamen des virtuellen Computers ändern möchten, geben Sie den neuen Namen im Feld "Name des virtuellen Computers" ein.
- Soll Backup Exec einen virtuellen Computer überschreiben können, wenn bereits ein virtueller Computer mit dem gleichen Namen existiert, stellen Sie sicher, dass die Option "Virtuellen Computer überschreiben, wenn bereits vorhanden" ausgewählt ist. Falls diese Option nicht aktiviert ist und der Name des virtuellen Computers bereits vorhanden ist, schlägt der Auftrag fehl.
- Geben Sie im Feld "Vollständiger Pfad des ISO-Image von VMware Tools" den

Speicherort ein. Der Pfad sollte mit den Standardidentifikationsdaten zugänglich sein. Der Pfad muss auf einen lokalen Datenträger des Backup Exec-Servers verweisen. Das ISO-Image ist erforderlich, um den virtuellen Computer startfähig zu machen.

Hinweis: In einer CAS-Umgebung sollte dieser Pfad lokal zum verwalteten Backup Exec-Server sein, den der Auftrag zum Ziel hat.

- Wenn Sie die Anzahl der CPUs oder die Größe des RAM für den virtuellen Zielcomputer ändern möchten, geben Sie auf der Registerkarte "Serverkonfiguration" unter "Virtueller Zielcomputer" die neuen Werte ein.
- Wenn Sie den Typ, den Controller oder den Speicherort eines virtuellen Datenträgers ändern möchten, klicken Sie auf der Registerkarte "Datenträgerkonfiguration" auf "Datenträgerkonfiguration bearbeiten" und geben dann die neuen Werte ein.

7 Klicken Sie auf "OK".

8 Klicken Sie im Dialogfeld "Eigenschaften der Backup-Definition" auf "OK", um den Auftrag zu erstellen.

Siehe ["Funktionsweise der Konvertierung eines physischen Computers in einen virtuellen in Backup Exec"](#) auf Seite 581.

Konvertierung in virtuellen Computer nach Backup-Auftrag

Backup Exec richtet diesen Konvertierungstyp als Phase ein, die nach dem Backup-Auftrag ausgeführt wird. Die vom Backup-Auftrag erstellten Backup-Sätze werden verwendet, um den virtuellen Computer zu erstellen.

Konvertierung in virtuellen Computer nach Backup-Auftrag

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" mit der rechten Maustaste auf den Server, der die Daten enthält, die Sie sichern und konvertieren möchten.
- 2 Wählen Sie "Backup" und dann "Auf Datenträger sichern und dann in virtuellen Computer konvertieren" oder "Auf Deduplizierungsdatenträger sichern und dann in virtuellen Computer konvertieren", je nach Typ des Speichergeräts, das Sie verwenden möchten.
- 3 Führen Sie einen der folgenden Schritte aus:

Ändern der Backup-Auswahl

Gehen Sie wie folgt vor:

- Im <Servername>-Feld klicken Sie auf Bearbeiten und wählen Sie dann die Elemente aus, die Sie sichern möchten.

Hinweis: Die Option "Simplified Disaster Recovery" muss den Status "EIN" haben.

- Klicken Sie auf "OK".

Ändern der Backup-Optionen

Gehen Sie wie folgt vor:

- Im Backup -Feld klicken Sie auf Bearbeiten und ändern Sie dann die Backup-Optionen wie gewünscht.
- Klicken Sie auf "OK".

- 4 Klicken Sie im Feld "Konvertierung in virtuellen Computer" auf "Bearbeiten".
- 5 Im linken Teilfenster wählen Sie "Planen" und wählen dann eine der folgenden Optionen aus:

So planen Sie die Konvertierung zu einem spezifischen Zeitpunkt

Gehen Sie wie folgt vor:

- Wählen Sie "Nach Zeitplan".
- Klicken Sie auf den Pfeil im Feld "Quelle", um entweder alle Backups oder das aktuellste vollständige Backup als Quelle für die Konvertierung auszuwählen.
- Wählen Sie "Wiederkehrend" und klicken Sie dann auf den Pfeil zum Festlegen des Wiederholungsmusters.

So erstellen Sie den Konvertierungsauftrag, ohne ihn zu planen

Gehen Sie wie folgt vor:

- Wählen Sie "Nach Zeitplan".
- Klicken Sie auf den Pfeil im Feld "Quelle", um entweder alle Backups oder das aktuellste vollständige Backup als Quelle für die Konvertierung auszuwählen.
- Wählen Sie "Ohne Zeitplan erstellen". Wenn Sie diese Option verwenden, wird der Auftrag nicht zum Zeitpunkt der Erstellung ausgeführt und hat keinen wiederkehrenden Zeitplan. Der Auftrag verbleibt im Zustand "ausstehend", bis Sie ihn ausführen. Sie können ein Auftragsautomatisierungs- oder Aufgabenplanungs-Tool eines anderen Herstellers verwenden, um den Auftrag später auszuführen.

So führen Sie die Konvertierung sofort nach Abschluss des Backup-Auftrags aus

Wählen Sie "Sofort nach Abschluss der Quellaufgabe virtuell konvertieren".

- 6 Optional: Wählen Sie im linken Teilfenster "Benachrichtigung", um die ausgewählten Empfänger zu benachrichtigen, sobald der Auftrag abgeschlossen wurde.
- 7 Klicken Sie im linken Teilfenster auf Konvertierungseinstellungen, um Optionen für die Konvertierung einzustellen.
- 8 Wählen Sie im Feld "Konvertieren für" entweder "Hyper-V" oder "VMware ESX/vCenter-Server" aus.
- 9 Konfigurieren Sie die Konvertierungsoptionen:

Wenn Sie in Schritt 8 "Hyper-V"
ausgewählt haben

So konfigurieren Sie die Konvertierungsoptionen

- Klicken Sie im Feld "Hyper-V-Servername", wählen Sie den Namen des Servers, in dem Sie den virtuellen Computer erstellen möchten, aus und klicken Sie dann auf "Hinzufügen".
- Geben Sie im Feld "Ziellaufwerk oder Pfad" den Speicherort auf dem physischen Computer ein, in dem die virtuellen Datenträger erstellt werden sollen. Geben Sie einen Laufwerksbuchstaben und einen Pfad ein.
- Wenn Sie den Standardnamen des virtuellen Computers ändern möchten, geben Sie den neuen Namen im Feld "Name des virtuellen Computers" ein.
- Soll Backup Exec einen virtuellen Computer überschreiben können, wenn bereits ein virtueller Computer mit dem gleichen Namen existiert, stellen Sie sicher, dass die Option "Virtuellen Computer überschreiben, wenn bereits vorhanden" ausgewählt ist. Falls diese Option nicht aktiviert ist und der Name des virtuellen Computers bereits vorhanden ist, schlägt der Auftrag fehl.
- Geben Sie im Feld "Vollständiger Pfad des ISO-Image von Hyper-V Integration Components" den Speicherort ein. Das ISO-Image ist erforderlich, um den virtuellen Computer startfähig zu machen.

Hinweis: Diese Option ist nicht für Hyper-V-Server mit Windows Server 2016 oder höher verfügbar. Solche Hyper-V-Server installieren Integrationsdienste direkt auf dem virtuellen Computer entweder über ein Windows-Update oder durch Herunterladen durch den Benutzer.

- Wenn Sie die Anzahl der CPUs oder die Größe des RAM für den virtuellen

Zielcomputer ändern möchten, geben Sie auf der Registerkarte "Serverkonfiguration" unter "Virtueller Zielcomputer" die neuen Werte ein.

- Wenn Sie den Typ, den Controller oder den Speicherort eines virtuellen Datenträgers ändern möchten, klicken Sie auf der Registerkarte "Datenträgerkonfiguration" auf "Datenträgerkonfiguration bearbeiten" und geben dann die neuen Werte ein.

Wenn Sie in Schritt 8 "VMware
ESX/vCenter-Server" ausgewählt haben

So konfigurieren Sie die Konvertierungsoptionen

- Klicken Sie im Feld "ESX/vCenter-Servername" auf den Pfeil und dann auf den Namen des Servers, auf dem der virtuelle Computer erstellt werden soll.
- Klicken Sie auf den Pfeil im Feld "Login-Konto" und wählen Sie dann das entsprechende Login-Konto für den ausgewählten Server aus.
- Klicken Sie neben dem Feld "ESX-/vCenter-Servername" auf "Auswählen". Backup Exec füllt die restlichen Informationen über den Server aus.
- Wählen Sie den Ordner für den virtuellen Computer und den Ressourcenpool aus, die mit dem ausgewählten Server verknüpft sind.

Hinweis: Wenn Sie einen ESX-Server als Ziel auswählen und einen Ressourcenpool auswählen, wird der neu erstellte virtuelle Computer nicht automatisch dem Ressourcenpool hinzugefügt. Sie können nach der Konvertierung den virtuellen Computer manuell in den geeigneten Ressourcenpool verschieben.

- Wenn Sie den Standardnamen des virtuellen Computers ändern möchten, geben Sie den neuen Namen im Feld "Name des virtuellen Computers" ein.
- Soll Backup Exec einen virtuellen Computer überschreiben können, wenn bereits ein virtueller Computer mit dem gleichen Namen existiert, stellen Sie sicher, dass die Option "Virtuellen Computer überschreiben, wenn bereits vorhanden" ausgewählt ist. Falls diese Option nicht aktiviert ist und der Name des virtuellen Computers bereits vorhanden ist, schlägt der Auftrag fehl.
- Geben Sie im Feld "Vollständiger Pfad des ISO-Image von VMware Tools" den

Speicherort ein. Der Pfad sollte mit den Standardidentifikationsdaten zugänglich sein. Der Pfad muss auf einen lokalen Datenträger des Backup Exec-Servers verweisen. Das ISO-Image ist erforderlich, um den virtuellen Computer startfähig zu machen.

Hinweis: In einer CAS-Umgebung sollte dieser Pfad lokal zum verwalteten Backup Exec-Server sein, den der Auftrag zum Ziel hat.

- Wenn Sie die Anzahl der CPUs oder die Größe des RAM für den virtuellen Zielcomputer ändern möchten, geben Sie auf der Registerkarte "Serverkonfiguration" unter "Virtueller Zielcomputer" die neuen Werte ein.
- Wenn Sie den Typ, den Controller oder den Speicherort eines virtuellen Datenträgers ändern möchten, klicken Sie auf der Registerkarte "Datenträgerkonfiguration" auf "Datenträgerkonfiguration bearbeiten" und geben dann die neuen Werte ein.

10 Klicken Sie auf "OK", um Ihre Einstellungen zu speichern.

11 Klicken Sie im Dialogfeld "Eigenschaften der Backup-Definition" auf "OK", um den Auftrag zu erstellen.

Siehe ["Funktionsweise der Konvertierung eines physischen Computers in einen virtuellen in Backup Exec"](#) auf Seite 581.

Hinzufügen einer Konvertierung in eine virtuelle Computer-Phase zu einem Backup-Auftrag

Sie können einer Backup-Definition eine Phase hinzufügen, um ein Backup in einen virtuellen Computer zu konvertieren. Für einen Auftrag zur Konvertierung in einen virtuellen Computer muss die Option "Simplified Disaster Recovery" in der Backup-Auswahl den Status "EIN" haben. Dieser Status bedeutet, dass alle Komponenten, die für Virtualisierung notwendig sind, ausgewählt werden. Backup Exec wählt automatisch die notwendigen Komponenten aus, wenn Sie eine Phase zum Konvertieren in einen virtuellen Computer hinzufügen.

So fügen Sie einem Backup-Auftrag eine Konvertierung in eine virtuelle Computer-Phase hinzu

- 1** Erstellen Sie einen Backup-Auftrag oder bearbeiten Sie einen vorhandenen Auftrag.
- 2** Klicken Sie im Dialogfeld Backup auf Phase hinzufügen.
- 3** Wählen Sie "In virtuellen Computer konvertieren", um nach Abschluss des Backup-Auftrags eine Konvertierung zu starten, oder wählen Sie "Gleichzeitig mit dem Backup nach virtuell konvertieren", um den Auftrag gleichzeitig mit dem Backup-Auftrag zu starten.
- 4** Klicken Sie im Feld "Konvertierung in virtuellen Computer" auf "Bearbeiten".
- 5** Wenn Sie die Option "In virtuellen Computer konvertieren" in Schritt 3 ausgewählt haben, gehen Sie wie folgt vor. Wenn Sie die Option "Gleichzeitig mit dem Backup nach virtuell konvertieren" in Schritt 3 ausgewählt haben, fahren Sie mit Schritt 6 fort.
 - Wählen Sie im linken Teilfenster "Planen", um die Konvertierung zu planen, und geben Sie dann an, ob Sie den Auftrag planen oder sofort nach Abschluss des Auftrags ausführen möchten.
 - (Optional) Wählen Sie im linken Teilfenster "Benachrichtigung", wenn Sie einen Empfänger benachrichtigen möchten, sobald der Auftrag abgeschlossen wurde.
- 6** Klicken Sie im linken Teilfenster auf Konvertierungseinstellungen, um Optionen für die Konvertierung einzustellen.
- 7** Wählen Sie im Feld "Konvertieren für" entweder "Hyper-V" oder "VMware ESX/vCenter-Server" aus.
- 8** Konfigurieren Sie die Konvertierungsoptionen:

Wenn Sie in Schritt 7 "Hyper-V"
auswählen

So konfigurieren Sie die Konvertierungsoptionen

- Klicken Sie im Feld "Hyper-V-Servername", wählen Sie den Namen des Servers, in dem Sie den virtuellen Computer erstellen möchten, aus und klicken Sie dann auf "Hinzufügen".
- Geben Sie im Feld "Ziellaufwerk oder Pfad" den Speicherort auf dem physischen Computer ein, in dem die virtuellen Datenträger erstellt werden sollen. Geben Sie einen Laufwerksbuchstaben und einen Pfad ein.
- Wenn Sie den Standardnamen des virtuellen Computers ändern möchten, geben Sie den neuen Namen im Feld "Name des virtuellen Computers" ein.
- Soll Backup Exec einen virtuellen Computer überschreiben können, wenn bereits ein virtueller Computer mit dem gleichen Namen existiert, stellen Sie sicher, dass die Option "Virtuellen Computer überschreiben, wenn bereits vorhanden" ausgewählt ist. Falls diese Option nicht aktiviert ist und der Name des virtuellen Computers bereits vorhanden ist, schlägt der Auftrag fehl.
- Geben Sie im Feld "Vollständiger Pfad des ISO-Image von Hyper-V Integration Components" den Speicherort ein. Das ISO-Image ist erforderlich, um den virtuellen Computer startfähig zu machen.

Hinweis: Diese Option ist nicht für Hyper-V-Server mit Windows Server 2016 oder höher verfügbar. Solche Hyper-V-Server installieren Integrationsdienste direkt auf dem virtuellen Computer entweder über ein Windows-Update oder durch Herunterladen durch den Benutzer.

- Wenn Sie die Anzahl der CPUs oder die Größe des RAM für den virtuellen

Zielcomputer ändern möchten, geben Sie auf der Registerkarte

"Serverkonfiguration" unter "Virtueller Zielcomputer" die neuen Werte ein.

- Wenn Sie den Typ, den Controller oder den Speicherort eines virtuellen Datenträgers ändern möchten, klicken Sie auf der Registerkarte "Datenträgerkonfiguration" auf "Datenträgerkonfiguration bearbeiten" und geben dann die neuen Werte ein.

Hinzufügen einer Konvertierung in eine virtuelle Computer-Phase zu einem Backup-Auftrag

Wenn Sie in Schritt 7 "VMware
ESX/vCenter-Server" ausgewählt haben

So konfigurieren Sie die Konvertierungsoptionen

- Klicken Sie im Feld "ESX/vCenter-Servername" auf den Pfeil und dann auf den Namen des Servers, auf dem der virtuelle Computer erstellt werden soll.
- Klicken Sie auf den Pfeil im Feld "Login-Konto" und wählen Sie dann das entsprechende Login-Konto für den ausgewählten Server aus.
- Klicken Sie neben dem Feld "ESX-/vCenter-Servername" auf "Auswählen". Backup Exec füllt die restlichen Informationen über den Server aus.
- Wählen Sie den Ordner für den virtuellen Computer und den Ressourcenpool aus, die mit dem ausgewählten Server verknüpft sind.

Hinweis: Wenn Sie einen ESX-Server als Ziel auswählen und einen Ressourcenpool auswählen, wird der neu erstellte virtuelle Computer nicht automatisch dem Ressourcenpool hinzugefügt. Sie können nach der Konvertierung den virtuellen Computer manuell in den geeigneten Ressourcenpool verschieben.

- Wenn Sie den Standardnamen des virtuellen Computers ändern möchten, geben Sie den neuen Namen im Feld "Name des virtuellen Computers" ein.
- Soll Backup Exec einen virtuellen Computer überschreiben können, wenn bereits ein virtueller Computer mit dem gleichen Namen existiert, stellen Sie sicher, dass die Option "Virtuellen Computer überschreiben, wenn bereits vorhanden" ausgewählt ist. Falls diese Option nicht aktiviert ist und der Name des virtuellen Computers bereits vorhanden ist, schlägt der Auftrag fehl.
- Geben Sie im Feld "Vollständiger Pfad des ISO-Image von VMware Tools" den

Speicherort ein. Der Pfad sollte mit den Standardidentifikationsdaten zugänglich sein. Der Pfad muss auf einen lokalen Datenträger des Backup Exec-Servers verweisen. Das ISO-Image ist erforderlich, um den virtuellen Computer startfähig zu machen.

Hinweis: In einer CAS-Umgebung sollte dieser Pfad lokal zum verwalteten Backup Exec-Server sein, den der Auftrag zum Ziel hat.

- Wenn Sie die Anzahl der CPUs oder die Größe des RAM für den virtuellen Zielcomputer ändern möchten, geben Sie auf der Registerkarte "Serverkonfiguration" unter "Virtueller Zielcomputer" die neuen Werte ein.
- Wenn Sie den Typ, den Controller oder den Speicherort eines virtuellen Datenträgers ändern möchten, klicken Sie auf der Registerkarte "Datenträgerkonfiguration" auf "Datenträgerkonfiguration bearbeiten" und geben dann die neuen Werte ein.

9 Klicken Sie auf "OK", um Ihre Einstellungen zu speichern.

10 Bearbeiten Sie im Dialogfeld "Eigenschaften der Backup-Definition" die Eigenschaften des Backup-Auftrags und klicken Sie auf "OK", um den Auftrag zu erstellen.

Siehe ["Funktionsweise der Konvertierung eines physischen Computers in einen virtuellen in Backup Exec"](#) auf Seite 581.

Konvertieren in einen virtuellen Computer von einem Zeitpunkt

Bei der Konvertierung auf einem virtuellen Computer von einem Zeitpunkt an werden vorhandene Backup-Sätze aus einem Backup-Auftrag konvertiert, bei dem die Option "Simplified Disaster Recovery" aktiviert war. Die Option "Simplified Disaster Recovery" bewirkt, dass alle kritischen Systemkomponenten für eine Konvertierung in einen virtuellen Computer in den Backup-Auftrag eingeschlossen werden.

Hinweis: Die Option "Aus Zeitpunkt in virtuellen Computer konvertieren" steht erst dann zur Auswahl zur Verfügung, nachdem Sie mindestens ein vollständiges Backup ausgeführt haben, das sämtliche kritischen Systemkomponenten umfasst.

Die Option zur Konvertierung aus einem Zeitpunkt in einen virtuellen Computer ist bei der Notfallwiederherstellung nützlich, wenn ein ausgefallener Server schnell wiederhergestellt werden muss. Die Backup-Sätze enthalten alle notwendigen Komponenten des Systems. Zusätzlich können Sie Anwendungsdaten oder Benutzerdaten auswählen, um in die Konvertierung einzuschließen.

So konvertieren Sie aus einem Zeitpunkt in einen virtuellen Computer

- 1** Auf der Registerkarte "Backup und Wiederherstellung" wählen Sie den Server aus, der die Backup-Sätze enthält, die Sie konvertieren möchten.
- 2** Klicken Sie in der Gruppe "Konvertierungen" auf "In virtuellen Datenträger konvertieren" und klicken Sie dann auf "Aus Zeitpunkt in virtuellen Computer konvertieren".
- 3** Klicken Sie im Dialogfeld "Optionen" im Feld "Ausgewählter Zeitpunkt" auf "Bearbeiten".
- 4** Wählen Sie die Elemente, die Sie in die Konvertierung einschließen möchten, aus und klicken Sie dann auf "OK".
- 5** Klicken Sie im Dialogfeld "Optionen" im Feld "In virtuell konvertieren" auf "Bearbeiten".
- 6** Im linken Teilfenster wählen Sie "Planen", um auszuwählen, wann der Konvertierungsauftrag ausgeführt werden soll:

So führen Sie den Auftrag sofort aus

Klicken Sie auf "Jetzt ausführen".

So planen Sie die Konvertierung zu einem spezifischen Zeitpunkt

Klicken Sie auf "Ausführen am" und geben Sie Datum und Uhrzeit zum Ausführen des Auftrags ein.

So erstellen Sie den Konvertierungsauftrag, ohne ihn zu planen

Wählen Sie "Ohne Zeitplan erstellen". Wenn Sie diese Option verwenden, wird der Auftrag nicht zum Zeitpunkt der Erstellung ausgeführt und hat keinen wiederkehrenden Zeitplan. Der Auftrag verbleibt im Zustand "ausstehend", bis Sie ihn ausführen. Sie können ein Auftragsautomatisierungs- oder -Planungs-Tool eines anderen Herstellers verwenden, um den Auftrag später auszuführen.

- 7 (Optional) Wählen Sie im linken Teilfenster "Benachrichtigung", wenn Sie einen Empfänger benachrichtigen möchten, sobald der Auftrag abgeschlossen wurde.
- 8 Klicken Sie im linken Teilfenster auf "Konvertierungseinstellungen", um Optionen für die Konvertierung einzustellen.
- 9 Wählen Sie im Feld "Zeitpunkt" aus, wann die Konvertierung ausgeführt werden soll.
- 10 Wählend Sie im Feld "Name" alle Komponenten, die Sie in die Konvertierung einschließen möchten.
- 11 Im Feld "Anwendungsdaten oder systemunabhängige Benutzerdaten" wählen Sie zusätzliche in die Konvertierung einzuschließende Daten aus.
- 12 Klicken Sie auf "OK", um Ihre Einstellungen zu speichern.
- 13 Klicken Sie im Dialogfeld "Optionen" auf "OK".

Erstellen einer einmaligen Konvertierung in einen virtuellen Computer

Sie können einen einmaligen Konvertierungsauftrag erstellen, um einen laufenden physischen Computer in einen virtuellen Computer ohne separaten Backup-Auftrag zu konvertieren. Ein einmaliger Konvertierungsauftrag kann für einen späteren Zeitpunkt geplant, aber nur einmal ausgeführt werden.

Bei diesem Konvertierungstyp werden nur vollständige Backups unterstützt. Inkrementelle und Differenzial-Backups werden bei der einmaligen Konvertierung nicht unterstützt.

Hinweis: Kopier-Backups werden unter Hyper-V 2008 oder 2008 R2 nicht unterstützt. Stattdessen wird eine absturzkonsistente Konvertierung erstellt.

So erstellen Sie eine einmalige Konvertierung in einen virtuellen Computer

- 1 Auf der Registerkarte "Backup und Wiederherstellung" wählen Sie den Server aus, den Sie in einen virtuellen Computer konvertieren möchten.
- 2 Klicken Sie in der Gruppe "Konvertierungen" auf "In virtuellen Datenträger konvertieren" und klicken Sie dann auf "Einmalig in virtuellen Computer konvertieren".
- 3 Klicken Sie im Dialogfeld "Einmalig in virtuellen Computer konvertieren - Eigenschaften" im Feld "In virtuellen Datenträger konvertieren " auf "Bearbeiten".

- 4** Wählen Sie im linken Teilfenster "Planen" aus, um auszuwählen, wann der Konvertierungsauftrag ausgeführt werden soll:

So führen Sie den Auftrag sofort aus Klicken Sie auf "Jetzt ausführen".

So planen Sie die Konvertierung zu einem spezifischen Zeitpunkt Klicken Sie auf "Ausführen am" und geben Sie Datum und Uhrzeit zum Ausführen des Auftrags ein.

So erstellen Sie den Konvertierungsauftrag, ohne ihn zu planen Wählen Sie "Ohne Zeitplan erstellen".
Wenn Sie diese Option verwenden, wird der Auftrag nicht zum Zeitpunkt der Erstellung ausgeführt und hat keinen wiederkehrenden Zeitplan. Der Auftrag verbleibt im Zustand "ausstehend", bis Sie ihn ausführen. Sie können ein Auftragsautomatisierungs- oder Aufgabenplanungs-Tool eines anderen Herstellers verwenden, um den Auftrag später auszuführen.

- 5** (Optional) Wählen Sie im linken Teilfenster "Benachrichtigung", wenn Sie einen Empfänger benachrichtigen möchten, sobald der Auftrag abgeschlossen wurde.
- 6** Klicken Sie im linken Teilfenster auf Konvertierungseinstellungen, um Optionen für die Konvertierung einzustellen.
- 7** Wählen Sie im Feld "Konvertieren für" entweder "Hyper-V" oder "VMware ESX/vCenter-Server" aus.
- 8** Konfigurieren Sie die Konvertierungsoptionen:

Wenn Sie in Schritt 7 "Hyper-V"
auswählen

So konfigurieren Sie die Konvertierungsoptionen

- Klicken Sie im Feld "Hyper-V-Servername", wählen Sie den Namen des Servers, in dem Sie den virtuellen Computer erstellen möchten, aus und klicken Sie dann auf "Hinzufügen".
- Geben Sie im Feld "Ziellaufwerk oder Pfad" den Speicherort auf dem physischen Computer ein, in dem die virtuellen Datenträger erstellt werden sollen. Geben Sie einen Laufwerksbuchstaben und einen Pfad ein.
- Wenn Sie den Standardnamen des virtuellen Computers ändern möchten, geben Sie den neuen Namen im Feld "Name des virtuellen Computers" ein.
- Soll Backup Exec einen virtuellen Computer überschreiben können, wenn bereits ein virtueller Computer mit dem gleichen Namen existiert, stellen Sie sicher, dass die Option "Virtuellen Computer überschreiben, wenn bereits vorhanden" ausgewählt ist. Falls diese Option nicht aktiviert ist und der Name des virtuellen Computers bereits vorhanden ist, schlägt der Auftrag fehl.
- Geben Sie im Feld "Vollständiger Pfad des ISO-Image von Hyper-V Integration Components" den Speicherort ein. Das ISO-Image ist erforderlich, um den virtuellen Computer startfähig zu machen.

Hinweis: Diese Option ist nicht für Hyper-V-Server mit Windows Server 2016 oder höher verfügbar. Solche Hyper-V-Server installieren Integrationsdienste direkt auf dem virtuellen Computer entweder über ein Windows-Update oder durch Herunterladen durch den Benutzer.

- Wenn Sie die Anzahl der CPUs oder die Größe des RAM für den virtuellen

Zielcomputer ändern möchten, geben Sie auf der Registerkarte

"Serverkonfiguration" unter "Virtueller Zielcomputer" die neuen Werte ein.

- Wenn Sie den Typ, den Controller oder den Speicherort eines virtuellen Datenträgers ändern möchten, klicken Sie auf der Registerkarte "Datenträgerkonfiguration" auf "Datenträgerkonfiguration bearbeiten" und geben dann die neuen Werte ein.

Wenn Sie in Schritt 7 "VMware
ESX/vCenter-Server" ausgewählt haben

So konfigurieren Sie die Konvertierungsoptionen

- Klicken Sie im Feld "ESX/vCenter-Servername" auf den Pfeil und dann auf den Namen des Servers, auf dem der virtuelle Computer erstellt werden soll.
- Klicken Sie auf den Pfeil im Feld "Login-Konto" und wählen Sie dann das entsprechende Login-Konto für den ausgewählten Server aus.
- Klicken Sie neben dem Feld "ESX-/vCenter-Servername" auf "Auswählen". Backup Exec füllt die restlichen Informationen über den Server aus.
- Wählen Sie den Ordner für den virtuellen Computer und den Ressourcenpool aus, die mit dem ausgewählten Server verknüpft sind.

Hinweis: Wenn Sie einen ESX-Server als Ziel auswählen und einen Ressourcenpool auswählen, wird der neu erstellte virtuelle Computer nicht automatisch dem Ressourcenpool hinzugefügt. Sie können nach der Konvertierung den virtuellen Computer manuell in den geeigneten Ressourcenpool verschieben.

- Wenn Sie den Standardnamen des virtuellen Computers ändern möchten, geben Sie den neuen Namen im Feld "Name des virtuellen Computers" ein.
- Soll Backup Exec einen virtuellen Computer überschreiben können, wenn bereits ein virtueller Computer mit dem gleichen Namen existiert, stellen Sie sicher, dass die Option "Virtuellen Computer überschreiben, wenn bereits vorhanden" ausgewählt ist. Falls diese Option nicht aktiviert ist und der Name des virtuellen Computers bereits vorhanden ist, schlägt der Auftrag fehl.
- Geben Sie im Feld "Vollständiger Pfad des ISO-Image von VMware Tools" den

Speicherort ein. Der Pfad sollte mit den Standardidentifikationsdaten zugänglich sein. Der Pfad muss auf einen lokalen Datenträger des Backup Exec-Servers verweisen. Das ISO-Image ist erforderlich, um den virtuellen Computer startfähig zu machen.

Hinweis: In einer CAS-Umgebung sollte dieser Pfad lokal zum verwalteten Backup Exec-Server sein, den der Auftrag zum Ziel hat.

- Wenn Sie die Anzahl der CPUs oder die Größe des RAM für den virtuellen Zielcomputer ändern möchten, geben Sie auf der Registerkarte "Serverkonfiguration" unter "Virtueller Zielcomputer" die neuen Werte ein.
- Wenn Sie den Typ, den Controller oder den Speicherort eines virtuellen Datenträgers ändern möchten, klicken Sie auf der Registerkarte "Datenträgerkonfiguration" auf "Datenträgerkonfiguration bearbeiten" und geben dann die neuen Werte ein.

9 Klicken Sie auf "OK", um Ihre Einstellungen zu speichern.

10 Klicken Sie im Dialogfeld "Einmalig in virtuellen Computer konvertieren - Eigenschaften" auf "OK".

Siehe ["Funktionsweise der Konvertierung eines physischen Computers in einen virtuellen in Backup Exec"](#) auf Seite 581.

Einstellungsstandardoptionen für die Konvertierung in Aufträge für virtuelle Computer

Sie können Standardoptionen für alle Konvertierungen für Aufträge des virtuellen Computers festlegen. Sie können jedoch die Standardoptionen für einzelne Aufträge überschreiben.

So legen Sie Standardoptionen für die Konvertierung in Aufträge für virtuelle Computer fest

- 1** Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- 2** Wählen Sie "Auftragsstandardeinstellungen" und dann "In virtuellen Datenträger konvertieren".
- 3** Wählen Sie die Standard-Zeitplanoptionen aus, die bei der Konvertierung in virtuelle Aufträge verwendet werden sollen.

So planen Sie die Ausführung der Konvertierung in virtuelle Aufträge zu einem spezifischen Zeitpunkt

Gehen Sie wie folgt vor:

- Wählen Sie "Nach Zeitplan".
- Klicken Sie auf den Pfeil im Feld "Quelle", um entweder alle Backups oder das aktuellste vollständige Backup als Quelle für die Konvertierung auszuwählen.
- Wählen Sie "Wiederkehrend" und dann den Pfeil zum Festlegen des Wiederholungsmusters aus.

So erstellen Sie eine Konvertierung in virtuelle Aufträge, ohne sie zu planen

Gehen Sie wie folgt vor:

- Wählen Sie "Nach Zeitplan".
- Klicken Sie auf den Pfeil im Feld "Quelle", um entweder alle Backups oder das aktuellste vollständige Backup als Quelle für die Konvertierung auszuwählen.
- Wählen Sie "Ohne Zeitplan erstellen". Wenn Sie diese Option verwenden, wird der Auftrag nicht zum Zeitpunkt der Erstellung ausgeführt und hat keinen wiederkehrenden Zeitplan. Der Auftrag verbleibt im Zustand "ausstehend", bis Sie ihn ausführen. Sie können ein Auftragsautomatisierungs- oder Aufgabenplanungs-Tool eines anderen Herstellers verwenden, um den Auftrag später auszuführen.

So führen Sie die Konvertierung sofort nach Abschluss des Backup-Auftrags aus

Wählen Sie "Sofort nach Abschluss der Quellaufgabe virtuell konvertieren".

- 4** (Optional) Wählen Sie im linken Teilfenster "Benachrichtigung", und wählen Sie dann die Empfänger aus, die Benachrichtigungen über Konvertierungen in virtuelle Aufträge erhalten sollen.
- 5** Wählen Sie im linken Teilfenster "Konvertierungseinstellungen".
- 6** Wählen Sie im Feld "Konvertieren für" entweder "Hyper-V" oder "VMware ESX/vCenter-Server" aus.
- 7** Konfigurieren Sie die Konvertierungsoptionen:

Wenn Sie in Schritt 6 "Hyper-V" ausgewählt haben

So konfigurieren Sie die Konvertierungsoptionen

- Klicken Sie auf den Pfeil im Feld "Hyper-V-Servername", wählen Sie den Namen des Servers aus, auf dem die virtuellen Computer erstellt werden sollen, und klicken Sie dann auf "Hinzufügen".
- Geben Sie im Feld "Ziellaufwerk oder Pfad" den Speicherort auf dem physischen Computer ein, in dem die virtuellen Datenträger erstellt werden sollen. Geben Sie einen Laufwerksbuchstaben und einen Pfad ein.
- Soll Backup Exec einen virtuellen Computer überschreiben können, wenn bereits ein virtueller Computer mit dem gleichen Namen existiert, stellen Sie sicher, dass die Option "Virtuellen Computer überschreiben, wenn bereits vorhanden" ausgewählt ist. Falls diese Option nicht aktiviert ist und der Name des virtuellen Computers bereits vorhanden ist, schlägt der Auftrag fehl.
- Geben Sie im Feld "Vollständiger Pfad des ISO-Image von Hyper-V Integration Components" den Speicherort ein. Das ISO-Image ist erforderlich, um den virtuellen Computer startfähig zu machen.

Hinweis: Diese Option ist nicht für Hyper-V-Server mit Windows Server 2016 oder höher verfügbar. Solche Hyper-V-Server installieren Integrationsdienste direkt auf dem virtuellen Computer entweder über ein Windows-Update oder durch Herunterladen durch den Benutzer.

Wenn Sie in Schritt 6 "VMware ESX/vCenter-Server" ausgewählt haben

So konfigurieren Sie die Konvertierungsoptionen

- Klicken Sie im Feld "ESX/vCenter-Servername" auf den Pfeil und dann auf den Namen des Servers, auf dem die virtuellen Computer erstellt werden sollen.
- Klicken Sie auf den Pfeil im Feld "Login-Konto" und wählen Sie dann das entsprechende Login-Konto für den ausgewählten Server aus.
- Soll Backup Exec einen virtuellen Computer überschreiben können, wenn bereits ein virtueller Computer mit dem gleichen Namen existiert, stellen Sie sicher, dass die Option "Virtuellen Computer überschreiben, wenn bereits vorhanden" ausgewählt ist. Falls diese Option nicht aktiviert ist und der Name des virtuellen Computers bereits vorhanden ist, schlägt der Auftrag fehl.
- Geben Sie im Feld "Vollständiger Pfad des ISO-Image von VMware Tools" den Speicherort ein. Der Pfad sollte mit den Standardidentifikationsdaten zugänglich sein. Der Pfad muss auf einen lokalen Datenträger des Backup Exec-Servers verweisen. Das ISO-Image ist erforderlich, um den virtuellen Computer startfähig zu machen.

Hinweis: In einer CAS-Umgebung sollte dieser Pfad lokal zum verwalteten Backup Exec-Server sein, den der Auftrag zum Ziel hat.

8 Klicken Sie auf "OK".

Konfiguration und Einstellungen

In diesem Kapitel werden folgende Themen behandelt:

- Ändern der Standardeinstellungen für Backup-Aufträge
- Konfigurieren von Zeitplänen für Backup-Jobs
- Konfigurieren von Speicheroptionen für Backup-Aufträge
- Konfigurieren automatischer Testlaufaufträge für Backup-Aufträge
- Konfigurieren der automatischen Prüfung von Aufträgen
- Konfigurieren der Optionen für Instant GRT und Vollständige Katalogisierung zum Verbessern der Backup-Leistung von GRT-Aufträgen
- Konfigurieren von Advanced Open File-Optionen für Backup-Aufträge
- Konfigurieren der Auftragswiederaufnahme
- Konfigurieren von Befehlen vor oder nach Backup-Aufträgen
- Konfigurieren von Datei- und Ordneroptionen für Backup-Aufträge
- Standardmäßige Zeitplanoptionen für richtliniengesteuerte Aufträge und für Aufträge zum sofortigen Ausführen einstellen
- Ausschließen von Tagen vom Backup-Zeitplan für alle Backups
- Entfernen von Daten aus der Liste ausgeschlossener Tage
- Exportieren einer Liste von Daten, die aus allen Backups auf einem anderen Server ausgeschlossen sind
- Ändern der Standardeinstellungen

- Konfigurieren der Standardeinstellungen zum Sichern mehrerer Server oder Anwendungen
- Konfigurieren der Datenbankverwaltung und -sicherheit
- Exportieren des Backup Exec-Datenbankverschlüsselungscodes
- Aktualisieren von Backup Exec-Datenbankverschlüsselungscodes
- Konfigurieren der Verschlüsselung für die Verbindung zur Backup Exec-Datenbank
- Planen der Prüfung von Login-Konten durch Backup Exec
- Konfigurieren von Backup Exec, um Daten für Backup zu suchen
- Hinzufügen gefundener Server zur Liste von Servern in Backup Exec
- Backup-Netzwerke
- Netzwerk- und Sicherheitsoptionen für Backup Exec ändern
- Verwendung von Backup Exec mit Firewalls
- Verwendung von Verschlüsselung mit Backup Exec
- Verwaltung von Verschlüsselungscodes
- Erstellen von Verschlüsselungscodes
- Ersetzen eines Verschlüsselungscodes
- Löschen des Verschlüsselungsschlüssels
- Granular Recovery Technology
- Festlegen von Standardoptionen für Granular Recovery Technology festlegen (GRT)
- DBA-initiierte Auftragsvorlagen
- Erstellen DBA-initiiertter Auftragsvorlagen
- Bearbeiten von von DBA gestarteten Auftragsvorlagen
- Löschen von DBA-initiierten Auftragsvorlagen
- Konfigurieren der Einstellungen für Veritas™ Information Map
- Backup Exec-Login-Konten
- Starten und Anhalten von Backup Exec-Diensten

- Ändern der Identifikationsdaten für ein Dienstkonto
- Ändern der Startoptionen für Backup Exec-Dienste
- Konfigurieren von Überwachungsprotokollen
- Anzeigen des Überwachungsprotokolls
- Entfernen von Einträgen aus dem Überwachungsprotokoll
- Speichern eines Überwachungsprotokolls in einer Textdatei
- Kopieren von Konfigurationseinstellungen auf einen anderen Backup Exec-Server
- Anzeigen von Servereigenschaften
- Konfigurieren der Standardeinstellungen für das Backup

Ändern der Standardeinstellungen für Backup-Aufträge

Backup Exec wird mit Standardeinstellungen für Backup-Aufträge vorkonfiguriert. Sie können die Standardeinstellungen für Ihre Backup-Aufträge ändern. Wenn Sie einen Backup-Auftrag erstellen, wird dieser mit den von Ihnen konfigurierten Standardeinstellungen ausgeführt. Sie können die Standardeinstellungen übergehen, indem Sie sie beim Erstellen neuer Backup-Aufträge ändern. Zu den Einstellungen für Backup-Aufträge gehören u. a. Speicher-, Sicherheits- und Dateisystemoptionen für Backup-Aufträge.

Für die folgenden Typen von Backup-Aufträgen können individuelle Standardeinstellungen festgelegt werden:

- Auf Deduplizierungsspeichergerät sichern
- Backup-to-Disk
- Auf Band sichern
- Auf Deduplizierungsspeichergerät duplizieren
- Auf Band duplizieren
- Auf Cloud duplizieren
- In virtuellen Datenträger konvertieren

Hinweis: Backup Exec zeigt nur die Typen von Backup-Aufträgen an, für die Ihr System konfiguriert ist. Wenn Sie z. B. kein Bandlaufwerk haben, wird die Option "Auf Band sichern" nicht in der Liste der Typen von Backup-Aufträgen angezeigt.

So ändern Sie die Standardeinstellungen für Backup-Aufträge

- 1** Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und dann "Auftragsstandardeinstellungen".
- 2** Wählen Sie den Backup-Typ aus, für den Sie Standardoptionen einstellen möchten.

Beispiel: Wenn Sie die Standardoptionen für Backup-to-Disk einrichten möchten, wählen Sie "Backup-to-Disk". Die Optionen, die angezeigt werden, hängen von den konfigurierten Speichergerätetypen ab. Verschiedene Standardoptionen können für Backup-Aufträge auf verschiedenen Speichertypen konfiguriert werden.

3 Wählen Sie im linken Teilfenster die Einstellung, für die Sie Standardoptionen konfigurieren möchten.

Planen	<p>Wählen Sie diese Option aus, um die Standardeinstellungen von Zeit und Häufigkeit, mit der Backup-Aufträge ausgeführt werden, zu konfigurieren.</p> <p>Siehe "Konfigurieren von Zeitplänen für Backup-Jobs" auf Seite 635.</p>
Speicher	<p>Wählen Sie diese Option aus, um die Standardeinstellungen für das Speichergerät, das sie für Backup-Aufträge nutzen wollen, zu konfigurieren.</p> <p>Siehe "Konfigurieren von Speicheroptionen für Backup-Aufträge" auf Seite 645.</p>
Benachrichtigung	<p>Wählen Sie diese Option aus, um Backup Exec zur Benachrichtigung bestimmter Empfänger bei Abschluss eines Backup-Auftrags zu konfigurieren.</p> <p>Für jeden Backup-Auftrag können verschiedene Benachrichtigungsempfänger konfiguriert werden. Backup Exec kann Empfänger per E-Mail oder SMS benachrichtigen.</p> <p>Siehe "Benachrichtigungsoptionen für Aufträge" auf Seite 357.</p>
Probelauf	<p>Wählen Sie diese Option aus, um einen Testauftrag zu konfigurieren, der automatisch Speicherkapazität, Identifikationsdaten und Medienintegrität prüft.</p> <p>Der Testauftrag hilft Ihnen beim Feststellen von Problemen, die Backup-Aufträge möglicherweise davon abhalten, erfolgreich abzuschließen.</p> <p>Siehe "Konfigurieren automatischer Testlaufaufträge für Backup-Aufträge" auf Seite 653.</p>
Überprüfen	<p>Wählen Sie diese Option aus, um einen Auftrag zu erstellen, der nach Abschluss von Aufträgen automatisch überprüft, ob alle Daten erfolgreich gesichert wurden.</p> <p>Ein Überprüfungsauftrag unterstützt Sie beim Festlegen, ob die verwendeten Medien defekt sind.</p> <p>Siehe "Konfigurieren der automatischen Prüfung von Aufträgen" auf Seite 655.</p>

Instant GRT	<p>Wählen Sie diese Option aus, um den Vorgang Instant GRT oder Vollständige Katalogisierung für einen GRT-fähigen Auftrag zu konfigurieren. Sie können die vollständige Katalogisierung sofort nach Abschluss des Backup-Auftrags ausführen, für einen späteren Zeitpunkt planen oder im Rahmen des Backup-Auftrags einen Instant GRT-Vorgang durchführen.</p> <p>Siehe "Konfigurieren der Optionen für Instant GRT und Vollständige Katalogisierung zum Verbessern der Backup-Leistung von GRT-Aufträgen" auf Seite 656.</p>
Advanced Open File	<p>Wählen Sie diese Option aus, um die Snapshot-Einstellungen zu konfigurieren, die Backup Exec zum Durchführen von Backup-Aufträgen anwendet. Mit der Snapshot-Technologie kann Backup Exec alle Dateien erfassen, die geöffnet sind, wenn ein Backup ausgeführt wird.</p> <p>Sie können auch die Auftragswiederaufnahme aktivieren, mit der Sie unterbrochene Backup-Aufträge fortsetzen können.</p> <p>Siehe "Konfigurieren von Advanced Open File-Optionen für Backup-Aufträge" auf Seite 664.</p> <p>Siehe "Konfigurieren der Auftragswiederaufnahme" auf Seite 667.</p>
Advanced Disk-based Backup	<p>Wählen Sie diese Option aus, um die eine Off-Host-Backup-Verarbeitung für Backup-Aufträge zu konfigurieren.</p> <p>Siehe "Festlegen der Standard-Backup-Optionen für Advanced Disk Based Backup Feature" auf Seite 1522.</p>
Befehle vor/nach dem Auftrag	<p>Wählen Sie diese Option aus, um beliebige Befehle zu konfigurieren, die Sie vor dem Beginn oder nach dem Abschluss von Backup-Aufträgen ausführen wollen.</p> <p>Siehe "Konfigurieren von Befehlen vor oder nach Backup-Aufträgen" auf Seite 670.</p>
Dateien und Ordner	<p>Wählen Sie diese Option aus, um die Verarbeitung von Dateisystemattributen, wie zum Beispiel von Abzweigungen und symbolischen Links, zu konfigurieren.</p> <p>Siehe "Konfigurieren von Datei- und Ordneroptionen für Backup-Aufträge" auf Seite 676.</p>

Enterprise Vault	<p>Wählen Sie diese Option aus, um Enterprise Vault-Optionen für Backup-Aufträge zu konfigurieren.</p> <p>Siehe "Backup-Optionen für Enterprise Vault" auf Seite 1397.</p>
Linux und Macintosh	<p>Wählen Sie diese Option aus, um Optionen für alle Linux- oder Macintosh-Computer zu konfigurieren, die in Backup-Aufträgen integriert sind.</p> <p>Siehe "Linux-Backup-Optionen" auf Seite 1579.</p>
Microsoft Active Directory	<p>Wählen Sie diese Option aus, um Optionen für beliebige Microsoft Active Directory-Daten zu konfigurieren, die in Backup-Aufträgen integriert sind.</p> <p>Siehe "Optionen für Active Directory und ADAM/AD LDS-Backup-Aufträge bearbeiten" auf Seite 1442.</p>
Microsoft Exchange	<p>Wählen Sie diese Option aus, um Optionen für beliebige Microsoft Exchange-Daten zu konfigurieren, die in Backup-Aufträgen integriert sind.</p> <p>Siehe "Festlegen von Standard-Backup-Optionen für Exchange Server" auf Seite 1302.</p>
Virtuelle Computer	<p>Wählen Sie diese Option aus, um Optionen für alle virtuellen Computer zu konfigurieren, die in Backup-Aufträgen integriert sind.</p> <p>Siehe "Festlegen von Backup-Standardoptionen für virtuelle Computer" auf Seite 1109.</p> <p>Siehe "Festlegen der Standard- Backup-Optionen für Hyper-V" auf Seite 1175.</p>
Microsoft SharePoint	<p>Wählen Sie diese Option aus, um Optionen für beliebige Microsoft SharePoint-Daten zu konfigurieren, die in Backup-Aufträgen integriert sind.</p> <p>Siehe "Festlegen der Standard-Backup-Optionen für SharePoint" auf Seite 1326.</p>
Microsoft SQL	<p>Wählen Sie diese Option aus, um Optionen für beliebige Microsoft SQL-Daten zu konfigurieren, die in Backup-Aufträgen integriert sind.</p> <p>Siehe "Festlegen der Standard-Backup-Optionen für SQL Server" auf Seite 1244.</p>

NDMP	<p>Wählen Sie diese Option aus, um Optionen für beliebige NDMP-Daten zu konfigurieren, die in Backup-Aufträgen integriert sind.</p> <p>Siehe "NDMP-Backup-Optionen für NDMP-Server" auf Seite 1543.</p>
Oracle	<p>Wählen Sie diese Option aus, um Optionen für beliebige Oracle-Daten zu konfigurieren, die in Backup-Aufträgen integriert sind.</p> <p>Siehe "Backup-Optionen für Oracle" auf Seite 1367.</p>
Ausschlüsse	<p>Wählen Sie diese Option aus, um bestimmte Dateien oder bestimmte Dateitypen aus Backup-Aufträgen ein- oder auszuschließen.</p> <p>Siehe "Ausschließen von Dateien von Backups" auf Seite 195.</p>

- 4 Wählen Sie die entsprechenden Optionen aus.
- 5 Wenn Sie fertig sind, klicken Sie auf OK.

Konfigurieren von Zeitplänen für Backup-Jobs

Mit Exec können Sie Zeitpunkt und Häufigkeit für Backup-Aufträge konfigurieren. Sie können Aufträge sofort, einmalig an einem bestimmten Tag und zu einer bestimmten Uhrzeit oder mehrmals gemäß einem Zeitplan ausführen. Mit Backup Exec können Sie ein Wiederholungsmuster für den Zeitplan mit Minuten, Stunden, Tagen, Wochen, Monaten oder Jahren als Messeinheit erstellen. Alternativ können Sie bestimmte Tage im Monat auswählen, um einen wiederkehrenden Zeitplan zu erstellen, nach dem Aufträge ausgeführt werden sollen.

Siehe "[Wie die Joborganisation in Backup Exec arbeitet](#)" auf Seite 239.

Sie können Standardoptionen für Zeitpläne konfigurieren, die Ihre Aufträge beim Erstellen übernehmen. Oder Sie können die Standardzeitplaneinstellungen überschreiben, wenn Sie Aufträge erstellen.

So konfigurieren Sie Zeitpläne für Jobs

- 1 Sie haben folgende Möglichkeiten:

Um Nichterfüllung zu konfigurieren planen Sie Einstellungen für alle Backup-Jobs ein

- Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- Wählen Sie "Auftragsstandardeinstellungen" aus und wählen Sie dann den Backup-Typ aus, für den Sie Zeitplanoptionen konfigurieren möchten.

So konfigurieren Sie einen Zeitplan für spezifische Backup-Jobs

- Erstellen Sie eine neue Backup-Definition oder bearbeiten Sie eine vorhandene Backup-Definition.
- Klicken Sie im Dialogfeld "Backup" auf "Bearbeiten".

2 Klicken Sie im linken Teilfenster auf "Planen".

3 Geben Sie im Feld "Auftragsvorlagenname" den Namen der Auftragsvorlage ein, für die Sie einen Zeitplan konfigurieren möchten.

Auftragsvorlagen sind die Sammlung von Einstellungen, die Backup Exec verwendet, um Aufträge zu erstellen. Die Einstellungen für Backup-Aufträge können beispielsweise Planungsoptionen, Optionen für Speichergeräte oder Backup-Methoden für ausgewählte Datentypen umfassen. Wenn Sie ein Backup ausführen möchten, kombiniert Backup Exec die Auftragsvorlage mit der Backup-Auswahl, um einen Backup-Auftrag zu erstellen, der dann entsprechend der von ihnen angegebenen Optionen ausgeführt wird.

Der Auftragsvorlagenname, den Sie in diesem Feld eingeben, wird zum Erstellen des Auftragsnamen verwendet.

4 Geben Sie im Feld "Auftragsname" den Namen des Auftrags ein, für den Sie einen Zeitplan konfigurieren möchten.

Mit dem eindeutigen Auftragsname können Sie Backup-Aufträge in Backup Exec identifizieren. Diese Einstellung ist nur pro Auftrag verfügbar und kann nicht als Standardeinstellung für Backup-Aufträge festgelegt werden.

5 Für jeden Auftrag, für den Sie einen Zeitplan konfigurieren möchten, gehen Sie wie folgt vor:

So konfigurieren Sie wiederkehrende Jobs

Führen Sie die folgenden Schritte durch:

- Wählen Sie "Wiederkehrend" aus.
- Gehen Sie zu Schritt 6 über, das Wiederauftretenmuster zu konfigurieren.

Um Jobs zu konfigurieren, ohne beliebige Wiederauftreten sofort ausgeführt zu werden

Führen Sie die folgenden Schritte durch:

- Wählen Sie "Jetzt ohne regelmäßigen Zeitplan ausführen" aus.
- Fahren Sie mit Schritt 9 fort.

Hinweis: Diese Option ist nur für vollständige Backup-Aufträge verfügbar.

So konfigurieren Sie einen Job ohne einen Zeitplan

Führen Sie die folgenden Schritte durch:

- Wählen Sie "Ohne Zeitplan erstellen".
- Fahren Sie mit Schritt 10 fort.

Wenn Sie diese Option verwenden, werden die Jobs nicht zu der Zeit der Schaffung ausgeführt und sie haben keinen wiederkehrenden Zeitplan. Die Jobs bleiben ungeplant, bis Sie beschließen, sie auszuführen. Sie können ein Drittanbieter-Tool zur automatischen Auftragsausführung oder -planung verwenden, um den Auftrag später auszuführen.

Sie können ungeplante Backup-Aufträge später ausführen, indem Sie die Option "Nächstes Backup jetzt ausführen" verwenden oder Sie können den Auftrag mit der Option "Jetzt ausführen" manuell ausführen.

Wenn Sie diese Option zum Erstellen eines Auftrag verwenden, können Sie den Auftrag nicht anhalten. Sie können Aufträge nicht anhalten, es sei denn, dass sie geplant werden.

- 6 Um das Wiederauftretenmuster zu konfigurieren, schließen Sie die folgenden Optionen ab:

Stunden

Wählen Sie diese Option aus, um ein Wiederauftretensmuster zu erstellen, das in Stunden oder Minuten gemessen wird.

Wenn Sie "Stunden" auswählen, können Sie folgende Optionen konfigurieren:

- Alle X Stunden/Minuten
Gibt die Anzahl von Stunden oder Minuten zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz an.
- Sie müssen zwischen den folgenden Optionen auswählen:
 - Von
Gibt die Startzeit eines Auftrags an.
 - Zwischen
Schränkt den Auftrag auf bestimmte Stunden und Tage ein. Beispiel: Wenn der Auftrag nur während der Geschäftszeiten ausgeführt werden soll, können Sie 9:00 bis 17:00 Uhr am Montag, Dienstag, Mittwoch, Donnerstag und Freitag auswählen.
Die Start- und Endzeit können maximal 24 Stunden auseinander liegen, doch sie können sich über Mitternacht in den folgenden Tag hinein überschneiden.

Tage

Wählen Sie diese Option aus, um ein Wiederauftretensmuster zu erstellen, das in Tage gemessen wird.

Wenn Sie "Tage" auswählen, müssen Sie zwischen den folgenden Optionen auswählen:

- Alle X Tage
Gibt die Anzahl von Tagen zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz an.
- Jeden Wochentag
Wählen Sie diese Option aus, um den Job zu aktivieren, an Montagen, an Dienstagen, an Mittwochen, an Donnerstagen und an Freitag ausgeführt zu werden.

Wochen

Wählen Sie diese Option aus, um ein Wiederauftretenmuster zu erstellen, das in Wochen gemessen wird.

Wenn Sie ein Wiederholungsmuster erstellen, das in Wochen gemessen wird, müssen Sie das Feld "Alle X Wochen am" konfigurieren. Das Feld "Alle X Wochen am" gibt die Anzahl von Wochen zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz an. Es gibt außerdem die Wochentage an, an denen der Auftrag ausgeführt werden soll.

Monate

Wählen Sie diese Option aus, um ein Wiederauftretenmuster zu erstellen, das in Monate gemessen wird.

Wenn Sie "Monate" auswählen, müssen Sie zwischen den folgenden Optionen auswählen:

- **Tag X jedes X. Monats**
 Gibt den Tag an, an dem der Auftrag aufgeführt werden soll. Gibt die Anzahl von Tagen zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz an.
- **Jeden X X jedes X. Monats**
 Gibt den Tag an, an dem der Auftrag aufgeführt werden soll. Gibt die Anzahl von Tagen zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz an.
- **Ausgewählte Monatstage**
 Gibt die bestimmten Tage des Monats an, an denen Backup Exec den Auftrag ausführt. Sie wählen die Tage und die Wochen auf einem Raster aus. Das ausgewählte Wiederholungsmuster wird jeden Monat wiederholt.
 Standardmäßig wird der Auftrag jeden Monat ausgeführt und beginnt in der aktuellen Woche und am aktuellen Tag des Monats. Wenn Sie den Auftrag am dritten Montag im Monat erstellen, wird der Auftrag standardmäßig am dritten Montag jedes Monats ausgeführt.
 Sie können den Standard ändern oder zusätzliche Tage auswählen, an denen der Auftrag ausführen sollte. Wenn der Auftrag beispielsweise am letzten Freitag jedes Monats ausgeführt werden soll, wählen Sie das Kontrollkästchen für Freitag in der letzten Reihe des Rasters aus. Alle zusätzlich ausgewählten Tage werden dem monatlichen Wiederholungsmuster hinzugefügt.
- **Ausgewählte Monatstage**
 Gibt die Tage des Monats an, an denen Backup Exec den Auftrag ausführt. Das ausgewählte Wiederholungsmuster wird jeden Monat wiederholt.
 Standardmäßig wird der Auftrag jeden Monat ausgeführt und beginnt am aktuellen Tag des Monats. Wenn Sie den Auftrag am 15. April erstellen, wird der Auftrag standardmäßig am 15. jedes Monats ausgeführt.

Sie können den Standard ändern oder zusätzliche Tage auswählen, an denen der Auftrag ausführen sollte. Wenn der Auftrag beispielsweise am 1. und am 15. jedes Monats ausgeführt werden soll, wählen Sie im Kalender nur diese Daten aus. Alle zusätzlich ausgewählten Tage werden dem monatlichen Wiederholungsmuster hinzugefügt.

Wenn Sie den 31. auswählen, wird der Auftrag in Monaten, die keine 31 Tage haben, am letzten Tag des Monats ausgeführt. Wenn Sie den Auftrag beispielsweise so konfigurieren, dass er am 31. ausgeführt wird, wird er im September stattdessen am 30. ausgeführt.

Jahre

Wählen Sie diese Option aus, um ein Wiederauftretensmuster zu erstellen, das in Jahre gemessen wird.

Wenn Sie "Jahre" auswählen, können Sie die folgenden Optionen konfigurieren:

- **Alle X Jahre**
 Gibt die Anzahl von Jahren zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz an.
- **Sie müssen zwischen den folgenden Optionen auswählen:**
 - **"Am X"**
 Gibt das Datum an, an dem Backup Exec den Auftrag ausführt. Das in diesem Feld ausgewählte Datum entspricht der Anzahl von Jahren, die Sie im Feld "Alle X Jahre" ausgewählt haben. Wenn Sie festgelegt haben, dass der Auftrag alle zwei Jahre ausgeführt werden soll, und Sie in diesem Feld 28. Juni ausgewählt haben, wird der Auftrag alle zwei Jahre jeweils am 28. Juni ausgeführt.
 - **"Am X. X"**
 Gibt den Tag und den Monat an, an dem Backup Exec den Auftrag ausführt. Das in diesem Feld ausgewählte Datum entspricht der Anzahl von Jahren, die Sie im Feld "Alle X Jahre" ausgewählt haben. Wenn Sie festgelegt haben, dass der Auftrag alle zwei Jahre ausgeführt werden soll, und Sie in diesem Feld den vierten Donnerstag im Juni ausgewählt haben, wird der Auftrag alle zwei Jahre jeweils am vierten Donnerstag im Juni ausgeführt.

um

Geben Sie die Startzeit des ersten Auftrags im Wiederholungsmuster an.

Gestartet am

Geben Sie das Datum ein, an dem das Wiederholungsmuster beginnen soll.

Der Zeitplan tritt an diesem Datum in Kraft. Sie können ein beliebiges Datum in der Zukunft oder in der Vergangenheit auswählen. Wenn Sie ein Datum in der Vergangenheit wählen, berechnet Backup Exec das Datum des nächsten bevorstehenden Auftrags und führt dann wiederkehrende Aufträge ab diesem Datum aus.

Kalender	Klicken Sie auf diese Option, um alle geplanten Backup-Aufträge in einem Kalender anzuzeigen und nach Zeitplankonflikten zu suchen.
Erstes vollständiges Backup jetzt zusätzlich zum ausgewählten Zeitplan ausführen	Wählen Sie diese Option aus, um das volle zuerstbackup auszuführen, sobald der Job erstellt wird, ohne den Zeitplan von zukünftigen Jobs zu beeinflussen.
Auftrag neu planen, falls er X Stunden nach geplanter Startzeit noch immer nicht ausgeführt wird	Spezifizieren Sie die Dauer hinter dem eingeplanten Job Anlasszeit, zu der Sie Backup Exec den JobVollendungsstatus zu verfehlt ändern wünschen. Der Auftrag wird erneut geplant, um gemäß des von Ihnen festgelegten Zeitfensters ausgeführt zu werden. Siehe "Liste von Auftragsstatus in Backup Exec" auf Seite 322.
Abbrechen des Auftrags, falls er X Stunden nach geplanter Startzeit immer noch ausgeführt wird	Gibt den Zeitraum nach der geplanten Startzeit des Auftrags an, nach dessen Ablauf der Auftrag abgebrochen wird, wenn er noch ausgeführt wird. Backup Exec ändert den Auftragsabschlussstatus in "Abgebrochen, Zeitüberschreitung". Siehe "Liste von Auftragsstatus in Backup Exec" auf Seite 322.

- 7 Um bestimmte Daten zu konfigurieren und sie im Auftragszeitplan einzuschließen, wählen Sie die Registerkarte "Daten ein/ausschließen" aus und gehen wie folgt vor:
 - Klicken Sie auf "Daten einschließen".
 - Wählen Sie die Daten aus, die Sie mit dem wiederkehrenden Jobzeitplan einschließen möchten.
 - Klicken Sie auf "OK".

Der Auftrag wird an allen mit dieser Option ausgewählten Tagen ausgeführt, zusätzlich zu den Tagen, die Teil des normalen Zeitplans sind. Der Auftrag wird am nächsten im normalen Zeitplan festgelegten Tag nach dem eingeschlossenen Datum fortgesetzt.

Siehe ["Einschließlich ein spezifisches Datum im Zeitplan für einen Backup-Auftrag"](#) auf Seite 240.
- 8 Um spezifische Daten zu konfigurieren um vom Job auszuschließen planen Sie ein, wählen Sie aus das Einschliessung/schließen Sie Datumstabulator, aus und schließen Sie dann die folgenden Schritte ab:

- Klicken Sie auf "Daten ausschließen".
- Wählen Sie die Daten aus, die Sie vom wiederkehrenden Jobzeitplan ausschließen möchten.
- Klicken Sie auf "OK".

Der Auftrag wird an diesen Tagen nicht ausgeführt. Er wird am nächsten im normalen Zeitplan festgelegten Tag nach dem ausgeschlossenen Datum fortgesetzt.

Siehe ["Durchführung von Backup-Aufträgen zu einem bestimmten Datum verhindern"](#) auf Seite 242.

- 9 Wählen Sie "Auftrag in Wartestellung senden" aus, um Aufträge in Wartestellung zu senden.

Wählen Sie diese Option, wenn Sie den Auftrag senden möchten, dieser jedoch erst zu einem späteren Datum ausgeführt werden soll. Der Auftrag wird ausgeführt, wenn Sie den Wartestatus aufheben.

- 10 Klicken Sie auf "OK".

Siehe ["Ändern der Standardeinstellungen für Backup-Aufträge"](#) auf Seite 630.

Siehe ["Sichern von Daten"](#) auf Seite 174.

Konfigurieren von Speicheroptionen für Backup-Aufträge

Über die Speicheroptionen können Sie den Speicher und den Mediensatz auswählen, auf denen Sie den Backup-Auftrag ausführen möchten. Sie können für jeden Backup-Auftrag verschiedene Speichergeräte konfigurieren. Beispielsweise können Sie in derselben Backup-Definition für ein vollständiges Backup einen Datenträgerspeicher und für ein inkrementelles Backup einen Speicherpool auswählen.

Sie können globale Zeitplanoptionen als Standardeinstellungen für alle Backup-Aufträge konfigurieren. Wenn Sie die Standardoptionen für einen bestimmten Backup-Auftrag nicht verwenden möchten, können Sie sie übergehen, während Sie einen Backup-Auftrag erstellen. Sie müssen jedoch nicht für alle Backup-Aufträge Standardspeicheroptionen konfigurieren. Wenn Sie verschiedene Speicheroptionen für spezifische Backup-Aufträge konfigurieren möchten, können Sie diese beim Erstellen der Backup-Aufträge konfigurieren.

Konfigurieren von Speicheroptionen für Backup-Aufträge

- 1 Sie haben folgende Möglichkeiten:

Konfigurieren von
Standardspeicheroptionen für
alle Backup-Aufträge

Führen Sie die folgenden Schritte durch:

- Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie "Konfiguration und Einstellungen".
- Wählen Sie "Auftragsstandardeinstellungen" aus und dann den Backup-Typ, für den Sie Speicheroptionen konfigurieren möchten.

Konfigurieren von
Speicheroptionen für
bestimmte Backup-Aufträge

Führen Sie die folgenden Schritte durch:

- Erstellen Sie eine neue Backup-Definition oder bearbeiten Sie eine vorhandene.
- Klicken Sie im Dialogfeld "Backup" auf "Bearbeiten".

2 Klicken Sie im linken Teilfenster auf "Speicher".

3 Ergänzen Sie die folgenden Optionen, falls erforderlich:

Hinweis: Einige dieser Optionen werden nur in Umgebungen mit Central Admin Server(CAS)-Funktion angezeigt.

Priorität	<p>Wählen Sie die Priorität für den Zugriff auf die Speichergeräte für Backup-Aufträge aus.</p> <p>Diese Einstellung ist nur pro Auftrag verfügbar und kann nicht als Standardeinstellung für Backup-Aufträge festgelegt werden.</p> <p>Siehe "Ändern der Priorität für geplante Aufträge" auf Seite 297.</p>
Exec-Server oder Backup Exec-Server-Pool	<p>Gibt an, dass ein Auftrag auf Geräten auf einem speziellen verwalteten Backup Exec-Server oder auf Geräten, die sich in einer Gruppe verwalteter Backup Exec-Server befinden, ausgeführt wird.</p> <p>Dieses Option wird nur angezeigt, wenn Central Admin Server Feature (CASO) installiert ist. Dabei handelt es sich um einen zusätzlichen Filter, mit dem Sie steuern können, wohin bestimmte Aufträge delegiert werden. Um beispielsweise Backups von Exchange-Datenbanken immer nur auf den Geräten auszuführen, die an die verwalteten Backup Exec-Server in einem Pool namens "Exchange-Backups" angehängt sind, wählen Sie diese Option. Wählen Sie dann den Backup Exec-Server-Pool für Exchange-Backups aus.</p>
Speicher	<p>Wählen Sie das Speichergerät aus, an das Backup-Daten gesendet werden sollen.</p> <p>Siehe "Erstellen von Speichergerätepools" auf Seite 512.</p> <p>Siehe "Info zu Remote Media Agent for Linux " auf Seite 1598.</p> <p>Siehe "Funktionen und Typen des plattenbasierten und netzwerkbasierten Speichers" auf Seite 367.</p>

- 4** Wenn Sie im Feld "Speicher" die Option zum Konfigurieren eines OpenStorage-Geräts oder eines Deduplizierungsspeichergeräts ausgewählt haben, haben Sie folgende Möglichkeiten:

<p>Dem Remote-Computer ermöglichen, direkt auf das Speichergerät zuzugreifen und eine clientseitige Deduplizierung durchzuführen, falls diese unterstützt wird</p>	<p>Wählen Sie diese Option aus, wenn ein Remote-Computer Daten direkt an ein OpenStorage-Gerät oder an ein Deduplizierungsspeichergerät schicken und eine clientseitige Deduplizierung durchführen soll, wenn das Gerät dies unterstützt. Der Backup Exec-Server wird umgangen, wodurch er für andere Vorgänge zur Verfügung steht. Kann die clientseitige Deduplizierung nicht durchgeführt werden, wird entweder die Backup Exec-Server-Deduplizierung oder die Appliance-Deduplizierung durchgeführt.</p>
--	--

Diese Option wird angezeigt, wenn die Deduplizierungsfunktion installiert ist und im Feld "Speicher" ein OpenStorage-Gerät oder ein Deduplizierungsspeichergerät ausgewählt ist.

Siehe ["Einsatz der clientseitigen Deduplizierung"](#) auf Seite 1078.

<p>Dem Remote-Computer ermöglichen, über den Backup Exec-Server auf das Speichergerät zuzugreifen und eine serverseitige Backup Exec-Deduplizierung durchzuführen, falls diese unterstützt wird</p>	<p>Wählen Sie diese Option aus, wenn ein Remote-Computer Daten über den Backup Exec-Server an ein OpenStorage-Gerät oder an ein Deduplizierungsspeichergerät schicken und eine serverseitige Backup Exec-Deduplizierung durchführen soll, wenn dies unterstützt wird. Wenn der Backup Exec-Server die Deduplizierung nicht unterstützt, werden die Daten auf einem intelligenten Datenträgergerät, wie zum Beispiel PureDisk oder einem Gerät von einem externen Anbieter, dedupliziert.</p>
---	--

Diese Option wird angezeigt, wenn die Deduplizierungsfunktion installiert ist und im Feld "Speicher" ein OpenStorage-Gerät oder ein Deduplizierungsspeichergerät ausgewählt ist.

Siehe ["Info zu Deduplication Feature"](#) auf Seite 1047.

- 5** Geben Sie im Feld "Aufbewahren für" an, wie lange Sie die Backup-Sätze oder den Auftragsverlauf aufbewahren möchten.
- 6** Wenn Sie im Feld "Speicher" die Option zum Konfigurieren eines Bandgeräts ausgewählt haben, ergänzen Sie die folgenden Optionen, falls erforderlich:

Mediensatz

Wählen Sie den Mediensatz aus, der für den Backup-Auftrag verwendet werden soll. Der Mediensatz gibt den Überschreibschutzzeitraum und den Anhängezeitraum für die Backup-Daten auf den Medien an.

Wenn Sie einen neuen Mediensatz für diesen Backup-Auftrag erstellen möchten, klicken Sie auf das Symbol rechts neben dem Dropdown-Menü "Mediensatz".

Diese Option ist nur verfügbar, wenn Sie im Feld "Speicher" ein Bandgerät ausgewählt haben.

Siehe ["Standard-Mediensätze"](#) auf Seite 473.

Medium überschreiben

Wählen Sie diese Option aus, um die gesicherten Daten auf überschreibbare Medien zu platzieren. Vergewissern Sie sich, dass sich das entsprechende Medium im ausgewählten Speichergerät befindet.

Geeignete Medien für einen Überschreibungsauftrag:

- Temporäre Medien
- Medien, deren Überschreibschutzzeitraum abgelaufen ist

Zugeordnete oder importierte Medien können auch abhängig von der festgelegten Medienüberschreibschutzstufe überschrieben werden.

Abhängig von Ihrer Konfiguration werden überschreibbare Medien aus temporären oder wiederverwendbaren Medien ausgewählt.

Wenn die Medien im Speichergerät nicht überschreibbar sind, werden Sie aufgefordert, überschreibbare Medien zur Verfügung zu stellen.

Diese Option ist nur verfügbar, wenn Sie im Feld "Speicher" ein Bandgerät ausgewählt haben.

Siehe ["Verwalten von Bändern"](#) auf Seite 472.

Siehe ["Medienüberschreibschutzstufen für Bandmedien"](#) auf Seite 487.

Siehe ["So sucht Backup Exec nach überschreibbaren Medien in Bandlaufwerken"](#) auf Seite 488.

An Medium anhängen oder überschreiben, falls kein anhängbares Medium verfügbar ist	<p>Wählen Sie diese Option aus, um die gesicherten Daten an den angegebenen Mediensatz anzuhängen, wenn anhängbare Medien verfügbar sind. Andernfalls sucht Backup Exec nach überschreibbaren Medien und fügt sie dem Mediensatz hinzu.</p> <p>Wenn ein Anhängeauftrag ein Medium füllt, wird der Backup-Auftrag auf einem überschreibbaren Medium fortgeführt. Wenn die Medien im Speichergerät nicht überschreibbar sind, wird eine Warnmeldung mit der Aufforderung angezeigt, überschreibbare Medien zur Verfügung zu stellen.</p> <p>Diese Option ist nur verfügbar, wenn Sie im Feld "Speicher" ein Bandgerät ausgewählt haben.</p>
An Medium anhängen oder Auftrag abbrechen, falls kein anhängbares Medium verfügbar ist	<p>Wählen Sie diese Option aus, um die gesicherten Daten an den angegebenen Mediensatz anzuhängen, wenn anhängbare Medien verfügbar sind. Andernfalls beendet Backup Exec den Auftrag.</p> <p>Diese Option ist nur verfügbar, wenn Sie im Feld "Speicher" ein Bandgerät ausgewählt haben.</p>
Medium nach Auftragsabschluss auswerfen	<p>Wählen Sie diese Option aus, um die Medien vom Laufwerk oder Schacht auszuwerfen, wenn der Vorgang abgeschlossen wurde. Sie können auch einen Auftrag planen, um Medien auszuwerfen.</p> <p>Diese Option ist nur verfügbar, wenn Sie im Feld "Speicher" ein Bandgerät ausgewählt haben.</p> <p>Siehe "Auswerfen von Medien aus einer Plattenkassette oder einem Bandlaufwerk" auf Seite 555.</p>
Spannen eines Mediums vor einem Backup	<p>Wählen Sie diese Option aus, um das Band im Laufwerk vom Anfang bis zum Ende mit hoher Geschwindigkeit umzuspulen. Durch Spannen wird das Band gleichmäßig aufgewickelt und kommt gleichmäßig mit den Abtastköpfen des Bandlaufwerks in Kontakt. Diese Option ist nur verfügbar, wenn Sie ein Bandlaufwerk auswählen, das das Neuspannen unterstützt.</p>

Medien mit einem Schreib- und mehreren Lesevorgängen (WORM) verwenden

Wählen Sie diese Option aus, um das WORM-Medium (WORM, Write Once, Read Many – ein Schreib- und mehrere Lesevorgänge) für diesen Backup-Auftrag zu verwenden. Backup Exec bestätigt, dass das Zielgerät ein WORM-kompatibles Laufwerk ist oder enthält, und dass das WORM-Medium in diesem Laufwerk zur Verfügung steht. Wird kein WORM-Medium oder WORM-kompatibles Laufwerk gefunden, wird eine entsprechende Warnmeldung ausgegeben.

Siehe ["So werden WORM-Medien in Backup Exec verwendet"](#) auf Seite 495.

Medien nach Auftragsabschluss in Speicher exportieren

Wählen Sie diese Option aus, um die Medien aus dem Wechsler in den angegebenen Medienspeicher zu verschieben.

Dieser Vorgang verschiebt Medien aus den Wechslerschächten in ein Portal. Eine Warnmeldung erinnert Sie daran, die Medien aus dem Portal oder einem Schacht zu entfernen. Wenn ein Auftrag mehrere Medien erfordert, beginnt der Vorgang "Medien exportieren" nach dem Abschluss des Backup-Auftrags, nicht nachdem jedes Medium gefüllt wurde.

Diese Option ist nur verfügbar, wenn Sie im Feld "Speicher" ein Bandgerät ausgewählt haben.

Siehe ["Standardmedienspeicher"](#) auf Seite 496.

7 Im Feld "Komprimierung" können Sie die folgenden Optionen auswählen:

Keine	<p>Wählen Sie diese Option aus, um die Daten in ihrem ursprünglichen Format auf das Medium zu kopieren (nicht komprimiert). Durch die Verwendung eines Datenkomprimierungsverfahrens können Sie Backup-Vorgänge beschleunigen und Speicherplatz sparen.</p> <p>Die Hardware-Datenkomprimierung sollte nicht in Umgebungen verwendet werden, in denen sowohl Speichergeräte mit Unterstützung einer Hardwarekomprimierung als auch Geräte ohne diese Funktion verwendet werden. In dieser Situation wird die Hardwarekomprimierung automatisch deaktiviert. Sie können die Hardwarekomprimierung auf den entsprechenden Laufwerken zwar manuell wieder aktivieren, dies führt jedoch zu Inkonsistenzen zwischen den Medien. Wenn das Laufwerk mit Hardwarekomprimierung ausfällt, ist es nicht möglich, die komprimierten Medien mit dem nicht komprimierungsfähigen Laufwerk wiederherzustellen.</p>
Software	<p>Wählen Sie diese Option aus, um STAC-Software-Datenkomprimierung zu verwenden, bei der die Daten vor dem Übertragen an das Speichergerät komprimiert werden.</p>
Hardware (falls vorhanden, sonst keine)	<p>Wählen Sie diese Option aus, damit Hardware-Datenkomprimierung (sofern vom Speichergerät unterstützt) verwendet wird. Wenn das Laufwerk keine Datenkomprimierung unterstützt, werden die Daten unkomprimiert gesichert.</p>
Hardware (falls vorhanden, sonst Software)	<p>Wählen Sie diese Option aus, damit Hardware-Datenkomprimierung (sofern vom Speichergerät unterstützt) verwendet wird. Wenn das Laufwerk keine Hardware-Datenkomprimierung unterstützt, wird die Softwarekomprimierung STAC verwendet.</p>

- 8** Ergänzen Sie die folgenden Optionen, um eine Verschlüsselung zu konfigurieren:

Verschlüsselungstyp	Wählen Sie den gewünschten Verschlüsselungstyp aus (wenn vorhanden). Siehe " Verwendung von Verschlüsselung mit Backup Exec " auf Seite 727.
Verschlüsselungscode	Wählen Sie den gewünschten Verschlüsselungscode aus, den Sie verwenden möchten.
Schlüssel verwalten	Klicken Sie auf diese Option, einen neuen Verschlüsselungscode zu erstellen und die Verschlüsselung für Aufträge zu konfigurieren. Verwenden Sie diese Option nicht zum Ersetzen oder Löschen vorhandener Verschlüsselungscodes, die mit dem Auftrag verknüpft sind. Diese Option ist nur verfügbar, wenn Sie einen Verschlüsselungstyp auswählen. Siehe " Verwaltung von Verschlüsselungscodes " auf Seite 731.

- 9** Klicken Sie auf "OK".

Siehe "[Ändern der Standardeinstellungen für Backup-Aufträge](#)" auf Seite 630.

Siehe "[Sichern von Daten](#)" auf Seite 174.

Konfigurieren automatischer Testlaufaufträge für Backup-Aufträge

Mithilfe von Aufträgen für Testläufe wird versucht, festzustellen, ob ein geplanter Backup während des Ausführens fehlschlagen kann. Bei der Ausführung von Testaufträgen werden keine Daten gesichert. Stattdessen prüft Backup Exec Ihre Speicherkapazität, Login-Daten und Medien, um potenzielle Fehler zu finden. Wenn ein Fehler auftritt, wird der Auftrag weiterhin ausgeführt, bis er abgeschlossen ist. Der Fehler wird im Auftragsprotokoll angezeigt. Sie können Backup Exec auch konfigurieren, um eine Benachrichtigung an einen designierten Empfänger zu schicken.

Wenn es während eines Probelaufauftrags zu Fehlern kommt, können folgende Gründe vorliegen:

- Login-Daten sind falsch.

- Speicherkapazität reicht nicht aus.
- Bandkassettemedien oder -Datenträgermedien sind nicht verfügbar.
- Überschreibbare Medien sind nicht für einen Überschreibungsauftrag verfügbar.
- Anhängbare Medien sind nicht für einen Anhängeauftrag verfügbar.

Ein Probelaufauftrags prüft die Medienkapazität, die für den ausgewählten Auftrag verfügbar ist. Sie können jedoch prüfen, ob ausreichend Medien für mehrere Probelaufaufträge im Bericht "Probelaufergebnisse" verfügbar sind.

Siehe ["Bericht "Probelaufergebnisse""](#) auf Seite 849.

Sie können einen Testlaufauftrag jederzeit manuell ausführen.

Siehe ["Manuelle Ausführung von Probelaufaufträgen"](#) auf Seite 251.

Sie können Testlaufaufträge auch so konfigurieren, dass sie standardmäßig vor Ihren geplanten Backup-Aufträgen ausgeführt werden. Wenn Sie keinen Testlaufauftrag für einen bestimmten Backup-Auftrag verwenden möchten, können Sie die Standardeinstellungen übergehen, während Sie einen Backup-Auftrag erstellen. Sie müssen jedoch Testlaufaufträge nicht standardmäßig für alle Backup-Aufträge konfigurieren. Wenn Sie verschiedene Testlaufaufträge für spezifische Backup-Aufträge konfigurieren möchten, können Sie einen Testlaufauftrag beim Erstellen dieser Backup-Aufträge konfigurieren.

Konfigurieren automatischer Testlaufaufträge für Backup-Aufträge

1 Sie haben folgende Möglichkeiten:

Konfigurieren von
Testlaufaufträgen als
Standard für alle
Backup-Jobs

Führen Sie die folgenden Schritte durch:

- Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- Wählen Sie "Auftragsstandardeinstellungen" und wählen Sie dann den Backup-Typ aus, für den Sie Testlaufaufträge konfigurieren wollen.

Aktivieren von
Testlaufaufträgen für
bestimmte Backup-Aufträge

Führen Sie die folgenden Schritte durch:

- Erstellen Sie eine neue Backup-Definition oder bearbeiten Sie eine vorhandene Backup-Definition.
- Klicken Sie im Dialogfeld "Backup" auf "Bearbeiten".

2 Klicken Sie im linken Teilfenster auf "Testlauf".

3 Wählen Sie "Testlauf aktivieren" aus.

4 Klicken Sie auf "OK".

Siehe ["Ändern der Standardeinstellungen für Backup-Aufträge"](#) auf Seite 630.

Siehe ["Sichern von Daten"](#) auf Seite 174.

Konfigurieren der automatischen Prüfung von Aufträgen

Backup Exec kann eine Überprüfung durchführen, um sicherzustellen, ob die Medien gelesen werden können, sobald der Backup-Auftrag abgeschlossen wurde. Es wird empfohlen, dass Sie alle gesicherten Daten prüfen, um die Integrität der Datenerfassung und der Medien sicherzustellen, auf denen sie sich befindet.

Sie können einen Backup-Satz oder Auftragsverlauf jederzeit manuell prüfen. Sie können Backup-Sätze prüfen, wenn Sie nur die Daten prüfen möchten, die in einer bestimmten Backup-Auftragsinstanz gesichert wurden. Wenn Sie einen Auftrag und alle seine abhängigen Backup-Sätze prüfen möchten, können Sie einen Auftragsverlauf prüfen. Beispiel: Wenn Sie eine Backup-Definition prüfen möchten, die inkrementelle Backups nutzt, prüft Backup Exec alle entsprechenden Backups, einschließlich des letzten vollständigen.

Siehe ["Gesicherte Daten manuell überprüfen"](#) auf Seite 252.

Standardmäßig verifiziert Backup Exec automatisch gesicherte Daten am Ende eines Backup-Auftrags. Sie können aber auch festlegen, dass die Prüfung zu einem späteren Zeitpunkt ausgeführt werden soll, oder sie komplett deaktivieren. Sie können die Prüfungsoptionen von Backup Exec als Teil der Standardbackupeinstellungen oder für einzelne Backup-Aufträge anpassen.

So konfigurieren Sie die automatische Prüfung von Aufträgen

1 Sie haben folgende Möglichkeiten:

So konfigurieren Sie die automatische Prüfung für alle Backup-Aufträge

Führen Sie die folgenden Schritte durch:

- Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie "Konfiguration und Einstellungen".
- Wählen Sie "Auftragsstandardeinstellungen" und wählen Sie dann den zu prüfenden Backup-Typ aus.

So konfigurieren Sie die automatische Prüfung für spezifische Backup-Aufträge

Führen Sie die folgenden Schritte durch:

- Erstellen Sie eine neue Backup-Definition oder bearbeiten Sie eine vorhandene.
- Klicken Sie im Dialogfeld "Backup" auf "Bearbeiten".

2 Klicken Sie im linken Teilfenster auf "Prüfen".

3 Konfigurieren Sie folgende Optionen:

Nach Abschluss eines Auftrags	Wählen Sie diese Option, um eine Prüfung automatisch auszuführen, wenn der Backup-Auftrag abgeschlossen ist.
Als separater Auftrag nach Abschluss des Auftrags	<p>Wählen Sie diese Option, um eine Prüfung zu erstellen und zu planen, die als separater Auftrag ausgeführt werden soll, wenn der Backup-Auftrag abgeschlossen ist.</p> <p>Sie können die Option "Bearbeiten" verwenden, um Optionen für den separaten Prüfungsauftrag zu konfigurieren.</p>
Als separater geplanter Auftrag	<p>Wählen Sie diese Option, um eine Prüfung zu erstellen und zu planen, die als separater Auftrag zu einem späteren Zeitpunkt ausgeführt werden soll.</p> <p>Sie können die Option "Bearbeiten" verwenden, um Optionen für den separaten Prüfungsauftrag zu konfigurieren.</p>
Daten für diesen Auftrag nicht verifizieren	<p>Wählen Sie diese Option, um die Prüfung für den Backup-Auftrag zu deaktivieren.</p> <p>Hinweis: Dies ist die Standardeinstellung für Cloud-Speichergeräte.</p>

4 Klicken Sie auf "OK".

Siehe ["Ändern der Standardeinstellungen für Backup-Aufträge"](#) auf Seite 630.

Siehe ["Sichern von Daten"](#) auf Seite 174.

Konfigurieren der Optionen für Instant GRT und Vollständige Katalogisierung zum Verbessern der Backup-Leistung von GRT-Aufträgen

Beim Sichern von Daten erstellt Backup Exec einen Katalog mit Informationen über die Backup-Sätze und über das Speichergerät, auf dem die Backup-Sätze gespeichert werden.

Siehe ["Funktionsweise der Backup Exec-Kataloge"](#) auf Seite 277.

Die Katalogisierung kann zeitaufwändig sein. Sie benötigt Zugriff auf das für das Backup genutzte Speichergerät. Das Katalogisieren von Aufträgen, die für GRT aktiviert sind, dauert aufgrund der Menge der enthaltenen granularen Daten länger.

Im Dialogfeld "Optionen für Instant GRT und Vollständige Katalogisierung" können Sie entweder Instant GRT oder die vollständige Katalogisierung wählen.

Hinweis: Die Optionen für Instant GRT und Vollständige Katalogisierung werden beim Sichern auf Band nicht unterstützt. Wenn Sie ein GRT-Backup auf Band für Microsoft Exchange-, Microsoft SharePoint-, Microsoft Hyper-V- oder VMware-Daten erstellen, wird die Katalogisierung als Teil des Backup-Auftrags ausgeführt.

Siehe „[Vollständige Katalogisierung](#)“ auf Seite 657.

Siehe „[Instant GRT](#)“ auf Seite 658.

Siehe „[Unterschiede zwischen Instant GRT und Vollständige Katalogisierung](#)“ auf Seite 659.

Siehe "[Konfigurieren eines Vorgangs Instant GRT oder Vollständige Katalogisierung](#)" auf Seite 661.

Vollständige Katalogisierung

Für GRT-Aufträge können Sie die Katalogisierung verzögern und als separaten Vorgang ausführen, damit das Backup-Fenster weniger beeinträchtigt wird. Da die Katalogisierung separat vom Backup-Auftrag ausgeführt wird, wird der pünktliche Start eines anderen geplanten GRT-Backup-Auftrags nicht verhindert.

Siehe "[Granular Recovery Technology](#)" auf Seite 737.

Wenn Sie GRT für Microsoft Exchange-, Microsoft SharePoint-, Microsoft Hyper-V- oder VMware-Backups aktivieren, wird die vollständige Katalogisierung standardmäßig sofort nach dem Backup-Auftrag ausgeführt.

Für Exchange- und SharePoint-Backups mit Agent wird die vollständige Katalogisierung sofort nach allen vollständigen Backups ausgeführt. Sie wird einmal alle 24 Stunden für alle inkrementellen und differenziellen Backups ausgeführt, selbst wenn Sie mehr als einen GRT-Auftrag für diesen Zeitraum planen.

Für Hyper-V- und VMware-Backups wird die vollständige Katalogisierung standardmäßig sofort nach allen vollständigen, inkrementellen und differenziellen Backups ausgeführt.

Sie können die vollständige Katalogisierung so konfigurieren, dass sie nach einem Zeitplan ausgeführt wird, wenn Sie ihn nicht sofort nach dem Backup ausführen möchten.

Sie sollten die vollständige Katalogisierung außerhalb des Backup-Fensters planen, damit sie die Systemressourcen nicht beeinträchtigt. Wenn Sie die vollständige Katalogisierung planen, wird sie nur für den neuesten Backup-Satz seit der letzten Katalogisierung ausgeführt. In dieser Situation kann nur der neueste Backup-Satz seit der letzten Katalogisierung für die granulare Wiederherstellung verwendet werden.

Beispiel: Wenn Sie inkrementelle Backups so planen, dass sie alle 11 Stunden und die vollständige Katalogisierung um Mitternacht ausgeführt werden, werden folgenden Backup-Sätze erstellt:

- Vollständig (11:00 Uhr)
- Inkrementell 1 (22:00 Uhr)
- Katalog 1 (Mitternacht): Dieser Auftrag katalogisiert Inkrementell 1.
- Inkrementell 2 (09:00 Uhr)
- Inkrementell 3 (20:00 Uhr)
- Katalog 2 (Mitternacht). Dieser Auftrag katalogisiert Inkrementell 3. Inkrementell 2 ist nicht katalogisiert.
- Inkrementell 4 (07:00 Uhr)
- Inkrementell 5 (18:00 Uhr)
- Katalog 3 (Mitternacht): Dieser Auftrag katalogisiert Inkrementell 5. Inkrementell 4 ist nicht katalogisiert.
- Inkrementell 6 (5:00 Uhr): Dieses Backup wird nicht katalogisiert.

Im Beispiel wird die vollständige Katalogisierung nur für Inkrementell 5, Inkrementell 3 und Inkrementell 1 ausgeführt. Für solche Aufträge können Sie mit dem Suchassistenten die Daten durchsuchen oder nach einzelnen Elementen suchen, die wiederhergestellt werden sollen. Sie können zwar eine granulare Wiederherstellung auch mit Inkrementell 2, Inkrementell 4 und Inkrementell 6 ausführen, aber dies dauert länger, da sie nicht vollständig katalogisiert sind. Backup Exec zeigt die granularen Daten durch Bereitstellen des Backup-Satzes an.

Instant GRT

Der Vorgang Instant GRT wird im Rahmen des Backup-Auftrags ausgeführt und erfasst nur die unbedingt erforderlichen Kataloginformationen. Mit dem Suchassistenten können Sie die Backup-Sätze nicht nach einzelnen Elementen durchsuchen. Wenn Sie Backup-Sätze nach einzelnen Elementen durchsuchen, liest Backup Exec die granularen Daten und zeigt sie an. Je nach Backup-Satz (inkrementell oder differenziell) kann das Suchen nach einzelnen Elementen eine gewisse Zeit dauern.

Zum Ausführen des Vorgangs Instant GRT gelten folgende Anforderungen:

- Stellen Sie in einer CAS-Umgebung sicher, dass die Benutzerkonten für die Backups der Liste der Benutzerkonten auf dem zentralen Administrationsserver und den verwalteten Backup Exec-Servern hinzugefügt werden.
- Der Speicher für die Backup-Sätze muss online sein, wenn Sie nach einzelnen wiederherzustellenden Elementen suchen, da Backup Exec Backup-Sätze dynamisch bereitstellt. Für inkrementelle und differenzielle Backup-Sätze müssen diese zugehörigen Backup-Sätze ebenfalls während der Wiederherstellung verfügbar sein.
- Durchsucht in einer CAS-Umgebung ein Backup Exec-Server die Backup-Sätze eines anderen Backup Exec-Servers und ist zwischen diesen eine Firewall installiert, müssen Sie Ports auf den Servern öffnen.
Es wird empfohlen, die Backup-Sätze entweder über den verwalteten Backup Exec-Server, auf dem die Backup-Aufträge ausgeführt wurden, oder über den zentralen Administrationsserver auszuführen.
Siehe ["Backup ExecAnschlüsse"](#) auf Seite 724.
Siehe ["Backup Exec-Listener-Ports"](#) auf Seite 726.

Unterschiede zwischen Instant GRT und Vollständige Katalogisierung

Tabelle 15-1 Unterschiede zwischen Instant GRT und Vollständige Katalogisierung

Element	Instant GRT	Vollständige Katalogisierung
Suchen nach granularen Elementen mit dem Suchassistenten	Nicht verfügbar.	Sie können die Backup-Sätze nach granularen Daten durchsuchen.
Durchsuchen von Backup-Sätzen	Sie können Backup-Sätze dynamisch durchsuchen und die wiederherzustellenden Elemente auswählen.	Sie können Backup-Sätze durchsuchen und die wiederherzustellenden Elemente auswählen.
Verzögerung bei der Katalogisierung	Keine Verzögerung bei der Katalogisierung. Sie wird im Rahmen des Backup-Auftrags ausgeführt.	Sie können die Katalogisierung so planen, dass sie sofort nach dem Backup-Auftrag oder später ausgeführt wird.

Element	Instant GRT	Vollständige Katalogisierung
Katalogisierungszeit	Keine separate Katalogisierungszeit, da der Vorgang im Rahmen des Backup-Auftrags ausgeführt wird. Backup Exec erfasst nur die unbedingt erforderlichen Daten.	Die Katalogisierung wird als separater Auftrag ausgeführt. Dies dauert eine gewisse Zeit, da Backup Exec ausführliche Katalogisierungsdaten für den Backup-Auftrag erfasst.
Größe der Katalogdatei	Die Datei ist klein, da nur die unbedingt erforderlichen Daten katalogisiert werden.	Die Datei ist groß, da der vollständige Backup-Satz katalogisiert wird.
Zeit zum Durchsuchen granularer Daten für die granulare Wiederherstellung	<p>Etwas länger als die Zeit beim Durchsuchen der Daten bei einer vollständigen Katalogisierung, da Backup Exec den Backup-Satz dynamisch nach GRT-Daten durchsucht, wenn Sie Backup-Sätze erweitern, um granulare Elemente wiederherzustellen.</p> <p>Die zum Wiederherstellen benötigte Zeit entspricht der für einen vollständig katalogisierten Backup-Satz.</p>	Weniger Zeit als für das Durchsuchen von Daten beim Instant GRT, da die GRT-Daten bereits im ausführlichen, während der vollständigen Katalogisierung erfassten Katalog verfügbar sind.
Gerät belegt	Das Gerät ist lange Zeit nicht belegt, da der Katalog nicht ausführlich ist und im Rahmen des Backup-Auftrags ausgeführt wird.	Das Gerät ist lange Zeit belegt. Zuerst, wenn das Backup und dann wenn die vollständige Katalogisierung als separater Auftrag ausgeführt wird.

Sie können Standardeinstellungen für diese Optionen für alle GRT-Backup-Aufträge konfigurieren. Wenn die Standardannahmen nicht für einen bestimmten Job angebracht sind, können Sie sie außer Kraft setzen, wenn Sie den Job erstellen. Sie müssen jedoch keine Standardeinstellungen für Instant GRT oder Vollständige Katalogisierung erstellen. Wenn Sie diese Optionen nur für spezifische Aufträge konfigurieren möchten, können Sie die Einstellungen konfigurieren, wenn Sie die Aufträge erstellen.

Konfigurieren eines Vorgangs Instant GRT oder Vollständige Katalogisierung

1 Sie haben folgende Möglichkeiten:

Konfigurieren von Instant GRT oder Vollständige Katalogisierung für alle Backup-Aufträge

Führen Sie die folgenden Schritte durch:

- Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- Wählen Sie "Auftragsstandardeinstellungen" und dann den Backup-Typ, für den Sie den Vorgang Instant GRT oder Vollständige Katalogisierung konfigurieren möchten.

Konfigurieren von Instant GRT oder Vollständige Katalogisierung für bestimmte Backup-Aufträge

Führen Sie die folgenden Schritte durch:

- Erstellen Sie eine neue Backup-Definition oder bearbeiten Sie eine vorhandene.
- Klicken Sie im Dialogfeld "Backup" auf "Bearbeiten".

2 Im linken Teilfenster klicken Sie auf "Instant GRT".

3 Wählen Sie eine der folgenden Optionen:

Instant GRT aktivieren

Wählen Sie diese Option, wenn Sie Instant GRT für GRT-Backup-Aufträge ausführen möchten.

Diese Option ist die Standardeinstellung für alle neuen GRT-Backup-Aufträge unter einer neuen Installation von Backup Exec. Wenn Sie aus Backup Exec 15 Feature Pack 5 oder niedriger aktualisieren, ändert sich möglicherweise die Standardkatalogisierungsoption entsprechend Ihrer Backup Exec-Server-Umgebung und der ursprünglichen Version. Ist diese Option nach dem Upgrade nicht als Standardeinstellung festgelegt, sollten Sie dies tun, damit Sie schnellere Backups ausführen können.

Für die vorhandenen GRT-Backup-Aufträge, die Exchange-, SharePoint- oder virtuelle Computer mit dem virtuellen Backup schützen, wird die Standardoption für die vorhandenen Aufträge nicht geändert. Die vorhandenen Aufträge behalten die Standardoption bei, die vor dem Upgrade festgelegt wurde. Wenn nach dem Upgrade ein neues Gerät hinzugefügt wird, wird die Standardoption auf "Instant GRT aktivieren" festgelegt.

Diese wird im Rahmen des Backup-Auftrags ausgeführt und erfasst nur die unbedingt erforderlichen Kataloginformationen.

Mit dem Suchassistenten können Sie die Backup-Sätze nicht nach granularen Daten durchsuchen. Jedoch können Sie die Backup-Sätze durchsuchen. Wenn Sie granulare Daten aus den Backup-Sätzen wiederherstellen möchten, durchsucht Backup Exec die Backup-Sätze nach granularen Daten. Wenn Sie diese Option wählen, dauert das Suchen nach granularen Daten beim Wiederherstellen etwas länger.

Vollständige Katalogisierung
 sofort nach Abschluss des
 Backup-Auftrags als
 separaten Auftrag ausführen

Wählen Sie diese Option, um die vollständige
 Katalogisierung sofort nach dem Abschluss eines
 Backup-Auftrags auszuführen. Die Katalogisierung wird
 als separater Auftrag ausgeführt.

Für Exchange- und SharePoint-Backups mit Agent wird
 die vollständige Katalogisierung sofort nach allen
 vollständigen Backups ausgeführt. Sie wird einmal alle
 24 Stunden für alle inkrementelle und differenzielle
 Backups ausgeführt.

Für Hyper-V- und VMware-Backups wird die vollständige
 Katalogisierung sofort nach allen vollständigen,
 inkrementellen und differenziellen Backups ausgeführt.

Hinweis: Sie müssen die wiederherzustellenden Daten
 aus den Backup-Sätzen auswählen, bevor die
 vollständige Katalogisierung abgeschlossen ist. Der
 Suchassistent ist dafür nicht verfügbar. Der
 Suchassistent ist erst nach Abschluss der vollständigen
 Katalogisierung verfügbar.

Vollständige Katalogisierung
 nach Abschluss des
 Backup-Auftrags als
 separaten Auftrag planen

Wählen Sie diese Option, um die vollständige
 Katalogisierung als separaten geplanten Auftrag
 auszuführen. Wählen Sie dann die Startzeit und die
 Wochentage aus, an denen Sie die vollständige
 Katalogisierung ausgeführt werden soll.

Wenn Sie die vollständige Katalogisierung planen, wird
 sie nur für den neuesten Backup-Satz seit der letzten
 Katalogisierung ausgeführt. In dieser Situation kann nur
 der neueste Backup-Satz seit der letzten Katalogisierung
 für die granulare Wiederherstellung verwendet werden.

Hinweis: Sie müssen die wiederherzustellenden Daten
 aus den Backup-Sätzen auswählen, bevor die
 vollständige Katalogisierung abgeschlossen ist. Der
 Suchassistent ist dafür nicht verfügbar. Der
 Suchassistent ist erst nach Abschluss der vollständigen
 Katalogisierung verfügbar.

4 Klicken Sie auf "OK".

Siehe ["Ändern der Standardeinstellungen für Backup-Aufträge"](#) auf Seite 630.

Siehe ["Sichern von Daten"](#) auf Seite 174.

Siehe ["So funktioniert die Katalogisierung mit virtuellen Backups über Hyper-V"](#)
 auf Seite 1185.

Siehe ["So funktioniert die Katalogisierung mit virtuellen Backups über VMware"](#) auf Seite 1120.

Konfigurieren von Advanced Open File-Optionen für Backup-Aufträge

Die Backup Exec-Funktion "Advanced Open File" kann mithilfe von Snapshots alle Dateien erfassen, die geöffnet sind, wenn ein Backup ausgeführt wird. Sie können Optionen für Advanced Open File als Standardeinstellungen für alle Backup-Aufträge konfigurieren. Wenn die Standardeinstellungen nicht für einen bestimmten Auftrag geeignet sind, können Sie sie außer Kraft setzen, wenn Sie den Auftrag erstellen. Sie müssen jedoch keine Standardeinstellungen für Advanced Open File-Optionen erstellen. Wenn Sie Advanced Open File-Optionen nur für spezifische Aufträge verwenden möchten, können Sie die Einstellungen konfigurieren, wenn Sie diese Aufträge erstellen.

So konfigurieren Sie Advanced Open File-Optionen für Backup-Aufträge

1 Sie haben folgende Möglichkeiten:

So konfigurieren Sie Advanced Open File-Optionen für alle Backup-Aufträge

Führen Sie die folgenden Schritte durch:

- Klicken Sie auf die Schaltfläche "Backup Exec" und wählen Sie dann "Konfiguration und Einstellungen".
- Wählen Sie "Auftragsstandardeinstellungen" und wählen Sie dann den Backup-Typ aus, für den Sie Advanced Open File-Optionen konfigurieren möchten.

So konfigurieren Sie Advanced Open File-Optionen für spezifische Backup-Aufträge

Führen Sie die folgenden Schritte durch:

- Erstellen Sie eine neue Backup-Definition oder bearbeiten Sie eine vorhandene Backup-Definition.
- Klicken Sie im Dialogfeld "Backup" auf "Bearbeiten".

2 Klicken Sie im linken Teilfenster auf "Advanced Open File".

3 Konfigurieren Sie folgende Optionen:

Snapshot-Verfahren verwenden

Wählen Sie diese Option aus, um Snapshots für Backup-Aufträge zu aktivieren.

Snapshot-Provider

Wählen Sie einen der folgenden Snapshot-Provider aus:

- **Automatisch** - Auswahl des Snapshot-Providers durch VSS.
Wählen Sie diese Option, damit VSS den besten Provider für den ausgewählten Datenträger auswählen kann.
- **System** - Microsoft Softwareschattenkopie-Anbieter verwenden
- **Hardware** - Vom Hardwarehersteller zur Verfügung gestellte Technologie verwenden

Wenn Sie mehrere Datenträger auswählen, müssen Sie für alle Datenträger denselben Snapshot-Provider auswählen. Sie können Snapshots mehrerer Datenträger mit demselben Provider erstellen, oder Sie können mehrere Provider nutzen, aber der Einsatz von System- und Hardware-Providern im selben Snapshot ist nicht möglich.

Logische Datenträger für das Backup nacheinander verarbeiten

Wählen Sie diese Option aus, um mehrere Datenträger in einem Auftrag zu sichern, wobei immer nur der Snapshot eines logischen Datenträgers auf einmal erstellt wird. Um die Datenintegrität zu gewährleisten oder wenn ein Datenträger Bereitstellungspunkte enthält, müssen eventuell Snapshots mehrerer Datenträger nacheinander erstellt werden. Zum Erstellen eines Snapshot wird ein Datenträger mit Bereitstellungspunkten für andere Datenträger als logischer Datenträger betrachtet. Dieser Datenträger und die Bereitstellungspunkt datenträger werden daher gleichzeitig im selben Snapshot erfasst.

Nachdem ein Snapshot des logischen Datenträgers erstellt und der logische Datenträger gesichert wurde, wird der Snapshot erkannt, bevor ein Snapshot des nächsten logischen Datenträgers erstellt wird. Durch diese Option wird das Einhalten der Mindestruhezeit zum Abschließen des Snapshot erhöht.

Ein logischer Datenträger kann aus mehreren physischen Datenträgern bestehen, d. h. ein einzelner logischer Datenträger kann alle Datenträger der Datenbank umfassen.

Wenn diese Option nicht ausgewählt wurde, werden die Snapshots für alle Datenträger im Backup-Auftrag gleichzeitig erstellt. Für alle Datenträger muss die Mindestruhezeit eingehalten werden.

Diese Option ist nur für lokale Datenträger verfügbar.

Die Schattenkopie-Komponenten-Snapshots werden unter Verwendung von VSS erstellt. Der Vorgang wird im Auftragsprotokoll aufgezeichnet.

Auftragswiederaufnahme
aktivieren

Wählen Sie diese Option aus, um die Option "Auftragswiederaufnahme" zu aktivieren. Mit der Auftragswiederaufnahme kann Backup Exec einen Auftrag, der unterbrochen wurde, automatisch neu starten. Der Auftrag wird von dem Punkt neu gestartet, an dem er unterbrochen wurde. Nachdem der Auftrag beendet wurde, wartet Backup Exec zwei Minuten lang und versucht dann einmal, den unterbrochenen Auftrag neu zu starten. Wenn der Auftrag nicht automatisch neu gestartet werden kann, oder wenn die Auftragswiederaufnahme deaktiviert ist, müssen Sie ihn manuell neu starten. Bei einem manuellen Neustart wird der Auftrag vom Anfang anstatt von dem Punkt aus neu gestartet, an dem der Auftrag unterbrochen wurde.

Siehe ["Konfigurieren der Auftragswiederaufnahme"](#) auf Seite 667.

4 Klicken Sie auf "OK".

Siehe ["Ändern der Standardeinstellungen für Backup-Aufträge"](#) auf Seite 630.

Siehe ["Sichern von Daten"](#) auf Seite 174.

Konfigurieren der Auftragswiederaufnahme

Mit der Auftragswiederaufnahme kann Backup Exec einen Auftrag, der unterbrochen wurde, automatisch neu starten. Der Auftrag wird von dem Punkt neu gestartet, an dem er unterbrochen wurde. Nachdem der Auftrag beendet wurde, wartet Backup Exec zwei Minuten lang und versucht dann, den unterbrochenen Auftrag neu zu starten. Wenn der Auftrag nicht automatisch neu gestartet werden kann, oder wenn die Auftragswiederaufnahme deaktiviert ist, müssen Sie ihn manuell neu starten. Bei einem manuellen Neustart wird der Auftrag vom Anfang anstatt von dem Punkt aus neu gestartet, an dem der Auftrag unterbrochen wurde.

Hinweis: Die Auftragswiederaufnahme kann einen Backup-Auftrag erst neu starten, wenn mindestens 32 MB Daten gesichert wurden. Wenn ein Backup-Auftrag fehlschlägt, bevor er mindestens diese Datenmenge gesichert hat, können Sie ihn manuell erneut ausführen.

Sie können die Auftragswiederaufnahme für Aufträge aktivieren, die mit der Speicheroption "Medien überschreiben" konfiguriert sind. Wenn es jedoch keine überschreibbaren Medien gibt und der Auftrag unterbrochen wird, wird er angehalten,

bis überschreibbare Medien verfügbar sind. Wenn die Medien verfügbar sind, wird der Auftrag an dem Punkt neu gestartet, an dem er unterbrochen wurde.

Backup Exec bricht automatisch alle Aufträge ab, deren Ausführung gemäß den Zeitplaneinstellungen, die bei Auftragserstellung festgelegt haben, zu lange dauert. Wenn Backup Exec einen Auftrag automatisch abbricht, kann dieser nicht neu gestartet werden. Wenn Sie einen Auftrag manuell abbrechen, versucht Backup Exec nicht automatisch, ihn neu zu starten.

Hinweis: Wenn Sie das Central Admin Server Feature (CAS) verwenden, werden alle neu gestarteten Aufträge auf dem verwalteten Backup Exec-Server ausgeführt, auf dem der Auftrag fehlgeschlagen ist. Wenn der ursprüngliche Backup Exec-Server nicht verfügbar ist, wählt Backup Exec einen anderen Backup Exec-Server zum Ausführen des neu gestarteten Auftrags aus.

Sie können die Auftragswiederaufnahme bei der Erstellung von Backup-Aufträgen im Dialogfeld "Advanced Open File Option" aktivieren oder deaktivieren.

Siehe "[Konfigurieren von Advanced Open File-Optionen für Backup-Aufträge](#)" auf Seite 664.

Dieses Thema enthält folgende Informationen:

[Für die Auftragswiederaufnahme unterstützte Funktionen](#)

[Erwägungen zum Einsatz der Auftragswiederaufnahme](#)

[Ändern der Einstellungen für die Auftragswiederaufnahme](#)

Für die Auftragswiederaufnahme unterstützte Funktionen

Die Auftragswiederaufnahme wird nur für NTFS-Datenträger unterstützt. Die einzige Art von Snapshot-Technologie, die für die Auftragswiederaufnahme unterstützt wird, ist VSS.

Die Auftragswiederaufnahme wird für Folgendes nicht unterstützt:

- FAT-Datenträger
- FAT32-Datenträger
- UNIX-Computer
- Gemeinsam genutzte Datenträger (Cluster Shared Volumes, CSV)
- Anwendungsagenten
- Inkrementelle oder Differenzial-Backups
- Aufträge, die Kataloge verwenden, um zu bestimmen, ob eine Datei gesichert wurde

Siehe ["Ermittlung des Backup-Status von Dateien in Backup Exec"](#) auf Seite 218.

Erwägungen zum Einsatz der Auftragswiederaufnahme

Sie sollten Folgendes berücksichtigen, bevor Sie die Auftragswiederaufnahme verwenden:

- Wenn der Fehler während eines Anhängauftrags auftritt, können die Medien nicht mehr angehängt werden. Die Medien können erst wieder angehängt werden, wenn der Auftrag gelöscht oder überschrieben wurde oder die Aufbewahrungsdauer abgelaufen ist. Beim Neustart verwendet Backup Exec neue Medien. Sie sollten eine geeignete Stufe für den Medienüberschreibschutz auswählen, um sicherzustellen, dass der Neustart nicht die Medien überschreibt, die vor dem Fehlschlag des Auftrags verwendet wurden.
- Wenn der Fehler während eines Überprüfensauftrags oder eines Auftrags zur Überprüfung der Datenbankkonsistenz auftritt, wird der Auftrag komplett neu gestartet.
- Vollständige Backups, die zum Zeitpunkt des Auftretens des Fehlers unterbrochen und wieder aufgenommen wurden, werden nicht im Simplified Disaster Recovery-Assistenten "Computer wiederherstellen" angezeigt. Diese Backup-Sätze können aber manuell wiederhergestellt werden, nachdem Sie die erste Wiederherstellung mit dem Assistenten "Computer wiederherstellen" ausgeführt haben.
- Sie können die Auftragswiederaufnahme-Option für einen vollständigen Backup-Auftrag aktivieren, der die Option "Ausgewählte Dateien und Ordner nach erfolgreichem Backup löschen" verwendet. Wenn der Auftrag fehlschlägt und wieder aufgenommen wird, werden die Dateien nicht aus dem Quelldatenträger gelöscht, nachdem das Backup abgeschlossen ist.

Ändern der Einstellungen für die Auftragswiederaufnahme

Sie können die Standard- Auftragswiederaufnahmeeinstellungen in den Fehlerbehandlungsregeleinstellungen ändern. Sie können angeben, wie oft die Auftragswiederaufnahme einen fehlgeschlagenen Auftrag wiederholt, den Abstand zwischen Wiederaufnahmeversuchen und die endgültige Behandlung von Aufträgen, die nicht wiederaufgenommen werden konnten.

So ändern Sie die Standardeinstellungen für die Auftragswiederaufnahme

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Fehlerbehandlungsregeln".
- 2 Wählen Sie "Auftragswiederaufnahme" und klicken Sie dann auf "Bearbeiten".
- 3 Wählen Sie Fehlerbehandlungsregel aktivieren.
- 4 Wählen Sie "Auftrag wiederholen".

5 Füllen Sie die folgenden Felder aus:

Max. Anzahl von Wiederholungen	Geben Sie an, wie oft Backup Exec einen Auftrag wiederholen darf.
Wiederholungsintervall	Geben Sie den Zeitraum in Minuten ein, den Backup Exec warten soll, bevor ein Auftrag neu gestartet wird.

6 Im Gruppenfeld "Endgültige Auftragsbehandlung" wählen Sie eine der folgenden Optionen:

Auftrag anhalten, bis Fehlerbedingung manuell behoben wurde	Wählen Sie diese Option aus, wenn Backup Exec-Platz den Auftrag in Wartestellung zu setzen soll, falls der Auftrag nach der Höchstzahl von Wiederholungen nicht abgeschlossen werden kann. Der Auftrag verbleibt in Wartestellung, bis der Fehlerzustand manuell bereinigt worden ist.
Zeitplan des Auftrags für den nächsten geplanten Dienst ändern	Wählen Sie diese Option, wenn Backup Exec den Auftrag neu zu planen, wenn der Auftrag nicht nach der Höchstzahl von Wiederholungen erfolgreich abgeschlossen werden kann.

7 (Optional)Geben Sie im Feld "Hinweise" Anmerkungen zur Fehlerbehandlungsregel ein.

8 Klicken Sie auf "OK".

Konfigurieren von Befehlen vor oder nach Backup-Aufträgen

Sie können Befehle konfigurieren, die vor oder nach allen Backup-Aufträgen ausgeführt werden sollen. Beispiel: Sie können einen Befehl vor dem Auftrag erstellen, um eine Datenbank auszuschalten, bevor ein Backup-Auftrag ausgeführt wird. Sie können auch einen Befehl nach dem Auftrag erstellen, um die Datenbank nach Abschluss des Auftrags neu zu starten.

Für diese Befehle können Sie die folgenden Bedingungen festlegen:

- Backup-Auftrag nur ausführen, wenn der Befehl vor dem Auftrag erfolgreich war.
- Befehl nach dem Auftrag nur ausführen, wenn der Befehl vor dem Auftrag erfolgreich war.

- Befehl nach dem Auftrag selbst ausführen, wenn der Backup-Auftrag fehlschlägt.
- Backup Exec erlauben, die Rückgabecodes (oder Beendigungscodes) der Befehle vor und nach Aufträgen zu überprüfen, um festzustellen, ob die Befehle erfolgreich ausgeführt wurden
 Wenn Befehl vor oder nach Aufträgen einen Beendigungscode von null zurückgeben, zeigt Backup Exec an, dass der Auftrag erfolgreich abgeschlossen wurde. Backup Exec zeigt alle Beendigungscodes ungleich null an, um anzuzeigen, dass beim Auftrag ein Fehler aufgetreten ist.

Wenn es wichtig ist, dass der Auftrag nicht ausführt wird, wenn der Befehl vor dem Auftrag fehlschlägt, konfigurieren Sie Backup Exec, um die Rückgabecodes zu prüfen. Backup Exec verwendet die Rückgabecodes, um festzulegen, ob der Befehl vor dem Auftrag fehlschlug oder erfolgreich abgeschlossen wurde.

Falls z. B. ein Befehl zum Schließen einer Datenbank vor dem Auftrag fehlschlägt, kann die Datenbank unter Umständen durch den Backup-Vorgang beschädigt werden. In dieser Situation ist es wichtig, dass der Backup-Auftrag nicht ausgeführt wird, wenn der Befehl vor dem Auftrag fehlschlägt.

Wenn Backup Exec konfiguriert wird, um die Rückgabecodes zu prüfen und der Befehl nach dem Auftrag einen Code ungleich null zurückgegeben wird, gibt das Auftragsprotokoll an, dass der Befehl nach dem Auftrag fehlgeschlagen ist. Sie haben möglicherweise auch ausgewählt, dass der Auftrag nur ausgeführt wird, wenn der Befehl vor dem Auftrag erfolgreich ist. Selbst wenn der Befehl vor dem Auftrag und der Auftrag erfolgreich ausgeführt werden, kennzeichnet Backup Exec den Auftrag als fehlgeschlagen, wenn der Befehl nach dem Auftrag fehlschlägt.

Beispielsweise kann der Befehl vor dem Auftrag erfolgreich ausgeführt werden und die Datenbank herunterfahren. Der Backup-Auftrag kann auch erfolgreich ausgeführt werden. Wenn aber der Befehl nach dem Auftrag die Datenbank nicht neu starten kann, kennzeichnet Backup Exec den Auftrag und den Befehl nach dem Auftrag als im Auftragsprotokoll fehlgeschlagen.

Wenn Sie die Option "Auf jedem gesicherten Server" auswählen, trifft die Auswahl der Befehl vor und nach dem Auftrags auf jeden Server unabhängig zu. Die Befehle vor und nach Aufträgen werden für einen Server auf einmal ausgeführt und abgeschlossen, bevor sie auf dem nächsten ausgewählten Server ausgeführt werden.

Sie können Befehle vor oder nach dem Auftrag als Standardeinstellungen für alle Backup-Aufträge konfigurieren. Wenn die Standardannahmen nicht für einen bestimmten Job angebracht sind, können Sie sie außer Kraft setzen, wenn Sie den Job erstellen. Sie müssen jedoch keine Standardeinstellungen für Befehle vor oder nach dem Auftrag erstellen. Wenn Sie Befehle vor oder nach dem Auftrag nur für spezifische Aufträge konfigurieren möchten, können Sie die Einstellungen konfigurieren, wenn Sie die Aufträge erstellen.

Konfigurieren von Befehlen vor oder nach Backup-Aufträgen

1 Sie haben folgende Möglichkeiten:

Standardmäßige Befehle vor oder nach dem Auftrag für alle Backup-Aufträge konfigurieren

- Führen Sie die folgenden Schritte durch:
- Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
 - Wählen Sie "Auftragsstandardeinstellungen" und wählen Sie dann den Backup-Typ aus, für den Sie Befehle vor oder nach dem Auftrag konfigurieren wollen.

Konfigurieren von Befehlen vor oder nach bestimmten Backup-Aufträgen

- Führen Sie die folgenden Schritte durch:
- Erstellen Sie eine neue Backup-Definition oder bearbeiten Sie eine vorhandene Backup-Definition.
 - Klicken Sie im Dialogfeld "Backup" auf "Bearbeiten".

2 Klicken Sie im linken Teilfenster auf "Befehle vor/nach dem Auftrag".

3 Konfigurieren Sie folgende Optionen:

Geben Sie einen vor der Ausführung des Backups auszuführenden Befehl ein	<p>Führt einen Befehl auf dem angegebenen Server aus, bevor der Backup-Auftrag ausgeführt wird. Verwenden Sie lokale Pfade, und stellen Sie sicher, dass die Pfade auf jedem Server vorhanden und korrekt sind.</p> <p>Befehle mit Benutzereingriff (z. B. Aufforderungen) werden nicht unterstützt.</p>
Auftrag nur ausführen, wenn der Befehl vor dem Auftrag erfolgreich war	<p>Führt den Backup-Auftrag nur aus, wenn der Befehl vor dem Auftrag erfolgreich war. Bei Fehlschlagen des Befehls vor dem Auftrag, wird der Auftrag nicht ausgeführt und als fehlgeschlagen gekennzeichnet.</p> <p>Wenn es wichtig ist, dass der Auftrag nicht ausführt wird, wenn der Befehl vor dem Auftrag fehlschlägt, dann wählen Sie die Option "Backup Exec die Beendigungscode der Befehle prüfen lassen, um festzustellen, ob die Befehle erfolgreich abgeschlossen wurden". Wenn ein Beendigungscode ungleich null zurückgegeben wird, interpretiert Backup Exec ihn, um anzuzeigen, dass der Befehl vor dem Auftrag nicht erfolgreich ausgeführt wurde. Der Auftrag wird nicht ausgeführt, und der Auftragsstatus wird auf Fehlgeschlagen gesetzt.</p>
Geben Sie einen nach der Ausführung des Backups auszuführenden Befehl ein	<p>Führt einen Befehl auf dem angegebenen Server aus, nachdem der Backup-Auftrag ausgeführt wurde. Verwenden Sie lokale Pfade und stellen Sie sicher, dass die Pfade auf jedem Server vorhanden und korrekt sind.</p> <p>Befehle mit Benutzereingriff (z. B. Aufforderungen) werden nicht unterstützt.</p>
Befehl nach Auftrag nach Auftragsüberprüfung ausführen	<p>Führt nach der Überprüfung den Befehl nach dem Auftrag aus, wenn Sie einen Überprüfungsvorgang für den Auftrag konfiguriert haben.</p> <p>Siehe "Konfigurieren der automatischen Prüfung von Aufträgen" auf Seite 655.</p>

Befehl nach dem Auftrag nur ausführen, wenn der Befehl vor dem Auftrag erfolgreich war

Führt den Befehl nach dem Auftrag nur aus, wenn der Befehl vor dem Auftrag erfolgreich war.

Wenn es wichtig ist, dass der Befehl nach dem Auftrag nicht ausführt wird, wenn der Befehl vor dem Auftrag fehlschlägt, dann wählen Sie die Option "Backup Exec die Beendigungscode der Befehle prüfen lassen, um festzustellen, ob die Befehle erfolgreich abgeschlossen wurden". Wenn ein Beendigungscode ungleich null zurückgegeben wird, interpretiert Backup Exec ihn, um anzuzeigen, dass der Befehl vor dem Auftrag nicht erfolgreich ausgeführt wurde. Der Befehl nach dem Auftrag wird nicht ausgeführt.

Wenn Sie außerdem die Option "Auftrag nur ausführen, wenn der Befehl vor dem Auftrag erfolgreich war" auswählen und die Ausführung des Befehls vor dem Auftrag sowie des Auftrags selbst erfolgreich waren, der Befehl nach dem Auftrag jedoch einen Code ungleich Null zurückgibt, werden sowohl der Auftrag als auch der Befehl nach dem Auftrag im Auftragsprotokoll als fehlgeschlagen aufgeführt.

Befehl nach dem Auftrag ausführen, auch wenn Auftrag fehlschlägt

Führt den Befehl nach dem Auftrag unabhängig davon aus, ob der Auftrag erfolgreich ist.

Wenn Sie ebenfalls die Option "Backup Exec die Beendigungscode der Befehle prüfen lassen, um festzustellen, ob die Befehle erfolgreich abgeschlossen wurden" auswählen und der Befehl nach dem Auftrag einen Code ungleich Null zurückgibt, wird der Befehl nach dem Auftrag im Auftragsprotokoll als fehlgeschlagen aufgeführt.

Backup Exec die Beendigungscode der Befehle prüfen lassen, um festzustellen, ob die Befehle erfolgreich abgeschlossen wurden	<p>Ermöglicht Backup Exec die Überprüfung der Rückgabecodes von Befehlen vor und nach dem Auftrag, um festzustellen, ob sie erfolgreich abschlossen wurden.</p> <p>Backup Exec interpretiert einen Beendigungscode von null entweder vom Befehle vor oder nach Aufträgen, um anzuzeigen, dass der Befehl erfolgreich abgeschlossen wurde. Backup Exec interpretiert einen Beendigungscode ungleich null, um anzuzeigen, dass der Befehl mit einem Fehler beendet wurde.</p> <p>Nachdem Backup Exec die Rückgabecodes geprüft hat, fährt das Programm mit der Verarbeitung entsprechend der Auswahl fort, die Sie für das Ausführen für Befehle vor und nach Aufträgen vorgenommen haben.</p> <p>Wird diese Option nicht ausgewählt, wird die erfolgreiche Ausführung der Befehle vor und nach Aufträgen nicht anhand der Rückgabecodes ermittelt.</p>
Auf diesem Backup Exec-Server	Führt Befehle vor und nach dem Auftrag nur auf diesem Backup Exec-Server aus.
Auf jedem gesicherten Server	<p>Führt Befehle vor und nach Aufträgen einmal auf jedem Server aus, der gesichert wird.</p> <p>Die ausgewählten Optionen für die Befehle vor und nach Aufträgen gelten unabhängig voneinander für jeden Server. Wenn Sie diese Option auswählen, werden die Befehle vor und nach Aufträgen auf jedem Server vollständig ausgeführt, bevor die Verarbeitung auf dem nächsten Server begonnen wird.</p>
Befehl abbrechen, falls nicht abgeschlossen innerhalb von x Minuten	Gibt die Anzahl der Minuten an, die Backup Exec warten soll, bevor ein nicht beendeter Befehl vor oder nach Aufträgen abgebrochen wird. Die Standardzeitüberschreitung ist 30 Minuten.

4 Klicken Sie auf "OK".

Siehe ["Ändern der Standardeinstellungen für Backup-Aufträge"](#) auf Seite 630.

Siehe ["Sichern von Daten"](#) auf Seite 174.

Konfigurieren von Datei- und Ordneroptionen für Backup-Aufträge

Ermöglicht die Konfiguration von Optionen für die Verarbeitung von Dateisystemattributen, wie zum Beispiel von Abzweigungen und symbolischen Links.

Datei- und Ordneroptionen können als Standardeinstellungen für alle Backup-Aufträge konfiguriert werden. Wenn die Standardannahmen nicht für einen bestimmten Job angebracht sind, können Sie sie außer Kraft setzen, wenn Sie den Job erstellen. Sie müssen jedoch keine Standardeinstellungen für Dateien und Ordner erstellen. Wenn Sie Dateien und Ordner nur für bestimmte Aufträge konfigurieren möchten, können Sie die Einstellungen konfigurieren, wenn Sie die Aufträge erstellen.

Konfigurieren von Datei- und Ordneroptionen für Backup-Aufträge

1 Sie haben folgende Möglichkeiten:

Konfigurieren von standardmäßigen Datei- und Ordneroptionen für alle Backup-Aufträge

Führen Sie die folgenden Schritte durch:

- Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- Wählen Sie "Auftragsstandardeinstellungen" und wählen Sie dann den Backup-Typ aus, für den Sie Datei- und Ordneroptionen konfigurieren wollen.

Konfigurieren von Datei- und Ordneroptionen für bestimmte Backup-Aufträge

Führen Sie die folgenden Schritte durch:

- Erstellen Sie eine neue Backup-Definition oder bearbeiten Sie eine vorhandene Backup-Definition.
- Klicken Sie im Dialogfeld "Backup" auf "Bearbeiten".

2 Klicken Sie im linken Teilfenster auf "Dateien und Ordner".

3 Konfigurieren Sie folgende Optionen:

Backup-Methode für Dateien

Wählen Sie eine der folgenden Backup-Methoden:

- **Nach Änderungszeit**

Wenn Backup Exec ein vollständiges oder inkrementelles Backup ausführt, wird die Startzeit des Backups in der Backup Exec-Datenbank aufgezeichnet. Backup Exec fügt den Zeitpunkt des Backup-Auftrags nur dann der Backup Exec-Datenbank hinzu, wenn der vollständige Backup-Auftrag erfolgreich abgeschlossen wird. Beim nächsten inkrementellen oder Differenzial-Backup-Auftrag vergleicht Backup Exec die Dateisystemzeit mit der Backup-Zeit. Wenn die Dateisystemzeit einen späteren als den in der Datenbank aufgezeichneten Zeitpunkt angibt, wird die Datei gesichert. Wenn das Änderungsdatum der Datei älter als das Änderungsdatum des vorherigen Backups ist, wird diese Datei nicht gesichert. Wird der Auftrag nicht erfolgreich abgeschlossen, werden bei folgenden inkrementellen oder Differenzial-Backup-Aufträgen sämtliche Daten anstatt nur der geänderten Daten gesichert.

Hinweis: Das Datum und der Zeitstempel der letzten Änderung ändern sich nicht, wenn die Datei kopiert oder verschoben wird. Um sicherzustellen, dass die Dateien geschützt sind, führen Sie nach dem Kopieren oder Verschieben der Dateien ein vollständiges Backup aus.

Wenn Sie einen inkrementellen Backup-Auftrag ausführen, zeichnet Backup Exec eine neue Zeit in der Backup Exec-Datenbank auf. Die Datenbankzeit wird bei Differenzial-Backup-Aufträgen nicht aktualisiert.

Wenn Sie die Methode "Geänderte Uhrzeit" auswählen, verwendet Backup Exec das Windows-Änderungsjournal, um zu ermitteln, ob eine Datei seit ihrer letzten Sicherung geändert wurde. Wenn das Änderungsjournal nicht verfügbar ist, vergleicht Backup Exec die Dateinformationen mit der vorherigen Backup-Zeit, um zu ermitteln, ob die Datei geändert wurde.

Bei Verwendung der Methode "Geänderte Uhrzeit" kann Backup Exec präzisere inkrementelle oder Differenzial-Backups ausführen, selbst wenn andere Vorgänge Archivbits von geänderten Dateien haben.

- **Archivbit verwenden**

Backup Exec verwendet das Archivbit des Dateisystems, um zu ermitteln, ob eine Datei seit ihrer letzten Sicherung geändert wurde.

Verwenden Sie das Archivbit, setzt Backup Exec das Archivbit zurück, wenn eine Datei gesichert wird. Durch das Zurücksetzen wird Backup Exec angezeigt, dass die Datei gesichert wurde. Wenn die Datei vor dem nächsten Backup wieder geändert wird, wird das Bit wieder aktiviert. Backup Exec sichert die Datei im nächsten Backup.

Wenn der nächste Backup-Auftrag ein vollständiger oder ein inkrementeller Backup-Auftrag ist, wird das Bit bei Abschluss des Backup-Auftrags deaktiviert. Wenn der nächste Backup-Auftrag ein Differenzial-Backup-Auftrag ist, bleibt das Archivbit intakt.

- **Kataloge verwenden**

Backup Exec vergleicht Pfadnamen, Änderungszeit, gelöschte und umbenannte Dateien und Ordner sowie andere Attribute. Wenn Sie die Katalog-Methode auswählen, verwendet Backup Exec das Windows-Änderungsjournal, um zu ermitteln, ob eine Datei seit ihrer letzten Sicherung geändert wurde. Wenn das Änderungsjournal nicht verfügbar ist, vergleicht Backup Exec die Dateiinformationen mit vorherigen Katalogen, um festzustellen, ob eine Änderung stattgefunden hat.

Hinweis: Sie können Backup Exec-Kataloge nicht verwenden, um zu bestimmen, ob Dateien für beliebige differenzielle Backups gesichert wurden.

Die Katalog-Methode ist nur verfügbar, wenn Advanced Disk-based Backup Feature (ADBO) installiert ist.

Hinweis: Die Off-Host-Backup-Funktion von ADBO unterstützt die Katalog-Methode nicht.

Siehe ["Ermittlung des Backup-Status von Dateien in Backup Exec"](#) auf Seite 218.

Single Instance-Backup für NTFS-Datenträger aktivieren Wählen Sie diese Option aus, wenn Backup Exec den NTFS-Datenträger auf identische Dateien überprüfen soll. Wenn mehrere Exemplare einer Datei gefunden werden, wird nur eines davon gesichert.

Die Single Instance-Backup kann den für Ihre Backups benötigten Speicherplatz deutlich verringern. In zahlreichen Anwendungen werden automatisch einige Dateien mit identischem Inhalt generiert. Der tatsächliche Speicherplatz, der durch diese Funktion gespart werden kann, hängt von der Anzahl der Dateiduplikate auf dem Datenträger ab.

Diese Option wird nur bei Verwendung von Microsoft Windows Single Instance Store (SIS) angezeigt.

Diese Option ist nicht relevant, wenn die zu sichernden Daten sich auf einem Computer mit Windows Server 2016 oder höher befinden, da Microsoft die Funktion "Einzelinstanzspeicher" (SIS) nicht mehr unterstützt.

Warnung: Wenn der Backup-Auftrag nicht vollständig ausgeführt wird, sind die Dateidaten möglicherweise nicht im Backup-Satz enthalten. Wiederholen Sie den Backup-Auftrag, bis sie erfolgreich abgeschlossen wird. Wenn die inkrementelle Backup-Methode verwendet wurde, werden beim erneuten Ausführen des Auftrags nicht dieselben Dateien gesichert. Um sicherzustellen, dass alle Dateien vollständig gesichert wurden, müssen Sie einen vollständigen oder Duplizierungs-Backup-Auftrag ausführen.

Dateien und Verzeichnisse nach Abzweigungen und Bereitstellungspunkten sichern

Wählen Sie diese Option aus, um Informationen über die Abzweigungen sowie die Dateien und die Verzeichnisse, mit denen sie verbunden sind, zu sichern. Wenn dieses Kontrollkästchen nicht aktiviert wird, werden nur die Informationen über die Abzweigungen gesichert. Die Dateien und Verzeichnisse, mit denen die Abzweigungen verknüpft sind, werden nicht gesichert.

Backup Exec folgt nicht den von Microsoft Windows automatisch erstellten Abzweigungen, da dies zum wiederholten Backup derselben Daten führen kann.

Sie können keine eingerichteten Laufwerke auswählen, denen kein Laufwerksbuchstabe zugewiesen ist. Die Dateien und die Verzeichnisse, mit denen sie verknüpft sind, werden gesichert, unabhängig davon, ob diese Option ausgewählt ist.

Wenn die Dateien und Verzeichnisse, mit denen die Abzweigungen verknüpft sind, auch in den Backup-Auswahlen enthalten sind, werden sie zweimal gesichert. Sie werden einmal während des vollständigen Datei- und Verzeichnisbackups und dann noch einmal von der Abzweigung gesichert.

Warnung: Wenn eine Abzweigung mit einem Speicherort verknüpft ist, der sie umgibt, findet eine Rekursion statt (d. h. Daten werden wiederholt gesichert). Die Rekursion führt zu einem Fehler und dem Scheitern des Auftrags. Wenn beispielsweise c:\junctionpoint mit c:\ verknüpft ist, findet eine Rekursion statt, wenn Backup Exec versucht, c:\junctionpoint zu sichern. Dies führt zum Scheitern des Backup-Auftrags.

Bei Backup von Dateien und Verzeichnissen symbolischen Verknüpfungen folgen

Wählen Sie diese Option aus, um Informationen über die symbolischen Verknüpfungen sowie die Dateien und Verzeichnisse, mit denen sie verbunden sind, zu sichern.

Wenn Sie diese Option nicht wählen, werden nur die symbolischen Verknüpfungen gesichert. Die Dateien und Verzeichnisse, auf die sie verweisen, bleiben von dem Backup ausgeschlossen.

Verweist die symbolische Verknüpfung auf Dateien und Verzeichnisse auf einem Remote-Computer, werden die Dateien und Verzeichnisse auf dem Remote-Computer nicht gesichert.

Daten in Remotespeicher sichern

Wählen Sie diese Option aus, um alle Daten, die vom Hauptspeicher zum sekundären Speichermedium migriert worden sind, zu sichern. Die Daten werden nicht an den ursprünglichen Speicherort zurückverschoben, sondern direkt auf dem Backup-Medium gesichert.

Wenn diese Option ausgewählt wird, sollten Sie kein Backup Ihres gesamten Systems ausführen. Backup Exec muss die Daten laden, die auf ein sekundäres Speichermedium migriert wurden, und es ist zusätzliche Zeit für migrierte Daten erforderlich.

Wenn Sie dieses Kontrollkästchen deaktivieren, wird nur der Platzhalter zum Speicherort der Daten im sekundären Speicher gesichert. Die Daten selbst werden nicht gesichert.

Diese Option sollte nicht ausgewählt werden, wenn das Gerät, das für sekundäre Speichermedien und Backups verwendet wird, nur ein Laufwerk enthält. Wenn es nur ein Laufwerk gibt, versuchen sowohl Remote-Speicher als auch Backup Exec, auf das Laufwerk zuzugreifen.

Sichern offener Dateien

Wählen Sie eine der folgenden Optionen aus, um festzulegen, wie Backup Exec alle geöffneten Dateien für den Backup-Auftrag verarbeitet.

Folgende Optionen sind verfügbar:

- **Nie**
Backup Exec überspringt während des Backup-Vorgangs erkannte geöffnete Dateien. Eine Liste aller Dateien, die übersprungen wurden, wird im Auftragsprotokoll angezeigt.
- **Beim Schließen innerhalb von x Sekunden**
Backup Exec wartet entsprechend des angegebenen Zeitintervalls, bis Dateien geschlossen werden, bevor es sie überspringt und den Backup-Auftrag fortsetzt. Dateien, die nicht innerhalb dieser Zeit geschlossen werden, werden übersprungen. Eine Liste von übersprungenen Dateien wird im Auftragsprotokoll angezeigt.

Wenn mehrere Dateien geöffnet sind, wartet Backup Exec das angegebene Zeitintervall für jede Datei ab. Abhängig von der Anzahl von geöffneten Dateien erhöht möglicherweise die Wartezeit erheblich die für das Backup erforderliche Zeit.

- **Mit Sperre**
Backup Exec versucht die aktuell verwendeten Dateien zu öffnen. Wenn Backup Exec die Datei öffnen kann, wird sie während des Backups gesperrt. Das Sperren der Datei hindert andere Prozesse daran, in diese zu schreiben.
Das Sichern geöffneter Dateien ist nicht so effektiv wie das Schließen von Anwendungen. Wenn keine Anwendungen geöffnet sind, können die Dateien in einem konsistenten Zustand gesichert werden.
- **Ohne Sperre**
Backup Exec versucht die aktuell verwendeten Dateien zu öffnen. Wenn Backup Exec die Datei öffnen kann, wird sie während des Backups nicht gesperrt. So können andere Anwendungen während des Backups Daten in die Datei schreiben.

Warnung: Diese Option ermöglicht das Sichern von Dateien, die inkonsistente und eventuell beschädigte Daten enthalten.

Backup-Methode	<p>Wählen Sie die Backup-Methode aus, die Sie zum Sichern von Dateien und Ordnern für jeden Backup-Auftrag in der Backup-Definition verwenden wollen.</p> <p>Siehe "Backup-Methoden in Backup Exec" auf Seite 205.</p>
Ausgewählte Dateien und Ordner nach erfolgreichem Backup löschen	<p>Wählen Sie diese Option aus, wenn Backup Exec die Daten löschen soll, die Sie für das Backup ausgewählt haben, nachdem der Backup-Auftrag erfolgreich abgeschlossen wurde.</p> <p>Backup Exec sichert die ausgewählten Daten, überprüft die Backup-Sätze und löscht dann die Daten vom Server. Das Login-Konto, das Sie zum Ausführen des Auftrags verwenden, muss auch über Rechte zum Löschen von Dateien verfügen. Andernfalls werden die Daten zwar gesichert, aber nicht gelöscht.</p> <p>Hinweis: Diese Option ist beim Konfigurieren von Backup-Aufträgen verfügbar. Sie können sie nicht als Standardeinstellung für alle Backup-Aufträge konfigurieren.</p> <p>Siehe "Konfigurieren von Backup Exec, um Dateien nach einem Backup automatisch zu löschen" auf Seite 222.</p>
Struktur beim Sichern und Löschen beibehalten	<p>Wählen Sie diese Option aus, um die Verzeichnisstruktur des Dateisystems für die Dateien beizubehalten, die durch einen vollständigen Backup-Auftrag gesichert werden. Diese Option ist nur verfügbar, wenn Sie die Option "Ausgewählte Dateien und Ordner nach erfolgreichem Backup löschen" auswählen.</p>

4 Klicken Sie auf "OK".

Siehe ["Ändern der Standardeinstellungen für Backup-Aufträge"](#) auf Seite 630.

Siehe ["Sichern von Daten"](#) auf Seite 174.

Standardmäßige Zeitplanoptionen für richtliniengesteuerte Aufträge und für Aufträge zum sofortigen Ausführen einstellen

Sie können standardmäßige Zeitplanoptionen für regelbasierte Aufträge und für Aufträge zum sofortigen Ausführen konfigurieren. Backup Exec wendet die Zeitplanoptionen an, wenn Sie einen richtliniengesteuerten Auftrag oder einen Auftrag zum sofortigen Ausführen in einen wiederkehrenden geplanten Auftrag ändern. Ein richtliniengesteuerter Auftrag ist ein Auftrag, der mit einem anderen Auftrag verknüpft ist. Der richtliniengesteuerte Auftrag wird ausgeführt, wenn der Auftrag, mit dem er verknüpft ist, beendet wurde. Ein Beispiel: Ein richtliniengesteuerter Auftrags würde doppelt ausgeführt, wenn er nach einem vollständigen Backup-Auftrag abgeschlossen werden soll. Wenn Sie die Zeitplaneinstellungen des doppelt ausgeführten Auftrags ändern, nutzt Backup Exec die Standardzeitplaneinstellungen für die doppelte Staffelung. Sie können die Standardeinstellungen übergehen, wenn Sie den neu geplanten Auftrag bearbeiten.

Standardmäßige Zeitplanoptionen für richtliniengesteuerte Aufträge und für Aufträge zum sofortigen Ausführen einstellen

- 1 Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und dann "Auftragsstandardeinstellungen".
- 2 Wählen Sie "Zeitplan" aus.
- 3 Im Gruppenfeld "Wiederholungsmuster" wählen Sie die Standard-Häufigkeit für Backup-Aufträge aus:

So führen Sie Aufträge alle x Stunden oder Minuten aus Klicken Sie auf "Stunden" und geben Sie dann im Feld "Alle x Stunden/Minuten" die Häufigkeit ein.

Wählen Sie aus folgenden Optionen:

- Von
Gibt die Startzeit eines Auftrags an.
- Zwischen
Schränkt den Auftrag auf bestimmte Stunden und Tage ein. Beispiel: Wenn der Auftrag nur während der Geschäftszeiten ausgeführt werden soll, können Sie 9:00 bis 17:00 Uhr am Montag, Dienstag, Mittwoch, Donnerstag und Freitag auswählen.

So führen Sie Aufträge alle x Tage aus Klicken Sie auf "Tage" und wählen Sie dann aus folgenden Optionen:

- Alle X Tage
Gibt die Anzahl von Tagen zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz an.
- Jeden Wochentag
Gibt an, dass der Auftrag Montag, Dienstag, Mittwoch, Donnerstag und Freitag ausgeführt werden soll.

So führen Sie Aufträge alle x Wochen aus Klicken Sie auf "Wochen" und geben Sie dann die Anzahl Wochen zwischen der Startzeit eines Auftrags und der Startzeit der nächsten Auftragsinstanz im Feld "Alle x Wochen um" field.

Wählen Sie die Tage und die Zeit aus, an denen Aufträge ausgeführt werden sollen.

So führen Sie Aufträge alle x Monate aus Klicken Sie auf "Monate" und wählen Sie dann aus folgenden Optionen:

- **Tag X jedes X. Monats**
Geben Sie den bestimmten Tag an, an dem Aufträge ausgeführt werden sollen und geben Sie die Anzahl von Monaten zwischen der Startzeit eines Auftrags und der Startzeit der folgenden Auftragsinstanz an.
- **Jeden X X jedes X. Monats**
Geben Sie den Tag an, an dem Aufträge ausgeführt werden sollen und geben Sie die Anzahl von Monaten zwischen der Startzeit eines Auftrags und der Startzeit der folgenden Auftragsinstanz an.
- **Ausgewählte Monatstage**
Geben Sie die Tage des Monats an, an denen Backup Exec Aufträge ausführen soll. Das ausgewählte Wiederholungsmuster wird jeden Monat wiederholt.
Standardmäßig wird der Auftrag jeden Monat ausgeführt und beginnt in der aktuellen Woche und am aktuellen Tag des Monats. Wenn Sie beispielsweise den Auftrag am dritten Montag im Monat erstellen, wird der Auftrag standardmäßig am dritten Montag jedes Monats ausgeführt.
Sie können zusätzliche Tage auswählen, an denen der Auftrag ausgeführt werden soll. Alle zusätzlichen ausgewählten Tage werden dem monatlichen Wiederholungsmuster hinzugefügt.
- **Ausgewählte Daten des Monats**
Geben Sie die Daten des Monats an, an denen Backup Exec Aufträge ausführen soll. Das ausgewählte Wiederholungsmuster wird jeden Monat wiederholt.
Standardmäßig wird der Auftrag jeden Monat ausgeführt und beginnt am aktuellen Tag des Monats. Wenn Sie den Auftrag beispielsweise am 15. April erstellen, wird der Auftrag standardmäßig am 15. jedes Monats ausgeführt.
Sie können zusätzliche Tage auswählen, an denen der Auftrag ausgeführt werden soll. Alle zusätzlichen ausgewählten Tage werden dem monatlichen Wiederholungsmuster hinzugefügt.
Wenn Sie den 31. auswählen, wird der Auftrag in Monaten, die keine 31 Tage haben, am letzten Tag des Monats ausgeführt. Beispiel: Im September wird der Auftrag am 30. ausgeführt.

So führen Sie Aufträge alle x Jahre aus Klicken Sie auf "Stunden" und geben Sie dann im Feld "Alle x Jahre" die Häufigkeit ein.

Wählen Sie aus folgenden Optionen:

- "Am X"
Geben Sie das Datum an, an dem Backup Exec Aufträge ausführen soll.
- "Am X. X"
Geben Sie den Tag und den Monat des Jahres an, an dem Backup Exec Aufträge ausführen soll.

- 4 (Optional) Klicken Sie auf "Kalender", um alle geplanten Backup-Aufträge in einem Kalender anzuzeigen und nach Zeitplankonflikten zu suchen.
- 5 Geben Sie im Feld "Auftrag neu planen, falls er x Stunden nach geplanter Startzeit noch immer nicht gestartet wird." den Zeitraum nach der geplanten Startzeit an, nach dessen Ablauf Backup Exec den Auftragsabschlussstatus in "Verpasst" ändert. Der Auftrag wird so neu geplant, dass er im konfigurierten Zeitraum ausgeführt wird. Der Auftrag wird so neu geplant, das im konfigurierten Zeitfenster ausgeführt wird.
- 6 Geben Sie im Feld "Auftrag abbrechen, falls er x Stunden nach geplanter Startzeit noch immer ausgeführt wird" den Zeitraum nach der geplanten Startzeit des Auftrags ein, an der Sie der Auftrag abgebrochen werden soll, wenn er noch aktiv ist. Backup Exec ändert den Auftragsabschlussstatus in "Abgebrochen, Zeitüberschreitung".
- 7 Klicken Sie auf "OK".

Siehe ["Wie die Joborganisation in Backup Exec arbeitet"](#) auf Seite 239.

Siehe ["Liste von Auftragsstatus in Backup Exec"](#) auf Seite 322.

Ausschließen von Tagen vom Backup-Zeitplan für alle Backups

Sie können bestimmte Tage, wie etwa Feiertage, von Ihrem Backup-Zeitplan ausschließen. Sie sollten Feiertage ausschließen, z.B. um sicherzustellen, dass Backup Exec keine Aufträge an jenen Tagen ausführt. Sie können Tage vom Zeitplan für einen bestimmten Backup-Auftrag oder für alle Backup-Aufträge ausschließen.

Wenn Sie Tage für alle Backups ausschließen, werden geplante Backup-Aufträge an diesen Tagen nicht ausgeführt. Die Ausführung aller Aufträge wird nach dem normalen Zeitplan nach dem ausgeschlossenen Datum fortgesetzt. Sie können

Backup-Aufträge und Wiederherstellungsaufträge auch an ausgeschlossenen Tagen ausführen, dies dürfen jedoch keine geplanten Backups sein.

Um in Backup Exec Tage auszuschließen, wählen Sie diese im Dialogfeld "Auszuschließende Tage" aus oder geben Sie sie dort ein. Oder Sie können eine .txt-Datei mit einer Liste der auszuschließenden Tage erstellen und diese Datei importieren.

Nachdem Sie die Liste der auszuschließenden Tage erstellt haben, können Sie eine neue .txt-Datei mit diesen Tagen exportieren. Das Exportieren der .txt-Datei ist empfehlenswert, wenn Sie die auszuschließenden Tage von einem Backup Exec-Server auf einen anderen kopieren möchten.

Siehe ["Exportieren einer Liste von Daten, die aus allen Backups auf einem anderen Server ausgeschlossen sind"](#) auf Seite 691.

Sie können Daten aus allen Backup in den Auftragsstandardeinstellungen ausschließen oder indem Sie den Backup-Kalender verwenden. Mit beiden Funktionen können Sie Daten aus allen Backups ausschließen. Sie können Daten nur unter Verwendung der Standardeinstellungen importieren. Der Backup-Kalender bietet eine grafische Darstellung aller geplanten Aufträge.

Dieses Thema umfasst die folgenden Vorgänge:

[So schließen Sie Tagen aus dem Backup-Zeitplan für alle Backups aus](#)

[So schließen Sie mit dem Backup-Kalender Tage aus allen Backups aus](#)

So schließen Sie Tagen aus dem Backup-Zeitplan für alle Backups aus

- 1** Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und dann "Auftragsstandardeinstellungen".
- 2** Wählen Sie "Auszuschließende Tage".
- 3** Sie haben folgende Möglichkeiten:

So geben Sie das Datum
manuell ein

Führen Sie die folgenden Schritte durch:

- Geben Sie im Feld "Datum auswählen" das Datum des Tags ein, das Sie aus dem Backup-Zeitplan ausschließen möchten.
- Klicken Sie auf "Hinzufügen".

Hinweis: Sie können nur ein Datum auf einmal hinzufügen.

So wählen Sie das Datum im Kalender Klicken Sie auf das auszuschließende Datum.

Der Kalender zeigt 3 Monate auf einmal an. Sie können weitere Monate vor und nach dem Datum anzeigen, indem Sie die Pfeile anklicken.

Hinweis: Sie können immer nur ein Datum hinzufügen.

So importieren Sie eine Liste von Daten Führen Sie die folgenden Schritte durch:

- Klicken Sie auf "Durchsuchen".
- Wählen Sie die .txt-Datei aus, die die auszuschließenden Tage enthält.
- Klicken Sie auf "Öffnen".
- Klicken Sie auf "Importieren".

So entfernen Sie ein Datum aus der Liste der auszuschließenden Daten Führen Sie die folgenden Schritte durch:

- Wählen Sie den Tag oder die Tage aus, den/die Sie aus der Liste entfernen möchten.
- Klicken Sie auf "Löschen".

4 Klicken Sie nach dem Auswählen der Tage auf "OK".

So schließen Sie mit dem Backup-Kalender Tage aus allen Backups aus

- 1** Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" unter "Backups" auf "Backup-Kalender".
- 2** Wählen Sie das Datum, das Sie vom Backup-Zeitplan ausschließen möchten.
- 3** Klicken Sie auf "Auszuschließende Tage".
- 4** Klicken Sie auf "Auszuschließenden Tag für alle Backups hinzufügen".

Hinweis: Klicken Sie zum Entfernen eines Ausschlusses eines ausgewählten Datums auf "Auszuschließenden Tage für alle Backups entfernen".

5 Klicken Sie auf "Schließen".

Entfernen von Daten aus der Liste ausgeschlossener Tage

Soll ein Datum nicht mehr aus dem Backup-Zeitplan ausgeschlossen werden, können Sie ihn aus der entsprechenden Liste entfernen. Dieses Datum wird dann in den normalen Backup-Zeitplan aufgenommen. Alle für diesen Tag geplanten

Exportieren einer Liste von Daten, die aus allen Backups auf einem anderen Server ausgeschlossen sind

wiederkehrenden Aufträge, werden jetzt nicht mehr übersprungen, sondern ausgeführt.

So entfernen Sie Daten aus der Liste ausgeschlossener Tage

- 1 Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und dann "Auftragsstandardeinstellungen".
- 2 Wählen Sie "Auszuschließende Tage".
- 3 Wählen Sie das Datum oder die Daten aus, die Sie aus der Liste ausgeschlossener Daten entfernen möchten.
Klicken Sie auf die ausgeschlossenen Daten im Kalender, um Daten aus der Liste ausgeschlossener Tage zu entfernen.
- 4 Klicken Sie auf "Löschen".
- 5 Klicken Sie anschließend auf "OK".

Siehe ["Ausschließen von Tagen vom Backup-Zeitplan für alle Backups"](#) auf Seite 688.

Exportieren einer Liste von Daten, die aus allen Backups auf einem anderen Server ausgeschlossen sind

Sie können bestimmte Tage, wie etwa Feiertage, von Ihrem Backup-Plan ausschließen. Wenn Sie Tage ausschließen, werden regelmäßig geplante Backups an diesen Tagen nicht ausgeführt. Sie können eine Liste von Tagen erstellen, die in Backup Exec ausgeschlossen werden sollen.

Siehe ["Ausschließen von Tagen vom Backup-Zeitplan für alle Backups"](#) auf Seite 688.

Sie können eine Liste von auszuschließenden Tagen als .txt-Datei importieren oder exportieren. Dies kann nützlich sein, falls Sie eine Liste von auszuschließenden Tagen von einem Backup Exec-Server auf einen anderen kopieren möchten.

So exportieren Sie eine Liste von auszuschließenden Tagen

- 1 Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und dann "Auftragsstandardeinstellungen".
- 2 Wählen Sie "Auszuschließende Tage".
- 3 Klicken Sie auf "Exportieren".
- 4 Öffnen Sie den Speicherort, in dem die .txt-Datei gespeichert werden soll.
- 5 Klicken Sie auf "Speichern".

Ändern der Standardeinstellungen

Sie können die Einstellungen für die Anzeige verschiedener Bildschirme, Anzeigen und Warnmeldungen in Backup Exec ändern.

So ändern Sie die Standardeinstellungen

- 1** Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Backup Exec-Einstellungen".
- 2** Klicken Sie im linken Teilfenster auf "Einstellungen".

3 Konfigurieren Sie eine der folgenden Einstellungen:

Eröffnungsbildschirm beim Starten anzeigen	Löschen Sie diese Option, damit die Backup Exec-Administratorkonsole anstelle des Splash-Bildschirms angezeigt wird, wenn Sie Backup Exec starten.
Fortschrittsanzeige für Backup-Aufträge einblenden. Hierfür ist zusätzliche Zeit für den Vorab-Scan der Ressource erforderlich	<p>Wählen Sie diese Option aus, um den Fortschritt eines Backup-Auftrags in Prozent anzuzeigen. Diese Anzeigen erscheinen im Dialogfeld "Auftragsaktivität". Sie ermöglichen Ihnen, den Fortschritt des aktiven Auftrags zu überwachen. Wenn diese Option aktiviert ist, dauern Backup-Vorgänge möglicherweise länger, da die Backup-Ressourcen gescannt werden müssen, um festzustellen, wie groß die zu sichernde Datenmenge ist.</p> <p>Wegen des Zeitraums, der erforderlich ist, um die Backup-Quellen zu scannen, sollten Sie diese Option nicht auswählen, wenn Sie Remote-Ressourcen sichern.</p>
Backup Exec ermöglichen, anonyme Benutzerinformationen zu melden (es werden keine persönlichen Daten gesendet).	<p>Aktivieren Sie diese Option, um am Backup Exec-Produktverbesserungsprogramm teilzunehmen.</p> <p>Allgemeine Backup Exec-Nutzungsdaten und statistische Informationen werden regelmäßig gesammelt und anonym gesendet, um die Backup Exec-Benutzerfreundlichkeit zu verbessern.</p> <p>Hinweis: Backup Exec erfasst zwar Nutzungsdaten und statistische Informationen, niemals jedoch spezifische Benutzerinformationen.</p>
Abwechselnde Farben für Zeilen verwenden	Zeigt die Zeilen aller Listen in Backup Exec in abwechselnden Farben an. Abwechselnde Zeilenfarben erleichtern das Unterscheiden zwischen Zeilen.
Erneut aktivieren	Aktiviert alle Meldungen, die Sie deaktiviert haben.

4 Klicken Sie auf "OK".

Konfigurieren der Standardeinstellungen zum Sichern mehrerer Server oder Anwendungen

Es können mehrere Server oder Anwendungen gleichzeitig zum Sichern ausgewählt werden. Sie können sie als Teil einer Backup-Definition oder einzeln in separaten

Backup-Definitionen sichern. Es ist möglicherweise einfacher für Sie, die Sicherung von mehreren Servern als Teil einer Backup-Definition zu verwalten. Es ist jedoch auch einfacher, Fehler bei fehlgeschlagenen Aufträgen zu beheben, wenn jeder Server seine eigene Backup-Definition hat.

Bei jedem Erstellen einer Backup-Definition, die mehrere Server oder Anwendungen enthält, können Sie auswählen, ob Sie nur eine Backup-Definition oder mehrere separate Backup-Definitionen erstellen möchten. Sie können ein Standardszenario zum Sichern von mehreren Servern oder Anwendungen erstellen, sodass Backup Exec automatisch entweder nur eine Backup-Definition oder mehrere separate Backup-Definitionen erstellt.

So konfigurieren Sie die Standardeinstellungen zum Sichern mehrerer Server oder Anwendungen

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Backup Exec-Einstellungen".
- 2 Wählen Sie im linken Teilfenster "Backups".
- 3 Wählen Sie eine der folgenden Optionen aus:
 - Ein Backup erstellen, das alle Server oder Anwendungen umfasst
 - Separate Backups für jeden Server bzw. jede Anwendung erstellen
- 4 Wenn Sie jedes Mal, wenn Sie die Option zum Sichern mehrerer Server oder Anwendungen wählen, eine Aufforderung erhalten möchten, wählen Sie "Jedesmal beim Erstellen von Backups für mehrerer Server anzeigen".

Wenn Sie die Aufforderung deaktivieren, verwendet Backup Exec automatisch die Einstellung, die Sie im Feld "Beim Erstellen von Backups für mehrere Server" ausgewählt haben. Sie können die Aufforderung jederzeit aktivieren.

Siehe ["Sichern von Daten"](#) auf Seite 174.

Konfigurieren der Datenbankverwaltung und -sicherheit

Mit der Option "Datenbankverwaltung und -sicherheit" können Sie die Backup Exec-Datenbank verwalten. Jeder Datenbankverwaltungsvorgang wird für jede Datenbank einzeln durchgeführt. In der Backup Exec-Datenbank werden Datensätze zu den von Ihnen konfigurierten Dateien und Daten aufbewahrt.

Die Datenbankverwaltung ermöglicht die folgenden Vorgänge:

- Optimieren der Datenbankgröße
- Löschen abgelaufener Daten

- Speichern von Inhalten der Datenbankdateien
- Ausführen von Datenbank-Konsistenzprüfungen

Backup Exec generiert bei jedem Datenbankverwaltungsvorgang jeweils eine informatorische Warnmeldung zu Beginn und am Ende des Vorgangs. Diese Meldungen enthalten Informationen zum Typ der durchgeführten Verwaltungsvorgänge in jeder Datenbank und der für die Vorgänge benötigten Zeit. Wenn der Datenbankverwaltungsvorgang fehlschlägt, gibt die Meldung an, an welcher Stelle und warum der Fehler aufgetreten ist.

Sie müssen nicht alle Optionen aktivieren. Über jede Option wird jedoch ein anderer Vorgang durchgeführt, mit dem Sie die Datenbank schützen und verwalten können. Wenn Sie alle Optionen auswählen, können Sie die Datenbank schnell wiederherstellen und eine optimale Leistung beibehalten.

Außerdem können Sie den Backup Exec-Datenbankverschlüsselungscode exportieren. Der Backup Exec-Datenbankverschlüsselungscode wird verwendet, um die Backup Exec-Datenbank zu schützen. Der Code ist für eine Reihe von Notfallwiederstellungs- und Migrationsvorgängen erforderlich. Sie sollten den Verschlüsselungscode in einen sicheren Speicherort exportieren, um sicherzustellen, dass er später verfügbar ist.

So konfigurieren Sie die Datenbankverwaltung und -sicherheit

- 1** Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Backup Exec-Einstellungen".
- 2** Klicken Sie im linken Teilfenster auf "Datenbankverwaltung und -sicherheit".
- 3** Wählen Sie die Option "Backup Exec-Datenbankverwaltung aktivieren".

4 Konfigurieren Sie eine der folgenden Optionen:

Datenbankverwaltung täglich durchführen um	<p>Wählen Sie die Zeit aus, zu der Sie die Datenbankwartung durchführen möchten.</p> <p>Die ganze Wartung tritt einmal täglich auf, zu der Zeit, die Sie angeben.</p>
Veraltete Daten löschen	<p>Wählen Sie diese Option, um den abgelaufenen Auftragsverlauf, die Auftragsprotokolle, den Warnmeldungsverlauf sowie die Berichte aus der Backup Exec-Datenbank nach Ablauf der angegebenen Anzahl von Tagen zu löschen.</p>
Auftragsverlauf für Daten auf Medien mit aktivierten Überschreibschutzzeiträumen beibehalten	<p>Wählen Sies diese Option, um alle Auftragsverlaufsdaten für Medien zu behalten, bei denen aktuell ein Überschreibschutzzeitraum zugewiesen ist.</p> <p>Nach Ablauf des Überschreibschutzzeitraum des Mediums können die Auftragsverlaufsdaten gelöscht werden.</p>
Auftragsverlauf für eine bestimmte Anzahl an Tagen aufbewahren	<p>Wählen Sies diese Option, um anzugeben, wie lange die Auftragsverlaufsdaten in der Datenbank aufbewahrt werden sollen, bevor sie gelöscht werden.</p> <p>Zu den Auftragsverlaufsdaten gehören Übersichtsstatistiken für einen Auftrag sowie Details zu Medien, Geräten und Backup-Sätzen, die zur Auftragsverarbeitung verwendet wurden.</p>
Auftragsprotokolle	<p>Geben Sie an, wie lange Auftragsprotokolle in der Datenbank aufbewahrt werden sollen, bevor sie gelöscht werden.</p> <p>Auftragsprotokolle enthalten detaillierte Informationen zum Auftrag.</p>
Warnmeldungsverlauf	<p>Geben Sie an, wie lange die Warnmeldungsverlaufsdaten in der Datenbank aufbewahrt werden sollen, bevor sie gelöscht werden.</p> <p>Zu den Meldungsverlaufsdaten gehören Eigenschafts- und Antwortinformationen für die Meldung.</p>

Berichte	<p>Geben Sie an, wie lange die Berichtsdaten in der Datenbank aufbewahrt werden sollen, bevor sie gelöscht werden.</p> <p>Zu den Berichtsdaten gehören Eigenschaftsinformationen zu erzeugten Berichtsaufträgen. Der Bericht selbst wird nicht gelöscht.</p>
Überwachungsprotokolle	<p>Geben Sie die Anzahl der Tage an, für die die Überwachungsprotokolldaten vor dem Löschen in der Datenbank gespeichert werden.</p> <p>Das Überwachungsprotokoll enthält Informationen über Vorgänge, die in Backup Exec durchgeführt werden.</p> <p>Siehe "Konfigurieren von Überwachungsprotokollen" auf Seite 779.</p>
Datenbank-Konsistenzprüfung durchführen	<p>Wählen Sie diese Option, um die logische und physische Übereinstimmung der Daten in der Datenbank zu prüfen.</p> <p>Diese Option ist standardmäßig deaktiviert. Es wird empfohlen, dass Sie regelmäßig und zu einem Zeitpunkt mit minimaler Backup Exec-Aktivität eine Konsistenzprüfung ausführen.</p>
Datenbankinhalt im Backup Exec-Datenverzeichnis speichern	<p>Wählen Sie diese Option, um die Daten der Datenbank im Backup Exec-Datenverzeichnis zu speichern, damit die Datenbank-Backup-Datei (BEDB.bak) gesichert werden kann.</p> <p>Die Datei wird im Datenverzeichnis aufrechterhalten, bis der folgende Datenbankwartungsprozess durchgeführt ist und dann diese Datei überschrieben wird. Mit dieser Option können Sie die Datenbank im Notfall wiederherstellen.</p>
Datenbankgröße optimieren	<p>Wählen Sie diese Option, um fragmentierte Seiten neu zu organisieren und die Größe der physischen Datenbank auf 10 Prozent oberhalb der eigentlichen Nutzung zu verringern.</p>

- 5 Zum Exportieren des Datenbankverschlüsselungscodes füllen Sie folgende Felder aus:

Hinweis: Sie sollten den Verschlüsselungscode in einen sicheren Speicherort exportieren, um sicherzustellen, dass er später verfügbar ist. Sie benötigen den Verschlüsselungscode zum Ausführen der Notfallwiederherstellung oder zum Migrieren des Backup Exec-Server. Der Code wird mit einem eindeutigen Hash-Wert benannt. Backup Exec verwendet den Namen, um den Code später zu identifizieren.

Siehe ["Exportieren des Backup Exec-Datenbankverschlüsselungscodes"](#) auf Seite 698.

Pfad	Geben Sie den Pfad zu einem sicheren Speicherort ein, in den der Backup Exec-Datenbank-Verschlüsselungscode exportiert werden soll.
Export-Pfad speichern Durch Aktivieren dieses Kontrollkästchens, erklären Sie sich bereit, dass Backup Exec den Exportpfad beim Importieren speichert und anzeigt.	<p>Aktivieren Sie diese Option, damit Backup Exec den Pfad speichert, in dem der Datenbankverschlüsselungscode exportiert wurde.</p> <p>Wenn Sie diese Option aktivieren, kann Backup Exec versuchen, um den Datenbankverschlüsselungscode automatisch wiederherzustellen, falls dieser einen Fehler verursacht. Wenn Sie diese Option nicht aktivieren, müssen Sie den Datenbankverschlüsselungscode manuell importieren, falls er einen Fehler verursacht.</p>
Exportieren	Klicken Sie auf diese Option, um den Backup Exec-Datenbankverschlüsselungscode in den im Feld "Pfad" definierten Speicherort zu exportieren.

- 6 Klicken Sie auf "OK".

Siehe ["Konfigurieren der Verschlüsselung für die Verbindung zur Backup Exec-Datenbank"](#) auf Seite 702.

Exportieren des Backup Exec-Datenbankverschlüsselungscodes

Backup Exec speichert vertrauliche Information mit Verschlüsselung in der Backup Exec-Datenbank. Wenn Sie Backup Exec installieren oder aktualisieren, wird automatisch ein Datenbankverschlüsselungscode erstellt. Der

Datenbankverschlüsselungscodes werden beispielsweise verwendet, um Login-Konto-Identifikationsdaten und Backup-Aufträge zu verschlüsseln. Er wird im Backup Exec-Installationsordner im Unterordner "Data" abgelegt.

Sie müssen den Backup Exec-Datenbankverschlüsselungscodes in folgenden Fällen zur Verfügung zu stellen:

- Durchführen einer manuellen Notfallwiederherstellung eines Backup Exec-Servers
- Durchführen einer Notfallwiederherstellung eines Backup Exec-Servers mit Simplified Disaster Recovery (SDR)
- Migrieren von Backup Exec von einem Computer auf einen anderen
- Vorgehensweise bei beschädigtem oder fehlendem Datenbankverschlüsselungscodes auf dem Backup Exec-Server

Es wird empfohlen, dass Sie den Backup Exec-Datenbankverschlüsselungscodes in einen sicheren Speicherort exportieren, damit Sie später darauf zugreifen können. Sie sollten folgendes Verfahren auf jedem Backup Exec-Server in Ihrer Umgebung, einschließlich den zentralen Administrationsserver und allen verwalteten Backup Exec-Servern in Central Admin Server Feature-Bereitstellungen (CAS) wiederholen.

Gewährleisten Sie, dass Sie den Datenbankverschlüsselungscodes in einen Speicherort exportieren, der die folgenden Kriterien erfüllt:

- Das Ziel ist ein auf einem physischen Datenträger, der einem Laufwerksbuchstaben oder einer über einen UNC-Pfad definierten Netzwerkfreigabe zugeordnet ist. Netzwerkfreigaben, die Laufwerksbuchstaben zugeordnet sind, werden nicht unterstützt.
- Auf dem Ziel ist genügend Speicherplatz verfügbar.
- Das Ziel ist vom Backup Exec-Server aus verfügbar.
- Backup Exec hat Schreibzugriff auf das Ziel.

So exportieren Sie den Backup Exec-Datenbankverschlüsselungscodes

- 1 Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Backup Exec-Einstellungen".
- 2 Klicken Sie im linken Teilfenster auf "Datenbankverwaltung und -sicherheit".
- 3 Geben Sie im Feld "Pfad" den Speicherort ein, in den der Verschlüsselungscodes exportiert werden soll.

- 4 Wenn Backup Exec den Pfad speichern soll, in den der Datenbankverschlüsselungscode exportiert wurde, aktivieren Sie die Option "Export-Pfad speichern. Durch Aktivieren dieses Kontrollkästchens, erklären Sie sich bereit, dass Backup Exec den Exportpfad beim Importieren speichert und anzeigt.

Wenn Sie diese Option aktivieren, kann Backup Exec versuchen, um den Datenbankverschlüsselungscode automatisch wiederherzustellen, falls dieser einen Fehler verursacht. Wenn Sie diese Option nicht aktivieren, müssen Sie den Datenbankverschlüsselungscode manuell importieren, falls er einen Fehler verursacht.

- 5 Klicken Sie auf "Exportieren".

Der Code wird in den angegebenen Speicherort exportiert. Der Code wird mit einem eindeutigen Hash-Wert benannt. Backup Exec verwendet den Namen, um den Code später zu identifizieren. Wenn Sie den Schlüssel in zusätzliche Speicherorte exportieren möchten, wiederholen Sie Schritt 3 bis 5.

- 6 Klicken Sie auf "OK".

Siehe ["Konfigurieren der Datenbankverwaltung und -sicherheit"](#) auf Seite 694.

Siehe ["Aktualisieren von Backup Exec-Datenbankverschlüsselungscodes"](#) auf Seite 700.

Siehe ["Konfigurieren der Verschlüsselung für die Verbindung zur Backup Exec-Datenbank"](#) auf Seite 702.

Aktualisieren von Backup Exec-Datenbankverschlüsselungscodes

Backup Exec speichert vertrauliche Information mit Verschlüsselung in der Backup Exec-Datenbank. Der Datenbankverschlüsselungscode wird beispielsweise verwendet, um Login-Konto-Identifikationsdaten und Backup-Aufträge zu verschlüsseln. Er wird im Backup Exec-Installationsordner im Unterordner "Data" abgelegt. Er ist für viele Notfallwiederherstellungs- und Migrationsvorgänge erforderlich.

Backup Exec erstellt den Backup Exec-Datenbankverschlüsselungscode automatisch. Jedoch sollten Sie den Schlüssel aktualisieren, wenn der vorhandene Schlüssel auf irgendeine Weise gefährdet ist. Eventuell ist es erforderlich, den Schlüssel zu ändern, wenn Ihre Unternehmensrichtlinien erfordern, dass Schlüssel oder Kennwörter regelmäßig geändert werden müssen.

Hinweis: Sie benötigen einen funktionierenden Datenbankverschlüsselungscodes, um das Verfahren abzuschließen.

Schließen Sie das folgende Verfahren ab, um den Backup Exec-Datenbankverschlüsselungscodes zu aktualisieren.

So aktualisieren Sie Backup Exec-Datenbankverschlüsselungscodes

- 1 Unter Windows klicken Sie auf "Start" und dann auf "Ausführen".
- 2 Geben Sie Regedit ein und klicken Sie dann auf "OK".

Warnung: Ein falscher Einsatz des Windows-Registrierungseditors kann dazu führen, dass das Betriebssystem nicht mehr richtig funktioniert. Beim Vornehmen von Änderungen an der Windows-Registrierung ist Vorsicht geboten. Änderungen an der Registrierung sollten nur von erfahrenen Benutzern durchgeführt werden. Es wird empfohlen, ein vollständiges Backup der Registrierung und des Computers zu erstellen, bevor Sie Änderungen an der Registrierung vornehmen.

- 3 Klicken Sie mit der rechten Maustaste auf den folgenden Registrierungsschlüssel:

HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Backup Exec For Windows\Backup Exec\Server\DatabaseEncryptionAction

- 4 Klicken Sie auf "Ändern".
- 5 Geben Sie im Feld "Wertdaten" den Wert "2" ein.
- 6 Klicken Sie auf "OK".
- 7 Starten Sie alle Backup Exec Services neu.

Backup Exec erstellt einen neuen Backup Exec-Datenbankverschlüsselungscodes. Es wird empfohlen, den neuen Schlüssel in einen sicheren Speicherort zu exportieren, damit Sie später bei Bedarf auf ihn zugreifen können.

Siehe ["Exportieren des Backup Exec-Datenbankverschlüsselungscodes"](#) auf Seite 698.

Konfigurieren der Verschlüsselung für die Verbindung zur Backup Exec-Datenbank

Die Backup Exec-Datenbank enthält vertrauliche Information über Ihr Unternehmen (z. B. Identifikationsdaten und gesicherte Daten). Das Schützen der Verbindung zwischen Microsoft SQL Server und der Backup Exec-Datenbank ist ein wichtiger Schritt beim Schützen des Netzwerks vor dem Zugriff von außen. Zusätzlich empfiehlt Microsoft, dass Sie die SSL-Verschlüsselung verwenden, wenn Daten vom SQL-Server über ein Netzwerk an eine Anwendung gesendet werden.

Die Datenübertragung zwischen den Backup Exec-Diensten und der SQL-Instanz kann in den folgenden Szenarien über das Netzwerk erfolgen:

- Sie konfigurieren die Backup Exec-Datenbank als zentrale Datenbank, die sich auf einem zentralen Administrationsserver in einer CAS-Umgebung befindet. Daten können auf ähnliche Weise über das Netzwerk übertragen werden. Beispiel: Sie verwenden einen verwalteten Backup Exec-Server oder einen gemeinsam genutzten Speicher.
- Sie verwenden eine Remote-SQL-Instanz für die Backup Exec-Datenbank, damit die Backup Exec Services auf die Datenbank über das Netzwerk zugreifen müssen.

Backup Exec aktiviert automatisch die SSL-Verschlüsselung, wenn Sie die standardmäßige lokale SQL Express-Instanz "BKUPEXEC" verwenden. Ist Backup Exec so konfiguriert, dass eine andere SQL Server-Instanz verwendet wird, müssen Sie die Verschlüsselung selbst konfigurieren.

SQL Server nutzt Zertifikate zum Verschlüsseln von Daten. Sie können Ihre eigenen Zertifikate generieren, oder Sie können SQL Server so konfigurieren, dass ein automatisch erzeugtes, selbstsigniertes Zertifikat verwendet wird. Standardmäßig verwendet Backup Exec die selbstsignierten Zertifikate, die SQL Server automatisch erzeugt. Es wird jedoch empfohlen, eigene Zertifikate zu erzeugen und zu verwenden, um die Sicherheit zu erhöhen.

Hinweis: Die Verschlüsselung kann die Leistung der Kommunikation zwischen SQL Server und der Backup Exec-Datenbank beeinträchtigen. Die Daten werden ein weiteres Mal um das Netzwerk gesendet und das Verschlüsseln und Entschlüsseln der Daten dauert eine gewisse Zeit.

In der Microsoft-Supportdatenbank finden Sie weitere Informationen zu Secure Sockets Layer (SSL) und das Verschlüsseln von Verbindungen zu SQL Server.

Informationen zu den Best Practices zum Verwalten der Datenbankverschlüsselung finden Sie unter *Best Practices für Backup Exec*.

So erzeugen und installieren Sie Zertifikate für sichere SQL-Verbindungen (optional)

Sie können Ihre eigenen Zertifikate verwenden, oder Sie können zulassen, dass SQL Server ein automatisch erstelltes, selbstsigniertes Zertifikat nutzt. Es wird empfohlen, eigene Zertifikate zu verwenden, um die Sicherheit zu erhöhen. Sobald Sie Ihr Zertifikat erzeugt und installiert haben, können Sie die sichere SQL-Verbindung zur Backup Exec-Datenbank konfigurieren.

Microsoft hat Anforderungen, die erfüllt sein müssen, wenn Sie Ihre eigenen Zertifikate für SQL Server verwenden. Zertifikate können entweder selbstsigniert oder von einer Zertifizierungsstelle ausgestellt werden. Zertifizierungsstellen können entweder eine lokale Authority in der Domäne Ihres Unternehmens oder eine bekannte Authority eines anderen Anbieters sein.

Weitere Informationen zu den Zertifizierungsanforderungen von Microsoft finden Sie im folgenden Artikel:

[Encrypting Connections to SQL Server](#)

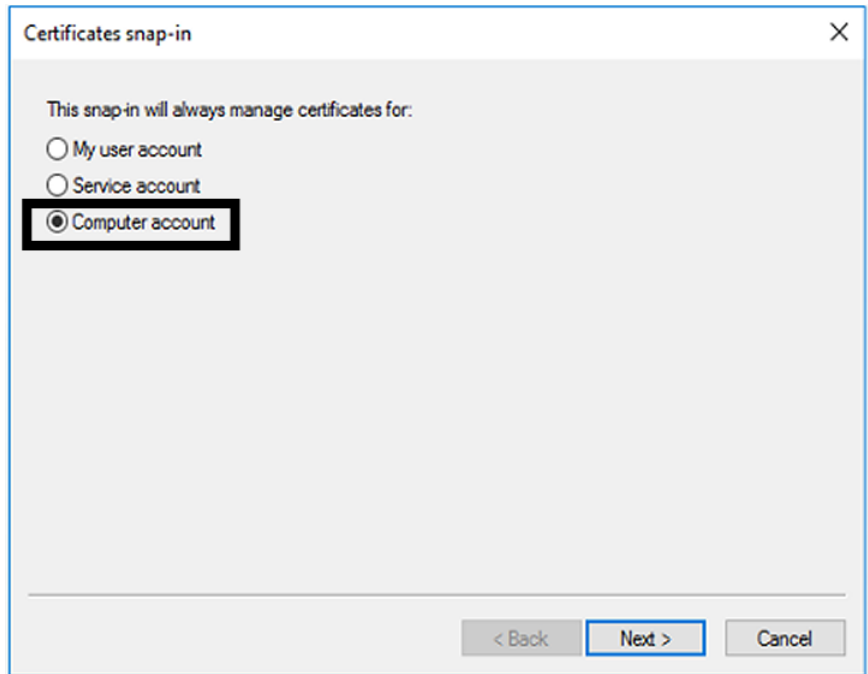
Bevor Sie die Verschlüsselung konfigurieren, müssen Sie die gewünschten Zertifikate in den lokalen Zertifikatsspeicher des Computers importieren, der die Backup Exec-Datenbank hostet.

Weitere Informationen zum Importieren und Installieren eines Zertifikats auf dem Server finden Sie im folgenden Microsoft-Artikel:

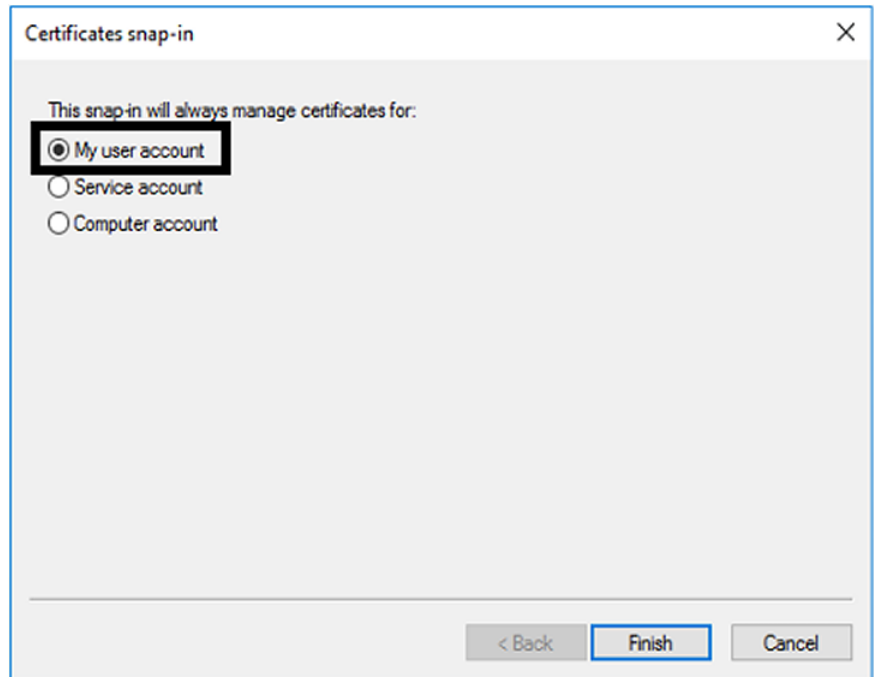
[How to: Enable Encrypted Connections to the Database Engine \(SQL Server Configuration Manager\)](#)

Beim Importieren von Zertifikaten sollten Sie dasselbe Benutzerkonto verwenden, unter dem der SQL Server-Dienst ausgeführt wird:

- Wenn SQL Server unter einem Standard- Computerkonto wie zum Beispiel LocalSystem, NetworkService oder LocalService ausgeführt wird, dann sollten Sie die Option "Computerkonto" verwenden, wenn Sie das Zertifikat importieren. Das Verwalten von Zertifikaten für das Computerkonto stellt sicher, dass das Zertifikat im persönlichen Speicher des Standard-Computerkontos abgelegt wird.



- Wenn SQL Server unter einem bestimmten Domänenkonto ausgeführt wird, müssen Sie mit demselben Konto eingeloggt sein, um das Zertifikat zu importieren. Wenn Sie in Microsoft Management Console protokollieren, wählen Sie die Option "Mein Benutzerkonto". Das Verwalten von Zertifikaten für das Benutzerkonto stellt sicher, dass das Zertifikat im persönlichen Speicher des Benutzers abgelegt wird, der das SQL-Dienstkonto ausführt.



So konfigurieren Sie sichere SQL-Verbindungen zur Backup Exec-Datenbank

Backup Exec aktiviert automatisch die SSL-Verschlüsselung für SQL-Verbindungen, wenn Sie die standardmäßige lokale SQL Express-Instanz "BKUPEXEC" verwenden. Ist Backup Exec so konfiguriert, dass eine andere SQL Server-Instanz verwendet wird, müssen Sie die Verschlüsselung selbst konfigurieren. Sie sollten die sichere Verbindung auf dem Computer konfigurieren, auf dem die SQL-Instanz die Backup Exec-Datenbank hostet.

In bestimmten Backup Exec-Umgebungen müssen Sie möglicherweise die sichere Verbindung mehrmals konfigurieren:

Für gruppierte Backup Exec-Umgebungen

Sie müssen eine sichere SQL-Verbindung auf allen Knoten im Cluster konfigurieren.

Wenn der Cluster nicht noch erstellt worden ist, konfigurieren Sie die sichere SQL-Verbindung, bevor Sie den Assistenten für die Clusterkonfiguration in Backup Exec ausführen.

Wurde der Cluster bereits erstellt:

- Bringen Sie den Backup Exec-Cluster mit dem Failover-Clustermanager von Windows offline.
- Führen Sie den folgenden Vorgang auf allen Knoten im Cluster aus.
- Bringen Sie den Backup Exec-Cluster mit dem Failover-Clustermanager von Windows online.

Für CAS-Umgebungen (Central Admin Server Feature):

Sie müssen auf allen Computern in der CAS-Umgebung, auch dem zentralen Administrationsserver und allen verwalteten Backup Exec-Servern, eine sichere SQL-Verbindung konfigurieren.

Verwenden Sie den SQL Server-Konfigurationsmanager, um die Eigenschaften der Protokolle für den Server zu bearbeiten, den Sie konfigurieren möchten. Wenn Sie die Verschlüsselung für die standardmäßige lokale Datenbankinstanz konfigurieren möchten, die von Backup Exec installiert wird, bearbeiten Sie die "Protokolle für BKUPEXEC". Wählen Sie das gewünschte Zertifikat aus, wenn Sie eines erstellt haben. Geben Sie dann an, ob die Verschlüsselung für die Datenbankverbindung erzwungen werden soll. Starten Sie anschließend den SQL Server und die Backup Exec Services aus dem Dienst-Manager neu.

Weitere Informationen und Anweisungen zum Konfigurieren von verschlüsselten SQL-Verbindungen finden Sie in der Microsoft-Supportdatenbank.

Planen der Prüfung von Login-Konten durch Backup Exec

Sie können planen, dass Backup Exec prüft, ob die Backup-Quellen in Aufträgen über die von Ihnen ausgewählten Login-Konten aufgerufen werden können. Indem Sie prüfen, ob Ihre Login-Konten Zugriff auf Backup-Quellen haben, können Sie vor dem Ausführen von Backup-Aufträgen gegebenenfalls vorhandene Zugriffsprobleme diagnostizieren und beheben. Wenn Backup Exec Backup-Quellen findet, auf die mit den von Ihnen ausgewählten Login-Konten nicht zugegriffen werden kann, meldet es den Fehler in einer Warnmeldung.

Standardmäßig ist der Zeitplan so konfiguriert, dass Backup Exec die Login-Konten täglich um 14:00 Uhr prüft.

Hinweis: Die Standardzeit von 14:00 Uhr gilt nur für neue Installationen von Backup Exec 15 Feature Pack 3 und höher. Bei niedrigeren Versionen und Server, die auf Backup Exec 15 Feature Pack 3 und höher aktualisiert wurden, bleibt die Standardzeit 01:00 Uhr.

Sie können die Prüfung deaktivieren, wenn Backup Exec die Login-Konten nicht regelmäßig überprüfen soll. Sie können die Prüfung auch neu planen, sodass sie seltener erfolgt.

So planen Sie die Prüfung von Login-Konten durch Backup Exec

- 1 Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Backup Exec-Einstellungen".
- 2 Wählen Sie im linken Teilfenster "Login-Konten".
- 3 Konfigurieren Sie eine der folgenden Optionen:

Prüfen, ob die Backup-Quellen in Aufträgen über die ausgewählten Login-Konten aufgerufen werden können	Wählen Sie diese Option, um zu prüfen, ob Backup Exec mit den von Ihnen ausgewählten Login-Konten auf die Backup-Quellen in Ihren Backup-Aufträgen zugreifen kann.
Prüfung ausführen alle X Tage um X	Geben Sie das Intervall an, in dem Backup Exec die Login-Konten prüfen soll. Backup Exec prüft automatisch die Login-Konten in dem von Ihnen in diesem Feld ausgewählten Intervall. Sie können die Uhrzeit, zu der Backup Exec die Prüfung ausführen soll, sowie die Anzahl der Tage zwischen den Prüfungen auswählen.
Login-Konten nur auf Serverebene prüfen	Wählen Sie diese Option aus, um die Prüfung der Login-Konten auf die Serverebene zu beschränken. Wenn Sie diese Option auswählen, prüft Backup Exec nur, ob die Login-Konten auf Backup-Quellen auf Serverebene zugreifen können. Auf dem Server residierende Ressourcen werden nicht geprüft. Die Prüfung der Login-Konten nimmt weniger Zeit in Anspruch, wenn Sie nur die Konten auf Serverebene prüfen, sie ist jedoch auf diese Weise weniger gründlich.

- 4 Klicken Sie auf "OK".

Siehe ["Backup Exec-Login-Konten"](#) auf Seite 762.

Konfigurieren von Backup Exec, um Daten für Backup zu suchen

Die Option "Daten für Backup suchen" von Backup Execs erkennt neuen Backupinhalt innerhalb einer Windows- oder Active Directory-Domäne. Mit dieser Option können Sie einen Auftrag planen, der nach neuen Serverdatenträgern, Datenbanken oder Anwendungsdaten sucht.

Standardmäßig wird der Datenerkennungsvorgang jeden Tag um 12:00 Uhr ausgeführt. Er wird zudem jedes Mal ausgeführt, wenn die Backup Exec-Dienste neu gestartet werden. Backup Exec bricht den Vorgang ab, wenn er nach vier Stunden noch nicht abgeschlossen ist. Sie können den Vorgang deaktivieren oder die Standardeinstellungen in den globalen Backup Exec-Einstellungen ändern.

Die Option "Daten für Backup suchen" führt drei Hauptaufgaben durch:

- Erkennt alle Top-Level-Computer oder -Computerinhalte
Wenn der Datenerkennungsvorgang Top-Level-Computer oder -Computerinhalte erkennt, fügt er diese dem Teilfenster "Identifikationsdaten" auf der Registerkarte "Backup und Wiederherstellung" hinzu. Bei diesem Vorgang werden alle Informationen über die Computer oder die Computerinhalte und deren Backup-Status aktualisiert. Sie können Informationen über Backup-Quellen im Teilfenster Identifikationsdaten anzeigen.
- Erkennt alle Server, auf denen kein Agent for Windows installiert ist
Wenn bei diesem Vorgang Server erkannt werden, auf denen kein Agent for Windows installiert ist, zeigt Backup Exec eine Warnmeldung an. Sie können die Server der Liste von Servern hinzufügen, indem Sie den Assistenten "Server hinzufügen" verwenden. Nachdem Sie der Serverliste die Server hinzugefügt haben, können Sie sie sichern und überwachen.
[Siehe "Hinzufügen gefundener Server zur Liste von Servern in Backup Exec" auf Seite 710.](#)
- Erkennt und validiert Instanzen des Agents for Windows
Der Datenerkennungsvorgang sucht nach allen Instanzen des Agents for Windows in Ihrem Netzwerk. Wenn ein Agent for Windows gefunden wird, wird dessen Version geprüft, um sicherzustellen, dass er auf dem neuesten Stand ist. Wenn ein Agent for Windows nicht die aktuelle Version aufweist, sendet Backup Exec eine Warnmeldung.

Der Datenerkennungsvorgang findet nur die Server, die die folgenden Kriterien erfüllen:

- Gehört zur gleichen Domäne wie der Backup Exec-Server
- Verfügt über den Windows Management Instrumentation(WMI)-Dienst, der aktiviert ist und ausgeführt wird

- Ermöglicht WMI-Zugriff für den gleichen Benutzer, unter dem der Backup Exec-Management-Dienst ausgeführt wird
Mitglieder der "Administrator"-Gruppe des Servers verfügen über Zugriffsrechte auf dieser Ebene.
- Verfügt über Firewalls, die konfiguriert werden, um WMI-Netzwerkverkehr zu ermöglichen

So konfigurieren Sie Backup Exec, um Daten für Backup zu suchen

- 1** Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Backup Exec-Einstellungen".
- 2** Wählen Sie im linken Teilfenster die Option "Daten für Backup suchen".
- 3** Konfigurieren Sie eine der folgenden Optionen:

Server suchen, die nicht gesicherte Daten enthalten	<p>Aktiviert die Erkennung von Daten, die gesichert werden müssen, in Backup Exec.</p> <p>Wenn diese Option ausgewählt ist, sucht Backup Exec automatisch im Netzwerk nach Daten, die nicht gesichert wurden.</p>
Häufigkeit	<p>Legt die Häufigkeit fest, mit der Backup Exec nach Daten sucht, die gesichert werden müssen.</p> <p>Sie können festlegen, ob Backup Exec täglich, wöchentlich oder monatlich nach Daten suchen soll, die gesichert werden müssen.</p>
Intervall	<p>Legt die Häufigkeit fest, mit der Backup Exec nach Daten sucht, die gesichert werden müssen.</p> <p>Sie können auf Basis der festgelegten Häufigkeit unterschiedliche Zeitabstände wählen.</p>
Erkennung abbrechen, falls nicht abgeschlossen innerhalb	<p>Legt fest, nach wie vielen Stunden die Datenerkennung abgebrochen werden soll, falls sie noch nicht abgeschlossen ist.</p> <p>Durch Abbrechen der Datenerkennung verringern Sie das Risiko einer negativen Auswirkung auf Systemressourcen.</p>

- 4** Klicken Sie auf "OK".

Hinzufügen gefundener Server zur Liste von Servern in Backup Exec

Sie können den Assistenten "Server hinzufügen" verwenden, um Agent for Windows auf jedem von Backup Exec mithilfe der Option "Daten für Backup suchen" gefundenen Server zu installieren. Sobald Sie Agent for Windows installiert haben, wird der Server zur Liste von Servern in Backup Exec hinzugefügt.

So fügen Sie gefundene Server zur Liste von Servern in Backup Exec hinzu

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" in der Gruppe "Server und virtuelle Hosts" auf "Hinzufügen".
- 2 Wählen Sie "Microsoft Windows-Computer und -Server", und klicken Sie dann auf "Weiter".
- 3 Wählen Sie "Zulassen, dass Backup Exec ein Vertrauensverhältnis mit den Servern herstellt", und klicken Sie dann auf "Weiter".
- 4 Klicken Sie auf "Durchsuchen".
- 5 Erweitern Sie "Server ohne Agent for Windows installiert", um die Namen der Server anzuzeigen, die durch den Datenerkennungsvorgang gefunden wurden.
- 6 Wählen Sie die Server aus, auf denen Agent for Windows installiert werden soll, und klicken Sie dann auf "OK".
- 7 Wählen Sie im Feld "Login-Konto" das Login-Konto aus, dass für den Zugriff auf den jeweiligen Server verwendet werden soll.
- 8 Klicken Sie auf "Weiter".
- 9 Wählen Sie eine der folgenden Optionen, und klicken Sie anschließend auf "Weiter".

Backup Exec Agent for Windows automatisch auf die aktuelle Version aktualisieren

Führt ein Upgrade des Agent for Windows auf dem Server aus, den Sie zur Liste von Servern hinzugefügt haben (falls erforderlich).

Remote-Computer automatisch neu starten, nachdem der Backup Exec Agent for Windows installiert wurde und wenn ein Neustart erforderlich ist

Führt einen Neustart des Remote-Computers aus, nachdem der Agent for Windows installiert wurde.

- 10 Klicken Sie auf "Installieren".

Siehe ["Konfigurieren von Backup Exec, um Daten für Backup zu suchen"](#) auf Seite 708.

Backup-Netzwerke

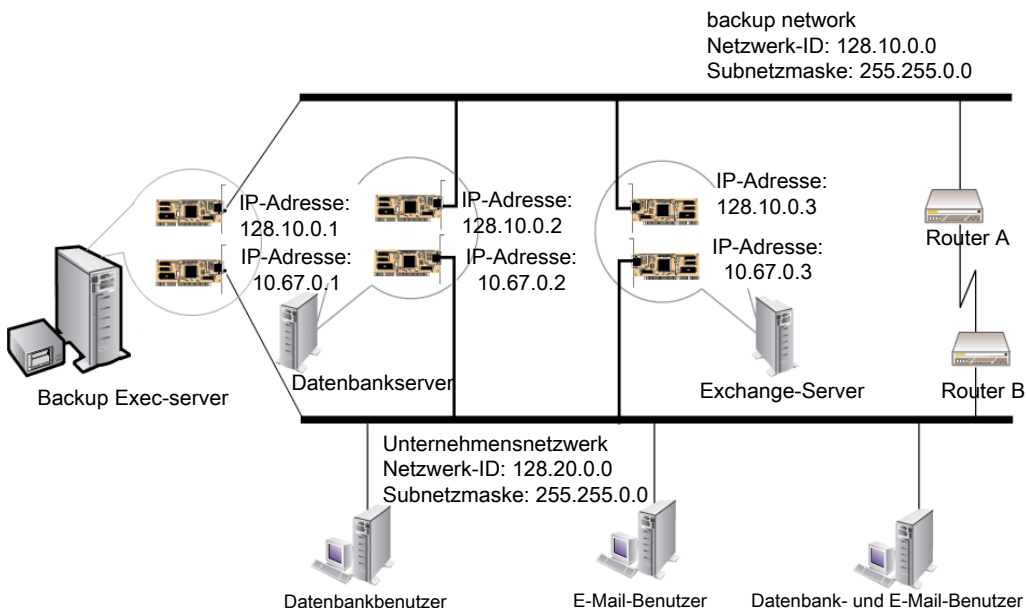
Mit der Backup-Netzwerkfunktion können Sie jeden Datenverkehr des primären Backups, den Backup Exec generiert, zu einem bestimmten lokalen Netzwerk leiten. Die Umleitung von Backup-Aufträgen in ein bestimmtes lokales Netzwerk isoliert die Backup-Daten, sodass andere verbundene Netzwerke nicht durch Backup-Vorgänge beeinträchtigt werden. Sie können auch ein Backup-Netzwerk verwenden, wenn Sie Daten wiederherstellen. Diese Funktion wird auf dem Backup Exec-Server aktiviert und ermöglicht das Schützen aller Remote-Computer, die sich in dem festgelegten lokalen Netzwerk befinden.

Wenn Sie ein Backup-Netzwerk angeben und einen Auftrag eingeben, überprüft Backup Exec, dass der Remote-Computer sich auf dem gleichen Subnetz befindet wie die ausgewählte Schnittstelle auf dem Backup Exec-Server. Wenn sich der Remote-Computer im ausgewählten Subnetz befindet, wird das Backup ausgeführt.

Wenn er sich dort nicht befindet, schlägt der Backup-Auftrag fehl. Sie können Backup Exec allerdings so einrichten, dass für das Backup von Remote-Computern ein beliebiges verfügbares Netzwerk verwendet wird.

In der folgenden Abbildung wird ein Beispiel einer Backup-Netzwerkconfiguration gezeigt.

Abbildung 15-1 Beispiel für ein Backup-Netzwerk



In diesem Beispiel sind der Datenbankserver und der E-Mail-Server mit dem Backup-Netzwerk und dem Unternehmensnetzwerk verbunden.

Wenn der Backup Exec-Server Backup-Vorgänge durchführt, verwenden die Backup-Daten entweder das Backup-Netzwerk oder das Unternehmensnetzwerk, um den Datenbankserver zu sichern. Wenn die Backup-Daten das Unternehmensnetzwerk durchlaufen, nimmt die Zeit des Backups des Datenbankservers zu. Der Zeitraum nimmt zu, weil die Netzwerkroute zwischen den zwei Computern länger ist. Benutzer können möglicherweise minimale Auswirkungen auf die Netzwerkleistung erkennen, wenn sie auf den E-Mail-Server zugreifen, da es eine Zunahme des Netzwerkverkehrs gibt.

Wenn Sie ein Backup-Netzwerk angeben und Sie den Datenbankserver sichern, ist dagegen der Backup-Daten-Datenverkehr zum Backup-Netzwerk isoliert. Benutzer, die auf den Mail-Server zugreifen, sind nicht betroffen. Das Backup-Netzwerk wird für alle Backup-Vorgänge verwendet, es sei denn, der Remote-Computer ist nicht mit dem Backup-Netzwerk verbunden.

Um alle Remote-Computer zu sichern, die nicht mit dem Backup-Netzwerk verbunden sind, verwenden Sie eine beliebige verfügbare Netzwerkroute. Über das verfügbare Netzwerk können Sie den Remote-Computer sichern, obwohl er sich nicht auf dem Backup-Netzwerk befindet.

Sie können globale Netzwerkeinstellungen für alle Backup-Aufträge im Teilfenster "Netzwerk und Sicherheit" in den Backup Exec-Einstellungen konfigurieren. Wenn Sie die globalen Einstellungen für einen bestimmten Backup-Auftrag übergehen möchten, können Sie beim Erstellen von Backups Netzwerkeinstellungen für einzelne Aufträge im Teilfenster "Netzwerk" konfigurieren.

Siehe ["Netzwerk- und Sicherheitsoptionen für Backup Exec ändern"](#) auf Seite 713.

Siehe ["Konfigurieren erweiterter Optionen für Backup-Aufträge"](#) auf Seite 223.

Siehe ["Verwendung von Backup Exec mit Firewalls"](#) auf Seite 722.

Verwenden von IPv4 und IPv6 in Backup Exec

Backup Exec unterstützt Version 4 und 6 von Internet Protocol (IP), gemeinhin als IPv4 und IPv6 bezeichnet. Sie können IPv4 und IPv6 für das Backup und Wiederherstellung von Netzwerken einsetzen. Die Unterstützung für IPv6 hängt von der Betriebssystemunterstützung für das Protokoll sowie der Netzwerkkonfiguration ab.

Backup Exec kann in einer gemischten IPv4/IPv6-Umgebung oder einer ausschließlichen IPv4-Umgebung verwendet werden.

Sie können überall in Backup Exec, wo Sie einen Computernamen eingeben können, eine IPv4- oder IPv6-Adresse eingeben mit Ausnahme der folgenden Stellen:

- Cluster Microsoft Windows unterstützt IPv6-Adressen nicht als Cluster-Computer.

- Das Dialogfeld "Mit Backup Exec-Server verbinden".

Ein Backup Exec Agent, der IPv6 unterstützt, kann nur von einem IPv6-kompatiblen Backup Exec-Server mit IPv6 gesichert oder wiederhergestellt werden.

Netzwerk- und Sicherheitsoptionen für Backup Exec ändern

Sie können konfigurieren, wie Backup Exec mit Ihrer Netzwerkkonfiguration und -Sicherheit funktioniert. Die Netzwerk- und Sicherheitsoptionen sind globale Optionen, die alle Backup Exec-Aufträge betreffen.

Wenn die global konfigurierten Netzwerk- und Sicherheitseinstellungen nicht auf einen bestimmten Backup-Auftrag angewandt werden, können Sie die Netzwerkeinstellungen beim Erstellen des Backup-Auftrags ändern.

Siehe ["Konfigurieren erweiterter Optionen für Backup-Aufträge"](#) auf Seite 223.

Bearbeiten der Netzwerk- und Sicherheitsoptionen

- 1 Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Backup Exec-Einstellungen".
- 2 Wählen Sie im linken Teilfenster "Netzwerk und Sicherheit".
- 3 Konfigurieren Sie eine der folgenden Optionen:

Netzwerkschnittstelle	Hier können Sie den Namen der Netzwerkkarte auswählen, die den Backup Exec-Server mit dem Netzwerk für diesen Backup-Auftrag verbindet. Die Liste umfasst alle verfügbaren Netzwerkschnittstellen auf dem Backup Exec-Server.
Protokoll	<p>Hier können Sie das Standardprotokoll auswählen, das für Backup-Aufträge verwendet werden soll.</p> <p>Folgende Optionen sind verfügbar:</p> <ul style="list-style-type: none"> ■ Beliebiges verfügbares Protokoll verwenden ■ IPv4 ■ IPv6
Subnetz	Hier können Sie die 32-Bit-Nummer auswählen, die das Subnetz festlegt, zu dem die Netzwerkkarte gehört.

<p>Einsatz von beliebigen verfügbaren Netzwerkschnittstellen, Subnetzen oder Protokollen für Backup Exec-Agents zulassen, die nicht an die oben genannten Netzwerkschnittstellen, Subnetze oder Protokolle gebunden sind</p>	<p>Wählen Sie diese Option aus, damit Backup Exec jedes verfügbare Netzwerk nutzen kann, wenn das Remote-System, das Sie für Backup oder Wiederherstellung ausgewählt haben, nicht Teil des angegebenen Backup-Netzwerks ist.</p> <p>Wenn Sie diese Option nicht auswählen und das Remote-System nicht Teil des angegebenen Backup-Netzwerks ist, schlägt der Auftrag fehlt. Backup Exec kann auf die Daten vom Remote-System nicht zugreifen.</p>
<p>Schnittstellendetails</p>	<p>Klicken Sie diese Option an, um die Media Access Control (MAC)-Adresse, den Adaptertypen, die Beschreibung, die IP-Adresse und die Subnetzpräfixe für die Schnittstelle anzusehen, die Sie für das Backup-Netz ausgewählt haben.</p>
<p>Auswahl von Benutzerfreigaben aktivieren</p>	<p>Wählen Sie diese Option aus, um benutzerdefinierte Freigaben in die Aufträge einzuschließen.</p> <p>Wenn Sie diese Option nicht aktivieren, können Sie beim Erstellen von Aufträgen keine benutzerdefinierte Freigaben auswählen.</p>
<p>Dynamischen Anschlussbereich für TCP aktivieren</p>	<p>Lässt Backup Exec-Agents verschiedene Ports für die Kommunikation verwenden.</p> <p>Sie legen den Anschlussbereich fest. Wenn der erste von Backup Exec gewählte Port nicht verfügbar ist, versucht Backup Exec einen der anderen Ports im Anschlussbereich zu nutzen. Wenn keiner der Ports im Bereich verfügbar ist, verwendet Backup Exec jeden verfügbaren dynamischen Port. Standard-Port-Bereiche sind 1025 bis 65535. Verwenden Sie einen Bereich von 25 zugeordneten Ports für den Remote-Computer, wenn Sie Backup Exec in Verbindung mit einer Firewall nutzen.</p> <p>Siehe "Verwendung von Backup Exec mit Firewalls" auf Seite 722.</p>

Benutzerdefinierten Port für den Empfang von Vorgangsanforderungen vom Oracle-Server verwenden	<p>Hier können Sie den Port angeben, den Backup Exec für die Kommunikation zwischen dem Backup Exec-Server und dem Remote-Computer für von DBA und dem Backup Exec-Server gestartete Vorgänge verwendet. Backup Exec verwendet standardmäßig Port 5633.</p> <p>Wenn Sie die Portnummer auf dem Windows- oder Linux-Remote-Computer ändern möchten, müssen Sie die Nummer ebenfalls auf dem Backup Exec Server ändern. Anschließend müssen Sie den Backup Exec Job Engine-Dienst auf dem Backup Exec-Server neu starten.</p> <p>Siehe "Info zur Änderung von Informationen der Oracle-Instanz" auf Seite 1362.</p>
FIPS 140-2-kompatible Softwareverschlüsselung verwenden	<p>Hier können Sie die mit den FIPS 140-2-Standards kompatible Softwareverschlüsselung aktivieren. Wenn Sie diese Option auswählen, müssen Sie einen AES-Verschlüsselungscode mit 256 Bit verwenden. Diese Option ist nur für Windows-Computer verfügbar.</p> <p>Sie müssen die Backup Exec Services anhalten und erneut starten, damit diese Änderung wirksam wird.</p>
Schlüssel verwalten	<p>Ermöglicht Ihnen die Erstellung eines neuen Verschlüsselungscode oder die Verwaltung der vorhandenen.</p>

Backup Exec-Konsole sichern

Ermöglicht das Schützen der Backup Exec-Konsole durch Bereitstellen folgender Funktionen, wenn Sie das Kontrollkästchen "Backup Exec-Konsole schützen" aktivieren.

- **Authentifizierung**

Nachdem Sie das Kontrollkästchen "Backup Exec-Konsole schützen" aktiviert haben, ist die Einstellung aktiviert. Beim nächsten Start von Backup Exec müssen Sie für die Verbindung zur Konsole die Backup Exec-Identifikationsdaten eingeben.

Wenn Sie die Identifikationsdaten nicht eingeben, können Sie keine Verbindung zur Backup Exec-Konsole herstellen.

- **Option "Konsole sperren"**

Nachdem Sie das Kontrollkästchen "Backup Exec-Konsole schützen" aktiviert haben, ist diese Option aktiviert. Sie können die Backup Exec-Sitzung sperren, an der Sie gerade arbeiten, und die Backup Exec-Konsole vor unbefugtem Zugriff schützen.

Wenn Sie die Backup Exec-Konsole nicht sperren, können Sie keine Aufgaben in der Backup Exec-Benutzeroberfläche ausführen.

Hinweis: Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

Diese Option ist nicht anwendbar für Remote Administration Console (RAC), da Sie immer die Identifikationsdaten für die Verbindung zur Backup Exec-Konsole angeben müssen.

Nur der Eigentümer eines System-Login-Kontos, der bei der Backup Exec-Konsole eingeloggt ist, verfügt über die Berechtigungen zum Ändern der Benutzerzugriffseinstellungen. Wenn Sie den Besitzer des System-Login-Kontos abrufen möchten, klicken Sie die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen > Login-Konten auswählen > Login-Konten verwalten". Im Dialogfeld "Login-Kontenverwaltung" wird in der Spalte "Besitzer" der Name angezeigt.

Wenn Sie bei einem parallelen Upgrade eine niedrigere Version von MMS und eine aktualisierte Version von CAS haben und eine Verbindung zu MMS aus CAS herstellen, ist dieses Kontrollkästchen zwar verfügbar,

kann aber nicht aktiviert werden. Diese Einstellung ist jedoch nicht für MMS aktiviert.

Siehe ["Sperren und Freigeben der Backup Exec-Konsole"](#) auf Seite 134.

Einstellen des Sperrmodus
für die
Datenträgerspeicherung

Die Funktion Ransomware-Resilience ermöglicht es Ihnen, die Einstellung für den Sperrmodus auf dem Datenträgerspeicher zu aktivieren bzw. zu deaktivieren.

Das Einstellen des Sperrmodus für die Datenträgerspeicherung schützt die plattenbasierte Sicherung, die mit Backup Exec konfiguriert wurde. Der Zugriff auf die Datenträgerspeicherung ist auf autorisierte Verfahren, wie die Backup Exec-Dienste, beschränkt. Nur Backup Exec darf auf den Datenträgerspeicher schreiben (Backup Exec-Dateiordner, wo die Backup-Aufträge abgelegt werden). Kein anderes Verfahren kann auf den Datenträgerspeicher schreiben.

Während der Sperrmodus aktiviert ist, laufen die Backups und Wiederherstellungen unverändert weiter.

Wenn die Datenträgerspeicherung auf einer Netzwerkfreigabe angelegt wird, die sich auf einem Remote Server befindet, kann Backup Exec lediglich die Schreibvorgänge vom Mediaserver überwachen. Wenn von einem anderen Server aus, auf dem Backup Exec nicht installiert ist, auf die Netzwerkfreigabe zugegriffen wird, wird der Schreibzugriff erlaubt.

Diese Einstellung ist standardmäßig aktiviert und ist die empfohlene Einstellung zum Schutz Ihrer Backup-Daten. Sie können die Einstellung durch Eingabe der Zugangsdaten für die Systemanmeldung deaktivieren.

Siehe "[Deaktivieren des Sperrmodus für Datenträgerspeicherung](#)" auf Seite 721.

Wenn der Sperrmodus aktiviert ist, zeigt der Status "Aktiviert" an.

Die Einstellung ist deaktiviert und der Sperrmodus-Status zeigt "Deaktiviert" an. Wir empfehlen dringend, diese Einstellung zu aktivieren, um die Datenträgerspeicherung zu schützen. Änderungen an der plattenbasierten Speicherung können nur mit Backup Exec vorgenommen werden.

Wenn der Sperrmodus deaktiviert ist, wird das Kontrollkästchen "Benachrichtigung versenden, wenn Sperrmodus für die Datenträgerspeicherung deaktiviert ist" aktiviert, damit Sie in regelmäßigen Abständen Warnmeldungen erhalten. Bis Sie den Sperrmodus wieder aktivieren, wird jeden Tag um 11 Uhr eine Warnmeldung generiert. Dieses Kontrollkästchen ist

standardmäßig aktiviert. Sie können das Kontrollkästchen deaktivieren, wenn Sie keine regelmäßigen Warnmeldungen mehr erhalten möchten.

Klicken Sie zum erneuten Aktivieren des Sperrmodus auf "Aktivieren".

Siehe ["So sehen Sie den Status des Sperrmodus für die Datenträgerspeicherung"](#) auf Seite 579.

4 Klicken Sie auf "OK".

Siehe ["Backup-Netzwerke"](#) auf Seite 711.

Deaktivieren des Sperrmodus für Datenträgerspeicherung

Der Sperrmodus für die Datenträgerspeicherung ist standardmäßig aktiviert und ist die empfohlene Einstellung zum Schutz Ihrer Backup-Daten. Sie können die Einstellung durch Eingabe der Zugangsdaten für die Systemanmeldung deaktivieren.

So deaktivieren Sie den Sperrmodus für die Datenträgerspeicherung

1 Klicken Sie auf "Deaktivieren".

Das Dialogfeld "Sperrmodus für Datenträgerspeicherung deaktivieren" wird angezeigt. Das Einstellen des Sperrmodus schützt die plattenbasierte Speicherung vor nicht autorisiertem Zugriff. Zum Deaktivieren dieser Einstellung müssen Sie die Zugangsdaten für die Anmeldung beim Dienst eingeben.

2 Gehen Sie wie folgt vor:

Benutzername	<p>Zeigt den Benutzernamen für das Konto zur Systemanmeldung an.</p> <p>Sie können den Benutzernamen nicht bearbeiten.</p>
Kennwort	<p>Geben Sie das Kennwort für das Konto zur Systemanmeldung ein.</p>
Grund für die Deaktivierung des Sperrmodus	<p>Geben Sie den Grund für die Deaktivierung des Sperrmodus ein.</p>

3 Klicken Sie auf "OK".

Wurde die Einstellung erfolgreich deaktiviert, wird eine Bestätigung angezeigt.
 Wurde die Einstellung nicht deaktiviert, wird eine Nachricht angezeigt.

4 Klicken Sie auf "OK".

Nachdem die Einstellung deaktiviert wurde, zeigt der Status des Sperrmodus "Deaktiviert" im Teilefenster "Netzwerk und Sicherheit" an. Wir empfehlen dringend, diese Einstellung zu aktivieren, um die Datenträgerspeicherung zu schützen. Änderungen an der plattenbasierten Speicherung können nur mit Backup Exec vorgenommen werden.

Siehe ["Netzwerk- und Sicherheitsoptionen für Backup Exec ändern"](#) auf Seite 713.

Verwendung von Backup Exec mit Firewalls

In Firewall-Umgebungen bietet Backup Exec folgende Vorteile:

- Die Anzahl der für Verbindungen zum Backup-Netzwerk verwendeten Ports wird auf ein Minimum beschränkt.
- Offene Ports auf dem Backup Exec-Server und auf Remote-Systemen sind dynamisch und bieten hohe Flexibilität beim Durchsuchen, Sichern und Wiederherstellen.
- Sie können bestimmte Firewall-Portbereiche festlegen und die Backup- und Wiederherstellungs-Netzwerke innerhalb dieser Bereiche angeben. Sie können bestimmte Bereiche verwenden, um Datenverkehr zu isolieren und eine hohe Zuverlässigkeit zu gewährleisten.

Hinweis: Zum Ausführen von standortfernen Backups und Wiederherstellungen benötigen Sie Agent for Windows.

Firewalls wirken sich auf die Systemkommunikation zwischen einem Backup Exec-Server und allen Remote-Systemen aus, die außerhalb der Firewall-Umgebung liegen. Sie sollten spezielle Portanforderungen für Ihre Firewall erwägen, wenn Sie Backup Exec konfigurieren.

Es wird empfohlen, dass Sie Port 10000 öffnen und sicherstellen, dass er auf dem Backup Exec-Server und allen Remote-Computern verfügbar ist. Zusätzlich müssen die dynamischen Portbereiche für die Kommunikation zwischen dem Backup Exec-Server und Backup Exec-Agents geöffnet sein.

Wenn ein Backup Exec-Server eine Verbindung zu einem Remote-System herstellt, verwendet er zuerst Port 10000. Der Agent überwacht Verbindungen auf diesem vordefinierten Port. Der Backup Exec-Server ist an einen verfügbaren Port

gebunden. Zusätzliche Verbindungen zum Agent werden jedoch auf jedem verfügbaren Port initiiert.

Wenn Sie Daten sichern, können bis zu zwei Ports auf dem Computer erforderlich sein, auf dem der Agent installiert ist. Um simultane Aufträge zu unterstützen, müssen Sie Ihre Firewall konfigurieren, damit ein ausreichend großer Bereich mit Ports die Anzahl der simultanen Vorgänge entsprechend unterstützen kann.

Wenn es einen Konflikt gibt, können Sie den Standardport in eine alternative Port-Nummer ändern, indem Sie die `%systemroot%\System32\drivers\etc\services`-Datei ändern. Sie können einen Texteditor wie Notepad verwenden, um Ihren NDMP-Eintrag zu ändern oder einen NDMP-Eintrag mit einer neuen Port-Nummer hinzuzufügen. Sie sollten den Eintrag wie folgt formatieren:

```
ndmp      9999/tcp      #Network Data Management Protocol
```

Hinweis: Ändern Sie den Standardport, müssen Sie ihn auf dem Backup Exec-Server und allen Remote-Systemen ändern, die durch die Firewall gesichert werden.

Wenn Sie dynamische TCP-Portbereiche einrichten, sollten Sie einen Bereich mit 25 zugeteilten Ports für den Remote-Computer verwenden. Die Anzahl der Ports, die von Remote-Computer erfordert werden, hängt von der Anzahl der Geräte ab, die Sie schützen, und der Anzahl der verwendeten Bandgeräte. Die Portbereiche müssen u. U. erweitert werden, um eine optimale Leistung zu gewährleisten.

Wenn Sie keinen bestimmten Bereich festlegen, verwendet Backup Exec den Gesamtbereich der verfügbaren dynamischen Ports. Wenn Sie Remote-Backups hinter einer Firewall durchführen, sollten Sie einen bestimmten Bereich im Dialogfeld "Netzwerk und Sicherheit" auswählen.

So durchsuchen Sie Systeme durch eine Firewall

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Backup Exec-Einstellungen".
- 2 Wählen Sie im linken Teilfenster "Netzwerk und Sicherheit".

- 3 Stellen Sie sicher, dass ein dynamischer Portbereich für den Backup Exec-Server und den Backup Exec-Agent eingerichtet wurde und die Firewall so konfiguriert ist, dass Verbindungen über diese Portbereiche und den Port 10000 (für die erste Verbindung zwischen Backup Exec-Server und Backup Exec-Agent) zugelassen werden.

Port 6101 muss geöffnet sein, um Windows-Systeme in der Backup-Auswahlstruktur zu durchsuchen.

- 4 Klicken Sie auf "OK".

Siehe ["Backup ExecAnschlüsse"](#) auf Seite 724.

Siehe ["Backup Exec-Listener-Ports"](#) auf Seite 726.

Siehe ["Infos zum Aktivieren einer SQL-Instanz hinter einer Firewall"](#) auf Seite 727.

Backup ExecAnschlüsse

Wenn Sie eine Firewall verwenden, haben Sie möglicherweise spezielle Portanforderungen für Backup Exec. Firewalls können sich manchmal auf die Systemkommunikation zwischen einem Backup Exec -Server und Remote-Systemen auswirken, die sich außerhalb der Firewall befinden.

Siehe ["Verwendung von Backup Exec mit Firewalls"](#) auf Seite 722.

In der folgenden Tabelle erhalten Sie ausführlichere Informationen zu den von Backup Exec und den zugehörigen Agents sowie Optionen verwendeten Ports:

Tabelle 15-2 Backup ExecAnschlüsse

Dienst oder Prozess	Anschluss	Anschlusstyp
Backup Exec Agent-Browser (Prozess "benetns.exe")	6101	TCP
Backup Exec Agent for Windows (Prozess "beremote.exe")	10000	TCP
Backup Exec-Server (Prozess "beremote.exe")	3527, 6106	TCP

Dienst oder Prozess	Anschluss	Anschlusstyp
MSSQL\$BKUPEXEC (Prozess "sqlservr.exe")	Eine Port-Nummer zwischen 49152 und 65535 (Windows 2008). In der Microsoft-Dokumentation erhalten Sie weitere Informationen zum Zuweisen der TCP/IP-Portnummern, die für die SQL-Kommunikation durch eine Firewall erforderlich ist.	TCP UDP
Agent for Oracle auf Windows- oder Linux-Servern	Beliebiger Port, sofern nicht anders konfiguriert	
Agent for Linux	Standard-NDMP-Anschluss, meist 10000	TCP
Backup Exec-Deduplizierungs-Engine (Prozess "spoold.exe")	10082	TCP
Backup Exec-Deduplizierungs-Engine (Prozess "spoold.exe")	10102	TCP
Backup Exec Management Service (process= BackupExecManagementService.exe)	50104	TCP
Kerberos	88	UDP
NETBIOS	135	TCP, UDP
NETBIOS-Namensdienst	137	UDP
NETBIOS-Datagrammdienst	138	UDP
NETBIOS-Sitzungsdienst	139	TCP
NETBIOS	445	TCP
DCOM/RPC	3106	TCP
Agent for Windows	6103	TCP

Dienst oder Prozess	Anschluss	Anschlusstyp
Push-Installation - Überprüfen Sie die Meldungswarteschlange für CAS (Teil von beserver.exe) auf Konflikte.	103x	TCP
Push-Installation	441	TCP
E-Mail-Benachrichtigung per SMTP	25 ausgehend vom Backup Exec-Server	TCP
SNMP	162 ausgehend vom Backup Exec-Server	TCP

Backup Exec-Listener-Ports

Wenn Sie eine Firewall verwenden, haben Sie möglicherweise spezielle Portanforderungen für Backup Exec. Firewalls können sich manchmal auf die Systemkommunikation zwischen einem Backup Exec-Server und Remote-Systemen auswirken, die sich außerhalb der Firewall befinden.

Siehe "[Verwendung von Backup Exec mit Firewalls](#)" auf Seite 722.

Wenn Backup Exec keine Vorgänge ausführt, überwacht das Programm die Anschlüsse nach eingehenden Daten anderer Dienste oder Agents. Die anfängliche Kommunikation für den Start eines Vorgangs zwischen Backup Exec und Agent erfolgt über einen statischen Listener-Port. Anschließend verwenden der Agent und der Backup Exec-Server für den Datenaustausch dynamische Ports.

Backup Exec verwendet folgende Abhöranschlüsse:

Tabelle 15-3 Backup Exec-Listener-Ports

Dienst	Anschluss	Anschlusstyp
Backup Exec Agent-Browser (benetns.exe)	6101	TCP
Backup Exec Agent for Windows (beremote.exe)	10000	TCP
Backup Exec-Server (beserver.exe)	3527, 6106	TCP
Backup Exec Management Service (process= BackupExecManagementService.exe)	50104	TCP

Dienst	Anschluss	Anschlusstyp
MSSQL\$BKUPEXEC (sqlsevr.exe)	1125	TCP
	1434	UDP
Agent for Linux (RALUS)	10000	TCP
DBA-initiierte Backups für Oracle	5633	TCP

Infos zum Aktivieren einer SQL-Instanz hinter einer Firewall

Wenn Sie eine Verbindung mit einer SQL-Instanz hinter einer Firewall herstellen möchten, muss die SQL-Instanz verbindungsfähig sein. Um die Verbindungsfähigkeit zu aktivieren, muss der SQL-Anschluss statisch sein und die Windows-Firewall konfiguriert werden.

Die SQL-Instanz von Backup Exec ist standardmäßig zur Verwendung eines dynamischen Anschlusses konfiguriert. Die Portnummer kann sich bei jedem Start des SQL-Servers ändern.

Die Windows-Firewall muss Verbindungen mit der SQL-Instanz zulassen. Je nach Systemkonfiguration gibt es mehrere Möglichkeiten, die Einstellungen der Windows-Firewall zu ändern. Sie können der Windows-Firewall-Liste für Ausnahmen die Einträge "sqlsvr.exe" und "sqlbrowser.exe" hinzufügen oder einen Anschluss in der Windows-Firewall für den TCP-Zugriff öffnen. Weitere Informationen erhalten Sie in der Microsoft-Supportdatenbank, um zu entscheiden, welche Methode für Ihr Netzwerk am geeignetsten ist.

Siehe ["Installieren eines verwalteten Backup Exec-Servers über eine Firewall "](#) auf Seite 1463.

Siehe ["Verwendung von Backup Exec mit Firewalls"](#) auf Seite 722.

Verwendung von Verschlüsselung mit Backup Exec

In Backup Exec können Sie Daten verschlüsseln. Durch Verschlüsseln von Daten werden diese vor unerlaubtem Zugriff geschützt. Für den Zugriff ist der von Ihnen erstellte Schlüssel erforderlich. Backup Exec bietet sowohl Softwareverschlüsselung als auch einige Geräte mit Hardwareverschlüsselung nach dem T10-Standard. Backup Exec konfiguriert die Verschlüsselung, wenn Sie die Speichergeräte, die Sie für einen Backup-Auftrag verwenden möchten, angeben.

Backup Exec unterstützt bei der Verschlüsselung zwei Sicherheitsstufen: 128-Bit Advanced Encryption Standard (AES) und 256-bit AES. Mit 256-Bit AES wird eine

höhere Sicherheitsstufe erreicht, da der Schlüssel bei 256-Bit AES länger als der Schlüssel bei 128-Bit AES ist. Mit 128-Bit AES-Verschlüsselung können Backup-Aufträge jedoch schneller verarbeitet werden. Die Hardwareverschlüsselung nach dem T10-Standard benötigt 256-Bit AES.

Wenn Sie einen Duplizierungs-Backup-Auftrag ausführen, werden Backup-Sätze, die bereits verschlüsselt sind, nicht neu verschlüsselt. Unverschlüsselte Backup-Sätze können dagegen verschlüsselt werden.

Informationen zu den Best Practices zur Softwareverschlüsselung von Backup Exec finden Sie unter *Best Practices für Backup Exec*.

Dieses Thema enthält folgende Informationen:

[Softwareverschlüsselung](#)

[Hardwareverschlüsselung](#)

[Verschlüsselungen](#)

[Eingeschränkte Schlüssel und gemeinsame Schlüssel](#)

[Passphrasen](#)

Softwareverschlüsselung

Wenn Sie Backup Exec installieren, installiert das Installationsprogramm Verschlüsselungssoftware auf dem Backup Exec-Server und auf allen Remote-Computern, die einen Backup Exec Agent verwenden. Backup Exec kann Daten auf einem Computer verschlüsseln, der Backup Exec Agent verwendet, und diese dann an den Backup Exec-Server übertragen. Anschließend schreibt Backup Exec die verschlüsselten Daten Satz für Satz auf ein Bandmedium oder in einen Festplattenspeicher.

Backup Exec verschlüsselt Daten der folgenden Typen:

- Benutzerdaten wie Dateien und Microsoft Exchange-Datenbanken
- Metadaten wie Dateinamen, Attribute und Betriebssysteminformationen
- Informationen zu Katalogdateien und Verzeichnissen auf dem Medium.

Backup Exec kann keine Backup Exec-Metadaten oder Informationen zu Katalogdateien und Verzeichnissen auf der Festplatte verschlüsseln.

Bei Backup-Aufträgen können Sie für die Verschlüsselung Softwarekomprimierung nutzen. Dabei komprimiert Backup Exec die Dateien und verschlüsselt sie anschließend. Backup-Aufträge, für die sowohl Verschlüsselung als auch Softwarekomprimierung genutzt werden, nehmen jedoch mehr Zeit in Anspruch.

Es wird empfohlen, in Verbindung mit der Softwareverschlüsselung keine Hardwarekomprimierung zu verwenden. Die Hardwarekomprimierung erfolgt nach der Verschlüsselung. Während des Verschlüsselungsvorgangs werden die Daten

randomisiert. In Verbindung mit randomisierten Daten funktioniert die Komprimierung nicht einwandfrei.

Hardwareverschlüsselung

Backup Exec unterstützt die Hardwareverschlüsselung für Speichergeräte mit dem T10-Verschlüsselungsstandard. Bei der Hardwareverschlüsselung werden die Daten vom Hostcomputer an das Speichergerät übermittelt und dort verschlüsselt. Die Schlüssel für den Zugriff auf die verschlüsselten Daten werden in Backup Exec verwaltet.

Backup Exec unterstützt ausschließlich für den T10-Standard autorisierte Geräte.

Hinweis: Die Hardwareverschlüsselung nach dem T10-Standard benötigt 256-Bit AES. Die Aktivierung der Hardwareverschlüsselung in Backup Exec ist nur in Verbindung mit Sicherheitsfragen von mindestens 16 Zeichen möglich.

Verschlüsselungen

Sie müssen Verschlüsselungsschlüssel erstellen, um Verschlüsselung in Backup Exec zu verwenden. Bei der Erstellung eines Verschlüsselungscodes durch einen Benutzer markiert Backup Exec den Schlüssel mit einer auf der Sicherheitsidentifikation des eingeloggten Benutzers basierenden ID. Der Benutzer, der den Schlüssel erstellt hat, wird als Eigentümer des Schlüssels bestimmt.

Wenn Sie Verschlüsselung für synthetische Backups verwenden, müssen alle verbundenen Backups den gleichen Verschlüsselungscode verwenden. Ändern Sie nicht den Verschlüsselungscode, nachdem die Basis erstellt ist. Der Verschlüsselungscode, den Sie für das Basis-Backup auswählen, wird automatisch auf alle verbundenen Backups angewendet.

Wenn Sie verschlüsselte Daten zum Wiederherstellen auswählen, überprüft Backup Exec, ob in der Datenbank Verschlüsselungen für die Daten verfügbar sind. Falls einer der Schlüssel nicht verfügbar ist, fordert Sie Backup Exec auf, den fehlenden Schlüssel neu zu erstellen. Wenn Sie den Schlüssel nach Einplanen des Auftrags löschen, schlägt der Auftrag fehl.

Findet Backup Exec während der Verarbeitung eines Katalogauftrags keine Verschlüsselung, wird von Backup Exec eine Meldung ausgegeben. Sie können, wenn Ihnen die Passphrase bekannt ist, den fehlenden Verschlüsselungscode dann neu erstellen.

Simplified Disaster Recovery unterstützt die Wiederherstellung von Computern mit vorher verschlüsselten Backup-Sätzen. Wenn die Simplified Disaster Recovery (SDR)-Backups während des Backups verschlüsselt werden, fordert der Assistent "Computer wiederherstellen" Sie auf, für jeden verschlüsselten Backup-Satz, der für die Wiederherstellung erforderlich ist, die Passphrase einzugeben.

Siehe ["Verwaltung von Verschlüsselungscodes"](#) auf Seite 731.

Eingeschränkte Schlüssel und gemeinsame Schlüssel

Backup Exec unterstützt die folgenden Typen von Verschlüsselungscodes:

Tabelle 15-4 Typen von Verschlüsselungscodes

Schlüsseltyp	Beschreibung
Gemeinsam	Ein solcher Schlüssel kann von jedem Benutzer zur Verschlüsselung von Daten bei Backups und zur Wiederherstellung der verschlüsselten Daten verwendet werden.
Eingeschränkt	Jeder kann den Schlüssel verwenden, um Daten während eines Backup-Auftrags zu verschlüsseln, aber Benutzer, die den Schlüssel nicht besitzen, müssen die Passphrase kennen. Wenn ein Benutzer, der den Schlüssel nicht besitzt, die verschlüsselten Daten wiederherstellen möchte, fordert Backup Exec den Benutzer auf, die Passphrase einzugeben. Wenn Sie die richtige Passphrase für den Schlüssel nicht eingeben können, können Sie die Daten nicht wiederherstellen.

Passphrasen

Für die Verschlüsselung sind Sicherheitsfragen erforderlich. Diese funktionieren ähnlich wie Kennwörter. Sicherheitsfragen sind normalerweise länger als Kennwörter und bestehen aus mehreren Wörtern oder Textgruppen. Eine gute Passphrase ist zwischen 8 und 128 Zeichen lang. Eine 128-Bit-AES-Verschlüsselung muss aus mindestens acht Zeichen bestehen. Eine 256-Bit-AES-Verschlüsselung muss aus mindestens 16 Zeichen bestehen. Es wird empfohlen, mehr als nur die minimale Zeichenanzahl zu verwenden.

Hinweis: Die Hardwareverschlüsselung nach dem T10-Standard benötigt 256-Bit AES. Die Aktivierung der Hardwareverschlüsselung in Backup Exec ist nur in Verbindung mit Sicherheitsfragen von mindestens 16 Zeichen möglich.

Wirkungsvolle Sicherheitsfragen enthalten sowohl Groß- als auch Kleinbuchstaben, Ziffern und Sonderzeichen. Zitate aus Literatur und anderen Texten sollten nicht als Sicherheitsfragen verwendet werden.

Sicherheitsfragen dürfen nur druckbare ASCII-Zeichen enthalten. Dies sind die Zeichen 32 bis 126. Das ASCII-Zeichen 32 ist das Leerzeichen und wird mithilfe der Leertaste auf der Tastatur eingegeben. Die ASCII-Zeichen 33 bis 126 sind die folgenden:

!"#\$%&'()*+,-./0123456789;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ

[]^_`abcdefghijklmnopqrstuvwxyz{|}~

Siehe ["Verwaltung von Verschlüsselungscodes"](#) auf Seite 731.

Verwaltung von Verschlüsselungscodes

Bei der Erstellung eines Verschlüsselungscodes durch einen Benutzer markiert Backup Exec den Schlüssel mit einer auf der Sicherheitsidentifikation des eingeloggtten Benutzers basierenden ID. Der Benutzer, der den Schlüssel erstellt hat, wird als Eigentümer des Schlüssels bestimmt.

Siehe ["Verwendung von Verschlüsselung mit Backup Exec"](#) auf Seite 727.

Backup Exec speichert Schlüssel in der Backup Exec-Datenbank. Die Sicherheitsfrage für die Schlüssel wird von Backup Exec jedoch nicht gespeichert. Der Eigentümer eines Schlüssels muss darauf achten, dass die Sicherheitsfrage für den Schlüssel nicht verloren geht.

Um die Schlüssel zu schützen, wird Folgendes empfohlen:

- Notieren Sie sich die Sicherheitsfragen. Bewahren Sie diese Notiz an einem sicheren Ort und nicht in der Nähe der verschlüsselten Backup-Sätze auf.
- Sichern Sie die Backup Exec-Datenbank. Die Schlüssel werden in der Datenbank aufgezeichnet.

Vorsicht: Wenn Sie keine Backup-Kopie der Backup Exec-Datenbank zur Verfügung haben und die Sicherheitsfragen vergessen, können Sie keine Daten von den verschlüsselten Medien wiederherstellen.

Ein Schlüssel, der auf einem Backup Exec-Server erstellt wird, ist nur für diesen zu verwenden. Sie können Schlüssel nicht zwischen Backup Exec-Server verschieben. Es ist jedoch möglich, auf einem anderen Backup Exec-Server unter Verwendung derselben Sicherheitsfragen neue Schlüssel zu erstellen. Eine Sicherheitsfrage erzeugt immer denselben Schlüssel. Darüber hinaus können versehentlich gelöschte Schlüssel mithilfe der Sicherheitsfrage erneut erstellt werden.

Wird eine Backup Exec-Datenbank auf einem Backup Exec-Server beschädigt und durch eine neue ersetzt, müssen Sie alle Verschlüsselungen, die in der Originaldatenbank gespeichert waren, manuell neu erstellen.

Wenn Sie eine Datenbank von einem Backup Exec-Server auf einen anderen Backup Exec-Server verschieben, bleiben die Verschlüsselungen bestehen, solange der neue Backup Exec-Server die folgenden Kriterien erfüllt:

- Verfügt über dieselben Benutzerkonten wie der ursprüngliche Backup Exec-Server.
- Befindet sich in derselben Domäne wie der ursprüngliche Backup Exec-Server.

Siehe ["Erstellen von Verschlüsselungscodes"](#) auf Seite 732.

Siehe ["Ersetzen eines Verschlüsselungscodes"](#) auf Seite 733.

Siehe ["Löschen des Verschlüsselungsschlüssels"](#) auf Seite 736.

Erstellen von Verschlüsselungscodes

Beim Erstellen einer Verschlüsselung wählen Sie auch den Verschlüsselungstyp aus.

So erstellen Sie einen Verschlüsselungscode:

- 1 Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Backup Exec-Einstellungen".
- 2 Wählen Sie im linken Teilfenster "Netzwerk und Sicherheit".
- 3 Klicken Sie auf "Schlüssel verwalten".
- 4 Klicken Sie auf "Neu".
- 5 Im "Schlüsselname" geben Sie einen eindeutigen Namen für diesen Schlüssel ein. Der Name kann bis zu 256 Zeichen lang sein.
- 6 Im Feld Verschlüsselungstyp wählen Sie den Verschlüsselungstyp für diesen Schlüssel aus. Zur Verfügung stehen 128-Bit AES und 256-Bit AES.

Der Standardtyp ist 256-Bit AES. Die Verschlüsselung mit 256-Bit AES bietet mehr Sicherheit als die Verschlüsselung mit 128-Bit AES. Die Verarbeitung von Backup-Aufträgen kann jedoch mit 256-Bit AES länger dauern als mit 128-Bit AES. Die Hardwareverschlüsselung nach dem T10-Standard benötigt 256-Bit AES.

- 7** Geben Sie im Feld "Passphrase" eine Passphrase für diesen Schlüssel ein. Es können nur druckbare ASCII-Zeichen verwendet werden.

Bei der 128-Bit AES-Verschlüsselung muss der Kennsatz mindestens aus acht Zeichen bestehen. Bei der 256-Bit AES-Verschlüsselung muss der Kennsatz mindestens aus 16 Zeichen bestehen.

Es wird empfohlen, mehr als nur die minimale Zeichenanzahl zu verwenden.

Warnung: Wenn ein in einem Backup genutzter Verschlüsselungscode nicht mehr verfügbar ist, müssen Sie beim Wiederherstellen die Passphrase angeben. Ohne Passphrase ist der Zugriff auf die Daten nicht möglich.

- 8** Geben Sie im Feld "Passphrase bestätigen" die Passphrase erneut ein, um sie zu bestätigen.
- 9** Wählen Sie im Gruppenfeld "Verschlüsselungscodetyp" aus, ob Sie einen gemeinsamen oder einen eingeschränkten Verschlüsselungscode erstellen möchten.

Bei gemeinsamen Schlüsseln können alle Benutzer dieser Backup Exec-Installation Daten mit dem Schlüssel sichern und wiederherstellen. Wenn ein Schlüssel eingeschränkt ist, kann jeder den Schlüssel zum Sichern von Daten verwenden. Die verschlüsselten Daten können jedoch nur vom Schlüsselinhaber oder einem Benutzer, der die Sicherheitsfrage kennt, wiederhergestellt werden.

- 10** Klicken Sie auf "OK".

Siehe ["Verwaltung von Verschlüsselungscodes"](#) auf Seite 731.

Siehe ["Verwendung von Verschlüsselung mit Backup Exec"](#) auf Seite 727.

Ersetzen eines Verschlüsselungscodes

Sie können einen Verschlüsselungscode für alle Backup-Aufträge und Aufträge zur Duplizierung von Backup-Sätzen durch einen anderen Schlüssel ersetzen.

Hinweis: Sie können einen Verschlüsselungscode nicht ersetzen, wenn er in einem Wiederherstellungsauftrag verwendet wird.

So ersetzen Sie einen Verschlüsselungscode

- 1** Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Backup Exec-Einstellungen".
- 2** Wählen Sie im linken Teilfenster "Netzwerk und Sicherheit".
- 3** Klicken Sie auf "Schlüssel verwalten".
- 4** Wählen Sie den Schlüssel, den Sie ersetzen möchten.
- 5** Klicken Sie auf "Ersetzen".
- 6** Führen Sie im Feld "Verschlüsselungscode auswählen, der <Codename> ersetzen soll" einen der folgenden Vorgänge aus:

Verwenden eines vorhandenen Schlüssels Wählen Sie den Schlüssel aus der Liste aus.

Erstellen eines
neuen Schlüssels

Führen Sie die folgenden Schritte durch:

- Klicken Sie auf "Neu".
- Geben Sie im Feld "Schlüsselname" einen eindeutigen Namen für den Schlüssel ein.
Der Name kann bis zu 256 Zeichen lang sein.
- Wählen Sie im Feld "Verschlüsselungstyp" den Typ der Verschlüsselung aus.
Zur Verfügung stehen 128-Bit-AES und 256-Bit-AES. Der Standardtyp ist 256-Bit AES.
Die Verschlüsselung mit 256-Bit AES bietet mehr Sicherheit als die Verschlüsselung mit 128-Bit AES. Die Verarbeitung von Backup-Aufträgen kann jedoch mit 256-Bit AES länger dauern als mit 128-Bit AES.
Die Hardwareverschlüsselung nach dem T10-Standard benötigt 256-Bit AES.
- Geben Sie im Feld "Passphrase" eine Passphrase für diesen Schlüssel ein.
Bei der 128-Bit AES-Verschlüsselung muss der Kennsatz mindestens aus acht Zeichen bestehen. Bei der 256-Bit AES-Verschlüsselung muss der Kennsatz mindestens aus 16 Zeichen bestehen. Es wird empfohlen, mehr als nur die minimale Zeichenanzahl zu verwenden.
Es können nur druckbare ASCII-Zeichen verwendet werden.
Warnung: Wenn ein in einem Backup genutzter Verschlüsselungscode nicht mehr verfügbar ist, müssen Sie beim Wiederherstellen die Passphrase angeben. Ohne Passphrase ist der Zugriff auf die Daten nicht möglich.
- Geben Sie im Feld "Passphrase bestätigen" die Passphrase erneut ein, um sie zu bestätigen.
- Wählen Sie im Gruppenfeld "Verschlüsselungscodetyp" aus, ob Sie einen gemeinsamen oder einen eingeschränkten Verschlüsselungscode erstellen möchten.
- Klicken Sie auf "OK".

7 Klicken Sie auf "OK".

Siehe ["Verwaltung von Verschlüsselungscodes"](#) auf Seite 731.

Siehe ["Verwendung von Verschlüsselung mit Backup Exec"](#) auf Seite 727.

Löschen des Verschlüsselungsschlüssels

Beim Löschen von Verschlüsselungsschlüsseln sollten Sie vorsichtig vorgehen. Wenn Sie einen Verschlüsselungsschlüssel löschen, können Sie die mit diesem Schlüssel verschlüsselten Backup-Sätze erst dann wiederherstellen, wenn Sie einen neuen Schlüssel erstellen, der denselben Verschlüsselungsschlüssel sowie denselben Kennsatz wie der Originalschlüssel verwendet.

Unter folgenden Umständen können Sie Verschlüsselungsschlüssel löschen:

- Wenn die verschlüsselten Daten auf dem Medium abgelaufen sind oder das Medium ausrangiert wurde.
- Wenn der Verschlüsselungsschlüssel nicht der Standardschlüssel ist.
- Der Verschlüsselungsschlüssel wird nicht in einem Auftrag verwendet. Wird der Schlüssel verwendet, müssen Sie einen neuen Schlüssel für den Auftrag wählen.

Wenn Sie einen Verschlüsselungsschlüssel löschen, der bei einem geplanten Wiederherstellungsauftrag zum Einsatz kommt, können Sie den Schlüssel nicht ersetzen. Daher schlägt jeder geplante Wiederherstellungsauftrag, bei dem ein Verschlüsselungsschlüssel gelöscht wird, fehl.

So löschen Sie eine Verschlüsselung:

- 1 Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Backup Exec-Einstellungen".
- 2 Wählen Sie im linken Teilfenster "Netzwerk und Sicherheit".
- 3 Klicken Sie auf "Schlüssel verwalten".
- 4 Wählen Sie den Schlüssel, den Sie löschen möchten.
- 5 Klicken Sie auf "Löschen".
- 6 Klicken Sie auf Ja.
- 7 Wird der Schlüssel in einem Auftrag verwendet, führen Sie folgende Schritte durch:
 - Wählen Sie im Feld Verschlüsselungsschlüssel auswählen, der "Schlüsselname" ersetzen soll den neuen Schlüssel für den Auftrag aus oder klicken Sie auf "Neu", um einen neuen Schlüssel zu erstellen.
 - Klicken Sie auf "OK".

Siehe ["Verwaltung von Verschlüsselungscodes"](#) auf Seite 731.

Siehe ["Verwendung von Verschlüsselung mit Backup Exec"](#) auf Seite 727.

Granular Recovery Technology

Sie können Granular Recovery Technology (GRT) verwenden, um bestimmte einzelne Elemente aus den Backup-Sätzen wiederherzustellen. Beispielsweise können Sie mit Agent for Microsoft Exchange Server eine E-Mail aus einem Backup wiederherstellen, ohne das vollständige Postfach wiederherstellen zu müssen. Verwenden Sie alternativ Agent for Microsoft SharePoint zum Wiederherstellen einer Liste, ohne die gesamte Site wiederherzustellen.

Um einzelne Objekte wiederherzustellen, muss die Funktion "Granular Recovery Technology" beim Erstellen eines Backup-Auftrags aktiviert werden.

GRT wird standardmäßig für Backups für die folgenden Agents aktiviert:

- Agent for Microsoft Active Directory
- Agent for Microsoft Exchange Server
- Agent for Microsoft SharePoint
- Agent for VMware and Hyper-V

Sie können entweder vollständige Backup-Sätze oder einzelne Elemente aus GRT-Backups wiederherstellen.

Standardmäßig verwendet der Agent for VMware und Hyper-V Granular Recovery Technology, um Dateien und Ordner auf einer granularen Ebene zu schützen. Sie können Granular Recovery auch für Microsoft Exchange-, SharePoint- und Active Directory-Anwendungsdaten auf virtuellen Computern aktivieren.

Beim Sichern von Daten erstellt Backup Exec einen Katalog mit Informationen über die Backup-Sätze und über das Speichergerät, auf dem die Backup-Sätze gespeichert werden. Das Katalogisieren von GRT-Backup-Aufträgen nimmt mehr Zeit in Anspruch aufgrund der Menge von granularer Informationen. Für GRT-Aufträge wird die Katalogisierung verzögert und als separater Vorgang ausgeführt, damit das Backup-Fenster weniger beeinträchtigt wird. Da die Katalogisierung separat vom Backup-Auftrag ausgeführt wird, wird der pünktliche Start eines anderen geplanten GRT-Backup-Auftrags nicht verhindert.

Wenn Sie GRT für Microsoft Exchange-, Microsoft SharePoint-, Microsoft Hyper-V- oder VMware-Backups aktivieren, wird die vollständige Katalogisierung standardmäßig sofort nach dem Backup-Auftrag ausgeführt.

Für Exchange- und SharePoint-Backups mit Agent wird die vollständige Katalogisierung sofort nach allen vollständigen Backups ausgeführt. Er wird alle 24 Stunden für inkrementelle und differenzielle Backups ausgeführt, selbst wenn Sie mehr als einen GRT-Auftrag innerhalb von 24 Stunden planen.

Für Hyper-V- und VMware-Backups wird die vollständige Katalogisierung standardmäßig sofort nach allen vollständigen, inkrementellen und differenziellen Backups ausgeführt.

Sie können die vollständige Katalogisierung so konfigurieren, dass sie nach einem Zeitplan ausgeführt wird, wenn Sie ihn nicht sofort nach dem Backup ausführen möchten. Sie können auch den Vorgang Instant GRT im Rahmen des Backup-Auftrags ausführen.

Siehe ["Konfigurieren der Optionen für Instant GRT und Vollständige Katalogisierung zum Verbessern der Backup-Leistung von GRT-Aufträgen"](#) auf Seite 656.

Informationen zu den Best Practices zum Einsatz von Backup Exec und Granular Recovery Technology (GRT) finden Sie unter *Best Practices für Backup Exec*.

Die folgende Tabelle listet die einzelnen Objekte auf, die Sie für jeden Agent wiederherstellen können.

Tabelle 15-5 Einzelne Objekte, die für jeden Agent wiederhergestellt werden können

Agent	Einzelne Objekte
Agent for Microsoft Active Directory	Sie können die folgenden einzelnen Objekte wiederherstellen: <ul style="list-style-type: none">■ Active Directory-Objekte und -Attribute■ Active Directory Application Mode (ADAM)- und Active Directory Lightweight Directory Services (AD LDS)-Objekte und -Attribute
Agent for Microsoft Exchange Server	Sie können die folgenden einzelnen Objekte wiederherstellen: <ul style="list-style-type: none">■ Postfächer■ E-Mail-Nachrichten und Anhänge■ Öffentliche Ordner■ Kalenderelemente■ Kontakte■ Hinweise■ Aufgaben

Agent	Einzelne Objekte
Agent for Microsoft SharePoint	<p>Im Folgenden finden Sie Beispiele der einzelnen Elemente, die wiederhergestellt werden können:</p> <ul style="list-style-type: none">■ Site-Sammlungen■ Sites oder Subsites■ Dokument- oder Bilderbibliotheken■ Listen■ Einzelne Listenelemente■ Dokumente, Bilder oder andere Dateien, die in den Bibliotheken gespeichert werden
Agent for VMware and Hyper-V	<p>Sie können Laufwerke, Ordner und Dateien von virtuellen Computern mit einem Windows-Betriebssystem wiederherstellen.</p> <p>Sie können Granular Recovery auch für Microsoft Exchange-, SQL- und Active Directory-Anwendungsdaten auf virtuellen Computern aktivieren.</p> <p>Siehe "Verwenden von Granular Recovery Technology (GRT) mit Agent for VMware" auf Seite 1115.</p>

Wenn Sie einen GRT-Backup-Auftrag ausführen, erstellt Backup Exec Medien mit einem IMG-Präfix (z. B. IMG00001). Ein IMG-Medium ist ein bestimmter Medientyp, den Backup Exec nur für Backups mit aktivierter GRT-Option erstellt. Wenn Sie einen Backup-Auftrag mit aktivierter GRT-Option ausführen, speichert das IMG-Medium die Backup-Daten.

Hinweis: Es wird empfohlen, dass Sie für GRT-Backup-Aufträge keine Software-Komprimierung oder -verschlüsselung verwenden. Das Komprimieren und Verschlüsseln nimmt viele Ressourcen in Anspruch. Das Aktivieren der Software-Komprimierung oder -verschlüsselung verringert möglicherweise die Leistung für GRT-Backup-Aufträge.

Sie sollten vor Beginn sorgfältig überlegen, welches Gerät Sie für Backups mit aktivierter GRT-Option verwenden. Berücksichtigen Sie ferner etwaige spezielle Anforderungen für die zu sichernden Daten.

Empfohlene Geräte für Backups mit Granular Recovery Technology

Es wird empfohlen, dass Sie ein Datenträgerspeichergerät für alle Backups mit Granular Recovery Technology (GRT) auswählen. Das Speichergerät sollte sich auf einem Datenträger ohne Dateigrößenbeschränkungen befinden. Ein

NTFS-Laufwerk ist ein Beispiel eines Datenträgers ohne Dateigrößenbeschränkungen. Beispiele von Datenträgern mit Dateigrößenbeschränkungen sind FAT und FAT32.

Hinweis: Wenn Sie die Verschlüsselung für GRT-Backup-Aufträge für Festplatte, Deduplizierung und Plattenkassettengeräte aktivieren, speichert Backup Exec die Backup-Sätze nicht verschlüsselt. Nur die Backup-Sätze für Backup-Quellen, die GRT nicht unterstützen, werden verschlüsselt gespeichert. Alle Backup-Sätze für Backup-Aufträge an Cloud-, OpenStorage- und Bandspeicher werden verschlüsselt.

Wenn Sie ein Speichergerät auf einem Datenträger mit Dateigrößenbeschränkungen verwenden müssen, ist für Backup Exec ein Stagingspeicherort erforderlich. Backup Exec speichert während des Backup-Auftrags vorübergehend eine kleine Menge Metadaten an diesem Speicherort. Es löscht die Daten aus dem Stagingspeicherort, wenn das Backup abgeschlossen ist. Der Stagingspeicherort ist jedoch nicht notwendig, wenn Sie ein Datenträgerspeichergerät auf einem Datenträger ohne Dateigrößenbeschränkungen als Ziel verwenden.

Der Standardpfad des Stagingspeicherorts ist C:\temp.

Der Datenträger, der als Stagingspeicherort für Backup-Aufträge verwendet wird, sollte die folgenden Anforderungen erfüllen:

- Er ist ein lokaler Datenträger des Backup Exec-Server.
- Er unterliegt keinen Dateigrößenbeschränkungen.

Darüber hinaus sollten zur Vermeidung von Speicherplatzproblemen folgende Anforderungen erfüllt sein:

- Er sollte kein Systemdatenträger sein.
- Er sollte mindestens 1 GB freien Speicherplatz aufweisen.

Backup Exec verwendet auch einen Stagingspeicherort, um GRT-Daten aus einem Band oder von einem Datenträgerspeichergerät auf Datenträgern mit Dateigrößenbeschränkungen wiederherzustellen. Der Stagingspeicherort muss sich auf einem Datenträger befinden, der keinen Dateigrößenbeschränkungen unterliegt und vom Backup Exec-Server lokal verwendet wird. Der Stagingspeicherort ist nicht erforderlich, wenn Sie GRT-aktivierte Daten vom Datenträgerspeicher auf einem Datenträger ohne Dateigrößenbeschränkungen wiederherstellen, wie etwa NTFS.

Backup Exec verwendet den Stagingbereich auf andere Weise für die folgenden Arten von Wiederherstellungen:

Tabelle 15-6 Staging

Speicherort der wiederherzustellenden Daten	Staging
Band	<p>Backup Exec kopiert die gesamten Backup-Sätze in den Stagingbereich. Der Stagingbereich muss genügend Speicherplatz für den gesamten Backup-Satz bzw. die -Sätze haben, aus denen ein einzelnes Objekt wiederhergestellt werden soll.</p> <p>Bevor Sie ein Bandgerät für ein GRT-Backup verwenden, stellen Sie sicher, dass genügend Speicherplatz verfügbar ist, um eine Wiederherstellung durchzuführen.</p> <p>Backup Exec löscht die Daten aus dem Stagingbereich, wenn der Wiederherstellungsauftrag abgeschlossen ist.</p>
Cloud	<p>Backup Exec verwendet einen gestaffelten Speicherort, um GRT-Daten aus dem Cloud-Speichergerät wiederherzustellen.</p> <p>Backup Exec kopiert die gesamten Backup-Sätze in den Stagingbereich. Der Stagingbereich muss genügend Speicherplatz für den gesamten Backup-Satz bzw. die -Sätze haben, aus denen ein einzelnes Objekt wiederhergestellt werden soll.</p> <p>Bevor Sie ein Cloud-Speichergerät für ein GRT-Backup verwenden, stellen Sie sicher, dass genug Speicherplatz für eine Wiederherstellung vorhanden ist.</p> <p>Backup Exec löscht die Daten aus dem Stagingbereich, wenn der Wiederherstellungsauftrag abgeschlossen ist.</p>
Datenträgerspeichergerät, das sich auf einem Datenträger mit Dateigrößenbeschränkungen befindet (wie z. B. FAT oder FAT32)	<p>Backup Exec muss eine kleine Menge mit dem Backup-Satz verbundener Metadaten in den Stagingbereich kopieren, um die Wiederherstellung abzuschließen.</p> <p>Backup Exec löscht die Daten aus dem Stagingbereich, wenn der Wiederherstellungsauftrag abgeschlossen ist.</p>

Der Standardpfad des Stagingspeicherorts ist C:\temp. Sie können die Standardbackup- und Wiederherstellungsstaffelspeicherorte in den Backup Exec-Einstellungen ändern.

Anforderungen für Aufträge mit Granular Recovery Technology

Beachten Sie die folgenden Anforderungen, wenn Sie Granular Recovery Technology (GRT) mit den aufgelisteten Agents verwenden:

Tabelle 15-7 Anforderungen für Granular Recovery Technology

Agent	Beschränkungen
Agent for Microsoft Active Directory	<p>Sie müssen einen Backup Exec-Server verwenden, der Windows Server 2012 R2 ausführt, um einen Active Directory-Server zu sichern, der Windows Server 2012 R2 ausführt.</p> <p>In einer CAS-Umgebung führt Backup Exec den Backup-Auftrag auf dem zentralen Administrationsserver durch, wenn auf diesem Windows Server 2012 R2 installiert und der Speicher lokal konfiguriert ist. Andernfalls versucht Backup Exec, einen verwalteten Backup Exec-Server mit Windows Server 2012 R2 zu finden, um den Auftrag durchzuführen. Wenn er keinen finden kann, schließt der Auftrag erfolgreich aber mit Ausnahmen ab, und die Backup-Sätze werden nicht GRT-aktiviert.</p> <p>Wenn der Active Directory-Server jedoch ein virtueller Computer ist, kann Backup Exec möglicherweise nicht erkennen, dass der Server Windows Server 2012 R2 ausführt. Das resultierende Backup wird möglicherweise ohne GRT ausgeführt.</p>

Agent	Beschränkungen
Agent for Microsoft Exchange Server	<p>Für Informationsspeichervorgänge muss Backup Exec Zugriff auf ein eindeutig benanntes Postfach innerhalb der Exchange-Organisation für Backup- und Wiederherstellungsaufträge haben.</p> <p>Siehe "Voraussetzungen für den Zugriff auf Exchange-Postfächer " auf Seite 1283.</p> <p>Backup Exec verwendet ein Plattenspeichergerät ohne Dateigrößenbeschränkungen auf dem Backup Exec-Server als Standard-Stagingspeicherort für GRT-Backups von Exchange-Daten. Backup Exec verwendet möglicherweise einen anderen Stagingspeicherort als den, der in den Standard-Backup-Optionen konfiguriert ist, da zum Ausführen von GRT-Vorgängen ein Datenträger mit derselben Datenträgergeometrie erforderlich ist. Der Speicherort hat jedoch keinen Einfluss auf die Leistung oder den Speicherplatz, der für die Vorgänge erforderlich ist.</p> <p>Sie können eine VHD- bzw. VHDX-Datei anstelle eines physischen Datenträgers als Stagingbereich erstellen, wenn Sie die Beanspruchung der Ressourcen gering halten möchten. Konfigurieren Sie die VHD- bzw. VHDX-Datei als Datenträger mit großen Sektoren und gewährleisten Sie, dass sie mindestens 1 GB groß ist. Stellen Sie dann die VHD- bzw. VHDX-Datei in einem Verzeichnis bereit. Backup Exec findet automatisch den virtuellen Datenträger, wenn es einen Bereitstellungsbereich benötigt, um alle Daten zu sichern, die sich auf einem Laufwerk mit großen Sektoren befinden.</p> <p>Empfohlene Geräte für Backups mit Granular Recovery Technology</p>
Agent for Microsoft SharePoint	<p>Sie müssen über eine aktuelle Version des Agents for Windows verfügen, die auf allen Servern in der SharePoint-Farm installiert ist.</p>

Agent	Beschränkungen
Agent for VMware and Hyper-V	<p>Sie können nur einzelne Elemente auf virtuellen Computern wiederherstellen, auf denen ein Windows-Betriebssystem ausgeführt wird.</p> <p>Standardmäßig verwendet der Agent for VMware und Hyper-V Granular Recovery Technology, um Dateien und Ordner auf einer granularen Ebene zu schützen. Sie können Granular Recovery auch für Microsoft Exchange-, SQL- und Active Directory-Anwendungsdaten auf virtuellen Computern aktivieren.</p> <p>Wenn Sie einen virtuellen Computer auf Band sichern, muss die Option "Speicherbasierte Kataloge verwenden" in den Einstellungen "Katalog" aktiviert werden, um sicherzustellen, dass Sie einzelne Elemente aus den Backup-Sätzen wiederherstellen können.</p> <p>Siehe "Konfigurieren der Standardoptionen für Kataloge" auf Seite 279.</p>

Siehe ["Festlegen von Standardoptionen für Granular Recovery Technology festlegen \(GRT\)"](#) auf Seite 744.

Festlegen von Standardoptionen für Granular Recovery Technology festlegen (GRT)

Mit der Granular Recovery Technology (GRT) von Backup Exec können Sie bestimmte einzelne Elemente aus den Backup-Sätzen wiederherstellen. Beispielsweise können Sie mit Agent for Microsoft Exchange Server eine E-Mail aus einem Backup wiederherstellen, ohne das vollständige Postfach wiederherstellen zu müssen. Verwenden Sie alternativ Agent for Microsoft SharePoint zum Wiederherstellen einer Liste, ohne die gesamte Site wiederherzustellen.

Siehe ["Granular Recovery Technology"](#) auf Seite 737.

Sie können Standardeinstellungen für Granular Recovery Technology konfigurieren. Backup Exec wendet die Standardeinstellungen für alle Backup-Aufträge an, die konfigurieren, um GRT zu verwenden.

Standardoptionen für "Granular Recovery Technology" festlegen (GRT)

- Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Backup Exec-Einstellungen".
- Wählen Sie im linken Teilfenster die Option "Granular Recovery Technology".

3 Konfigurieren Sie eine der folgenden Optionen:

- | | |
|--|---|
| <p>Wenn Granular Recovery Technology (GRT) für Backups aktiviert ist, geben Sie den Pfad zu einem NTFS-Volumen auf dem lokalen Backup Exec-Server ein, auf dem Backup Exec temporäre Daten staffeln kann</p> | <p>Hier können Sie einen Speicherort festlegen, an dem Backup Exec während der Verarbeitung GRT-aktivierter Aufträge temporäre Daten gestaffelt ablegen kann.</p> <p>Stellen Sie sicher, dass der Speicherort ein NTFS-Datenträger ist und kein Systemdatenträger ist. Wenn der Standardpfad von C:\TEMP nicht diese Bedingungen erfüllt, geben Sie einen anderen Pfad auf dem Backup Exec-Server ein, in dem Backup Exec vorübergehende Daten ablegen kann.</p> <p>Backup Exec löscht die Daten aus dem Staffelungsbereich, wenn der Wiederherstellungsauftrag abgeschlossen ist.</p> <p>Dafür ist mindestens 1 GB Speicherplatz erforderlich.</p> |
| <p>Geben Sie den Pfad zu einem NTFS-Datenträger auf dem lokalen Backup Exec-Server ein, wo Backup Exec temporäre Daten (Microsoft Hyper-V, Microsoft Exchange, Microsoft SharePoint, Microsoft Active Directory und VMware) ablegen kann</p> | <p>Hier können Sie einen Speicherort festlegen, an dem Backup Exec während der Verarbeitung GRT-aktivierter Aufträge temporäre Daten gestaffelt ablegen kann.</p> <p>Diese Option gilt nur bei der Wiederherstellung einzelner Objekte unter den folgenden Bedingungen:</p> <ul style="list-style-type: none"> ■ Das Backup von Microsoft Hyper-V, Microsoft Exchange, Microsoft SharePoint, Microsoft Active Directory oder VMware Virtual Infrastructure wurde für Backup Exec GRT aktiviert. ■ Das Backup wird auf einem Band durchgeführt. ■ Das Backup erfolgt auf einem Datenträgerspeicher auf einem Datenträger, der Größenbeschränkungen aufweist. FAT und FAT32 sind Beispiele für Datenträgertypen mit Dateigrößenbeschränkungen. <p>Geben Sie den Pfad zu einem Ordner auf einem NTFS-Datenträger auf diesem Backup Exec-Server ein. Wiederherstellungsdaten und Metadaten für diesen Auftrag werden hier vorübergehend gespeichert, bevor die einzelnen Objekte wiederhergestellt werden. Die abgelegten Daten werden nach Abschluss des Wiederherstellungs-Auftrags automatisch gelöscht.</p> <p>Es wird davon abgeraten, Systemdatenträger als temporäre Speicherorte zu verwenden.</p> |

4 Klicken Sie auf "OK".

DBA-initiierte Auftragsvorlagen

Wenn Sie einen von DBA gestarteten Backup-Vorgang erstellen, können Sie die Standard-Auftragsvorlage in Backup Exec angeben. Sie können auch eine neue Auftragsvorlage angeben, die Sie in Backup Exec erstellen. Die Auftragsvorlage enthält die Einstellungen, die Backup Exec auf DBA-gestartete Aufträge anwendet.

Stellen Sie sicher, dass der Name der gewünschten Auftragsvorlage auch in den Instanzinformationen auf dem Windows-Computer konfiguriert wird.

Siehe ["Konfigurieren des Oracle Agent auf Windows-Computern und -Linux-Servern"](#) auf Seite 1342.

Siehe ["Informationen über die Durchführung eines von DBA gestarteten Backup-Auftrags für Oracle"](#) auf Seite 1366.

Beachten Sie die folgenden Hinweise zu von DBA gestarteten Aufträgen:

- Von DBA gestartete Aufträge schlagen fehl, wenn die zugehörige Auftragsvorlage gelöscht wird. Um die Ausführung der DBA-gestarteten Aufträge zu verhindern, löschen Sie die entsprechende Vorlage für die DBA-gestarteten Aufträge.
- Alle von DBA gestarteten Backup- und Wiederherstellungsaufträge werden nach Beendigung gelöscht.
- Es ist nicht möglich, für DBA-gestartete Aufträge Mindestgeräteanforderungen festzulegen.

Siehe ["Erstellen DBA-initiierten Auftragsvorlagen"](#) auf Seite 746.

Siehe ["Bearbeiten von von DBA gestarteten Auftragsvorlagen"](#) auf Seite 747.

Siehe ["Löschen von DBA-initiierten Auftragsvorlagen"](#) auf Seite 748.

Erstellen DBA-initiierten Auftragsvorlagen

Sie können eine neue Auftragsvorlage erstellen, die Backup Exec bei von DBA gestarteten Aufträgen anwendet.

So erstellen Sie DBA-initiierte Auftragsvorlagen

- 1 Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Backup Exec-Einstellungen".
- 2 Wählen Sie im linken Teilfenster "Einstellungen für von DBA gestartete Aufträge".
- 3 Klicken Sie auf "Neu".

- 4 Im linken Teilfenster wählen Sie den Typ der festzulegenden Optionen aus. Die erforderlichen Optionen hängen von den Anforderungen Ihrer Umgebung ab.

- 5 Klicken Sie auf "OK".

Siehe ["DBA-initiierte Auftragsvorlagen"](#) auf Seite 746.

Siehe ["Speicheroptionen für von DBA gestartete Aufträge"](#) auf Seite 748.

Siehe ["Allgemeine Optionen für DBA-initiierte Aufträge"](#) auf Seite 753.

Siehe ["Netzwerkooptionen für DBA-initiierte Aufträge"](#) auf Seite 753.

Siehe ["Optionen von Migrator for Enterprise Vault"](#) auf Seite 1427.

Siehe ["Benachrichtigungsoptionen für Aufträge"](#) auf Seite 357.

Siehe ["Duplizieren von Auftragseinstellungen für DBA-initiierte Aufträge"](#) auf Seite 755.

Bearbeiten von von DBA gestarteten Auftragsvorlagen

Sie können die Auftragsvorlageneinstellungen bearbeiten, die Backup Exec auf von DBA gestartete Aufträge anwendet.

So bearbeiten Sie Vorlagen für von DBA gestartete Aufträge

- 1 Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Backup Exec-Einstellungen".
- 2 Wählen Sie im linken Teilfenster "Einstellungen für von DBA gestartete Aufträge".
- 3 Wählen Sie die Auftragsvorlage aus, die Sie bearbeiten möchten.
- 4 Klicken Sie auf "Bearbeiten".
- 5 Im linken Teilfenster wählen Sie den Typ der Optionen aus, die Sie bearbeiten möchten. Diese Optionen hängen von den Anforderungen Ihrer Umgebung ab.
- 6 Klicken Sie auf "OK".

Siehe ["DBA-initiierte Auftragsvorlagen"](#) auf Seite 746.

Siehe ["Speicheroptionen für von DBA gestartete Aufträge"](#) auf Seite 748.

Siehe ["Allgemeine Optionen für DBA-initiierte Aufträge"](#) auf Seite 753.

Siehe ["Netzwerkooptionen für DBA-initiierte Aufträge"](#) auf Seite 753.

Siehe ["Optionen von Migrator for Enterprise Vault"](#) auf Seite 1427.

Siehe ["Benachrichtigungsoptionen für Aufträge"](#) auf Seite 357.

Siehe ["Duplizieren von Auftragseinstellungen für DBA-initiierte Aufträge"](#) auf Seite 755.

Löschen von DBA-initiierten Auftragsvorlagen

Sie können die Vorlagen löschen, die Backup Exec auf DBA-initiierte Aufträge anwendet, wenn Sie sie nicht mehr benötigen.

So löschen Sie eine Auftragsvorlage für DBA-initialisierte Aufträge

- 1 Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Backup Exec-Einstellungen".
- 2 Wählen Sie im linken Teilfenster "Einstellungen für von DBA gestartete Aufträge".
- 3 Wählen Sie die Auftragsvorlage aus, die Sie löschen möchten.
- 4 Klicken Sie auf Löschen.
- 5 Klicken Sie auf Ja.

Siehe ["DBA-initiierte Auftragsvorlagen"](#) auf Seite 746.

Speicheroptionen für von DBA gestartete Aufträge

Sie können Speichereinstellungen für DBA-initiierte Aufträge konfigurieren.

Siehe ["DBA-initiierte Auftragsvorlagen"](#) auf Seite 746.

Tabelle 15-8 Speicheroptionen für von DBA gestartete Aufträge

Element	Beschreibung
Speicher	<p>Gibt das Speichergerät an, zu dem Sie Backup-Daten für die DBA-initiierten Aufträge senden möchten.</p> <p>Siehe "Erstellen von Speichergerätepools" auf Seite 512.</p> <p>Siehe "Info zu Remote Media Agent for Linux" auf Seite 1598.</p> <p>Siehe "Funktionen und Typen des plattenbasierten und netzwerkbasierten Speichers" auf Seite 367.</p>

Element	Beschreibung
Dem Remote-Computer ermöglichen, direkt auf das Speichergerät zuzugreifen und eine clientseitige Deduplizierung durchzuführen, falls diese unterstützt wird	<p>Ist diese Option aktiviert, kann ein Remote-Computer Daten direkt an ein OpenStorage-Gerät oder an ein Deduplizierungsspeichergerät senden und die clientseitige Deduplizierung durchführen, wenn das Gerät diese unterstützt. Der Backup Exec-Server wird umgangen, wodurch er für andere Vorgänge zur Verfügung steht. Kann die clientseitige Deduplizierung nicht durchgeführt werden, wird entweder die Backup Exec-Server-Deduplizierung oder die Appliance-Deduplizierung durchgeführt.</p> <p>Diese Option wird angezeigt, wenn die Deduplizierungsfunktion installiert ist und ein OpenStorage-Gerät oder ein Deduplizierungsspeichergerät im Feld "Speicher" ausgewählt ist.</p> <p>Siehe "Einsatz der clientseitigen Deduplizierung" auf Seite 1078.</p>
Dem Remote-Computer ermöglichen, über den Backup Exec-Server auf das Speichergerät zuzugreifen und eine serverseitige Backup Exec-Deduplizierung durchzuführen, falls diese unterstützt wird	<p>Ist diese Option aktiviert, kann ein Remote-Computer Daten über den Backup Exec-Server an ein OpenStorage-Gerät oder an ein Deduplizierungsspeichergerät senden und eine serverseitige Backup Exec-Deduplizierung durchführen, wenn diese unterstützt wird. Wenn der Backup Exec-Server die Deduplizierung nicht unterstützt, werden die Daten auf einem intelligenten Datenträgergerät, wie zum Beispiel PureDisk oder einem Gerät von einem externen Anbieter, dedupliziert.</p> <p>Diese Option wird angezeigt, wenn die Deduplizierungsfunktion installiert ist und im Feld "Speicher" ein OpenStorage-Gerät oder ein Deduplizierungsspeichergerät ausgewählt ist.</p> <p>Siehe "Info zu Deduplication Feature" auf Seite 1047.</p>
Aufbewahren für	Gibt an, wie lange Sie die Backup-Sätze oder den Auftragsverlauf für DBA-initiierte Aufträge aufbewahren möchten.

Element	Beschreibung
Mediensatz	<p>Gibt den Mediensatz an, der für DBA-initiierte Aufträge verwendet werden soll. Der Mediensatz gibt den Überschreibschutzzeitraum und den Anhängenzeitraum für die Backup-Daten auf den Medien an.</p> <p>Wenn Sie einen neuen Mediensatz für diesen Backup-Auftrag erstellen möchten, klicken Sie auf das Symbol rechts neben dem Dropdown-Menü "Mediensatz".</p> <p>Diese Option ist nur verfügbar, wenn Sie im Feld "Speicher" ein Bandgerät ausgewählt haben.</p> <p>Siehe "Standard-Mediensätze" auf Seite 473.</p>
Medium überschreiben	<p>Gibt an, dass der Backup-Auftrag auf überschreibbaren Medien gespeichert wird. Vergewissern Sie sich, dass sich das entsprechende Medium im ausgewählten Speichergerät befindet.</p> <p>Geeignete Medien für einen Überschreibungsauftrag:</p> <ul style="list-style-type: none"> ■ Temporäre Medien ■ Medien, deren Überschreibschutzzeitraum abgelaufen ist <p>Zugeordnete oder importierte Medien können auch abhängig von der festgelegten Medienüberschreibschutzstufe überschrieben werden.</p> <p>Abhängig von Ihrer Konfiguration werden überschreibbare Medien aus temporären oder wiederverwendbaren Medien ausgewählt.</p> <p>Wenn die Medien im Speichergerät nicht überschreibbar sind, werden Sie aufgefordert, überschreibbare Medien zur Verfügung zu stellen.</p> <p>Diese Option ist nur verfügbar, wenn Sie im Feld "Speicher" ein Bandgerät ausgewählt haben.</p> <p>Siehe "Verwalten von Bändern" auf Seite 472.</p> <p>Siehe "Medienüberschreibschutzstufen für Bandmedien" auf Seite 487.</p> <p>Siehe "So sucht Backup Exec nach überschreibbaren Medien in Bandlaufwerken" auf Seite 488.</p>

Element	Beschreibung
An Medium anhängen oder überschreiben, falls kein anhängbares Medium verfügbar ist	<p>Hängt diesen Backup-Auftrag an den angegebenen Mediensatz an, wenn anhängbare Medien verfügbar sind. Andernfalls sucht Backup Exec nach überschreibbaren Medien und fügt sie dem Mediensatz hinzu.</p> <p>Wenn ein Anhängeauftrag ein Medium füllt, wird der Backup-Auftrag auf einem überschreibbaren Medium fortgeführt. Wenn die Medien im Speichergerät nicht überschreibbar sind, werden Sie aufgefordert, überschreibbare Medien zur Verfügung zu stellen.</p> <p>Diese Option ist nur verfügbar, wenn Sie im Feld "Speicher" ein Bandgerät ausgewählt haben.</p>
An Medium anhängen oder Auftrag abbrechen, falls kein anhängbares Medium verfügbar ist	<p>Hängt diesen Backup-Auftrag an den angegebenen Mediensatz an, wenn anhängbare Medien verfügbar sind. Andernfalls beendet Backup Exec den Auftrag.</p> <p>Diese Option ist nur verfügbar, wenn Sie im Feld "Speicher" ein Bandgerät ausgewählt haben.</p>
Medium nach Auftragsabschluss auswerfen	<p>Wirft die Medien im Laufwerk oder Schacht aus, wenn der Vorgang abgeschlossen wurde. Sie können auch einen Auftrag planen, um Medien auszuwerfen.</p> <p>Diese Option ist nur verfügbar, wenn Sie im Feld "Speicher" ein Bandgerät ausgewählt haben.</p> <p>Siehe "Auswerfen von Medien aus einer Plattenkassette oder einem Bandlaufwerk" auf Seite 555.</p>
Spannen eines Mediums vor einem Backup	<p>Spult das Band im Laufwerk vom Anfang bis zum Ende mit hoher Geschwindigkeit um. Durch Spannen wird das Band gleichmäßig aufgewickelt und kommt gleichmäßig mit den Abtastköpfen des Bandlaufwerks in Kontakt. Diese Option ist nur verfügbar, wenn Sie ein Bandlaufwerk auswählen, das das Neuspannen unterstützt.</p>
Medien mit einem Schreib- und mehreren Lesevorgängen (WORM) verwenden	<p>Gibt die Verwendung des WORM-Mediums (ein Schreib- und mehrere Lesevorgänge) als Standard für DBA-initiierte Aufträge an. Backup Exec bestätigt, dass das Zielgerät ein WORM-kompatibles Laufwerk ist oder enthält, und dass das WORM-Medium in diesem Laufwerk zur Verfügung steht. Wird kein WORM-Medium oder WORM-kompatibles Laufwerk gefunden, wird eine entsprechende Warnmeldung ausgegeben.</p> <p>Siehe "So werden WORM-Medien in Backup Exec verwendet" auf Seite 495.</p>

Element	Beschreibung
Komprimierung	<p>Folgende Komprimierungsoptionen stehen zur Verfügung:</p> <ul style="list-style-type: none"> ■ Keine Kopiert die Daten in ihrem ursprünglichen Format auf das Medium (nicht komprimiert). Durch die Verwendung eines Datenkomprimierungsverfahrens können Sie Backup-Vorgänge beschleunigen und Speicherplatz sparen. Die Hardware-Datenkomprimierung sollte nicht in Umgebungen verwendet werden, in denen sowohl Speichergeräte mit Unterstützung einer Hardwarekomprimierung als auch Geräte ohne diese Funktion verwendet werden. In dieser Situation wird Hardwarekomprimierung automatisch deaktiviert. Sie können die Hardwarekomprimierung auf den entsprechenden Laufwerken zwar manuell wieder aktivieren, dies führt jedoch zu Inkonsistenzen zwischen den Medien. Wenn das Laufwerk mit Hardwarekomprimierung ausfällt, ist es nicht möglich, die komprimierten Medien mit dem nicht komprimierungsfähigen Laufwerk wiederherzustellen. ■ Software Mithilfe der STAC-Software-Datenkomprimierung werden die Daten komprimiert, bevor sie an das Speichergerät gesendet werden. ■ Hardware (falls vorhanden, sonst keine) Verwendet die Hardware-Datenkomprimierung (falls vom Speichergerät unterstützt). Wenn das Laufwerk keine Datenkomprimierung unterstützt, werden die Daten unkomprimiert gesichert. ■ Hardware (falls vorhanden, sonst Software) Verwendet die Hardware-Datenkomprimierung (falls vom Speichergerät unterstützt). Wenn das Laufwerk keine Hardware-Datenkomprimierung unterstützt, wird die Softwarekomprimierung STAC verwendet.
Verschlüsselungstyp	<p>Gibt den gewünschten Verschlüsselungstyp an (wenn vorhanden).</p> <p>Siehe "Verwendung von Verschlüsselung mit Backup Exec" auf Seite 727.</p>
Verschlüsselungscode	<p>Gibt den Verschlüsselungscode an, den Sie verwenden möchten, wenn Sie eine Verschlüsselung verwenden.</p> <p>Siehe "Verwendung von Verschlüsselung mit Backup Exec" auf Seite 727.</p>

Element	Beschreibung
Schlüssel verwalten	<p>Ermöglicht die Verwaltung Ihrer Verschlüsselungscodes.</p> <p>Sie können vorhandene Verschlüsselungscodes löschen oder ersetzen. Sie können auch einen neuen Verschlüsselungscode erstellen.</p> <p>Diese Option ist nur verfügbar, wenn Sie einen Verschlüsselungstyp auswählen.</p> <p>Siehe "Verwaltung von Verschlüsselungscodes" auf Seite 731.</p>

Allgemeine Optionen für DBA-initiierte Aufträge

Sie können allgemeine Optionen für DBA-initiierte Aufträge konfigurieren.

Siehe "[DBA-initiierte Auftragsvorlagen](#)" auf Seite 746.

Tabelle 15-9 Allgemeine Optionen für DBA-initiierte Aufträge

Element	Beschreibung
Auftragsname	Gibt den Namen für diese Backup-Vorlage an. Sie können den angezeigten Standardnamen akzeptieren oder einen Namen eingeben. Der Name muss eindeutig sein.
Beschreibung des Backup-Satzes	Beschreibt die Informationen im Backup-Satz für zukünftige Referenz.
Nach Backup überprüfen	Führt automatisch eine Überprüfung durch, um sicherzustellen, dass die Medien nach Abschluss des Backups gelesen werden können. Die Überprüfung sämtlicher Backups wird empfohlen.

Netzwerkoptionen für DBA-initiierte Aufträge

Sie können Netzwerkoptionen für DBA-initiierte Aufträge konfigurieren.

Siehe "[DBA-initiierte Auftragsvorlagen](#)" auf Seite 746.

Hinweis: Einige diese Optionen können nicht in einer CAS-Umgebung angezeigt werden.

Tabelle 15-10 Netzwerkoptionen für DBA-initiierte Aufträge

Element	Beschreibung
Netzwerkschnittstelle	Gibt den Namen der Netzwerkschnittstellenkarte an, die den Backup Exec-Server mit dem Netzwerk, das Sie für diesen Backup-Auftrag verwenden möchten, verbindet. Die Liste umfasst alle verfügbaren Netzwerkschnittstellen auf dem Backup Exec-Server.
Protokoll	Gibt das Protokoll an, das Sie für diesen Backup-Auftrag verwenden möchten. Folgende Optionen sind verfügbar: <ul style="list-style-type: none"> ■ Beliebiges verfügbares Protokoll verwenden ■ IPv4 verwenden ■ Ipv6 verwenden
Subnetz	Zeigt die 32-Bit-Nummer an, die das Subnetz festlegt, zu dem die Netzwerkkarte gehört.
Verwendung einer beliebigen verfügbaren Netzwerkschnittstelle, eines -subnets oder -protokolls für Backup Exec Agents, die nicht an die obige Netzwerkschnittstelle, das -subnet oder -protokoll gebunden sind	Backup Exec kann hierdurch jedes verfügbare Netzwerk nutzen, wenn das Remote-System, das Sie für Backup oder Wiederherstellung ausgewählt haben, nicht Teil des angegebenen Backup-Netzwerks ist. Wenn Sie diese Option nicht auswählen und das Remote-System nicht Teil des angegebenen Backup-Netzwerks ist, schlägt der Auftrag fehl. Backup Exec kann auf die Daten vom Remote-System nicht zugreifen.
Schnittstellendetails	Zeigt die Media Access Control (MAC)-Adresse, den Adaptertyp, die Beschreibung, die IP-Adressen und die Subnet-Präfixe für die Schnittstelle an, die Sie für das Backup-Netzwerk ausgewählt haben.
Zulassen, dass der verwaltete Backup Exec-Server eine beliebige Netzwerkschnittstelle für den Zugriff auf Backup Exec Agents verwendet	Mit dieser Option kann ein Auftrag jede beliebige Netzwerkschnittstelle verwenden, um auf Backup Exec Agents zuzugreifen, wenn die ausgewählte Netzwerkschnittstelle nicht verfügbar ist. Durch das Aktivieren dieser Option kann der verwaltete Backup Exec-Server eine alternative Netzwerkschnittstelle verwenden, um alle wichtigen Backup-Aufträge auszuführen, die andernfalls fehlschlagen würden. Diese Option ist nur verfügbar, wenn Central Admin Server Feature (CAS) installiert ist. Siehe "Infos zu Central Admin Server Feature" auf Seite 1450.

Duplizieren von Auftragseinstellungen für DBA-initiierte Aufträge

Sie können duplizierte Auftragsvorlageeinstellungen für DBA-initiierte Aufträge konfigurieren.

Siehe ["DBA-initiierte Auftragsvorlagen"](#) auf Seite 746.

Tabelle 15-11 Duplizieren von Auftragseinstellungen für DBA-initiierte Aufträge

Element	Beschreibung
Einstellungen zum Duplizieren von Backup-Sätzen für diesen Auftrag aktivieren	Aktiviert die Einstellungen für eine Vorlage zum Duplizieren von Backup-Sätzen.
Speicherort	Gibt das Speichergerät an, an das Sie Backup-Daten für die DBA-initiierten Deduplizierungs-Aufträge senden möchten.
Aufbewahren für	Gibt an, wie lange Sie die Backup-Sätze oder den Auftragsverlauf für DBA-initiierte Deduplizierungs-Aufträge aufbewahren möchten.
Mediensatz	<p>Gibt den Mediensatz an, der für DBA-initiierte Aufträge verwendet werden soll. Der Mediensatz gibt den Überschreibschutzzeitraum und den Anhängezeitraum für die Backup-Daten auf den Medien an.</p> <p>Wenn Sie einen neuen Mediensatz für diesen Backup-Auftrag erstellen möchten, klicken Sie auf das Symbol rechts neben dem Dropdown-Menü "Mediensatz".</p> <p>Siehe "Standard-Mediensätze" auf Seite 473.</p>

Element	Beschreibung
Medium überschreiben	<p>Gibt an, dass der Backup-Auftrag auf überschreibbaren Medien gespeichert wird. Vergewissern Sie sich, dass sich das entsprechende Medium im ausgewählten Speichergerät befindet.</p> <p>Geeignete Medien für einen Überschreibungsauftrag:</p> <ul style="list-style-type: none"> ■ Temporäre Medien ■ Medien, deren Überschreibschutzzeitraum abgelaufen ist <p>Abhängig von Ihrer Konfiguration werden überschreibbare Medien aus temporären oder wiederverwendbaren Medien ausgewählt.</p> <p>Wenn die Medien im Speichergerät nicht überschreibbar sind, wird eine Warnmeldung mit der Aufforderung angezeigt, überschreibbare Medien zur Verfügung zu stellen.</p> <p>Siehe "Verwalten von Bändern" auf Seite 472.</p> <p>Siehe "Medienüberschreibschutzstufen für Bandmedien" auf Seite 487.</p> <p>Siehe "So sucht Backup Exec nach überschreibbaren Medien in Bandlaufwerken" auf Seite 488.</p>
An Medium anhängen oder überschreiben, falls kein anhängbares Medium verfügbar ist	<p>Hängt diesen Backup-Auftrag an den angegebenen Mediensatz an, wenn anhängbare Medien verfügbar sind. Andernfalls sucht Backup Exec nach überschreibbaren Medien und fügt sie dem Mediensatz hinzu.</p> <p>Wenn ein Anhängeauftrag ein Medium füllt, wird der Backup-Auftrag auf einem überschreibbaren Medium fortgeführt. Wenn die Medien im Speichergerät nicht überschreibbar sind, wird eine Warnmeldung mit der Aufforderung angezeigt, überschreibbare Medien zur Verfügung zu stellen.</p>
An Medium anhängen oder Auftrag abbrechen, falls kein anhängbares Medium verfügbar ist	<p>Hängt diesen Backup-Auftrag an den angegebenen Mediensatz an, wenn anhängbare Medien verfügbar sind. Andernfalls beendet Backup Exec den Auftrag.</p>
Medium nach Auftragsabschluss auswerfen	<p>Wirft die Medien im Laufwerk oder Schacht aus, wenn der Vorgang abgeschlossen wurde. Sie können auch einen Auftrag planen, um Medien auszuwerfen.</p> <p>Siehe "Auswerfen von Medien aus einer Plattenkassette oder einem Bandlaufwerk" auf Seite 555.</p>

Element	Beschreibung
Neuspannen eines Mediums vor einem Backup	Spult das Band im Laufwerk vom Anfang bis zum Ende mit hoher Geschwindigkeit um. Durch Spannen wird das Band gleichmäßig aufgewickelt und kommt gleichmäßig mit den Abtastköpfen des Bandlaufwerks in Kontakt. Diese Option ist nur verfügbar, wenn Sie ein Bandlaufwerk auswählen, das das Neuspannen unterstützt.
Medien mit einem Schreib- und mehreren Lesevorgängen (WORM) verwenden	<p>Gibt die Verwendung des WORM-Mediums (ein Schreib- und mehrere Lesevorgänge) als Standard für DBA-initiierte Aufträge an. Backup Exec bestätigt, dass das Zielgerät ein WORM-kompatibles Laufwerk ist oder enthält, und dass das WORM-Medium in diesem Laufwerk zur Verfügung steht. Wird kein WORM-Medium oder WORM-kompatibles Laufwerk gefunden, wird eine entsprechende Warnmeldung ausgegeben.</p> <p>Siehe "So werden WORM-Medien in Backup Exec verwendet" auf Seite 495.</p>
DirectCopy auf Band aktivieren	<p>Aktiviert Backup Exec, um das direkte Verschieben von Daten vom virtuellen Speicher zu einem physischen Speichergerät zu koordinieren.</p> <p>Der Backup Exec-Server zeichnet Informationen über die Daten im Katalog auf. Deshalb können Sie Daten entweder vom virtuellen Speicher oder vom physischen Speicher wiederherstellen.</p> <p>Siehe "Kopieren von Daten von einer virtuellen Bandbibliothek auf ein physisches Bandgerät mit DirectCopy" auf Seite 255.</p>

Element	Beschreibung
Komprimierung	<p>Folgende Komprimierungsoptionen stehen zur Verfügung:</p> <ul style="list-style-type: none"> ■ Keine Kopiert die Daten in ihrem ursprünglichen Format auf das Medium (nicht komprimiert). Durch die Verwendung eines Datenkomprimierungsverfahrens können Sie Backup-Vorgänge beschleunigen und Speicherplatz sparen. Die Hardware-Datenkomprimierung sollte nicht in Umgebungen verwendet werden, in denen sowohl Speichergeräte mit Unterstützung einer Hardwarekomprimierung als auch Geräte ohne diese Funktion verwendet werden. In dieser Situation wird Hardwarekomprimierung automatisch deaktiviert. Sie können die Hardwarekomprimierung auf den entsprechenden Laufwerken zwar manuell wieder aktivieren, dies führt jedoch zu Inkonsistenzen zwischen den Medien. Wenn das Laufwerk mit Hardwarekomprimierung ausfällt, ist es nicht möglich, die komprimierten Medien mit dem nicht komprimierungsfähigen Laufwerk wiederherzustellen. ■ Software Mithilfe der STAC-Software-Datenkomprimierung werden die Daten komprimiert, bevor sie an das Speichergerät gesendet werden. ■ Hardware (falls vorhanden, sonst keine) Verwendet die Hardware-Datenkomprimierung (falls vom Speichergerät unterstützt). Wenn das Laufwerk keine Datenkomprimierung unterstützt, werden die Daten unkomprimiert gesichert. ■ Hardware (falls vorhanden, sonst Software) Verwendet die Hardware-Datenkomprimierung (falls vom Speichergerät unterstützt). Wenn das Laufwerk keine Hardware-Datenkomprimierung unterstützt, wird die Softwarekomprimierung STAC verwendet.
Verschlüsselungstyp	<p>Gibt bei Bedarf den gewünschten Verschlüsselungsschlüssel an.</p> <p>Siehe "Verwendung von Verschlüsselung mit Backup Exec" auf Seite 727.</p>
Verschlüsselungsschlüssel	<p>Gibt den Verschlüsselungsschlüssel an, den Sie verwenden möchten, wenn Sie eine Verschlüsselung verwenden.</p> <p>Siehe "Verwendung von Verschlüsselung mit Backup Exec" auf Seite 727.</p>

Element	Beschreibung
Schlüssel verwalten	<p>Ermöglicht die Verwaltung Ihrer Verschlüsselungsschlüssel.</p> <p>Sie können vorhandene Verschlüsselungsschlüssel löschen oder ersetzen. Sie können auch einen neuen Verschlüsselungsschlüssel erstellen.</p> <p>Diese Option ist nur verfügbar, wenn Sie einen Verschlüsselungstyp auswählen.</p> <p>Siehe "Verwaltung von Verschlüsselungscodes" auf Seite 731.</p>
Bevorzugtes Quellgerät	Gibt das bevorzugte Quellgerät an, das Sie als Speicher für den Duplizierungsauftrag verwenden möchten.
Nach Backup überprüfen	Führt automatisch eine Überprüfung durch, um sicherzustellen, dass die Daten gelesen werden können, sobald das Backup abgeschlossen wurde. Die Überprüfung sämtlicher Backups wird empfohlen.

Konfigurieren der Einstellungen für Veritas™ Information Map

Sie können die Einstellungen zum Registrieren von Backup Exec bei Veritas™ Information Map konfigurieren.

So konfigurieren Sie die Einstellungen für Veritas™ Information Map

- 1 Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Backup Exec-Einstellungen".
- 2 Wählen Sie im linken Teilfenster die Option "Veritas Information Map".
- 3 Konfigurieren Sie die folgenden Einstellungen:

Metadaten zu Elementen in den Backup-Sätzen an Veritas Information Map senden	<p>Aktivieren Sie dieses Kontrollkästchen, um Metadaten zu Elementen in den Backup-Sätzen aus Backup Exec an Veritas Information Map zu senden.</p> <p>Wenn Sie dieses Kontrollkästchen deaktivieren, werden keine Metadaten mehr gesendet. Aktivieren Sie das Kontrollkästchen erneut, wenn wieder Metadaten gesendet werden sollen.</p>
Servername	Geben Sie hier den Server an, auf dem der Information Map-Agent installiert ist.

Port	<p>Geben Sie die Port-Nummer für die Verbindung zum Information Map-Agent ein.</p> <p>Geben Sie den Port ein, der vom Information Map-Connector-Dienst (ConnectorService.exe) verwendet wird. Standardmäßig wird Port 8286 verwendet.</p> <p>Wenn Sie die Port-Nummer während der Installation des Information Map-Agent geändert haben, geben Sie diese an.</p> <p>So prüfen Sie, welche Port-Nummer verwendet wird</p> <ul style="list-style-type: none"> ■ Öffnen Sie den Ordner, in dem der Information Map-Agent installiert ist. Der Standardordner ist: <code>C:\<Backup Exec-Installationsordner>\InformationMapAgent \connectorFramework\connectorService</code> ■ Öffnen Sie die Datei <code>webService</code> im Editor und suchen Sie die Zeile <code>app.hostPort=</code>. Verwenden Sie die dort aufgeführte Port-Nummer.
Login-Konto	<p>Wählen Sie das Login-Konto für den Server, auf dem der Information Map-Agent installiert ist.</p> <p>Befindet sich das korrekte Login-Konto nicht in der Liste, klicken Sie auf "Hinzufügen/Bearbeiten", um es der Liste hinzuzufügen.</p> <p>Hinweis: Das Login-Konto muss sich in der Gruppe "lokale Administratoren" auf dem Server befinden, auf dem der Agent installiert ist.</p>
Agent-Status	<p>Zeigt den Registrierungsstatus von Backup Exec beim Information Map-Agent an.</p>

4 Klicken Sie auf "Registrieren".

Hinweis: Einrichtungsdetails für Information Map werden erst gespeichert, nachdem die Verbindung registriert wurde.

- 5 Das Dialogfeld "Vertrauenswürdige Verbindung einrichten" wird angezeigt.
Sie müssen das Sicherheitszertifikat verifizieren, um eine vertrauenswürdige Verbindung mit dem Information Map-Server herstellen zu können.
- 6 Klicken Sie auf "Zertifikat anzeigen" und vergleichen Sie den öffentlichen Schlüssel des Zertifikats mit dem auf dem Information Map-Agent-Server verfügbaren.

Um den öffentlichen Schlüssel für das Zertifikat auf dem Server zu bestimmen, auf dem Information Map-Agent installiert ist, gehen Sie in folgender Reihenfolge vor:

- Öffnen Sie die Eingabeaufforderung auf dem Server, auf dem Information Map-Agent installiert ist.
- Wechseln Sie in den Ordner `C:<Backup
Exec-Installationsordner>\InformationMapAgent\bin`

Hinweis: Dies ist der Pfad, in dem der Information Map-Agent standardmäßig installiert wird.

- Führen Sie den Befehl `connector_config.exe generate_webserver_cert` aus.
 Es wird eine `.cert`-Datei erzeugt. Öffnen Sie diese Datei und rufen Sie den öffentlichen Schlüssel ab. Vergleichen Sie diesen Schlüssel mit dem Zertifikatschlüssel, der angezeigt wird, wenn Sie auf "Zertifikat anzeigen" klicken.

7 Wenn das Zertifikat gültig ist, klicken Sie "Ja".

Backup Exec wird beim Information Map-Agent registriert und anschließend wird eine Bestätigungsmeldung angezeigt.

8 Wählen Sie den Zeitraum in Tagen aus, innerhalb der die Backup-Sätze, deren Daten genutzt werden sollen, erstellt wurden. Backup Exec sendet die neuesten in den Backup-Sätzen verfügbaren Metadaten zu Dateien und Ordnern der geschützten Servern an den Information Map-Agent.

Der Standardwert ist 45.

Hinweis: Metadaten werden an Information Map für eine bestimmte Ressource mindestens einmal gesendet, und danach findet Backup Exec keine Backups dieser Ressource, die innerhalb des konfigurierten Zeitraums erstellt wurden. Backup Exec betrachtet die Ressource nicht mehr als Teil der live und aktiv geschützten Ressourcen, und die Metadaten werden aus Information Map gelöscht.

- 9 Aktivieren Sie dieses Kontrollkästchen, wenn Metadaten zu Elementen in den Backup-Sätzen, die mit einem gemeinsamen Verschlüsselungscode verschlüsselt sind, an Information Map gesendet werden sollen.

Hinweis: Die Metadaten zu Elementen in Backup-Sätzen, die mit einem eingeschränkten Code verschlüsselt sind, werden nicht an Information Map gesendet.

- 10 (Optional) Um die Details des Information Map-Agent zu aktualisieren, bearbeiten Sie die erforderlichen Einstellungen und klicken Sie dann auf "Aktualisieren".

Metadaten zu den geschützten Daten eines virtuellen Agent

Sollen Metadaten zu geschützten Daten eines virtuellen Agent gesendet werden, müssen die Backup-Aufträge mit der entsprechenden Option auf der Registerkarte "Instant GRT" konfiguriert sein. Wählen Sie "Konfiguration und Einstellungen > Auftragsstandardeinstellungen > Backup auf Festplatte > Instant GRT". Wählen Sie auf dieser Registerkarte eine der folgenden Optionen aus:

- Vollständige Katalogisierung sofort nach Abschluss des Backup-Auftrags als separaten Auftrag ausführen
- Vollständige Katalogisierung nach Abschluss des Backup-Auftrags als separaten Auftrag planen

Siehe [Kapitel 22](#) auf Seite 1017.

Backup Exec-Login-Konten

Ein Backup Exec-Login-Konto speichert die Anmeldedaten eines Benutzerkontos, das Sie für den Zugriff auf einen Computer verwenden. Mit Backup Exec-Login-Konten können Benutzernamen und Kennwörter in Backup Exec verwaltet sowie Computer durchsucht oder Aufträge verarbeitet werden. Mit Backup Exec-Login-Konten können Sie Änderungen der Anmeldedaten auf die Aufträge anwenden, die diese Daten nutzen.

Backup Exec-Login-Konten werden zum Durchsuchen lokaler und standortferner Computer verwendet. Jedes Mal, wenn Backup Exec-Login-Daten zwischen dem Backup Exec-Server und dem standortfernen Computer gesendet werden, werden die Daten verschlüsselt.

Backup Exec-Login-Konten können auch mit Backup-Daten für einzelne Geräte, z. B. Freigaben, Datenbanken usw. verknüpft sein. Wenn Sie die Anmeldedaten bearbeiten müssen, können Sie das Backup Exec-Login-Konto bearbeiten. Alle

Änderungen werden auf die ausgewählten Computer angewendet, die das Backup Exec-Login-Konto verwenden.

Backup Exec-Login-Konten sind keine Benutzerkonten. Beim Erstellen eines Backup Exec-Login-Kontos wird ein Eintrag für das Konto in der Backup Exec-Datenbank eingegeben. Dabei werden keine Betriebssystemkonten erstellt. Wenn sich Ihre Benutzerkontenangaben ändern, müssen Sie das Backup Exec-Login-Konto mit den neuen Informationen aktualisieren. In Backup Exec wird keine Verbindung mit dem Benutzerkonto aufrechterhalten.

Sie können Backup Exec-Login-Konten anzeigen, erstellen, bearbeiten, ersetzen und löschen.

Backup Exec enthält die folgenden Typen von Login-Konten:

[Backup Exec-Standard-Login-Konto](#)

[Backup Exec-System-Login-Konto](#)

[Eingeschränkte Login-Konten](#)

Backup Exec-Standard-Login-Konto

Mit dem Backup Exec-Standard-Login-Konto können Sie Daten durchsuchen, auswählen oder wiederherstellen. Beim ersten Starten von Backup Exec müssen Sie mit dem Assistenten für das Login-Konto ein Backup Exec-Standard-Login-Konto festlegen. Sie können ein bereits vorhandenes Backup Exec-Login-Konto auswählen oder ein neues Konto erstellen.

Sie können mehrere Backup Exec-Login-Konten erstellen, wobei jedoch jeder Backup Exec-Benutzer nur über je ein Backup Exec-Standard-Login-Konto verfügen kann.

Über das Backup Exec-Standard-Login-Konto können folgende Vorgänge durchgeführt werden:

- **Durchsuchen von Daten.** Mit dem Backup Exec-Standard-Login-Konto können Sie beim Erstellen von Backup-Aufträgen lokale und standortferne Computer durchsuchen. Um Computer zu durchsuchen, muss jeder Benutzer über ein Backup Exec-Standard-Login-Konto verfügen, das mit seinem Benutzerkonto verknüpft ist. Der Benutzername des Backup Exec-Login-Kontos muss nicht mit dem des Benutzerkontos übereinstimmen, über das die Anmeldung bei Backup Exec erfolgt.

Beispiel: Sie sind als lokaler Windows-Administrator bei einem Backup Exec-Server mit dem Namen BACKUPSERVER eingeloggt. Beim Starten von Backup Exec werden Sie dazu aufgefordert, ein Backup Exec-Standard-Login-Konto für den lokalen Administrator zu erstellen, da noch kein Konto vorhanden ist. Sie können ein Backup Exec-Login-Konto für den lokalen Administrator erstellen, das die Angaben für einen

Domänenadministrator enthält. Das Backup Exec-Login-Konto hat die folgenden Eigenschaften:

Benutzername: DOMÄNE\Administrator

Beschreibung: BACKUPSERVER\Administrator-Standardkonto

Besitzer: BACKUPSERVER\Administrator

Wenn Sie Ihr Backup Exec-Standard-Login-Konto ändern, können Sie das neue Backup Exec-Standard-Login-Konto sofort zum Durchsuchen von Computern verwenden. Das System muss nicht neu gestartet werden, damit die Änderungen wirksam werden.

Siehe ["Ändern des Backup Exec-Standard-Login-Kontos"](#) auf Seite 772.

- Treffen von Backup-Auswahlen – Bei der Auswahl der Backup-Optionen können Sie ein anderes Backup Exec-Login-Konto festlegen. Wenn für das Standard-Login-Konto keine Berechtigungen vorliegen, wird das Dialogfeld "Login-Konto auswählen" angezeigt, in dem Sie ein anderes Backup Exec-Login-Konto erstellen oder auswählen können.
Siehe ["Voraussetzungen für die Verwendung des SQL Agent"](#) auf Seite 1220.
Siehe ["Voraussetzungen für den Zugriff auf Exchange-Postfächer"](#) auf Seite 1283.
- Wiederherstellen – Sie können beim Erstellen von Wiederherstellungsaufträgen Computern Backup Exec-Login-Konten zuordnen. Das Backup Exec-Standard-Login-Konto wird verwendet, es sei denn, Sie wählen ein anderes Backup Exec-Login-Konto beim Erstellen des Wiederherstellungsauftrags aus.

Backup Exec-System-Login-Konto

Das Backup Exec-System-Login-Konto (SLA) wird bei der Installation von Backup Exec erstellt. Bei der Erstellung des System-Login-Kontos stimmen Benutzername und Kennwort mit den Anmeldedaten überein, die bei der Installation für die Backup Exec-Dienste bereitgestellt wurden. Der Besitzer des System-Login-Kontos ist der Benutzer, der Backup Exec installierte. Es ist standardmäßig ein allgemeines Konto. Allgemeine Konten sind freigegebene Konten, auf die alle Benutzer zugreifen können.

Siehe ["Erstellen von neuen Backup Exec-System-Login-Konten"](#) auf Seite 773.

Über das Backup Exec-System-Login-Konto kann auf die meisten oder möglicherweise auf alle Daten zugegriffen werden, da es die Anmeldedaten für die Backup Exec-Dienste enthält. Wenn Sie Backup Exec sicherer gestalten möchten, können Sie das System-Login-Konto einschränken. Sie können es auch löschen, nachdem Sie ein anderes Login-Konto als Standardkonto festgelegt haben. Wenn Sie das System-Login-Konto löschen, treten jedoch bei den Aufträgen, in denen das Konto verwendet wird, möglicherweise Fehler auf. Wenn das System-Login-Konto gelöscht ist, können Sie es im Dialogfeld "Login-Kontenverwaltung" neu erstellen.

Das System-Login-Konto wird für die folgenden Aufgaben und Aufträge verwendet:

- Aufträge, die aus einer vorherigen Version von Backup Exec migriert wurden
- Duplizierungs-Backup-Aufträge
- Befehlszeilen-Applet (bemcli.exe)

Eingeschränkte Login-Konten

Die Backup Exec-Login-Konten können allgemein oder eingeschränkt sein. Wenn Sie ein Backup Exec-Login-Konto erstellen, können Sie es als eingeschränktes Konto kennzeichnen. Um ein eingeschränktes Login-Konto zu verwenden, müssen Sie Eigentümer des Login-Kontos sein oder das Kennwort für das Login-Konto kennen. Die Person, die das Login-Konto erstellt hat, ist der Eigentümer. Wenn Sie nur wenigen Leuten die Berechtigung erteilen, Daten zu sichern oder wiederherzustellen, können Sie aus dem Login-Konto ein eingeschränktes Login-Konto machen.

Es gibt folgende wesentliche Gründe, ein Login-Konto einzuschränken:

- Der Zugriff auf die für das Backup verfügbaren Computer soll eingeschränkt werden.
- Die Computer, auf denen Sie eine Wiederherstellung durchführen können, sollen eingeschränkt werden.

Wenn Sie ein eingeschränktes Login-Konto verwenden, um die Daten für einen Auftrag auszuwählen, werden die Login-Kontodaten mit der Auswahlliste gespeichert. Jeder, der den Auftrag zu bearbeiten versucht, muss das Kennwort für das eingeschränkte Login-Konto angeben. Backup Exec lädt die Auswahlen für diesen Auftrag nur, wenn das Kennwort für das eingeschränkte Login-Konto angegeben wird.

Mit bestimmten Funktionen in den globalen Backup Exec-Einstellungen können Sie ein Login-Konto einrichten. Beispiel: Simplified Disaster Recovery oder Veritas Information Map, bei denen ein Login-Konto angegeben werden muss. Klicken Sie zum Aufrufen der globalen Einstellungen auf die Backup Exec-Schaltfläche und wählen Sie "Konfiguration und Einstellungen" > "Backup Exec-Einstellungen". Standardmäßig wird das Backup Exec-System-Login-Konto für eine Funktion zugewiesen. Da diese Einstellungen für Backup Exec global gelten, ist das zugewiesene Login-Konto für alle eingeloggt Benutzer von Backup Exec verfügbar. Prüfen Sie als Best Practice für die Sicherheit die Login-Konten in den globalen Einstellungen, die den Funktionen zugewiesen sind. Es wird empfohlen, Login-Konten mit den minimalen Berechtigungen für die jeweilige Funktion zu erstellen und zuzuweisen und als Kontotyp "Gemeinsam" auszuwählen, der für alle Benutzer von Backup Exec freigegeben werden kann.

Siehe ["Erstellen von Backup Exec-Login-Konten"](#) auf Seite 766.

Siehe ["Bearbeiten von Backup Exec-Login-Konten"](#) auf Seite 768.

Siehe ["Ändern des Kennworts für ein Backup Exec-Login-Konto"](#) auf Seite 770.

Siehe ["Ersetzen von Backup Exec-Login-Konten"](#) auf Seite 770.

Siehe ["Löschen von Backup Exec-Login-Konten"](#) auf Seite 771.

Siehe ["Kopieren von Login-Konto-Informationen auf einen anderen Backup Exec-Server"](#) auf Seite 774.

Erstellen von Backup Exec-Login-Konten

Sie können Backup Exec-Login-Konten mit dem Assistenten für das Login-Konto erstellen, der Sie durch die Erstellung eines Backup Exec-Login-Kontos führt. Wahlweise können Sie das Konto auch im Dialogfeld "Login-Kontenverwaltung" erstellen. Sie können beim Erstellen des Backup Exec-Login-Kontos die entsprechenden Eigenschaftsinformationen eingeben. Backup Exec ordnet allerdings den Eigentümer des Backup Exec-Login-Kontos dem Benutzernamen zu, mit dem Sie sich bei Backup Exec eingeloggt haben. Der Eigentümer des Backup Exec-Login-Kontos kann nicht geändert werden.

Dieses Thema enthält folgende Informationen:

[So erstellen Sie ein Backup Exec-Login-Konto unter Verwendung des Login-Konto-Assistenten](#)

[So erstellen Sie ein Backup Exec-Login-Konto manuell](#)

So erstellen Sie ein Backup Exec-Login-Konto unter Verwendung des Login-Konto-Assistenten

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- 2 Wählen Sie "Login-Konten" und dann "Assistent für das Login-Konto".
- 3 Klicken Sie auf "Neues Login-Konto hinzufügen" und klicken Sie dann auf "Weiter".
- 4 Geben Sie einen Benutzernamen und ein Kennwort ein.
- 5 Klicken Sie auf "Weiter".
- 6 Geben Sie im Bereich "Login-Konto-Name" den eindeutigen Namen für das Backup Exec-Login-Konto ein.

- 7 Geben Sie unter "Konto erstellen" an, ob das Konto ein gemeinsames Login-Konto oder ein eingeschränktes Login-Konto sein soll.

Gemeinsame Login-Konten sind gemeinsam genutzte Konten, auf die alle Benutzer zugreifen können. Eingeschränkte Login-Konten können nur vom Besitzer des Login-Kontos oder von Personen, die das Kennwort kennen, verwendet werden.
- 8 Wenn Sie dieses Konto zum Standard-Login-Konto machen möchten, über das Sie Daten auf Ihren lokalen und Remote-Computern durchsuchen, auswählen und wiederherstellen können, wählen Sie "Standard-Login-Konto".
- 9 Klicken Sie auf "Weiter".
- 10 Überprüfen Sie die ausgewählten Optionen und klicken Sie dann auf "Fertigstellen", um das Login-Konto zu erstellen.

So erstellen Sie ein Backup Exec-Login-Konto manuell

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- 2 Wählen Sie "Login-Konten" und dann "Login-Konten verwalten".
- 3 Klicken Sie auf "Hinzufügen".
- 4 Geben Sie in das Feld "Benutzername" den vollständig qualifizierten Benutzernamen für das Backup Exec-Login-Konto ein,

z.B. "DOMÄNE\Administrator".

Der Benutzername wird beim Verbindungsaufbau mit einem Computer bereitgestellt. Beim Benutzernamen muss nicht auf Groß- und Kleinschreibung geachtet werden für die Computer, auf die zugegriffen wird.

- 5 Geben Sie im Feld "Kennwort" das Kennwort für das neue Konto ein.

Das eingegebene Kennwort wird aus Sicherheitsgründen verschlüsselt. Sie können dieses Feld frei lassen, wenn für das Backup Exec-Login-Konto kein Kennwort erforderlich ist.
- 6 Geben Sie im Feld "Kennwort bestätigen" das Kennwort erneut ein, um es zu bestätigen.
- 7 Geben Sie im Feld "Kontoname" den eindeutigen Namen für das Backup Exec-Login-Konto ein.
- 8 Geben Sie im Feld "Hinweise" ein, wie das Backup Exec-Login-Konto verwendet werden soll.

- 9** Wählen Sie die Option "Dies ist ein eingeschränktes Login-Konto", wenn das Backup Exec-Login-Konto nur vom Besitzer des Login-Kontos, und denen, die das Kennwort kennen, genutzt werden soll.

Wenn diese Option nicht ausgewählt ist, wird das Backup Exec-Login-Konto als gemeinsames Konto erstellt. Alle Benutzer können auf gemeinsam genutzte Konten zugreifen.

- 10** Aktivieren Sie "Dies ist mein Standardkonto", wenn Sie dieses Backup Exec-Login-Konto zum Durchsuchen, Auswählen oder Wiederherstellen von Daten auf lokalen und Remote-Computern verwenden möchten.

Siehe ["Backup Exec-Login-Konten"](#) auf Seite 762.

Bearbeiten von Backup Exec-Login-Konten

Beim Bearbeiten eines Backup Exec-Login-Kontos werden die Änderungen automatisch auf alle Inhalte übertragen, die das Backup Exec-Login-Konto verwenden. Die an einem Backup Exec-Login-Konto vorgenommenen Änderungen werden unmittelbar übernommen. Das System muss nicht neu gestartet werden, damit Änderungen wirksam werden.

Sie können die folgenden Eigenschaften für ein Backup Exec-Login-Konto bearbeiten:

- Typ (Eingeschränkt, Gemeinsam oder Standard)
- Kontoname
- Kennwort
- Benutzername
- Hinweise

So bearbeiten Sie ein Backup Exec-Login-Konto:

- 1** Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Login-Konten".
- 2** Wählen Sie "Login-Konten verwalten".
- 3** Wählen Sie das zu ändernde Backup Exec-Login-Konto aus und klicken Sie dann auf "Bearbeiten".

Wenn Sie bei Backup Exec nicht mit demselben Benutzernamen wie der Eigentümer des Backup Exec-Login-Kontos eingeloggt sind, können Sie das Konto erst nach der Eingabe des Kennworts bearbeiten.

4 Bearbeiten Sie eine der folgenden Eigenschaften:

Benutzername	<p>Geben Sie hier den voll qualifizierten Benutzernamen für das Backup Exec-Login-Konto ein. z. B. "DOMÄNE\Administrator".</p> <p>Der Benutzername wird beim Verbindungsaufbau mit einem Computer bereitgestellt. Bei der Eingabe des Benutzernamens muss nicht auf Groß- bzw. Kleinschreibung geachtet werden.</p>
Kennwort ändern	<p>Klicken Sie auf diese Option, um das Kennwort für das Konto zu ändern. Das eingegebene Kennwort wird aus Sicherheitsgründen verschlüsselt.</p>
Kontoname	<p>Geben Sie einen eindeutigen Namen für das Backup Exec-Login-Konto ein. Der Benutzername wird automatisch hinzugefügt, wenn Sie in diesem Feld keine Informationen eingeben.</p>
Hinweise	<p>Geben Sie optionale Notizen dazu ein, wie das Backup Exec-Login-Konto verwendet wird.</p>
Dies ist ein eingeschränktes Login-Konto	<p>Wählen Sie diese Option aus, um dieses Backup Exec-Login-Konto einzuschränken. Ein eingeschränktes Login-Konto kann nur vom Eigentümer des Login-Kontos und den Benutzern, die das Kennwort kennen, verwendet werden. Wenn diese Option nicht aktiviert ist, ist das Backup Exec-Login-Konto ein gemeinsames Konto. Alle Benutzer können auf gemeinsam genutzte Konten zugreifen.</p>
Dies ist mein Standardkonto	<p>Aktivieren Sie diese Option, um dieses Backup Exec-Login-Konto als Standardkonto festzulegen. Über Ihr Standardkonto können Sie Daten auf lokalen und Remote-Computern durchsuchen, auswählen und wiederherstellen.</p>

5 Klicken Sie im Dialogfeld "Login-Daten bearbeiten" auf "OK".

6 Klicken Sie im Dialogfeld "Login-Kontenverwaltung" auf "OK".

Siehe "[Backup Exec-Login-Konten](#)" auf Seite 762.

Ändern des Kennworts für ein Backup Exec-Login-Konto

Das Kennwort eines Backup Exec-Login-Kontos kann wie folgt geändert werden. Die an einem Kennwort eines Backup Exec-Login-Kontos vorgenommenen Änderungen werden unmittelbar übernommen.

So ändern Sie das Kennwort für ein Backup Exec-Login-Konto

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Login-Konten".
- 2 Wählen Sie "Login-Konten verwalten".
- 3 Wählen Sie das zu ändernde Backup Exec-Login-Konto aus und klicken Sie dann auf "Bearbeiten".

Wenn Sie bei Backup Exec nicht mit demselben Benutzernamen wie der Eigentümer des Backup Exec-Login-Kontos eingeloggt sind, können Sie das Konto erst nach der Eingabe des Kennworts bearbeiten.

- 4 Klicken Sie auf "Kennwort ändern".
- 5 Geben Sie unter "Kennwort" ein neues Kennwort ein.
- 6 Geben Sie unter "Kennwort bestätigen" das Kennwort erneut ein, und klicken Sie dann auf "OK".
- 7 Klicken Sie im Dialogfeld "Login-Daten bearbeiten" auf "OK".
- 8 Klicken Sie im Dialogfeld "Login-Kontenverwaltung" auf "OK".

Siehe ["Backup Exec-Login-Konten"](#) auf Seite 762.

Ersetzen von Backup Exec-Login-Konten

Sie können ein Backup Exec-Login-Konto innerhalb aller vorhandenen Aufträge ersetzen. Die Daten in den vorhandenen Aufträgen, die das Backup Exec-Login-Konto verwenden, werden aktualisiert, sodass das neue Backup Exec-Login-Konto verwendet wird. Wenn das neue Backup Exec-Login-Konto eingeschränkt ist, müssen Sie das Kennwort eingeben.

So ersetzen Sie ein Backup Exec-Login-Konto

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Login-Konten".
- 2 Wählen Sie "Login-Konten verwalten".
- 3 Wählen Sie das zu ersetzende Backup Exec-Login-Konto aus und klicken Sie dann auf "Ersetzen".

- 4 Wählen Sie im Dialogfeld "Login-Konto ersetzen" das Backup Exec-Login-Konto, durch das das ausgewählte Backup Exec-Login-Konto ersetzt werden soll.

Wenn das Backup Exec-Login-Konto eingeschränkt ist und Sie nicht mit dem gleichen Benutzernamen wie der Eigentümer des Backup Exec-Login-Kontos eingeloggt sind, können Sie das Konto erst nach der Eingabe des Kennworts auswählen.

- 5 Klicken Sie auf "OK".

Siehe ["Backup Exec-Login-Konten"](#) auf Seite 762.

Löschen von Backup Exec-Login-Konten

Wenn Sie ein Backup Exec-Login-Konto nicht mehr benötigen, können Sie es löschen.

Unter folgenden Umständen kann ein Backup Exec-Login-Konto nicht gelöscht werden:

- Ein Auftrag verweist auf dieses Konto.
- Es gehört einem Benutzer, der auf dem Backup Exec-Server eingeloggt ist.
- Es ist als Standard-Backup Exec Login-Konto eines auf dem Backup Exec-Server eingeloggten Benutzers festgelegt.

Wenn ein Login-Konto in einer dieser Situationen verwendet wird, müssen Sie es durch ein anderes Login-Konto ersetzen, bevor Sie es löschen können.

So löschen Sie ein Backup Exec-Login-Konto

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Login-Konten".
- 2 Wählen Sie "Login-Konten verwalten".
- 3 Wählen Sie das zu löschende Backup Exec-Login-Konto aus, und klicken Sie dann auf "Löschen".
- 4 Sie haben folgende Möglichkeiten:

Wenn das Login-Konto nicht durch beliebige Backup-Aufträge aufgerufen wird

Klicken Sie auf "Ja", um den Löschvorgang zu bestätigen.

Wenn das Login-Konto durch Backup-Aufträge aufgerufen wird

Führen Sie die folgenden Schritte durch, um das Login-Konto in beliebigen Backup-Aufträgen durch ein anderes zu ersetzen.

- Klicken Sie im Dialogfeld "Login-Konto löschen" auf "Ersetzen".
- Wählen Sie im Dialogfeld "Login-Konto ersetzen" das Backup Exec-Login-Konto, durch das das ausgewählte Backup Exec-Login-Konto ersetzt werden soll.

Wenn das Backup Exec-Login-Konto eingeschränkt ist und Sie nicht mit dem gleichen Benutzernamen wie der Eigentümer des Backup Exec-Login-Kontos eingeloggt sind, können Sie das Konto erst nach der Eingabe des Kennworts auswählen.

Das hier ausgewählte Login-Konto ersetzt das vorherige Login-Konto in allen vorhandenen Aufträgen und Auswahllisten.

5 Klicken Sie auf "OK".

Siehe ["Backup Exec-Login-Konten"](#) auf Seite 762.

Siehe ["Ersetzen von Backup Exec-Login-Konten"](#) auf Seite 770.

Ändern des Backup Exec-Standard-Login-Kontos

Sie können Ihr Backup Exec-Standard-Login-Konto ändern, mit dem Sie Daten durchsuchen, auswählen oder wiederherstellen können.

So ändern Sie das Backup Exec-Standard-Login-Konto

- 1** Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Login-Konten".
- 2** Wählen Sie "Login-Konten verwalten".
- 3** Wählen Sie das Backup Exec-Login-Konto, das Sie als Backup Exec-Standard-Login-Konto verwenden möchten, und führen Sie anschließend einen der folgenden Schritte aus:
 - Klicken Sie auf "Als Standard einrichten".
 - Klicken Sie auf "Bearbeiten", wählen Sie "Dies ist mein standardmäßiges Konto", und klicken Sie dann auf "OK".
- 4** Klicken Sie auf "OK".

Siehe ["Backup Exec-Login-Konten"](#) auf Seite 762.

Erstellen von neuen Backup Exec-System-Login-Konten

Das Backup Exec-System-Login-Konto ermöglicht die Durchführung verschiedener Vorgänge. Wenn Sie das Backup Exec-System-Login-Konto löschen, sollten Sie ein neues erstellen, das Ihnen die Durchführung der angegebenen Vorgänge ermöglicht.

So erstellen Sie ein neues Backup Exec-System-Login-Konto

- 1** Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Login-Konten".
- 2** Wählen Sie "Login-Konten verwalten".
- 3** Klicken Sie auf "Systemkonto".

4 Konfigurieren Sie folgende Optionen:

Benutzername	<p>Geben Sie hier den voll qualifizierten Benutzernamen für das Backup Exec-Login-Konto ein. z. B. "DOMÄNE\Administrator".</p> <p>Der Benutzername wird beim Verbindungsaufbau mit einem Computer bereitgestellt. Bei der Eingabe des Benutzernamens muss nicht auf Groß- bzw. Kleinschreibung geachtet werden.</p>
Kennwort ändern	<p>Klicken Sie auf diese Option, um das Kennwort für das Konto zu ändern. Das eingegebene Kennwort wird aus Sicherheitsgründen verschlüsselt.</p>
Kontoname	<p>Geben Sie einen eindeutigen Namen für das Backup Exec-Login-Konto ein. Der Benutzername wird automatisch hinzugefügt, wenn Sie in diesem Feld keine Informationen eingeben.</p>
Hinweise	<p>Geben Sie optionale Notizen dazu ein, wie das Backup Exec-Login-Konto verwendet wird.</p>
Dies ist ein eingeschränktes Login-Konto	<p>Wählen Sie diese Option aus, um dieses Backup Exec-Login-Konto einzuschränken. Ein eingeschränktes Login-Konto kann nur vom Eigentümer des Login-Kontos und den Benutzern, die das Kennwort kennen, verwendet werden. Wenn diese Option nicht aktiviert ist, ist das Backup Exec-Login-Konto ein gemeinsames Konto. Alle Benutzer können auf gemeinsam genutzte Konten zugreifen.</p>
Dies ist mein Standard-Einloggkonto	<p>Aktivieren Sie diese Option, um dieses Backup Exec-Login-Konto als Standardkonto festzulegen. Über Ihr Standardkonto können Sie Daten auf lokalen und Remote-Computern durchsuchen, auswählen und wiederherstellen.</p>

5 Klicken Sie auf "OK", um das System-Login-Konto zu erstellen.

Siehe ["Backup Exec-Login-Konten"](#) auf Seite 762.

Kopieren von Login-Konto-Informationen auf einen anderen Backup Exec-Server

Sie können Login-Konto-Informationen von einem Backup Exec-Server auf einen anderen kopieren.

So kopieren Sie Login-Konto-Informationen auf einen anderen Backup Exec-Server

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Login-Konten".
- 2 Wählen Sie "Login-Konten verwalten".
- 3 Wählen Sie das zu kopierende Login-Konto aus und klicken Sie anschließend auf "Auf Server kopieren".
- 4 Wenn Sie dazu aufgefordert werden, geben Sie das Kennwort für das Login-Konto ein, das Sie ausgewählt haben.
- 5 Sie haben folgende Möglichkeiten:
 - Um einzelne Server manuell hinzuzufügen, geben Sie im Feld "Servername" den Namen des Backup Exec-Servers ein, auf den Sie die Login-Konto-Informationen kopieren möchten, und klicken Sie anschließend auf "Hinzufügen".
 - Um mehrere Server aus einer Liste hinzuzufügen, klicken Sie auf "Liste importieren" und navigieren Sie dann zur Liste der Servernamen.
- 6 Wenn ein Login-Konto mit dem gleichen Namen auf dem Ziel-Backup Exec-Server gegebenenfalls überschrieben werden soll, aktivieren Sie die Option "Login-Konto überschreiben, wenn bereits ein Login-Konto mit dieser Beschreibung auf dem Zielsystem vorhanden ist".
- 7 Klicken Sie auf "OK".

Siehe ["Backup Exec-Login-Konten"](#) auf Seite 762.

Testen von Login-Konten

Sie können Backup Exec-Login-Konten testen, um sicherzustellen, dass diese auf die Backup-Quellen zugreifen können, bevor Sie Aufträge ausführen. Wenn Sie die Login-Konten testen, bevor Sie Aufträge ausführen, können Sie möglicherweise Fehler verhindern und Zeit sparen.

So testen Sie Login-Konten

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Login-Konten".
- 2 Wählen Sie "Login-Konten verwalten".
- 3 Klicken Sie auf "Test".
- 4 Wählen Sie im Feld "Login-Konto" das gewünschte Konto aus.

- 5 Wählen Sie im Feld "Server" den Server aus, auf den mit dem Login-Konto zugegriffen werden soll.
- 6 Klicken Sie auf "Test".
Backup Exec prüft, ob das Login-Konto auf den ausgewählten Server zugreifen kann.
- 7 Wenn Sie das Testen von Login-Konten abgeschlossen haben, klicken Sie auf "Schließen".
- 8 Klicken Sie auf "OK".

Siehe ["Backup Exec-Login-Konten"](#) auf Seite 762.

Starten und Anhalten von Backup Exec-Diensten

Sie können Backup Exec-Dienste mit dem Backup Exec-Dienstmanager starten, anhalten und neu starten.

So starten Sie die Backup Exec Services oder halten sie an

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Backup Exec-Dienste" aus.
- 2 Wählen Sie den Server aus, für den Sie Dienste starten oder anhalten möchten.
- 3 Sie haben folgende Möglichkeiten:

Starten aller Dienste für den ausgewählten Server Klicken Sie auf "Alle Dienste starten".

Anhalten aller Dienste für den ausgewählten Server Klicken Sie auf "Alle Dienste anhalten".

Neustarten aller Dienste für den ausgewählten Server Klicken Sie auf "Alle Dienste neu starten".

- 4 Klicken Sie auf "OK".

Siehe ["Ändern der Identifikationsdaten für ein Dienstkonto"](#) auf Seite 777.

Siehe ["Ändern der Startoptionen für Backup Exec-Dienste"](#) auf Seite 778.

Ändern der Identifikationsdaten für ein Dienstkonto

Auf dem Backup Exec-Server werden alle Backup Exec-Dienste im Rahmen eines Benutzerkontos ausgeführt, das für die Backup Exec-Systemdienste konfiguriert wurde.

Hinweis: Das Backup Exec-Dienstkonto und das Backup Exec-System-Login-Konto werden auf denselben Benutzernamen festgelegt, wenn Backup Exec installiert wird. Wenn Sie den Benutzernamen für das Dienstkonto ändern müssen oder dieses nicht mehr verwendet wird, sollten Sie auch das Backup Exec-System-Login-Konto ändern und neue Identifikationsdaten verwenden.

Wenn dieser Computer Mitglied einer Domäne ist, geben Sie die Kontodaten eines Domänenadministrators oder eines gleichwertigen Kontos ein, das Mitglied der Domänenadministratorgruppe ist. Wählen Sie den Domänennamen in der Liste der Domänen aus oder geben Sie ihn ein.

Wenn dieser Computer Mitglied einer Arbeitsgruppe ist, geben Sie die Kontodaten eines Administrators oder eines gleichwertigen Kontos ein, das Mitglied der Administratorgruppe auf diesem Computer ist. Wählen Sie den Computernamen in der Liste der Domänen aus oder geben Sie ihn ein.

Dem für Backup Exec Services bestimmten Konto (ob neu erstellt oder bereits vorhanden) werden die folgenden Rechte zugewiesen:

- Authentifizierung als beliebiger Benutzer. Sie erhalten als beliebiger Benutzer Zugriff auf Ressourcen.
- Erstellung eines Tokenobjekts, das dann für den Zugriff auf lokale Ressourcen verwendet werden kann
- Einloggen als Dienst
- Administrative Rechte (erteilt dem Computer absolute und uneingeschränkte Rechte)
- Backup-Operatorrechte (erteilt Rechte zum Wiederherstellen von Dateien und Verzeichnissen)
- Verwaltung des Überwachungs- und Sicherheitsprotokolls

Siehe ["Erforderliche Benutzerrechte für Backup-Aufträge"](#) auf Seite 165.

Aufgrund von Sicherheitsvorschriften für Microsoft Small Business Server muss das Dienstkonto das Administratorkonto sein.

So ändern Sie die Identifikationsdaten für ein Dienstkonto

- 1** Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Backup Exec-Dienste" aus.
- 2** Wählen Sie im Dialogfeld "Backup Exec-Dienstmanager" den gewünschten Server und dann den Dienst, für den Sie das Dienstkonto ändern möchten.
- 3** Klicken Sie auf "Identifikationsdaten bearbeiten".
- 4** Aktivieren Sie das Kontrollkästchen "Dienstkonto-Identifikationsdatendaten ändern".
- 5** Füllen Sie die folgenden Felder aus:

Alter Benutzername	Geben Sie den aktuellen Benutzernamen für das Dienstkonto ein.
Altes Kennwort	Geben Sie das aktuelle Kennwort für das Dienstkonto ein.
Neuer Benutzername	Geben Sie den neuen Benutzernamen für das Dienstkonto ein.
Neues Kennwort	Geben Sie das neue Kennwort für das Dienstkonto ein.
Kennwort bestätigen	Geben Sie das neue Kennwort erneut ein, um es zu bestätigen.
Rechte für Dienstkonto gewähren	Wählen Sie diese Option, i, dem Dienstkonto die richtigen Systemdienstrechte zuzuweisen.

- 6** Klicken Sie auf "OK".
- 7** Klicken Sie auf "Schließen".

Siehe ["Starten und Anhalten von Backup Exec-Diensten"](#) auf Seite 776.

Siehe ["Ändern der Startoptionen für Backup Exec-Dienste"](#) auf Seite 778.

Ändern der Startoptionen für Backup Exec-Dienste

Sie können Startoptionen für Backup Exec-Dienste ändern. Jeder einzelne Dienst kann für den automatischen oder den manuellen Start konfiguriert werden. Sie können einen Dienst auch völlig deaktivieren.

Dienste, die für den automatischen Start konfiguriert wurden, werden automatisch beim Start des Servers gestartet. Dienste, die für den manuellen Start konfiguriert wurden, werden nicht automatisch gestartet. Sie müssen diese Dienste manuell

starten. Sie können Dienste im Backup Exec-Dienstmanager starten, beenden oder neu starten.

So ändern Sie Startoptionen für Dienste

- 1** Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Backup Exec-Dienste" aus.
- 2** Wählen Sie im Dialogfeld "Backup Exec-Dienstmanager" den gewünschten Server und dann den Dienst, für den Sie die Startoptionen ändern möchten.
- 3** Klicken Sie auf "Identifikationsdaten bearbeiten".
- 4** Aktivieren Sie das Kontrollkästchen "Startoptionen ändern".
- 5** Sie haben folgenden Möglichkeiten:

Automatisch	Wählen Sie diese Option aus, um das Dienstkonto beim Systemstart automatisch zu starten.
Manuell	Wählen Sie diese Option aus, um den automatischen Start des Dienstkontos beim Systemstart zu verhindern. Wenn Sie diese Option auswählen, müssen Sie das Dienstkonto manuell starten.
Deaktiviert	Wählen Sie dieses Option aus, um das Dienstkonto beim Systemstart zu deaktivieren.

- 6** Klicken Sie auf "OK".
- 7** Klicken Sie auf "Schließen".

Siehe ["Starten und Anhalten von Backup Exec-Diensten"](#) auf Seite 776.

Siehe ["Ändern der Identifikationsdaten für ein Dienstkonto"](#) auf Seite 777.

Konfigurieren von Überwachungsprotokollen

Sie können Überwachungsprotokolle verwenden, um Informationen über Vorgänge zu prüfen, die in Backup Exec ausgeführt wurden. Im Überwachungsprotokoll werden Datum und Uhrzeit der Aktivität, der ausführende Benutzer, die Art der Aktivität und eine Beschreibung der Aktivität angezeigt.

Überwachungsprotokolle können konfiguriert werden, Informationen zu Aktivitäten für einzelne oder alle der folgenden Elemente anzuzeigen:

- Meldungen
- Überwachungsprotokolle
- Backup-Satz-Aufbewahrung

- Geräte und Medien
- Verschlüsselungen
- Fehlerbehandlungsregeln
- Installation
- Aufträge
- Login-Konten
- Serverkonfiguration

Sie können die Überwachungsprotokolle als Teil der Backup Exec-Datenbankverwaltung löschen und in einer Textdatei speichern. Die an einem Überwachungsprotokoll vorgenommenen Änderungen, die z. B. bei der Datenbankverwaltung auftreten, können ebenfalls im Überwachungsprotokoll aufgeführt werden.

So konfigurieren Sie Überwachungsprotokolle

- 1 Klicken Sie auf die Schaltfläche "Backup Exec" und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Überwachungsprotokoll".
- 2 Klicken Sie auf "Protokollierung konfigurieren".
- 3 Aktivieren Sie im Dialogfeld "Überwachungsprotokollkonfiguration" das Kontrollkästchen für die Kategorie, die im Überwachungsprotokoll angezeigt werden soll.

Erweitern Sie die Kategorie durch Klicken auf den Pfeil links neben der Kategorie. Wählen Sie die für die Kategorie anzuzeigenden Vorgänge aus.

Deaktivieren Sie das Kontrollkästchen für alle nicht anzuzeigenden Optionen oder Vorgänge.

- 4 Klicken Sie auf "OK".

Siehe ["Anzeigen des Überwachungsprotokolls"](#) auf Seite 780.

Siehe ["Entfernen von Einträgen aus dem Überwachungsprotokoll"](#) auf Seite 781.

Siehe ["Speichern eines Überwachungsprotokolls in einer Textdatei"](#) auf Seite 781.

Anzeigen des Überwachungsprotokolls

Sie können die Überwachungsprotokolle anzeigen, um zu sehen, welche Änderungen von welchen Benutzern in Backup Exec vorgenommen wurden.

So zeigen Sie das Überwachungsprotokoll an:

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Überwachungsprotokoll".
- 2 In "Anzuzeigende Kategorie auswählen" wählen Sie die Kategorie aus, für die Sie Überwachungsinformationen anzeigen möchten.
- 3 Mit der Bildlaufleiste im unteren Bereich des Fensters "Überwachungsprotokoll" können Sie den gesamten Eintrag anzeigen. Darüber hinaus können Sie durch Doppelklicken auf den Eintrag die gleichen Informationen in einem benutzerfreundlichen Überwachungsprotokolldatensatz anzeigen.

Siehe ["Konfigurieren von Überwachungsprotokollen"](#) auf Seite 779.

Entfernen von Einträgen aus dem Überwachungsprotokoll

Sie können die Einträge für alle Kategorien oder für eine ausgewählte Kategorie entfernen.

So entfernen Sie Einträge aus dem Überwachungsprotokoll

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Überwachungsprotokoll".
- 2 In "Anzuzeigende Kategorie auswählen" wählen Sie die Kategorie aus, für die Sie Informationen anzeigen möchten.
- 3 Klicken Sie auf "Kategorieprotokoll löschen", um alle Einträge aus einer Überwachungsprotokollkategorie zu entfernen.

Wenn Sie bestimmte Kategorien auswählen, werden nur die Protokolle für die ausgewählten Kategorien gelöscht, wenn Sie auf "Kategorieprotokoll löschen" klicken.

Siehe ["Konfigurieren von Überwachungsprotokollen"](#) auf Seite 779.

Speichern eines Überwachungsprotokolls in einer Textdatei

Sie können das Überwachungsprotokoll als Textdatei speichern.

So speichern Sie das Überwachungsprotokoll in einer Textdatei

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Überwachungsprotokoll".
- 2 Klicken Sie auf "Protokoll in Datei speichern", um die Einträge im Überwachungsprotokoll unter dem angegebenen Dateinamen und am festgelegten Speicherort zu speichern.

Siehe ["Konfigurieren von Überwachungsprotokollen"](#) auf Seite 779.

Kopieren von Konfigurationseinstellungen auf einen anderen Backup Exec-Server

Wenn Central Admin Server Feature (CAS) installiert ist, können Sie Konfigurationseinstellungen und Login-Daten von einem Backup Exec-Server auf einen anderen kopieren. Mit dieser Kopierfunktion können Sie auf schnelle Weise eine Gruppe von Backup Exec-Servern mit denselben Konfigurations- oder Login-Einstellungen einrichten.

Hinweis: Um Konfigurationseinstellungen und Login-Daten auf andere Backup Exec-Server zu kopieren, müssen Sie die Funktion "Serverkonfigurationen kopieren" installieren.

Siehe ["Installieren zusätzlicher Agents und Funktionen auf dem lokalen Backup Exec-Server"](#) auf Seite 66.

So kopieren Sie Konfigurationseinstellungen auf einen anderen Backup Exec-Server

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie "Konfiguration und Einstellungen" und dann "Einstellungen auf andere Server kopieren".
- 2 Wählen Sie eine der folgenden Optionen:

Standardplan	Mithilfe dieser Option können Sie Einstellungen für den Standardplan von diesem Backup Exec-Server auf einen anderen Backup Exec-Server kopieren.
Fehlerbehandlungsregeln	Mithilfe dieser Option können Sie Fehlerbehandlungsregeln von diesem Backup Exec-Server auf einen anderen Backup Exec-Server kopieren.
Warnmeldungskonfiguration	Mithilfe dieser Option können Sie die Warnmeldungskonfiguration von diesem Backup Exec-Server auf einen anderen Backup Exec-Server kopieren.

- 3 Wählen Sie den oder die Backup Exec-Server, auf den oder die Sie die ausgewählten Einstellung kopieren möchten.

Wenn der Zielsever nicht in der Liste ist, führen Sie einen der folgenden Schritte aus:

- Um einen Server manuell hinzuzufügen, klicken Sie auf "Hinzufügen" und wählen Sie dann den oder die Server aus, die Sie der Liste hinzufügen möchten.
- Um eine Liste von Servern zu importieren, klicken Sie auf "Liste importieren", navigieren Sie zu der auszuwählenden Liste und klicken Sie dann auf "Öffnen".

- 4 Klicken Sie auf "OK".

Siehe ["Infos zu Central Admin Server Feature"](#) auf Seite 1450.

Anzeigen von Servereigenschaften

Sie können Eigenschaften für den lokalen Backup Exec-Server oder jeden anderen Server anzeigen, den Sie mit Backup Exec überwachen.

Sie können die folgenden Eigenschaften für den lokalen Backup Exec-Server anzeigen:

- Servername

- Serverbeschreibung
- Serverstatus
- Version und Lizenzinformationen
- Datums- und Zeitzoneinformationen
- Betriebssysteminformationen
- Arbeitsspeicher- und Seitendateiinformationen

Sie können die folgenden Eigenschaften für jeden Server anzeigen, den Sie mit Backup Exec überwachen.

- Servername
- Serverbeschreibung
- Betriebssysteminformationen
- Backup Exec-Version und Lizenzinformationen

Wenn Sie Central Admin Server Feature (CAS) verwenden, können Sie außerdem Informationen über die Backup Exec-Datenbank, die Geräte- und Mediendatenbank und die Katalogdatenbank anzeigen.

Siehe ["Anzeigen der Einstellungen für einen zentralen Administrationsserver"](#) auf Seite 1511.

So zeigen Sie Servereigenschaften an

- ◆ Sie haben folgende Möglichkeiten:

So zeigen Sie Eigenschaften des lokalen Backup Exec-Servers an

- Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Eigenschaften des lokalen Servers".
- Wenn Sie alle Eigenschaften des lokalen Server angezeigt und geprüft haben, klicken Sie auf "OK".

So zeigen Sie andere Eigenschaften des Servers an

- Auf der Registerkarte "Backup und Wiederherstellung" doppelklicken Sie auf den Server, dessen Eigenschaften Sie anzeigen möchten.
- Klicken Sie im linken Teilfenster auf "Eigenschaften".

Konfigurieren der Standardeinstellungen für das Backup

Sie können die Methode für Hyper-V-Backups auswählen. Diese Option wird für den Backup Exec-Server festgelegt, d. h. die gewählte Methode gilt für alle Backups von virtuellen Hyper-V-Computern, die vom Backup Exec-Server geschützt werden.

Es sind drei verschiedene Methoden verfügbar:

- Die Methode Resilient Change Tracking (RCT). Diese Methode verfolgt die Änderungen für virtuelle Computer, die gesichert werden sollen. Die RCT-Methode bietet eine höhere Belastbarkeit als Standardverarbeitungsmethoden und schnellere Verarbeitungsmethoden. Backups für größere virtuelle Computer werden im Vergleich zu den anderen beiden Methoden schneller ausgeführt. Die RCT-Methode macht keinen Gebrauch von der VSS- Infrastruktur auf dem Hyper-V-Host. Diese Methode ist nur für Hyper-V-Server mit Windows 2016 und höher verfügbar.
- Die Standardmethode. Diese Methode liest den gesamten virtuellen Datenträger und identifiziert die Änderungen, die gesichert werden müssen. Die erkannten geänderten Daten werden dann gesichert.
- Die schnellere Methode. Diese Methode ist schneller als die Standardmethode, da alle Änderungen auf einen neuen Datenträger geschrieben werden und dann nur dieser Datenträger gesichert wird. Dies spart Zeit, da nicht der gesamte Datenträger gelesen werden muss.

Tabelle 15-12 Der Unterschied zwischen Resilient Change Tracking, Standardmethode und schnelleren Verarbeitungsmethoden ist wie folgt

Verarbeitungsmethode	Unterstützte Hyper-V-Server	Backup-Typ	Speicherplatz	Auswirkungen auf die Systemleistung
Resilient Change Tracking (RCT)-Methode	Windows 2016 und höher.	<ul style="list-style-type: none"> ■ Differenzielles Backup ■ Inkrementelles Backup 	Kein zusätzlicher Speicher erforderlich.	Keine Beeinträchtigung der Leistung

Verbindungs- methode	Unterstützte Hyper-V-Server	Backup-Typ	Speicherplatz	Auswirkungen auf die Systemleistung
Standardmethode	Windows 2008 und höher.	<ul style="list-style-type: none"> ■ Differenzielles Backup ■ Differenzielles mit inkrementellem Backup 	Kein zusätzlicher Speicher erforderlich.	Keine Beeinträchtigung der Leistung

Verarbeitungsmethode	Unterstützte Hyper-V-Server	Backup-Typ	Speicherplatz	Auswirkungen auf die Systemleistung
Schnellere Verarbeitungsmethode	Windows 2012 und höher.	<ul style="list-style-type: none"> ■ Inkrementelles Backup ■ Vollständiges Backup ■ Differenzielle Backups werden als inkrementelle Backups ausgeführt und der Auftrag wird mit dem Status "Erfolgreich mit Ausnahmen" abgeschlossen. 		Hierbei kann es zu einer verringerten Systemleistung kommen, da immer ein Kontrollpunkt pro virtuellen Computer vorhanden ist, der mithilfe dieser Methode gesichert wird.

Verbindungs­methode	Unterstützte Hyper-V-Server	Backup-Typ	Speicherplatz	Auswirkungen auf die Systemleistung
			<p>Erfordert zusätzlichen Speicherplatz auf dem Hyper-V-Host, auch nach dem Backup. Wie viel zusätzlicher Speicherplatz benötigt wird, hängt davon ab, wie lange es dauert, bis der Kontrollpunkt wieder mit dem übergeordneten Datenträger zusammengeführt wird, und wie viele Schreibvorgänge bis dahin ausgeführt wurden. Der Speicherplatz, der pro virtuellen Computer benötigt wird, ist möglicherweise gering, doch bei vielen virtuellen Computern innerhalb einer Umgebung beanspruchen die Kontrollpunkte möglicherweise sehr viel Speicherplatz.</p> <p>Diese Methode kann jedoch</p>	

Verbindungs-methode	Unterstützte Hyper-V-Server	Backup-Typ	Speicherplatz	Auswirkungen auf die Systemleistung
			verwendet werden, wenn Sie häufig Backups durchführen und der Speicherplatz keiner Beschränkung unterworfen ist.	

Wie Upgrades sich auf die Einstellungen für Hyper-V-Backups auswirken

Im Folgenden finden Sie Informationen zu Upgrades:

- Wenn Sie von Backup Exec 15 Feature Pack 3 und höher aktualisieren, wird die vorhandene Einstellung für Hyper-V-Backups nicht geändert. Vorhandene und neue Backup-Aufträge nutzen die Einstellung, die in Feature Pack 3 konfiguriert war, es sei denn, Sie ändern sie.
- Wenn Sie aus Backup Exec 15 Feature Pack 2 oder niedriger aktualisieren, lautet die Standardeinstellung für vorhandene Hyper-V-Backup-Aufträge "Standardmethode verwenden". Vorhandene und neue Backup-Aufträge nutzen diese Einstellung, es sei denn, Sie ändern sie. In diesem Szenario ist die Resilient Change Tracking (RCT)-Methode deaktiviert.
- Für den Backup Exec Server wird grundsätzlich empfohlen, die Resilient Change Tracking (RCT)-Methode auszuwählen. Wenn die RCT-Methode ausgewählt ist, wird sie, wo immer anwendbar, eingesetzt. Wird RCT von einem virtuellen Computer nicht unterstützt, wird eine der beiden anderen Methoden, Standardverarbeitung oder schnellere Verarbeitung, verwendet.

So konfigurieren Sie die Einstellungen für inkrementelle oder differenzielle Hyper-V-Backups

- 1 Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Backup Exec-Einstellungen".
- 2 Klicken Sie im linken Teilfenster auf "Virtuelle Computer".

3 Wählen Sie die Verarbeitungsmethode aus, die Sie für alle inkrementellen und differenziellen Hyper-V-Backups verwenden wollen.

Verwenden Sie das Resilient Change Tracking, wo auch immer anwendbar

Aktivieren Sie diese Option, wenn sowohl inkrementelle als auch differenzielle Backups ausgeführt werden sollen. Wenn die RCT-Methode ausgewählt wurde, wird sie eingesetzt, wo auch immer anwendbar, und ist die empfohlene Methode. Wenn ein virtueller Computer RCT nicht unterstützt, wird die Standardmethode oder eine schnellere Methode angewendet, je nach der von Ihnen getroffenen Auswahl.

Hinweis: Diese Option ist nur für Hyper-V-Server mit Windows Server 2016 und höher verfügbar.

Wenn Sie die RCT-Methode nicht ausgewählt haben und ein Windows Server 2016-Host oder höher gefunden wird, sendet Backup Exec in regelmäßigen Abständen Benachrichtigungen, die Sie daran erinnern, die RCT-Methode zu aktivieren. Wenn Sie nicht möchten, dass Backup Exec die Benachrichtigungen anzeigt, können Sie die Benachrichtigen durch Bearbeiten des folgenden Registrierungsschlüssels deaktivieren:

Registrierungspfad:

```
HKEY_LOCAL_MACHINE\Software\Symantec\Backup  
Exec For Windows\Backup Exec\Server  
ValueName = SupressRCTAlert
```

Wenn Sie den Wert auf 1 setzen, sind die Benachrichtigungen deaktiviert.

Schnellere Methode verwenden

Wählen Sie diese Methode, wenn inkrementelle Backups so schnell wie möglich verarbeitet und keine differenziellen Backups ausgeführt werden sollen. Bei dieser Option werden differenzielle Backups nicht unterstützt. Ist diese Option aktiviert, werden alle differenziellen Hyper-V-Backups inkrementell verarbeitet.

Hinweis: Diese Option ist nur für Hyper-V-Server mit Windows Server 2012 und höher verfügbar. Für alle unterstützten vorherigen Versionen von Windows muss die Standardmethode gewählt werden.

Standardmethode verwenden	Aktivieren Sie diese Option, wenn sowohl inkrementelle als auch differenzielle Backups ausgeführt werden sollen.
---------------------------	--

Hinweis: Wenn Sie eine andere inkrementelle Backup-Methode auswählen, wird der nächste Auftrag als vollständiges und nicht als inkrementelles oder differenzielles Backup ausgeführt.

Hinweis: Stimmt in einer CAS-Umgebung die Methode auf dem zentralen Administrationsserver nicht mit dem auf dem verwalteten Backup Exec-Server überein, wird die für den verwalteten Backup Exec-Server festgelegte Methode verwendet, wenn ein Auftrag vom zentralen Administrationsserver delegiert wird.

4 Klicken Sie auf "OK".

Ändern der Validierungseinstellungen des virtuellen Computers für VMware und Hyper-V

In den "Validierungseinstellungen des virtuellen Computers" können Sie die Zeitüberschreitungseinstellungen eines virtuellen Computers für VMware und Hyper-V ändern. Nachdem Sie einen Validierungsauftrag für einen virtuellen Computer erstellt haben, können Sie vor dem Ausführen des Auftrags die maximal zulässige Zeit für den Start eines virtuellen Computers ändern. Dies ist eine globale Einstellung, die für alle Validierungsaufträge gilt. Wird der virtuelle Computer nicht innerhalb des ausgewählten Zeitraums gestartet, schlägt die Validierung fehl.

So ändern Sie die Validierungseinstellungen des virtuellen Computers für VMware und Hyper-V

- 1** Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Backup Exec-Einstellungen".
- 2** Klicken Sie im linken Teilfenster auf "Virtuelle Computer".
- 3** Stellen Sie unter der Option "Wählen Sie die maximale Startzeit für einen virtuellen Computer" den gewünschten Zeitraum in Minuten ein.

Standardmäßig ist ein Zeitraum von 5 Minuten ausgewählt. Sie können einen Zeitraum von 1 bis 60 Minuten auswählen.

Berichte

In diesem Kapitel werden folgende Themen behandelt:

- [Berichte in Backup Exec](#)
- [Einen Bericht jetzt ausführen](#)
- [Planen eines Berichts](#)
- [Erstellen eines benutzerdefinierten Berichts](#)
- [Speichern eines Berichts](#)
- [Drucken eines Berichts in der Backup Exec-Berichtsanzeige](#)
- [Anzeigen abgeschlossener Berichte](#)
- [Bearbeiten eines Berichts](#)
- [Erneutes Ausführen eines abgeschlossenen Berichts](#)
- [Löschen eines Berichts](#)
- [Festlegen der Standards für Standard- und benutzerdefinierte Berichte](#)
- [Anzeigen der Berichtseigenschaften](#)
- [Liste von Backup Exec-Standardberichten](#)

Berichte in Backup Exec

Backup Exec schließt mehr als 40 Standardberichte ein, die ausführliche Information über die Warnmeldungen, die Geräte, die Medien und die Aufträge in Ihrer Backup Exec-Umgebung zur Verfügung stellen können. Darüber hinaus liefert Backup Exec die Fähigkeit, benutzerdefinierte Berichte zu erstellen, damit Sie Berichte entsprechend Ihrer Umgebung und Ihren Bedürfnissen erstellen können. Sowohl

Standard- als auch benutzerdefinierte Berichte können bei Bedarf jederzeit ausgeführt werden, für einen spezifischen Zeitpunkt geplant werden oder an einem wiederkehrenden Zeitplan ausgeführt werden. Wenn Sie einen Berichtsauftrag planen, können Sie E-Mail-Benachrichtigung einrichten, damit Sie oder jemand anderes benachrichtigt werden können, wenn der Berichtsauftrag abschließt, und Sie können eine Kopie des Berichts in der E-Mail einschließen.

Berichte können in den folgenden Formaten angezeigt und gedruckt werden:

- PDF
- HTML
- XML
- XLS (Microsoft Excel)
- Datei mit Kommas als Trennzeichen (CSV)

Berichte werden über auf der Registerkarte "Berichte" nach Kategorien gruppiert. Beispielsweise werden Berichte, die sich auf Geräte beziehen, in der Berichtgruppe "Geräte" gruppiert. Um Namen und Beschreibungen der Standardberichte für eine Gruppe anzuzeigen, klicken Sie auf den Namen der entsprechenden Berichtgruppe.

Hinweis: Die Berichtgruppe "Abgeschlossene aufrufen" umfasst nur die geplanten Berichte, die abgeschlossen sind. Sofort ausgeführte Berichte werden beim Schließen von Report Viewer gelöscht.

Informationen zu den Best Practices zum Einsatz von Backup-Berichten finden Sie unter *Best Practices für Backup Exec*.

Anforderungen für Berichte

Bevor Sie versuchen, Standardberichte oder benutzerdefinierte Berichte auszuführen, überprüfen Sie die folgenden Anforderungen:

- Wenn Sie in der Windows-Systemsteuerung unter "Drucker" einen Standarddrucker konfigurieren, werden die integrierten Backup Exec-Berichte ordnungsgemäß formatiert. Dies ist auch dann erforderlich, wenn kein Drucker am System angeschlossen ist. Informationen über das Konfigurieren eines Druckers mithilfe der Windows-Systemsteuerung finden Sie in der Microsoft Windows-Dokumentation.
- Wenn Berichte auf mehreren Backup Exec-Servern ausgeführt werden sollen, müssen Sie Backup Exec Enterprise Server Feature installieren, auch wenn es sich nicht um eine Shared Storage-Umgebung handelt.
- Zum Anzeigen von Berichten im Format PDF muss die neueste Version von Adobe Acrobat Reader installiert sein.

Berichte und die Auftragsüberwachung

Berichte können nicht von Registerkarte "Auftragsüberwachung" überwacht werden. Berichte, die ausgeführt werden, geplant sind oder abgeschlossen sind, werden nicht unter der Registerkarte "Auftragsüberwachung" angezeigt. Alle Berichtvorgänge werden auf der Registerkarte "Berichte" angezeigt.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Liste von Backup Exec-Standardberichten"](#) auf Seite 814.

Einen Bericht jetzt ausführen

Beim Ausführen eines Berichts können Sie die Kriterien angeben, anhand derer die entsprechenden im Bericht angezeigten Elemente festgelegt werden. Die jeweils zur Auswahl verfügbaren Einstellungen oder Parameter hängen von der Art der Daten ab, die in den Bericht aufgenommen werden können. Im fertigen Bericht werden nur die Elemente angezeigt, die den festgelegten Kriterien entsprechen.

Wenn Sie den Bericht nicht sofort ausführen möchten, sollten Sie stattdessen die Option "Neuer geplanter Bericht" verwenden.

Siehe ["Planen eines Berichts"](#) auf Seite 794.

So führen Sie einen Bericht aus:

- 1 Klicken Sie auf der Registerkarte "Berichte" unter "Berichtgruppen" auf die Berichtgruppe mit dem Bericht, den Sie jetzt ausführen möchten.
- 2 Klicken Sie mit der rechten Maustaste auf den Bericht, den Sie ausführen möchten, und klicken Sie dann auf "Jetzt ausführen".
- 3 Wenn die Eigenschaftenseite "Bericht jetzt ausführen - <Berichtsname>" angezeigt wird, legen Sie die benötigten Einstellungen für die Daten fest, die Sie in den Bericht einbeziehen möchten, und klicken Sie auf "OK".
- 4 Wenn Sie den Bericht wieder schließen möchten, klicken Sie auf "OK".

Backup Exec löscht automatisch den Bericht, wenn Sie die Berichtsanzeige schließen.

Planen eines Berichts

Sie können einen Bericht planen, der einmal zu einem spezifischen Zeitpunkt oder mehrmals im Rahmen eines wiederkehrenden Zeitplans ausgeführt wird. Geplante Berichte werden in der Berichtsgruppe "Anstehende aufrufen" auf der Registerkarte "Berichte" aufgelistet. Sie können geplante Berichte bearbeiten oder löschen.

So planen Sie einen Bericht

- 1** Auf der Registerkarte "Berichte" unter "Berichtsgruppen" klicken Sie auf die Berichtsgruppe, die den zu planenden Bericht enthält.
- 2** Klicken Sie mit der rechten Maustaste auf den Berichtsnamen und klicken Sie dann auf "Bericht planen".
- 3** Geben Sie einen Namen für den Bericht ein.
- 4** Wenn eine der folgenden Optionen im linken Teilfenster angezeigt wird, klicken Sie auf den Optionsnamen und geben Sie dann die Kriterien für die Daten ein, die Sie in den Bericht aufnehmen möchten. Beachten Sie, dass einige Berichte keine der folgenden Optionen enthalten:
 - Validierungsstatus
 - Gesicherte Server
 - Bereiche
 - Überwachungsprotokollkategorie
 - Auftragsstatus
 - Mediensätze
 - Speicher
- 5** (Optional) Soll eine E-Mail an Sie oder an jemand anderen gesendet werden, wenn der Bericht abgeschlossen ist, führen Sie folgende Schritte durch:
 - Im linken Teilfenster klicken Sie auf "Benachrichtigung".
 - Wählen Sie einen vorhandenen Empfänger aus oder klicken Sie auf "Empfänger verwalten", um einen neuen Empfänger hinzuzufügen.
 - Aktivieren Sie bei Bedarf das Kontrollkästchen "Bericht in E-Mail-Benachrichtigungen einschließen".

- 6** Im linken Teilfenster klicken Sie auf "Planen" und wählen dann eine der folgenden Planungsoptionen aus:

Wiederkehrend	Hier können Sie planen, den Auftrag mehrmals auszuführen. Sie können das Wiederholmuster für den Auftrag einstellen:
Jetzt ohne regelmäßigen Zeitplan ausführen	Wenn Sie diese Option wählen, wird der Auftrag sofort ausgeführt.
Ausführen am	Legen Sie Datum und Uhrzeit zum Ausführen des Berichts fest.
Ohne Zeitplan erstellen	Hier können Sie den Bericht erstellen und speichern, aber nicht planen oder ausführen. Wenn Sie diese Option auswählen, können Sie ein externes Planungs-Tool verwenden, um den Auftrag so zu planen, dass er an einem bestimmten Zeitpunkt ausgeführt wird. Sie können auch zu einem beliebigen Zeitpunkt den Auftrag manuell ausführen. Obwohl der Auftrag nicht geplant ist, wird der Bericht in der Berichtsgruppe "Anstehende aufrufen" auf der Registerkarte "Bericht" aufgelistet.

- 7** Klicken Sie auf "OK".

Der geplante Bericht wird in der Berichtsgruppe "Anstehende aufrufen" gespeichert. Nachdem der Bericht ausgeführt wurde, wird er in der Berichtsgruppe "Abgeschlossene aufrufen" gespeichert.

Siehe ["Anzeigen abgeschlossener Berichte"](#) auf Seite 810.

Erstellen eines benutzerdefinierten Berichts

Sie können benutzerdefinierte Berichte erstellen, die Informationen entsprechend den spezifischen Anforderungen ihres Unternehmens enthalten. Sie wählen die in den Bericht einzuschließenden Daten aus und bestimmen, wie die Daten gefiltert, sortiert und gruppiert werden. Darüber hinaus können Sie ein Kreisdiagramm oder ein Balkendiagramm einrichten, um die Berichtsdaten grafisch darzustellen.

Mithilfe von Filtern können Sie die Berichte so anpassen, dass nur die Informationen, die bestimmte Kriterien erfüllen, mit einbezogen werden. Beispielsweise können Sie Filter verwenden, um die Aufträge zu finden, die ein bestimmtes Wort, die

Warnmeldungen, die an einem bestimmten Tag auftraten oder die Medien enthalten, die in einem bestimmten Speicherort sind. Sie können Filterkriterien verwenden, um Filterausdrücke zu erstellen. Sie können einen Filterausdruck oder mehrere Filterausdrücke verwenden. Ein Filterausdruck besteht aus einem Feldnamen, einem Operator und einem Wert.

Der folgende Filterausdruck findet alle Fehlerwarnmeldungen:

Tabelle 16-1 Filterausdruck für das Finden von Warnmeldungen für Fehler

Filtertyp	Daten
Feldname	Meldungstyp
Operator	= (ist gleich)
Wert	Fehler

Wenn Sie im Bericht nur Warnmeldungen für Fehler einschließen möchten, die nur an einem bestimmten Tag auftraten, fügen Sie einen weiteren Filterausdruck für dieses Datum und diese Uhrzeit hinzu wie im Beispiel aufgeführt:

Tabelle 16-2 Filterausdruck für das Finden von Warnmeldungen an einem bestimmten Tag

Filtertyp	Daten
Feldname	Eingegebenes Datum
Operator	= (ist gleich)
Wert	03.06.2011 <Zeit>

Durch das Gruppieren von Feldern wird der Bericht in Abschnitte unterteilt. Wenn Sie beispielsweise nach Backup Exec-Server gruppieren, erstellt Backup Exec einen Abschnitt für jeden Backup Exec-Server, der den Filterkriterien entspricht. In jedem Abschnitt für einen Backup Exec-Server zeigt der Bericht die Daten an, die den verbleibenden Feldern entsprechen, die Sie für den Bericht ausgewählt haben.

Sie können einen benutzerdefinierten Bericht anhand von bis zu drei der für den Bericht ausgewählten Felder sortieren. Wenn Sie anhand von Feldern sortieren, ordnet Backup Exec alle Daten, die den Sortierkriterien entsprechen, gemeinsam im Bericht an. Wenn Sie beispielsweise auf dem Backup Exec-Server-Feld in aufsteigender Reihenfolge sortieren, werden alle Daten für den Backup Exec-Server "A" zuerst angezeigt, gefolgt von allen Daten für den Backup Exec-Server "B" usw.

So erstellen Sie einen benutzerdefinierten Bericht

- 1 Klicken Sie auf der Registerkarte "Berichte" auf "Neuer benutzerdefinierter Bericht".
- 2 Geben Sie im Dialogfeld "Benutzerdefinierter Bericht" einen Namen und eine Beschreibung für den Bericht ein.
- 3 Wenn in dem Bericht die standardmäßigen Kopf- und Fußzeileneinstellungen nicht enthalten sein sollen, deaktivieren Sie die Option "Verwenden Sie die in den Backup Exec-Einstellungen angegebenen Einstellungen für Kopf- und Fußzeilen".

Die Standardeinstellungen für Kopf- und Fußzeilen können ein angepasstes Logo, eine benutzerdefinierte Farbe für den Banner und Text für die Fußzeile umfassen. Diese Elemente werden in den Standardeinstellungen von Backup Exec eingestellt.

Siehe ["Festlegen der Standards für Standard- und benutzerdefinierte Berichte"](#) auf Seite 811.

- 4 Klicken Sie im linken Teilfenster auf "Feldauswahl".
- 5 Wählen Sie im Feld "Kategorie" eine Gruppe aus, für die Sie einen Bericht erstellen möchten.
- 6 Klicken Sie für zusätzliche Feldauswahlen auf "Erweiterte Felder anzeigen".
- 7 Wählen Sie aus der Liste "Verfügbare Felder" die Felder, die Sie in dem Bericht einschließen möchten und klicken Sie dann auf die Schaltfläche mit dem Pfeil nach rechts (>), um die Felder in die Liste "Für den Bericht ausgewählte Felder" zu verschieben.
- 8 Nachdem Sie alle Felder, die im Bericht erscheinen sollen, in die Liste "Für den Bericht ausgewählte Felder" verschoben haben, bestimmen Sie die Reihenfolge, in der die Felder angezeigt werden sollen.

Die Felder werden im Bericht in der Reihenfolge angezeigt, in der sie in der Liste "Für den Bericht ausgewählte Felder" aufgelistet sind. Dabei wird das erste Feld in der Liste als erstes oben links im Bericht angezeigt. Um ein Feld zu verschieben, wählen Sie es von der Liste "Für den Bericht ausgewählte Felder" aus und klicken Sie dann auf "Nach oben" oder "Nach unten", um es auf den entsprechenden Speicherort in der Liste zu verschieben.

- 9 So passen Sie die Spaltenbreite für ein Feld an
 - Klicken Sie in der Liste "Für den Bericht ausgewählte Felder" auf einen Feldnamen.
 - Geben Sie im Feld "Spaltenbreite" die neue Breite ein.
 - Klicken Sie auf "Festlegen".

10 (Optional) wenn Sie die Daten im Bericht filtern möchten, führen Sie folgende Schritte durch:

- Klicken Sie im linken Teilfenster auf "Filter".
- Wählen Sie in der Liste "Feldname" das Feld aus, auf dem Sie Daten filtern möchten.
- Wählen Sie aus der Liste "Operator" den Operator aus, den Sie für diesen Filter verwenden möchten.
- Wählen Sie im Feld "Wert" die Daten aus, die Sie in den Bericht einschließen möchten, oder geben Sie sie ein.
- Klicken Sie auf "Hinzufügen".
- Um Sätze von Filterausdrücken zu kombinieren, führen Sie einen der folgenden Schritte durch:

<p>So kombinieren Sie zwei Filterausdrücke so, dass beide Ausdrücke wahr sein müssen, damit das Ergebnis wahr ist</p>	<p>Klicken Sie auf "UND".</p> <p>Um alle fehlgeschlagenen Backup-Aufträge zu finden, können Sie beispielsweise folgende Ausdrücke hinzufügen:</p> <ul style="list-style-type: none"> ■ Status = Fehlgeschlagen ■ Typ = Backup <p>Nach dem Erstellen der Filterausdrücke gehen Sie wie folgt vor:</p> <ul style="list-style-type: none"> ■ Klicken Sie auf "UND", um die beiden Ausdrücke zu verbinden. <p>Der gesamte Ausdruck lautet dann:</p> <p>Status = Fehlgeschlagen UND Typ = Backup</p>
---	--

<p>So kombinieren Sie zwei Filterausdrücke so, dass einer der beiden Ausdrücke wahr sein muss, damit das Ergebnis wahr ist</p>	<p>Klicken Sie auf "ODER".</p> <p>Um alle Backup-Aufträge zu finden, die entweder fehlgeschlagen sind oder abgebrochen wurden, können Sie beispielsweise folgende Ausdrücke hinzufügen:</p> <ul style="list-style-type: none"> ■ Status = Fehlgeschlagen ■ Status = Abgebrochen <p>Nach dem Erstellen der Filterausdrücke gehen Sie wie folgt vor:</p> <ul style="list-style-type: none"> ■ Klicken Sie auf ODER, um beide Filterausdrücke zu verbinden. <p>Der gesamte Ausdruck lautet dann:</p> <p>Status = Fehlgeschlagen ODER Typ = Backup</p>
--	---

So kombinieren Sie zwei Filterausdrücke innerhalb eines Ausdrucks

Klicken Sie auf "() +"

Um fehlgeschlagene Backup- und Wiederherstellungsaufträge zu finden, können Sie beispielsweise folgende Ausdrücke hinzufügen:

- Status = Fehlgeschlagen
- Typ = Backup
- Typ = Wiederherstellung

Nach dem Erstellen der Filterausdrücke gehen Sie wie folgt vor:

- Verwenden Sie ODER, um die Filterausdrücke "Typ = Backup" und "Typ = Wiederherstellung" zu verbinden.
- Halten Sie die STRG-Taste gedrückt während Sie auf "Typ = Backup" und "Typ = Wiederherstellung" klicken.
- Klicken Sie auf "() +", um die Filterausdrücke "Typ = Backup" und "Typ = Wiederherstellung" zu verbinden.
- Verwenden Sie UND, um die Filterausdrücke "Status = Fehlgeschlagen" und ("Typ = Backup" ODER "Typ = Wiederherstellung") zu verbinden.

Der gesamte Ausdruck lautet dann:

Status = Fehlgeschlagen UND (Typ = Backup ODER Typ = Wiederherstellung)

So trennen Sie zwei Filterausdrücke, die innerhalb eines Ausdrucks kombiniert waren

Klicken Sie auf "() -".

Wenn Sie beispielsweise "() +" verwenden, um "Typ = Backup" und "Typ = Wiederherstellung" in einem Ausdruck zu verbinden, wird dieser im Dialogfeld "Filter" wie folgt angezeigt:

(Typ = Backup ODER Typ = Wiederherstellung)

Um den kombinierten Ausdruck in zwei Einzelausdrücke aufzulösen, gehen Sie wie folgt vor:

- Halten Sie die STRG-Taste gedrückt während Sie auf "Typ = Backup" und "Typ = Wiederherstellung" klicken.
- Klicken Sie auf "() -".

Nachdem Sie die Ausdrücke getrennt haben, werden diese ohne die Klammern angezeigt.

11 (Optional) wenn Sie den Bericht in Abschnitte organisieren möchten, führen Sie folgende Schritte durch:

- Klicken Sie im linken Teilfenster auf "Gruppieren".
- Wählen Sie aus der Liste "Gruppieren nach" das Feld aus, das Sie als Gruppe verwenden möchten.
- Klicken Sie auf "Aufsteigend" oder "Absteigend".

Eine aufsteigende Reihenfolge führt Zahlen von der kleinsten bis zur größten und Buchstaben in alphabetischer Folge auf. Eine absteigende Reihenfolge führt Zahlen von der größten bis zur kleinsten und Buchstaben in umgekehrter alphabetischer Folge auf.

- Wenn Sie die Daten weiter gruppieren möchten, wählen Sie die Felder in den Listen "Anschließend gruppieren nach" aus und klicken Sie dann auf "Aufsteigend" oder "Absteigend" für jene Felder.
Ein Bericht muss mindestens ein Feld aufweisen, das nicht gruppiert wurde. Wenn Sie beispielsweise im Bericht drei Felder ausgewählt haben, können nur zwei davon gruppiert werden. Wenn Sie alle Felder gruppieren, werden keine Daten im Bericht angezeigt, da alle Daten in den Titeln der Gruppenabschnitte aufgeführt werden. Darüber hinaus müssen Sie mindestens vier Felder im Bericht aufnehmen, um alle drei Gruppierungsfelder verwenden zu können.

12 (Optional) wenn Sie die Daten in dem Bericht sortieren möchten, führen Sie folgende Schritte durch:

- Klicken Sie im linken Teilfenster auf "Sortieren".
- Wählen Sie aus der Liste "Sortieren nach" das Feld aus, auf dem Sie die Daten im Bericht sortieren möchten.
- Klicken Sie auf "Aufsteigend" oder "Absteigend".
Eine aufsteigende Reihenfolge führt Zahlen von der kleinsten bis zur größten und Buchstaben in alphabetischer Folge auf. Eine absteigende Reihenfolge führt Zahlen von der größten bis zur kleinsten und Buchstaben in umgekehrter alphabetischer Folge auf.
- Wenn Sie die Daten weiter sortieren möchten, wählen Sie die Felder in den Listen "Anschließend sortieren nach" aus und klicken Sie dann auf "Aufsteigend" oder "Absteigend" für jene Felder.

13 (Optional) wenn Sie dem Bericht ein Kreis- oder Balkendiagramm hinzufügen möchten, führen Sie folgende Schritte durch:

- Klicken Sie im linken Teilfenster auf "Diagrammoptionen".
- Wählen Sie aus der Liste "Diagrammtyp" entweder "Balkendiagramm" oder "Kreisdiagramm" aus.
- Wählen Sie die Datentypen aus, die Sie im Diagramm mit einschließen möchten.

14 (Optional) Wenn Sie sehen möchten, wie der Bericht aussieht, bevor Sie ihn speichern, klicken Sie auf "Vorschau".

15 Klicken Sie auf "OK", um den benutzerdefinierten Bericht zu speichern.

Hinzufügen oder Entfernen von Feldern für einen benutzerdefinierten Bericht

Um die Daten zu ändern die in einem benutzerdefinierten Bericht angezeigt werden, fügen Sie neue Felder hinzu oder entfernen Sie vorhandene.

So fügen Sie Felder einem benutzerdefinierten Bericht hinzu oder entfernen sie

- 1 Klicken Sie auf der Registerkarte "Berichte" unter "Berichtgruppen" auf "Benutzerdefiniert".
- 2 Klicken Sie mit der rechten Maustaste auf den Bericht, der die zu ändernden Felder enthält, und klicken Sie auf "Bearbeiten".
- 3 Klicken Sie im linken Teilfenster auf "Feldauswahl".
- 4 Sie haben folgende Möglichkeiten:

So fügen Sie dem Bericht neue Felder hinzu

- Wählen Sie eine Kategorie aus.
- Wählen Sie unter "Verfügbare Felder" die Felder, die Sie hinzufügen möchten, und klicken Sie auf die Schaltfläche "Nach-Rechts" (>>).

So entfernen Sie Felder aus dem Bericht

Klicken Sie unter "Für den Bericht ausgewählte Felder" auf das Feld, das Sie entfernen möchten, und klicken Sie dann auf die Schaltfläche "Nach links" (<<).

Ändern der Filter für einen benutzerdefinierten Bericht

Führen Sie folgende Schritte durch, um die existierenden Filter auf einem benutzerdefinierten Bericht zu ändern.

So ändern Sie die Filter für einen benutzerdefinierten Bericht

- 1 Klicken Sie auf der Registerkarte "Berichte" unter "Berichtgruppen" auf "Benutzerdefinierte Berichte".
- 2 Klicken Sie in der Berichtsliste mit der rechten Maustaste auf den zu ändernden Bericht und klicken Sie anschließend auf "Bearbeiten".
- 3 Klicken Sie im linken Teilfenster auf "Filter".
- 4 Erstellen Sie einen Filter, indem Sie einen oder mehrere Filter-Ausdrücke definieren.

So fügen Sie einen neuen Filterausdruck hinzu	Wählen Sie einen Feldnamen und einen Operator aus und geben Sie dann einen Wert ein. Klicken Sie auf "Hinzufügen".
So bearbeiten Sie einen vorhandenen Filterausdruck	<p>Gehen Sie wie folgt vor:</p> <ul style="list-style-type: none"> ■ Unter "Filterkriterien" wählen Sie den Filterausdruck, den Sie bearbeiten möchten, aus und klicken Sie dann auf "Bearbeiten". ■ Unter "Filterausdruck" bearbeiten Sie die Werte des Ausdrucks. ■ Unter "Filterausdruck" klicken Sie auf "Aktualisieren".
So löschen Sie einen Filterausdruck	Unter "Filterkriterien" wählen Sie den Filterausdruck, den Sie löschen möchten, aus und klicken Sie dann auf "Entfernen".

5 Um Sätze von Filterausdrücken zu kombinieren, führen Sie einen der folgenden Schritte durch:

So kombinieren Sie zwei Filterausdrücke so, dass beide Ausdrücke wahr sein müssen, damit das Ergebnis wahr ist	<p>Klicken Sie auf "UND".</p> <p>Um alle fehlgeschlagenen Backup-Aufträge zu finden, können Sie beispielsweise folgende Ausdrücke hinzufügen:</p> <ul style="list-style-type: none"> ■ Status = Fehlgeschlagen ■ Typ = Backup <p>Nach dem Erstellen der Filterausdrücke gehen Sie wie folgt vor:</p> <ul style="list-style-type: none"> ■ Klicken Sie auf "UND", um die beiden Ausdrücke zu verbinden. <p>Der gesamte Ausdruck lautet dann:</p> <p>Status = Fehlgeschlagen UND Typ = Backup</p>
--	--

<p>So kombinieren Sie zwei Filterausdrücke so, dass einer der beiden Ausdrücke wahr sein muss, damit das Ergebnis wahr ist</p>	<p>Klicken Sie auf "ODER".</p> <p>Um alle Backup-Aufträge zu finden, die entweder fehlgeschlagen sind oder abgebrochen wurden, können Sie beispielsweise folgende Ausdrücke hinzufügen:</p> <ul style="list-style-type: none"> ■ Status = Fehlgeschlagen ■ Status = Abgebrochen <p>Nach dem Erstellen der Filterausdrücke gehen Sie wie folgt vor:</p> <ul style="list-style-type: none"> ■ Klicken Sie auf ODER, um beide Filterausdrücke zu verbinden. <p>Der gesamte Ausdruck lautet dann:</p> <p>Status = Fehlgeschlagen ODER Typ = Backup</p>
<p>So kombinieren Sie zwei Filterausdrücke innerhalb eines Ausdrucks</p>	<p>Klicken Sie auf "() +"</p> <p>Um fehlgeschlagene Backup- und Wiederherstellungsaufträge zu finden, können Sie beispielsweise folgende Ausdrücke hinzufügen:</p> <ul style="list-style-type: none"> ■ Status = Fehlgeschlagen ■ Typ = Backup ■ Typ = Wiederherstellung <p>Nach dem Erstellen der Filterausdrücke gehen Sie wie folgt vor:</p> <ul style="list-style-type: none"> ■ Verwenden Sie ODER, um die Filterausdrücke "Typ = Backup" und "Typ = Wiederherstellung" zu verbinden. ■ Halten Sie die STRG-Taste gedrückt während Sie auf "Typ = Backup" und "Typ = Wiederherstellung" klicken. ■ Klicken Sie auf "() +", um die Filterausdrücke "Typ = Backup" und "Typ = Wiederherstellung" zu verbinden. ■ Verwenden Sie UND, um die Filterausdrücke "Status = Fehlgeschlagen" und ("Typ = Backup" ODER "Typ = Wiederherstellung") zu verbinden. <p>Der gesamte Ausdruck lautet dann:</p> <p>Status = Fehlgeschlagen UND (Typ = Backup ODER Typ = Wiederherstellung)</p>

<p>So trennen Sie zwei Filterausdrücke, die innerhalb eines Ausdrucks kombiniert waren</p>	<p>Klicken Sie auf "() -".</p> <p>Wenn Sie beispielsweise "() +" verwenden, um "Typ = Backup" und "Typ = Wiederherstellung" in einem Ausdruck zu verbinden, wird dieser im Dialogfeld "Filter" wie folgt angezeigt:</p> <p>(Typ = Backup ODER Typ = Wiederherstellung)</p> <p>Um den kombinierten Ausdruck in zwei Einzelausdrücke aufzulösen, gehen Sie wie folgt vor:</p> <ul style="list-style-type: none"> ■ Halten Sie die STRG-Taste gedrückt während Sie auf "Typ = Backup" und "Typ = Wiederherstellung" klicken. ■ Klicken Sie auf "() -". <p>Nachdem Sie die Ausdrücke getrennt haben, werden diese ohne die Klammern angezeigt.</p>
--	---

6 Klicken Sie auf "OK".

Ändern der Art, wie Daten in einem benutzerdefinierten Bericht gruppiert oder sortiert werden

Verwenden Sie die folgenden Schritte, um die Methode zu ändern, wie Daten in einem benutzerdefinierten Bericht gruppiert oder sortiert werden.

So ändern Sie die Gruppierung oder Sortierung in einem benutzerdefinierten Bericht

- 1** Klicken Sie auf der Registerkarte "Berichte" unter "Berichtgruppen" auf "Benutzerdefiniert".
- 2** In der Liste von benutzerdefinierten Berichten, klicken Sie mit der rechten Maustaste auf den Bericht, den Sie ändern möchten, und wählen Sie dann "Bearbeiten" aus.
- 3** Führen Sie einen der folgenden Schritte aus:

<p>So ändern Sie das Feld, das als Gruppe verwendet wird</p>	<ul style="list-style-type: none"> ■ Klicken Sie im linken Teilfenster auf "Gruppieren". ■ Klicken Sie in der Liste "Gruppieren nach" oder "Anschließend gruppieren nach", die das Feld enthält, das Sie ändern möchten, auf den Pfeil nach unten und wählen Sie dann das neue Feld aus, das als Gruppe verwendet werden soll.
--	--

So entfernen Sie eine Gruppe	<ul style="list-style-type: none"> ■ Klicken Sie im linken Teilfenster auf "Gruppieren". ■ Klicken Sie in der Liste "Gruppieren nach" oder "Anschließend gruppieren nach", die die Gruppe enthält, die Sie entfernen möchten, auf den Pfeil nach unten und anschließend auf "<Keine>".
So ändern Sie die Reihenfolge, in der Daten gruppiert werden	Klicken Sie auf "Aufsteigend" oder "Absteigend".
So ändern Sie das Feld, das zum Sortieren der Daten verwendet wird	<ul style="list-style-type: none"> ■ Klicken Sie im linken Teilfenster auf "Sortieren". ■ Klicken Sie in der Liste "Sortieren nach" oder "Anschließend sortieren nach", die die Sortieroption enthält, die Sie ändern möchten, auf den Pfeil nach unten und wählen Sie dann das neue Feld aus, das zum Sortieren verwendet werden soll.
So deaktivieren Sie das Sortieren	<ul style="list-style-type: none"> ■ Klicken Sie im linken Teilfenster auf "Sortieren". ■ Klicken Sie in der Liste "Sortieren nach" oder "Anschließend sortieren nach", die die Sortieroption enthält, die Sie entfernen möchten, auf den Pfeil nach unten und klicken Sie anschließend auf "<Keine>".
So ändern Sie die Reihenfolge, in der Daten sortiert werden	Klicken Sie auf "Aufsteigend" oder "Absteigend".

4 Klicken Sie auf "OK".

Ändern der Diagrammoptionen in den benutzerdefinierten Berichten

Sie können in benutzerdefinierte Berichte ein Balken- oder Kreisdiagramm integrieren.

Sie müssen im Dialogfeld "Feldauswahl" mindestens zwei Felder auswählen, um ein Kreisdiagramm zu erstellen, und drei Felder für ein Balkendiagramm.

So ändern Sie Diagrammoptionen für benutzerdefinierte Berichte

- 1 Klicken Sie auf der Registerkarte "Berichte" unter "Berichtgruppen" auf "Benutzerdefiniert".
- 2 Klicken Sie mit der rechten Maustaste auf den Bericht, den Sie bearbeiten möchten und wählen Sie dann "Bearbeiten" aus.
- 3 Klicken Sie im Fenster "Benutzerdefinierter Bericht" auf "Diagrammoptionen".
- 4 Ändern Sie den Diagrammtitel oder wählen Sie neue Felder aus, die für das Diagramm verwendet werden sollen.
- 5 Klicken Sie auf "OK".

Vorschau von benutzerdefinierten Berichten

Die Vorschaufunktion ermöglicht eine Überprüfung der Einstellungen des benutzerdefinierten Berichts.

Hinweis: Sie können benutzerdefinierte Berichte aus der Backup Exec Remote-Administratorkonsole nicht als Vorschau anzeigen.

So gelangen Sie zur Vorschau eines benutzerdefinierten Berichts

- 1 Klicken Sie auf der Registerkarte "Berichte" unter "Berichtgruppen" auf "Benutzerdefiniert".
- 2 Klicken Sie mit der rechten Maustaste auf den Bericht, den Sie bearbeiten möchten, und klicken Sie dann auf "Bearbeiten".
- 3 Klicken Sie im linken Teilfenster auf "Vorschau".

Kopieren eines benutzerdefinierten Berichts

Sie können eine oder mehrere Kopien eines benutzerdefinierten Berichts erstellen. Jede Kopie des benutzerdefinierten Berichts befindet sich zusammen mit dem ursprünglichen benutzerdefinierten Bericht in der Berichtgruppe "Benutzerdefiniert".

So kopieren Sie einen benutzerdefinierten Bericht

- 1 Klicken Sie auf der Registerkarte "Berichte" unter "Berichtgruppen" auf "Benutzerdefiniert".
- 2 Klicken Sie mit der rechten Maustaste auf den Bericht, den Sie kopieren möchten, und klicken Sie dann auf "Kopieren".
- 3 Geben Sie einen Namen für den Bericht ein und klicken Sie dann auf "OK".

Die Kopie des benutzerdefinierten Berichts wird in der Berichtgruppe "Benutzerdefiniert" angezeigt.

Speichern eines Berichts

Berichte können in jedem Speicherort gespeichert werden, den Sie auf Ihrer Festplatte oder Netzwerk in den folgenden Formate auswählen:

- HTML-Datei (.htm)
- Adobe PDF-Datei (.pdf)
- XML-Datei (.xml)
- Datei mit Trennkommas (.csv)
- Microsoft Office Excel-Arbeitsmappe (.xls)

Sie können einen Bericht sichern, der derzeit auf dem Bildschirm oder in der Berichtgruppe "Abgeschlossene aufrufen" angezeigt wird.

So speichern Sie einen Bericht

- 1 Klicken Sie im Bericht in der Berichtsanzeige auf "Speichern unter".

So sichern Sie einen Bericht, der derzeit auf dem Bildschirm angezeigt wird

Klicken Sie im Bericht in der Berichtsanzeige auf "Speichern unter".

So sichern Sie einen Bericht, der in der Berichtgruppe "Abgeschlossene aufrufen" aufgeführt wird

- Klicken Sie auf der Registerkarte "Berichte" unter "Berichtgruppen" auf "Abgeschlossene aufrufen".
- Klicken Sie auf "Speichern unter".
- Doppelklicken Sie auf einen abgeschlossenen Bericht, den Sie an einem neuen Speicherort speichern möchten.

- 2 Geben Sie den Dateinamen und den Ort ein, in dem Sie den Bericht speichern möchten.

- 3 Wählen Sie im Feld "Dateityp" ein Format aus, in dem der Bericht gespeichert werden soll.

Wenn Sie einen Bericht im HTML-Format speichern, werden sowohl die HTML-Datei als auch eine GIF-Grafikdatei gespeichert.

- 4 Klicken Sie auf "Speichern".

Drucken eines Berichts in der Backup Exec-Berichtsanzeige

Sie können Berichte auf einem lokalen oder einem Netzwerkdrucker drucken. Um einen Bericht zu drucken, muss der Drucker so konfiguriert werden, dass er im Querformat druckt.

Die folgenden Druckereinstellungen stellen sicher, dass der Bericht richtig ausgedruckt wird:

- Auf der Registerkarte "Layout" des Dialogfeldes "Drucken" unter "Ausrichtung" sollte die Option "Horizontal" ausgewählt sein. Beachten Sie, dass Sie möglicherweise zuerst die Registerkarte "Einstellungen" auswählen müssen, um auf die Registerkarte "Layout" zuzugreifen.
- Um alle Seiten eines mehrseitigen Berichts zu drucken, müssen Sie auf der Registerkarte "Optionen" des Dialogfeldes "Drucken", die Option "Alle verknüpften Dokumente drucken" auswählen.
- Um alle Seiten eines mehrseitigen Berichts in der richtigen Reihenfolge zu drucken, muss die erste Seite des Berichts auf dem Bildschirm angezeigt werden bevor der Druckauftrag initiiert wird.
- Wenn der Bericht nicht richtig ausgedruckt wird, müssen Sie möglicherweise die Optionen zum Einrichten der Seite in Internet Explorer ändern und die Kopf- und Fußzeile entfernen, um die Ränder zu reduzieren.

So drucken Sie einen Bericht in der Backup Exec-Berichtsanzeige

- 1 Führen Sie einen Bericht aus.
Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.
- 2 Klicken Sie unter "Berichtsanzeige" auf "Drucken".
- 3 Wählen Sie einen Drucker im Windows-Dialogfeld "Drucken" aus.
- 4 Klicken Sie auf "Drucken".

Anzeigen abgeschlossener Berichte

Nachdem ein geplanter Bericht ausgeführt wird, wird er in der Berichtgruppe "Abgeschlossene aufrufen" gespeichert.

So werden abgeschlossene Berichte angezeigt

- 1 Klicken Sie auf der Registerkarte "Berichte" unter "Berichtgruppen" auf "Abgeschlossene aufrufen".
- 2 Doppelklicken Sie auf den Bericht, den Sie anzeigen möchten.

Bearbeiten eines Berichts

Verwenden Sie die folgenden Schritte, um die Eigenschaften eines geplanten Standardberichts oder eines benutzerdefinierten Berichts zu bearbeiten, bevor er ausgeführt wird. Wenn der zu bearbeitende Bericht in einem vorhergehenden Berichtsauftrag ausgeführt wurde, können sich die jetzt von Ihnen vorgenommenen Änderungen auf die Anzeige des Berichts im Auftragsverlauf auswirken. Es wird empfohlen, den Bericht zu kopieren und dann zu bearbeiten.

So bearbeiten Sie einen geplanten Standardbericht oder einen benutzerdefinierten Bericht

- 1 Klicken Sie auf der Registerkarte "Berichte" unter "Berichtgruppen" auf "Anstehende aufrufen".

So bearbeiten Sie einen geplanten Standardbericht

Klicken Sie auf der Registerkarte "Berichte" unter "Berichtgruppen" auf "Anstehende aufrufen".

So bearbeiten Sie einen benutzerdefinierten Bericht

Klicken Sie auf der Registerkarte "Berichte" unter "Berichtgruppen" auf "Benutzerdefiniert".

- 2 Klicken Sie mit der rechten Maustaste auf den Bericht, den Sie ausführen möchten, und klicken Sie dann auf "Bearbeiten".
- 3 Bearbeiten Sie die Berichtseigenschaften und klicken Sie dann auf "OK".

Erneutes Ausführen eines abgeschlossenen Berichts

Berichte, die in der Berichtgruppe "Abgeschlossene aufrufen" angezeigt werden, können mehrfach ausgeführt werden.

So führen Sie einen abgeschlossenen Bericht erneut aus

- 1** Klicken Sie auf der Registerkarte "Berichte" unter "Berichtgruppen" auf "Abgeschlossene aufrufen".
- 2** Klicken Sie mit der rechten Maustaste auf einen Bericht und klicken Sie dann auf "Bericht jetzt erneut ausführen".

Backup Exec erstellt eine weitere Iteration des Berichts und führt sie aus.
- 3** Um den Bericht erneut anzuzeigen, doppelklicken Sie auf den neuen Bericht.

Löschen eines Berichts

Berichte, die Sie unter Verwendung der Option "Jetzt ausführen" erstellen, werden automatisch gelöscht, nachdem Sie sie angezeigt haben. Jedoch können auch benutzerdefinierte Berichte, abgeschlossene Berichte und geplante Berichte zu Ihrer Bequemlichkeit gelöscht werden.

Hinweis: Standard-Backup Exec-Berichte können nicht gelöscht werden.

So löschen Sie einen Bericht

- 1** Führen Sie auf der Registerkarte "Berichte" unter "Berichtgruppen" einen der folgenden Schritte aus:
 - Um einen benutzerdefinierten Bericht zu löschen, klicken Sie auf "Benutzerdefiniert".
 - Um einen geplanten Bericht zu löschen, klicken Sie auf "Anstehende aufrufen".
 - Um einen abgeschlossenen Bericht zu löschen, klicken Sie auf "Abgeschlossene aufrufen".
- 2** Klicken Sie mit der rechten Maustaste auf den Bericht, den Sie löschen möchten, und klicken Sie dann auf "Löschen".
- 3** Klicken Sie auf "Ja", um zu bestätigen, dass Sie den Bericht löschen möchten.

Festlegen der Standards für Standard- und benutzerdefinierte Berichte

Sie können Backup Exec so einstellen, dass alle Berichte entweder in HTML oder in PDF (Portable Document Format von Adobe) angezeigt werden. Die Standardeinstellung ist HTML. Das von Ihnen ausgewählte Format wirkt sich nicht

auf das Format der mithilfe der Benachrichtigungsfunktion an Benutzer gesendeten Berichte aus.

Für benutzerdefinierte Berichte können Sie folgende Schritte durchführen:

- Einbinden eines Logos in die Kopfzeile
- Wählen einer Farbe für das Banner in der Kopfzeile
Bei der Auswahl einer Farbe für das Banner können Sie die der jeweiligen Farbe entsprechende Nummer eingeben (RGB-Werte) oder die Farbe aus einer Tabelle auswählen.
- Einbinden von Text in der Fußzeile
- Einbinden der Uhrzeit in der Fußzeile

So stellen Sie Standards für Standard- und benutzerdefinierte Berichte ein

- 1** Klicken Sie auf die Schaltfläche "Backup Exec" und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Backup Exec-Einstellungen".
- 2** Klicken Sie im linken Teilfenster auf "Berichte".

3 Schließen Sie die Auswahl der passenden Optionen ab.

So wählen Sie ein Standard-Listenformat für Standard- und benutzerdefinierte Berichte aus	Unter "Berichtsformat" wählen Sie entweder "HTML" oder "PDF" aus.
So begrenzen Sie die Zeilenanzahl, die in benutzerdefinierten Berichten aufgeführt werden können	Geben Sie unter "Berichtsinhalte" in "Max. Anzahl von Zeilen in einem Bericht" die entsprechende Zahl ein.
So aktivieren Sie, dass in Standard- und benutzerdefinierten Berichten alle erzeugten Daten (auch duplizierte) angezeigt werden	Unter "Berichtsinhalte" klicken Sie auf "Alle Zeilen anzeigen".
So aktivieren Sie, dass in Standard- und benutzerdefinierten Berichten nur eindeutige Daten angezeigt werden	Unter "Berichtsinhalte" klicken Sie auf "Eindeutige Zeilen anzeigen".
So fügen Sie der Kopfzeile von benutzerdefinierten Berichten ein Logo hinzu	Aktivieren Sie unter "Kopfzeile" "Benutzerdefinierte Bilddatei verwenden" und geben Sie dann den Pfad zu der Bilddatei ein, die Sie verwenden möchten.
So passen Sie die Farben der Kopfzeile von benutzerdefinierten Berichten an	Geben Sie unter "Bannerfarbe" entweder die Nummern, die den Farben entsprechen, die Sie verwenden wollen, ein oder klicken Sie auf "Farben", um eine Farbe von einem Diagramm auszuwählen.
So schließen Sie Standardtext oder -Zeit in der Fußzeile von benutzerdefinierten Berichten ein	Unter "Fußzeile" im Feld "Text" geben Sie den Standardtext ein, der auf jedem benutzerdefinierten Bericht angezeigt werden soll. Wenn die Zeit des Berichts in der Fußzeile eingeschlossen werden soll, muss "Uhrzeit angeben" aktiviert sein.

4 Klicken Sie auf "OK".

Anzeigen der Berichtseigenschaften

Berichtseigenschaften liefern ausführliche Informationen über jeden Bericht, wie zum Beispiel den Dateinamen, die Dateigröße und das Berichterstellungsdatum. Diese Eigenschaften können zwar angezeigt, jedoch nicht bearbeitet werden.

So zeigen Sie Berichtseigenschaften an

- 1 Wählen Sie auf der Registerkarte "Berichte" unter "Berichtgruppen" eine Berichtgruppe aus.
- 2 Klicken Sie mit der rechten Maustaste auf den Bericht, dessen Eigenschaften angezeigt werden sollen, und wählen Sie "Eigenschaften".
- 3 Wenn Sie das Dialogfeld wieder schließen möchten, klicken Sie auf "OK".

Liste von Backup Exec-Standardberichten

Dieser Abschnitt liefert ausführliche Information über jeden Standardbericht, der in Backup Exec verfügbar ist. Die Daten, die auf jedem Bericht angezeigt werden, hängen von den Kriterien ab, die Sie für den Bericht ausgewählt haben..

Backup Exec enthält die folgenden Standardberichte:

Tabelle 16-3 Backup Exec-Standardberichte

Name des Berichts	Beschreibung
Meldungsverlauf	Listet alle Warnmeldungen im Warnmeldungsverlauf chronologisch auf, wobei die neuesten Warnmeldungen zuerst angezeigt werden. Siehe "Bericht "Meldungsverlauf"" auf Seite 819.
Warnmeldungsverlauf nach Backup Exec-Server	Listet alle Warnmeldungen im Warnmeldungsverlauf nach Backup Exec-Servern sortiert und gefiltert auf. Die aktuellen Warnmeldungen werden dabei zuerst angezeigt. Siehe "Bericht "Warnmeldungsverlauf nach Backup Exec-Server"" auf Seite 820.
Überwachungsprotokoll	Listet den Inhalt aller Überwachungsprotokolle für ausgewählte Server im angegebenen Zeitraum auf. Siehe "Bericht "Überwachungsprotokoll"" auf Seite 821.
Erfolgsrate des Backups von Aufträgen	Listet die Erfolgsrate für die Backup-Aufträge auf, die zur Sicherung ausgewählter Server ausgeführt werden. Siehe "Bericht "Erfolgsrate von Backup-Aufträgen"" auf Seite 821.
Backup-Empfehlungen	Listet alle Empfehlungen auf, die Ihnen helfen können, Ihre Backups besser zu verwalten. Siehe "Bericht "Backup-Empfehlungen"" auf Seite 822.

Name des Berichts	Beschreibung
Erfolgsrate des Backups von Ressourcen	<p>Listet die Erfolgsrate der Backup-Aufträge für die angegebene Anzahl vergangener Tage für Ressourcen auf ausgewählten Servern auf.</p> <p>Siehe "Bericht "Erfolgsrate des Backups von Ressourcen" auf Seite 822.</p>
Backup-Sätze nach Mediensatz	<p>Listet alle Backup-Sätze nach Mediensätzen sortiert auf.</p> <p>Siehe "Bericht "Backup-Sätze nach Mediensatz" auf Seite 823.</p>
Backup-Größe nach Ressource	<p>Listet die Backup-Größe für jeden Ressourcenauftrag für bis zu sieben zuvor ausgeführte Aufträge auf und berechnet dann die durchschnittliche Größe für bis zu sieben Ausführungen eines Auftrags.</p> <p>Siehe "Bericht "Backup-Umfang nach Ressourcen geordnet" auf Seite 824.</p>
Cloud-Speicherübersicht	<p>Gibt einen Überblick über die Größe des Cloud-Speichervolumens, das von den gesicherten Daten auf dem Backup Exec-Server belegt wird.</p> <p>Siehe "Bericht "Cloud-Speicherübersicht" auf Seite 824.</p>
Täglicher Geräteeinsatz	<p>Listet den Prozentsatz der vom Backup Exec-Server genutzten Kapazität des Speichergeräts auf.</p> <p>Siehe "Bericht "Täglicher Geräteeinsatz" auf Seite 825.</p>
Übersicht zu Deduplizierungsgeräten	<p>Zeigt eine Übersicht der Deduplizierungsvorgänge für lokale Deduplizierungdatenträger und gemeinsam genutzte Deduplizierungdatenträger an.</p> <p>Siehe "Bericht "Zusammenfassung zu Deduplizierungsgeräten" auf Seite 826.</p>
Deduplizierungsübersicht	<p>Zeigt eine Deduplizierungsübersicht für alle Deduplizierungsaufträge an, die auf dem Backup Exec-Server ausgeführt werden.</p> <p>Siehe "Bericht "Zusammenfassung zur Deduplizierung" auf Seite 827.</p>

Name des Berichts	Beschreibung
Gerätezusammenfassung	Listet die Gerätenutzung und Fehlerübersicht für jeden ausgewählten Backup Exec-Server auf. Siehe " Bericht "Gerätezusammenfassung" " auf Seite 827.
Übersicht zum Datenträgerspeicher	Zeigt Statistiken zur Auslastung des plattenbasierten Speichers für Backup Exec-Server-Datenträgerspeicher an. Siehe " Bericht "Zusammenfassung zum Datenträgerspeicher" " auf Seite 828.
Fehlerbehandlungsregeln	Listet alle definierten Fehlerbehandlungsregeln auf. Siehe " Bericht "Fehlerbehandlungsregeln" " auf Seite 829.
Ereignisempfänger	Listet alle Ereignisse auf, die von jedem Benachrichtigungsempfänger erhalten wurden. Siehe " Bericht "Ereignisempfänger" " auf Seite 830.
Fehlgeschlagene Backup-Aufträge	Listet alle fehlgeschlagenen Backup-Aufträge nach Ressourcenserver und Zeitrahmen sortiert auf. Siehe " Bericht "Fehlgeschlagene Backup-Aufträge" " auf Seite 831.
Auftragszusammenfassung	Listet alle in den letzten 72 Stunden ausgeführten Aufträge in chronologischer Reihenfolge auf. Siehe " Bericht "Auftragszusammenfassung" " auf Seite 832.
Verwalteten Backup Exec-Server	Listet den Status und die Konfiguration für alle Backup Exec-Server auf, die durch einen zentralen Administrationsserver verwaltet werden. Siehe " Bericht "Verwaltete Backup Exec-Server" " auf Seite 833.
Medienüberwachung	Listet die aktuellsten Medienkonfigurationsänderungen auf. Siehe " Bericht "Medienüberwachung" " auf Seite 834.
Medienfehler	Listet die Anzahl der Fehler in allen Medien auf. Siehe " Bericht "Medienfehler" " auf Seite 835.

Name des Berichts	Beschreibung
Für Wiederherstellung erforderliche Medien	<p>Listet die Medien mit den Backup-Sätzen für jedes System auf, das im angegebenen Zeitraum auf den ausgewählten Servern gesichert wurde. Dieser Bericht enthält unter Umständen ungenaue Angaben, wenn die Medien aufgrund der Einstellungen für das Überschreiben von Medien überschrieben werden können.</p> <p>Siehe "Bericht "Für Wiederherstellung erforderliche Medien"" auf Seite 836.</p>
Medien-Zusammenfassung	<p>Listet alle Mediensätze und Medien auf, die auf Backup Exec-Servern verwendet werden. Für alle Medien wird der aktuelle Speicherort angegeben. Listet auch statistische Informationen zur Nutzung für Medien und den Medienspeicherort innerhalb von Backup Exec-Mediansätzen auf.</p> <p>Siehe "Bericht "Medienzusammenfassung"" auf Seite 836.</p>
Medienspeicherinhalt	<p>Listet die Medien auf, die sich in jedem Medienspeicher befinden.</p> <p>Siehe "Bericht "Medienspeicherinhalt"" auf Seite 837.</p>
Medien zum Speicher verschieben	<p>Listet alle Medien auf, die in einen Medienspeicher verschoben werden können. Die aufgeführten Medien befinden sich derzeit nicht in einem Medienspeicher. Darüber hinaus ist der Medienanhängezeitraum abgelaufen.</p> <p>Siehe "Bericht "Medien zum Speicher verschieben"" auf Seite 838.</p>
Vorgangsübersicht	<p>Listet Daten zu früheren und zukünftigen Vorgängen für einen benutzerdefinierten Zeitraum auf.</p> <p>Siehe "Bericht "Vorgangsübersicht"" auf Seite 839.</p>

Name des Berichts	Beschreibung
Nächtliche Zusammenfassung	<p>Listet die Ergebnisse der Backup-Aufträge für die einzelnen Ressourcen in den letzten 24 Stunden auf. Dieser Bericht enthält Backup-Aufträge, die laut Zeitplan ausgeführt werden sollten, jedoch nicht ausgeführt wurden. Aufträge werden erst 24 Stunden nach Ablauf der geplanten Zeit als überfällig gekennzeichnet.</p> <p>Siehe "Bericht "Nächtliche Zusammenfassung"" auf Seite 841.</p>
Problemdateien	<p>Listet alle Problemdateien auf, die für Aufträge berichtet werden. Die Dateien werden nach Tag und Ressource sortiert.</p> <p>Siehe "Bericht "Problemdateien"" auf Seite 842.</p>
Kürzlich beschriebene Medien	<p>Listet alle Medien auf, die in den letzten 24 Stunden geändert wurden.</p> <p>Siehe "Bericht "Kürzlich beschriebene Medien"" auf Seite 842.</p>
Validierungsübersicht "Wiederherstellung bereit"	<p>Listet die Backup-Sätze auf, für die die Aufträge zum Validieren eines virtuellen Computers für die Wiederherstellung ausgeführt werden.</p> <p>Siehe "Validierungsübersicht "Wiederherstellung bereit"" auf Seite 843.</p>
Kürzlich geschützte Ressourcen	<p>Zeigt eine Liste mit allen Auftragsdetailstatistiken und Ausnahmen an, die auf einem Backup Exec-Server, für den Sie diesen Bericht ausführen, aufgetreten sind.</p> <p>Siehe "Bericht "Kürzlich geschützte Ressourcen"" auf Seite 844.</p>
Ressourcenrisikoanalyse	<p>Listet die Auftragsinformationen für Ressourcen auf, auf denen der zuletzt ausgeführte Backup-Auftrag fehlgeschlagen ist. Die Daten werden nach Ressourcenserver gefiltert.</p> <p>Siehe "Bericht "Ressourcenrisikoanalyse"" auf Seite 845.</p>

Name des Berichts	Beschreibung
Wiederherstellungssatz-Details nach Ressource	<p>Listet alle Wiederherstellungssätze auf, die innerhalb der letzten 72 Stunden ausgeführt wurden. Die Sätze werden nach Server und Ressourcen sortiert.</p> <p>Siehe "Bericht "Wiederherstellungssatz-Details nach Ressource"" auf Seite 845.</p>
Medium aus Speicher abrufen	<p>Listet alle mehrfach verwendbaren Medien auf, die sich derzeit im angegebenen Speicher befinden.</p> <p>Siehe "Bericht "Medium aus Speicher abrufen"" auf Seite 846.</p>
Wechslerinventar	<p>Listet die Inhalte von Schächten in den Wechslern auf, die an den Backup Exec-Servern angeschlossen sind. Für alle Medien werden statistische Informationen zur Nutzung angezeigt.</p> <p>Siehe "Bericht "Wechslerinventar"" auf Seite 847.</p>
Geplante Serverarbeitslast	<p>Listet die geschätzte geplante Serverarbeitslast für den kommenden Zeitraum von 24 Stunden auf.</p> <p>Siehe "Bericht "Geplante Serverarbeitslast"" auf Seite 848.</p>
Verfügbarkeit temporärer Medien	<p>Zeigt die Verteilung von Medien an. Zeigt an, wie viele Medien zum Überschreiben verfügbar sind und zu welchem Zeitpunkt andere Medien zum Überschreiben verfügbar werden.</p> <p>Siehe "Bericht "Verfügbarkeit temporärer Medien"" auf Seite 849.</p>
Probelaufergebnisse	<p>Listet die Ergebnisse der Probelaufaufträge für den ausgewählten Zeitraum und die ausgewählten Backup Exec-Server auf.</p> <p>Siehe "Bericht "Probelaufergebnisse"" auf Seite 849.</p>

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Meldungsverlauf"

Im Bericht "Warnmeldungsverlauf" sind alle Meldungen im Warnmeldungsverlauf chronologisch aufgeführt. Die neuesten Meldungen werden dabei zuerst angezeigt.

Tabelle 16-4 Bericht "Meldungsverlauf"

Element	Beschreibung
Uhrzeit	Datum und Uhrzeit der Warnmeldung.
Erhalten	Zeitpunkt, an dem die Warnmeldung aufgetreten ist.
Beantwortet	Uhrzeit der Reaktion des Benutzers auf die Warnmeldung.
Antwortender Benutzer	Benutzer, der auf die Warnmeldung reagiert hat.
Auftragsname	Zeigt den Namen des Auftrags an, der mit der Warnmeldung verknüpft ist.
Backup Exec-Server	Name des Backup Exec-Servers, auf dem die Warnmeldung auftrat.
Kategorie	Name der Warnmeldung, z. B. "Dienststart" oder "Auftrag fehlgeschlagen".
Meldung	Eine Beschreibung des Ereignisses, das die Warnmeldung verursachte.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Warnmeldungsverlauf nach Backup Exec-Server"

Im Bericht "Warnmeldungsverlauf nach Backup Exec-Server" sind alle Warnmeldungen im Warnmeldungsverlauf nach Backup Exec-Servern gefiltert und sortiert aufgeführt. Die aktuellen Warnmeldungen werden dabei zuerst angezeigt.

Tabelle 16-5 Bericht "Warnmeldungsverlauf nach Backup Exec-Server"

Element	Beschreibung
Backup Exec-Server	Name des Backup Exec-Servers, auf dem die Warnmeldung auftrat.
Uhrzeit	Datum und Uhrzeit der Warnmeldung.
Erhalten	Zeitpunkt, an dem die Warnmeldung aufgetreten ist.
Beantwortet	Uhrzeit der Reaktion des Benutzers auf die Warnmeldung.
Antwortender Benutzer	Benutzer, der auf die Warnmeldung reagiert hat.

Element	Beschreibung
Auftragsname	Name des Auftrags, der mit der Empfehlung verknüpft ist.
Kategorie	Name der Warnmeldung, z. B. "Dienststart" oder "Auftrag fehlgeschlagen".
Meldung	Beschreibt das Ereignis, das zur Warnmeldung geführt hat.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Überwachungsprotokoll"

Im Bericht "Überwachungsprotokoll" ist der Inhalt der Überwachungsprotokolle für ausgewählte Server im angegebenen Zeitraum aufgeführt.

Tabelle 16-6 Bericht "Überwachungsprotokoll"

Element	Beschreibung
Kategorie	Kategorie, in der eine Änderung vorgenommen wurde, z. B. "Login-Konto", "Warnmeldungen" oder "Auftrag".
Eingegebenes Datum	Zeitpunkt (Datum und Uhrzeit), an dem die Änderung vorgenommen wurde.
Meldung	Beschreibung der Änderung, die in Backup Exec vorgenommen wurde.
Benutzername	Benutzer, der die Änderung vorgenommen hat

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Erfolgsrate von Backup-Aufträgen"

Im Bericht "Erfolgsrate von Backup-Aufträgen" wird die Erfolgsrate von Backup-Aufträgen aufgeführt.

Tabelle 16-7 Bericht "Erfolgsrate von Backup-Aufträgen"

Element	Beschreibung
Server	Name des Servers, der gesichert wird.
Datum	Datum, an dem der Backup-Auftrag verarbeitet wurde.

Element	Beschreibung
Aufträge insgesamt	Gesamtanzahl der Aufträge, die durch den Backup Exec-Server verarbeitet wurden.
Erfolgreich	Gesamtanzahl der Aufträge, die durch den Backup Exec-Server erfolgreich ausgeführt werden.
Erfolgsrate	Prozentsatz erfolgreicher Aufträge, die durch den Backup Exec-Server verarbeitet wurden.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Backup-Empfehlungen"

Die Backup-Empfehlungsbericht listet Empfehlungen auf, die Ihnen helfen können, Ihre Backups besser zu verwalten. Die Empfehlungen umfassen möglicherweise bessere Methoden, bestimmte Typen von Daten zu sichern, oder Vorschläge, wie Sie andere Produkte verwenden.

Tabelle 16-8 Bericht "Backup-Empfehlungen"

Element	Beschreibung
Backup Exec-Server	Name des Backup Exec-Servers, für den die Empfehlung gilt.
Auftragsname	Name des Auftrags, der mit der Empfehlung verknüpft ist.
Startzeit	Datum und Uhrzeit, als der Auftrag, der mit der Empfehlung verknüpft ist, ausgeführt wurde.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Erfolgsrate des Backups von Ressourcen"

Im Bericht "Erfolgsrate des Backups von Ressourcen" ist die Erfolgsrate der Backup-Aufträge für die angegebenen Tage für Ressourcen auf ausgewählten Servern aufgeführt.

Tabelle 16-9 Bericht "Erfolgsrate des Backups von Ressourcen"

Element	Beschreibung
Ressource	Name des Systems, das gesichert wird.
Datum	Datum, an dem der Backup-Auftrag verarbeitet wurde.
Aufträge insgesamt	Gesamtanzahl der Aufträge, die durch den Backup Exec-Server verarbeitet wurden.
Erfolgreich	Gesamtanzahl der Aufträge, die durch den Backup Exec-Server erfolgreich ausgeführt werden.
Erfolgsrate	Prozentsatz erfolgreicher Aufträge, die durch den Backup Exec-Server verarbeitet wurden.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Backup-Sätze nach Mediensatz"

Im Bericht "Backup-Sätze nach Mediensatz" sind alle Backup-Sätze nach Mediensätzen sortiert aufgeführt.

Tabelle 16-10 Bericht "Backup-Sätze nach Mediensatz"

Element	Beschreibung
Mediensatz	Name des Mediensatzes, auf dem der Auftrag ausgeführt wurde.
Medienkennung	Medienkennung, die von Backup Exec oder dem Administrator zugewiesen wurde bzw. in einer zuvor zugewiesenen Barcodekennung enthalten ist.
Methode	Spezifische Art des Backups.
Geschäftskritisch	Gibt an, ob der Backup-Satz ein Element enthält, das als geschäftskritische Ressource gekennzeichnet wurde.
Datum/Uhrzeit	Datum und Uhrzeit des Daten-Backup.
Beschreibung des Backup-Satzes/Quelle	Angaben zu den gesicherten Daten und zu deren Speicherort.
Verzeichnisse	Anzahl der gesicherten Verzeichnisse.
Dateien	Anzahl der gesicherten Dateien.

Element	Beschreibung
Größe	Menge Daten, die gesichert wurden.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Backup-Umfang nach Ressourcen geordnet"

Im Bericht "Backup-Umfang nach Ressourcen geordnet" ist der Backup-Umfang für alle Ressourcenaufträge für bis zu sieben zuvor ausgeführte Aufträge aufgeführt. Darüber hinaus wird der Durchschnittswert berechnet, der die durchschnittliche Menge der zu sichernden Daten in den sieben zuvor ausgeführten Aufträgen angibt.

Tabelle 16-11 Bericht "Backup-Umfang nach Ressourcen geordnet"

Element	Beschreibung
Server	Name des Backup Exec-Servers, auf dem die Daten für den Backup-Auftrag gespeichert wurden.
Ressource	Name des Servers, der gesichert wurde.
Auftrag	Name des Backup-Auftrags.
Datum und Uhrzeit der Auftragsausführung	Zeitpunkt (Datum und Uhrzeit), an dem der Backup-Auftrag verarbeitet wurde.
Backup-Größe	Menge Daten, die gesichert wurden.
Durchschnittliche Größe	Durchschnittliche Menge Daten, die während der vorherigen sieben Ausführungen gesichert wurden.
Differenz %	Der Wert, um den sich die im aktuellen Auftrag zu sichernden Daten von vorherigen Backup-Aufträgen unterscheiden.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Cloud-Speicherübersicht"

Der Bericht "Cloud-Speicherübersicht" gibt einen Überblick über die Größe des Cloud-Speichervolumens, das von den gesicherten Daten auf dem Backup Exec-Server belegt wird.

Tabelle 16-12 Bericht "Cloud-Speicherübersicht"

Element	Beschreibung
Gerätename	Der Name des Cloud-Speichergeräts.
Cloud-Speicher-Server	Der vollqualifizierte Name des Servers, auf dem sich das Gerät befindet.
Cloud-Bucket	Der Name des Speicherorts auf dem Cloud-Speichergerät. Diese Speichereinheiten werden als "Buckets" bezeichnet.
Geschriebene Byte	Die Menge der Daten, die auf das Cloud-Speichergerät geschrieben wurden.
Gelesene Byte	Die Menge der Daten, die aus dem Cloud-Speichergerät ausgelesen wurden.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Täglicher Geräteeinsatz"

Dieser Bericht listet den Prozentsatz der vom Backup Exec-Server genutzten Kapazität des Speichergeräts auf.

Tabelle 16-13 Bericht "Täglicher Geräteeinsatz"

Element	Beschreibung
Laufwerkname	Name des Speichergeräts und des Backup Exec-Servers, auf dem sich das Gerät befindet.
Status	<p>Status des Speichergeräts</p> <p>Status für Speichergeräte sind wie folgt:</p> <ul style="list-style-type: none"> ■ Anhalten Das Speichergerät wird vorübergehend angehalten. ■ Aktivieren Die Speichergruppe ist für die Verwendung durch Backup Exec verfügbar. Wenn das Speichergerät deaktiviert ist, ist es für die Verwendung mit anderen Anwendungen verfügbar. ■ Online Die Speichergruppe ist für die Verwendung verfügbar. ■ Offline Backup Exec kann nicht auf die Speichergruppe zugreifen.
Datum	Datum, an dem das Speichergerät verwendet wurde.

Element	Beschreibung
Aufträge	Anzahl der Aufträge, die durch das Speichergerät des Backup Exec-Servers verarbeitet wurden.
Größe	Die Datenmenge, die vom Speichergerät des Backup Exec-Servers verarbeitet wurde.
Auslastung (%)	Prozentsatz der Geräteauslastung.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Zusammenfassung zu Deduplizierungsgeräten"

Der Übersichtsbericht zum Deduplizierungsgerät zeigt eine Übersicht der Deduplizierungsvorgänge des lokalen Deduplizierungdatenträgerspeichers und des gemeinsam genutzten Deduplizierungdatenträgerspeichers an.

Tabelle 16-14 Übersichtsbericht zu Deduplizierungsgeräten

Element	Beschreibung
Status	Gerätezustand (z. B. "Online" und "Aktiviert").
Erstellt	Erstellungsdatum der Medien.
Gesamtkapazität	Gesamtkapazität des Deduplizierungdatenträgers.
Kapazität genutzt	Die Kapazität, die momentan im Deduplizierungsspeicher genutzt wird.
Verfügbare Kapazität	Verbleibende Kapazität des Deduplizierungdatenträgers.
Vollständig (Prozent)	Prozentsatz des Speicherplatzes, der im Deduplizierungdatenträger verfügbar ist.
Anzahl geschützter Byte	Gesamtmenge der Daten, die für Backups in allen Aufträgen unter Verwendung des Geräts ausgewählt wurden, bevor die Deduplizierung erfolgt.
Deduplizierungs-Verhältnis	Das Verhältnis der Datenmenge vor der Deduplizierung und der Datenmenge nach der Deduplizierung.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Zusammenfassung zur Deduplizierung"

Dieser Bericht enthält eine Übersicht aller Deduplizierungsaufträge, die auf dem Backup Exec-Server ausgeführt werden.

Tabelle 16-15 Bericht "Zusammenfassung zur Deduplizierung"

Element	Beschreibung
Auftragsname	Name des Auftrags.
Startzeit	Zeitpunkt, zu dem Backup Exec versucht hat, den Auftrag zu starten.
Dauer	Der für den Verarbeitungsvorgang erforderliche Zeitraum.
Größe	Die Menge an verarbeiteten Daten.
Größe/Minute	Die pro Minute verarbeitete Datenmenge in KB, Megabyte oder Gigabyte.
Anzahl gescannter Byte	Gesamtmenge der für das Backup ausgewählten Daten in Megabyte vor der Deduplizierung.
Anzahl gespeicherter Byte	Die Menge der eindeutigen Daten, die nach erfolgter Deduplizierung gespeichert wird.
Deduplizierungs-Verhältnis	Das Verhältnis der Datenmenge vor der Deduplizierung und der Datenmenge nach der Deduplizierung.
Status	Status des Vorgangs, z. B. "Abgeschlossen" (Erfolg), "Fehlgeschlagen" oder "Abgebrochen".

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Gerätezusammenfassung"

Im Bericht "Gerätezusammenfassung" sind alle Geräte für jeden ausgewählten Backup Exec-Server aufgeführt.

Tabelle 16-16 Bericht "Gerätezusammenfassung"

Element	Beschreibung
Server	Name des Servers, auf dem sich das Gerät befindet.
Laufwerkname	Name des Laufwerks im Wechsler.
Ziel	Adresse des Speichergeräts, das zum Backup Exec-Server eine Verbindung hergestellt hat.
Status	Gerätestatus, z. B. "Online".
Erstellt	Erstellungsdatum des Datenträgers.
Gereinigt	Datum, an dem auf dem Laufwerk der letzte Reinigungsauftrag ausgeführt wurde.
Stunden	Anzahl der Stunden, die das Gerät seit dem letzten Reinigungsauftrag in Betrieb war.
Fehler	Anzahl der Fehler seit dem letzten Reinigungsauftrag.
Größe	Menge Daten, die seit dem letzten Reinigungsauftrag gelesen und geschrieben wurden.
Geladen	Anzahl der Ladevorgänge seit dem letzten Reinigungsauftrag.
Stunden	Gesamtanzahl der Stunden, die das Gerät verwendet wurde.
Fehler	Gesamtanzahl der im Gerät aufgetretenen Fehler.
Größe	Menge Daten, die auf dem Gerät gelesen und geschrieben wurden.
Geladen	Gesamtanzahl der Ladevorgänge für das Gerät.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Zusammenfassung zum Datenträgerspeicher"

Der Übersichtsbericht zum Datenträgerspeicher zeigt Statistiken zur Datenträgerbelegung für den Datenträgerspeicher von Backup Exec-Servern an.

Tabelle 16-17 Übersichtsbericht zum Datenträgerspeicher

Element	Beschreibung
Gerätename	Name des Datenträgerspeichergeräts.

Element	Beschreibung
Status	<p>Der Zustand des Geräts.</p> <p>Die folgenden Gerätezustände sind möglich:</p> <ul style="list-style-type: none"> ■ Online ■ Aktiviert ■ Offline ■ Angehalten ■ Deaktiviert
Lokaler Zugriffspfad	Pfad auf dem Datenträger, unter dem Backup-Daten gespeichert werden.
Gesamtkapazität	Gesamte Kapazität des Datenträgers.
Belegter Speicher	Der als Speicher verwendete Festplattenspeicher.
Freier Speicherplatz	Der verbleibende Speicherplatz.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Fehlerbehandlungsregeln"

Im Bericht "Fehlerbehandlungsregeln" sind alle Fehlerbehandlungsregeln aufgeführt und erläutert.

Tabelle 16-18 Bericht "Fehlerbehandlungsregeln"

Element	Beschreibung
Name der Regel	Name der Fehlerbehandlungsregel.
Hinweise	Die bei der Erstellung der Fehlerbehandlungsregel im Bereich "Hinweis" eingegebenen Informationen.
Auftragsstatus	<p>Endgültiger Auftragsstatus, mit dem die Regel aktiviert wird.</p> <p>Folgende Statusangaben sind verfügbar:</p> <ul style="list-style-type: none"> ■ Fehler ■ Abgebrochen

Element	Beschreibung
Fehlerkategorie	<p>Die Fehlerkategorie, auf die die Regel angewendet wird.</p> <p>Folgende Fehlerkategorien stehen zur Wahl:</p> <ul style="list-style-type: none"> ■ Gerät ■ Auftrag ■ Medien ■ Netzwerk ■ Sonstiges ■ Ressource ■ Sicherheit ■ Server ■ System
Aktiviert	Zeigt an, ob die Regel aktiviert oder deaktiviert ist.
Auftrag abbrechen	Wenn diese Option für die Fehlerbehandlungsregel ausgewählt ist, wird ein X angezeigt. Bei dieser Option werden alle Aufträge abgebrochen, wenn die maximale Anzahl von Wiederholungsversuchen erreicht wurde.
Auftrag anhalten	Wenn diese Option für die Fehlerbehandlungsregel ausgewählt ist, wird ein X angezeigt. Mit dieser Option wird die Ausführung des Auftrags in Backup Exec unterbrochen, bis der Fehler manuell behoben wurde.
Auftrag wiederholen	Wenn diese Option für die Fehlerbehandlungsregel ausgewählt ist, wird ein X angezeigt. Mit dieser Option wird der Auftrag in Backup Exec neu gestartet.
Max. Anzahl der Wiederholungen	Anzahl der Versuche, den Auftrag erneut zu starten.
Wiederholungsintervall (Minuten)	Anzahl der Minuten, die Backup Exec wartet, bevor es versucht, den Auftrag wieder auszuführen.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Ereignisempfänger"

Im Bericht "Ereignisempfänger" sind die von jedem Benachrichtigungsempfänger registrierten Ereignisse aufgeführt.

Tabelle 16-19 Bericht "Ereignisempfänger"

Element	Beschreibung
Empfängername	Name des Empfängers.
Empfängertyp	Kennzeichnet, an wen der Ereignisempfängerbericht gesendet wird, zum Beispiel an einen einzelnen Empfänger oder an eine Gruppe von Empfängern.
Ereignistyp	Warnmeldungskategorie oder Ad-hoc-Auftrag.
Ereignisname	Ausführliche Angaben zur Warnmeldungskategorie oder zum Ad-hoc-Auftrag.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Fehlgeschlagene Backup-Aufträge"

Der Bericht "Fehlgeschlagene Backup-Aufträge" listet alle fehlgeschlagenen Backup-Aufträge auf. Die Aufträge sind nach Server und festgelegtem Zeitraum geordnet.

Tabelle 16-20 Bericht "Fehlgeschlagene Aufträge"

Element	Beschreibung
Ressource	Name des Systems, das gesichert wird.
Startzeit	Zeitpunkt (Datum und Uhrzeit), an dem der Backup-Auftrag gestartet wurde.
Dauer	Der für den Verarbeitungsvorgang erforderliche Zeitraum.
Auftragsname	Name des fehlgeschlagenen Auftrags.
Geschäftskritisch	Gibt an, ob der Auftrag Elemente enthält, die als geschäftskritische Ressourcen gekennzeichnet wurden.
Kategorie	Die Kategorie des fehlgeschlagenen Auftrags, der auf einen System-, Auftrags-, Medien- oder Gerätefehler zurückzuführen ist.
Fehlercode	Zeigt den Fehlercode an, der dem Fehler entspricht.
Beschreibung	Beschreibt das Ereignis, das zur Fehlermeldung geführt hat.
Status	Status des Vorgangs, z. B. "Fehler".

Element	Beschreibung
Gerätename	Der Name des Geräts, auf dem der Auftrag ausgeführt wurde.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Auftragszusammenfassung"

Im Bericht "Auftragszusammenfassung" sind alle Aufträge aufgeführt, die im angegebenen Zeitraum ausgeführt wurden. Die Aufträge werden in chronologischer Reihenfolge angezeigt.

Tabelle 16-21 Bericht "Auftragszusammenfassung"

Element	Beschreibung
Startzeit	Zeitpunkt (Datum und Uhrzeit), an dem der Vorgang gestartet wurde.
Auftragsname	Name des abgeschlossenen Auftrags.
Dauer	Verarbeitungszeitraum des Vorgangs
Größe	Die Menge an verarbeiteten Daten.
Dateien	Anzahl der verarbeiteten Dateien.
Verzeichnisse	Anzahl der verarbeiteten Verzeichnisse.
Größe/Minute	Die pro Minute verarbeitete Datenmenge in KB, Megabyte oder Gigabyte.
Übersprungen	Anzahl Dateien, die während des Vorgangs übersprungen wurden.
Beschädigte Dateien	Anzahl beschädigter Dateien, die während des Vorgangs angetroffen wurden.
Dateien in Gebrauch	Anzahl der Dateien, die während des Vorgangs verwendet wurden.
Status	Status des Vorgangs, z. B. "Abgeschlossen" (Erfolg), "Fehlgeschlagen" oder "Abgebrochen".
Typ	Listet den Typ des Auftrags auf, den Backup Exec im angegebenen Zeitraum ausgeführt hat.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Verwaltete Backup Exec-Server"

Der Bericht "Verwaltete Backup Exec-Server" beinhaltet Status- und Konfigurationsinformationen für alle verwalteten Backup Exec-Server in einer Central Admin Server Feature-Umgebung.

Tabelle 16-22 Bericht "Verwaltete Backup Exec-Server"

Element	Beschreibung
CAS-Server	Namen der zentralen Administrationsserver.
Verwalteter Backup Exec-Server	Namen der verwalteten Backup Exec-Server.
Status	<p>Status des Servers.</p> <p>Folgende Statusmeldungen sind verfügbar:</p> <ul style="list-style-type: none"> ■ Online - Server kann verwendet werden. ■ Verzögert - Server reagiert nicht sofort auf Meldungen. ■ Keine Verbindung - Verbindung mit dem Server ist seit einer gewissen Zeit unterbrochen.
Verzögert	Zeitlimit, das für den Verbindungsstatus "Verzögert" festgelegt wurde.
Keine Verbindung	Zeitlimit, das für den Verbindungsstatus "Keine Verbindung" festgelegt wurde.
Katalogspeicherort	<p>Speicherort der Kataloginformationen.</p> <p>Folgende Speicherorte sind verfügbar:</p> <ul style="list-style-type: none"> ■ Lokal - die Kataloginformationen befinden sich auf dem verwalteten Backup Exec-Server. ■ CAS: die Kataloginformationen befinden sich auf dem zentralen Administrationsserver.
Protokolle	<p>Der Zeitpunkt, an dem die Auftragsprotokolle von einem verwalteten Server in die CAS-Datenbank geladen werden.</p> <p>Die Ladezeiten ergeben sie sich wie folgt:</p> <ul style="list-style-type: none"> ■ Festgelegter Zeitraum in Sekunden ■ Geplante Zeit ■ Auftragsabschluss ■ Nie

Element	Beschreibung
Verlauf	<p>Der Zeitpunkt, an dem der Auftragsverlauf von einem verwalteten Server in die CAS-Datenbank geladen wird.</p> <p>Die Ladezeiten ergeben sie sich wie folgt:</p> <ul style="list-style-type: none"> ■ Festgelegter Zeitraum in Sekunden ■ Geplante Zeit ■ Auftragsabschluss ■ Nie
Status	<p>Der Zeitpunkt, an dem der Status von einem verwalteten Server in die CAS-Datenbank geladen wird.</p> <p>Die Ladezeiten ergeben sie sich wie folgt:</p> <ul style="list-style-type: none"> ■ Festgelegter Zeitraum in Sekunden ■ Geplante Zeit ■ Auftragsabschluss ■ Nie
Meldung anzeigen	<p>Zeigt "Ja" an, wenn Sie eine Warnmeldung konfiguriert haben, für den Fall, dass der Zeitunterschied zwischen den Serveruhren des zentralen Administrationsservers und des verwalteten Backup Exec-Servers einen voreingestellten Wert (maximaler Toleranzwert für Zeitunterschied) überschreitet.</p>
s	<p>Maximaler Toleranzwert für Zeitunterschied in Sekunden, der für einen Server festgelegt wurde.</p>

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Medienüberwachung"

Im Bericht "Medienüberwachung" sind die aktuellen Konfigurationsänderungen aufgeführt, die an Ihren Medien vorgenommen wurden.

Wenn Sie in einer Central Admin Server Feature-(CAS-)Umgebung diesen Bericht vom zentralen Administrationsserver ausführen, liefert der Bericht nur Daten für die Medien für den zentralen Administrationsserver; er liefert keine Daten für die verwalteten Backup Exec-Server. Um Daten der Medienüberwachung auch für verwaltete Backup Exec-Server abzurufen, haben Sie folgende Möglichkeiten:

- Loggen Sie sich lokal beim verwalteten Backup Exec-Server ein und führen Sie den Bericht aus.

- Loggen Sie sich mithilfe der Funktion "Remote Administrator" von einem Remote-Windows-Server oder einer Windows-Arbeitsstation aus bei einem verwalteten Backup Exec-Server ein und führen Sie den Bericht aus.

Tabelle 16-23 Bericht "Medienüberwachung"

Element	Beschreibung
Eingegebenes Datum	Zeitpunkt (Datum und Uhrzeit), an dem die Änderung vorgenommen wurde.
Meldung	Beschreibung der Medienänderung
Benutzername	Benutzer, der die Änderung vorgenommen hat

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Medienfehler"

Der Bericht "Medienfehler" führt die Anzahl der Fehler in allen Medien auf.

Tabelle 16-24 Bericht "Medienfehler"

Element	Beschreibung
Medienkennung	Medienkennung, die von Backup Exec oder dem Administrator zugewiesen wurde bzw. in einer zuvor zugewiesenen Barcodekennung enthalten ist.
Geschäftskritisch	Gibt an, ob das Medium einen Backup-Satz enthält, der über eine geschäftskritische Ressource verfügt.
Geladen (Häufigkeit)	Gibt an, wie oft das Medium insgesamt bereitgestellt wurde.
Im Einsatz (Stunden insgesamt)	Gesamtanzahl der Stunden, die für das Medium benötigt wurden.
Fehler insgesamt	Gesamtanzahl Fehlerwarnmeldungen für das System, die Aufträge, die Medien und die Geräte.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Für Wiederherstellung erforderliche Medien"

Im Bericht "Für Wiederherstellung erforderliche Medien" sind die Medien mit den Backup-Sätzen für jedes System aufgeführt, das im angegebenen Zeitraum gesichert wurde. Dieser Bericht enthält jedoch unter Umständen ungenaue Angaben, wenn die Medien aufgrund der Einstellungen für das Überschreiben von Medien überschrieben werden können.

Tabelle 16-25 Bericht "Für Wiederherstellung erforderliche Medien"

Element	Beschreibung
Datum	Zeitpunkt (Datum und Uhrzeit), an dem der Backup-Auftragssatz erstellt wurde.
Name des Medienspeicherorts	Name des Speichergeräts, auf dem die für den Backup-Auftrag verwendeten Medien gespeichert werden.
Medienkennung	Medienkennung, die den Medien zugewiesen wird.
Geschäftskritisch	Gibt an, ob das Medium einen Backup-Satz enthält, der über eine geschäftskritische Ressource verfügt.
Wiederverwendungszeit	Zeigt den Zeitpunkt (Datum und Uhrzeit) an, ab dem das Medium überschrieben werden kann.
Backup-Methode	Spezifische Art des Backups.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Medienzusammenfassung"

Im Bericht "Medien-Zusammenfassung" sind alle Mediensätze und Medien aufgeführt, die auf Backup Exec-Servern verwendet wurden. Für alle Medien werden statistische Informationen zur Nutzung angezeigt.

Tabelle 16-26 Bericht "Medienzusammenfassung"

Element	Beschreibung
Medienkennung	Medienkennung, die von Backup Exec oder dem Administrator zugewiesen wurde bzw. in einer zuvor zugewiesenen Barcodekennung enthalten ist.
Medientyp	Typ der Medienkassette, z. B. "4 MM".

Element	Beschreibung
Zugewiesen	Datum, an dem das Medium als Ergebnis eines Überschreibvorgangs einem Mediensatz zugeordnet wurde.
Verändert	Datum, an dem zuletzt Daten auf das Medium geschrieben wurden.
Geschäftskritisch	Gibt an, ob das Medium einen Backup-Satz enthält, der über eine geschäftskritische Ressource verfügt.
Stunden	Gesamtanzahl der Stunden, die das Medium in Verwendung war.
Ladevorgänge	Gibt an, wie oft das Medium insgesamt bereitgestellt wurde.
Behebbarer Fehler	Anzahl behebbarer Lesefehler.
Nicht behebbarer Fehler	Anzahl nicht behebbarer Lesefehler.
Schreibgröße	Menge an Daten, die auf das Medium geschrieben wurde.
Aktuelle Größe	Schätzung der Menge von Daten, die sich derzeit auf dem Medium befinden.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Medienspeicherinhalt"

Im Bericht "Medienspeicherinhalt" sind alle Medien in einem bestimmten Medienspeicher aufgeführt.

Tabelle 16-27 Bericht "Medienspeicherinhalt"

Element	Beschreibung
Speichernamen	Speicherort des Mediums.
Medienkennung	Medienkennung, die von Backup Exec oder dem Administrator zugewiesen wurde bzw. in einer zuvor zugewiesenen Barcodeerkennung enthalten ist.
Enddatum für Überschreibschutz	Datum, ab dem die Daten auf dem Medium überschrieben werden können.
Speichermedienregel-Verschiebungsdatum	Datum, an dem das Medium in den Speicher verschoben werden kann.
Mediensatz	Name des Mediensatzes, dem dieses Medium zugeordnet ist.

Element	Beschreibung
Speichermedienregelname	Name der Speichermedienregel.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Medien zum Speicher verschieben"

Im Bericht "Medien zum Speicher verschieben" sind alle Medien aufgeführt, die in einen Medienspeicher verschoben werden können.

Die aufgeführten Medien befinden sich derzeit nicht in einem Medienspeicher und erfüllen eines der folgenden Kriterien:

- Das festgelegte Datum zum Verschieben der Medien in den Speicher wurde eingehalten oder überschritten.
- Der Anhängezeitraum ist abgelaufen, der Überschreibschutzzeitraum ist jedoch weiterhin aktuell (zugewiesen).

Tabelle 16-28 Bericht "Medien zum Speicher verschieben"

Element	Beschreibung
Backup Exec-Server	Name des Backup Exec-Servers, auf dem die Daten für den Backup-Auftrag gespeichert wurden.
Mediensatz	Name des Mediensatzes.
Medienkennung	Medienkennung, die von Backup Exec oder dem Administrator zugewiesen wurde bzw. in einer zuvor zugewiesenen Barcodekennung enthalten ist.
Speicherort	Speicherort des Mediums.
Enddatum des Anhängezeitraums	Datum, ab dem keine Daten mehr zum Medium hinzugefügt werden können.
Enddatum für Überschreibschutz	Datum, ab dem die Daten auf dem Medium überschrieben werden können.
Speichermedienregel-Verschiebungsdatum	Datum, an dem das Medium in den Speicher verschoben werden kann.
Speichername	Name des Speichers, in den das Medium verschoben werden soll.
Speichermedienregelname	Name der Speichermedienregel.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Vorgangsübersicht"

Im Bericht "Vorgangsübersicht" sind Details zu früheren und zukünftigen Backup Exec-Vorgängen aufgeführt.

Tabelle 16-29 Bericht "Vorgangsübersicht"

Element	Beschreibung
"Zusammenfassung abgeschlossener Aufträge: x Stunden"	Zeigt Informationen zur Backup Exec-Auftragsaktivität für den angegebenen Zeitraum an.
Fehler	Gesamtanzahl Fehlerwarnmeldungen für das System, die Aufträge, die Medien und die Geräte.
Warnungen	Gesamtanzahl Fehlerwarnmeldungen für die Aufträge, die Medien und die Geräte.
Informationen	Gesamtanzahl informativer Warnmeldungen für das System, die Aufträge, die Medien und die Geräte.
Bedienereingriff erforderlich	Gesamtanzahl der Warnmeldungen, auf die der Benutzer mit einer Antwort reagieren soll.
Abgeschlossen (fehlgeschlagen)	Gesamtanzahl der Aufträge, die fehlgeschlagen sind.
Abgeschlossen (abgebrochen)	Gesamtanzahl der Aufträge, die abgebrochen wurden.
Abgeschlossen (erfolgreich)	Gesamtanzahl der Aufträge, die erfolgreich abgeschlossen wurden.
Ausnahmen	Gesamtanzahl der Aufträge, die zwar erfolgreich abgeschlossen wurden, jedoch möglicherweise eine oder mehrere übergangene Dateien, beschädigte Dateien, von Viren infizierte Dateien oder gerade verwendete Dateien enthalten.
Insgesamt gesicherte Daten	Gesamtmenge an gesicherten Daten in Kilobyte, Megabyte oder Gigabyte.
Insgesamt verwendete Medien	Gesamtanzahl Medien, die verwendet wurden, um die abgeschlossenen Aufträge zu sichern.

Element	Beschreibung
Ausgelassen	Gesamtanzahl nicht eingehaltener Aufträge.
Wiederhergestellt	Gesamtanzahl wiederhergestellter Aufträge.
Aktive Aufträge	Gesamtanzahl der aktiven Aufträge.
Geplante Aufträge	Zeigt die Aufträge an, deren geplante Startzeiten innerhalb von 72 Stunden nach Erstellung des Auftrags beginnen. Aufträge mit wiederkehrenden Zeitplänen werden auch angezeigt, wenn deren Startzeiten innerhalb von 72 Stunden nach der letzten Startzeit des Auftrags anfangen.
Angehaltene Aufträge	Gesamtanzahl der angehaltenen Aufträge.
Auftragsstatus	Der Status der Aufträge.
Temporäre Medien	Gesamtanzahl der verfügbaren temporären Medien.
Weiterverwendbar	Gesamtanzahl der verfügbaren wiederverwendbaren Medien.
Importiert	Anzahl importierter Medien. Importierte Medien sind Medien, die mit anderen Produkten als dieser Backup Exec-Installation erstellt wurden.
Zugewiesen	Anzahl der zugewiesenen Medien (Medien, die zu einem Benutzermediensatz gehören).
Gesamte überschreibbare Medien	Gesamtanzahl der verfügbaren überschreibbaren Medien.
Gesamte anhängbare Medien	Gesamtanzahl der verfügbaren anhängbaren Medien.
Medien überschutze	Zeigt die Stufe des dem Medium zugewiesenen Überschreibschutzes an ("Vollständig", "Teilweise", "Keine").
Online-Geräte	Gesamtanzahl der Online-Geräte.
Offline-Geräte	Gesamtanzahl der Offline-Geräte.
Deaktivierte Geräte	Gesamtanzahl der deaktivierten Geräte.
Angehaltene Geräte	Gesamtanzahl angehaltener Geräte.
Deaktiviert	Listet den Namen der Geräte auf, die deaktiviert sind.

Element	Beschreibung
Angehalten	Name der angehaltenen Geräte.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Nächtliche Zusammenfassung"

Im Bericht "Nächtliche Zusammenfassung" sind die Ergebnisse der Backup-Aufträge für die einzelnen Ressourcen in den letzten 24 Stunden aufgeführt. Dieser Bericht enthält Backup-Aufträge, die laut Plan ausgeführt werden sollten, jedoch nicht ausgeführt wurden. Aufträge werden erst 24 Stunden nach Ablauf der geplanten Zeit als überfällig gekennzeichnet.

Tabelle 16-30 Bericht "Nächtliche Zusammenfassung"

Element	Beschreibung
Ressource	System, das gesichert wird.
Typ	Zeigt den Typ des Auftrags an, den Backup Exec ausführt, um den Nachtzusammenfassungsbericht zu erstellen. Weil der Bericht "Nächtliche Zusammenfassung" die Ergebnisse von Backup-Aufträgen für jede Ressource während der letzten 24 Stunden auflistet, wird als Auftragstyp immer "Backup" angezeigt.
Startzeit	Zeitpunkt (Datum und Uhrzeit), an dem der Vorgang gestartet wurde.
Geschäftskritisch	Gibt an, ob das Element als geschäftskritische Ressource gekennzeichnet wurde.
Status	Status des Vorgangs.
Fehlerkategorie	Die Kategorie des Auftrags, der auf einen System-, Auftrags-, Medien- oder Gerätefehler zurückzuführen ist.
Backup Exec-Server	Name des Backup Exec-Servers, auf dem der Auftrag ausführte.
Gerätename	Der Name des Geräts, auf dem der Auftrag ausgeführt wurde.
Aufgaben insgesamt	Gesamtanzahl der Aufträge, die in den letzten 24 Stunden ausgeführt wurden.
Nicht korrigierte Ausnahmen	Anzahl der Aufträge, die fehlgeschlagen sind und nicht noch einmal mit erfolgreichem Abschluss wiederholt wurden.

Element	Beschreibung
Dienstebene	Prozentsatz der Aufträge, die erfolgreich ausgeführt wurden.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Problemdateien"

Im Bericht "Problemdateien" sind alle Problemdateien aufgeführt, die bei Aufträgen gefunden wurden. Die Dateien werden nach Tag und Ressource sortiert.

Tabelle 16-31 Bericht "Problemdateien"

Element	Beschreibung
Datum	Datum, an dem die Problemdatei gefunden wurde.
Ressource	System, auf dem sich die Problemdatei befindet.
Uhrzeit	Uhrzeit, zu der die Problemdatei gefunden wurde.
Grund	Fehlercode, der in der Auftragsprotokollübersicht aufgelistet wird.
Dateiname	Name der Problemdatei.
Typ	Listet den Typ des Auftrags auf, den Backup Exec ausführt, wenn problematische Dateien erkannt wurden.
Backup Exec-Server	Name des Backup Exec-Servers, auf dem sich die Datei befindet.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Kürzlich beschriebene Medien"

Im Bericht "Kürzlich beschriebene Medien" sind alle Medien aufgeführt, die im angegebenen Zeitraum geändert wurden.

Tabelle 16-32 Bericht "Kürzlich beschriebene Medien"

Element	Beschreibung
Medienkennung	Medienkennung, die von Backup Exec oder dem Administrator zugewiesen wurde bzw. in einer zuvor zugewiesenen Barcodekennung enthalten ist.
Speicherort	Speicherort der Medien, z. B. der Speicher- oder Laufwerkname.
Satz	Name des Backup-Satzes.
Datum und Uhrzeit geändert	Zeitpunkt (Datum und Uhrzeit), an dem die Medien zuletzt geändert wurden.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Validierungsübersicht "Wiederherstellung bereit"

Die Validierungsübersicht "Wiederherstellung bereit" enthält eine Übersicht über die validierten virtuellen Computer.

Tabelle 16-33 Validierungsübersicht "Wiederherstellung bereit"

Element	Beschreibung
Backup-Satz-Details	<p>Zeigt Details zum Backup-Satz an: Name und Größe des Backup-Satzes und Name des Geräts</p> <ul style="list-style-type: none"> ■ Backup-Satz: Name des Backup-Satzes. ■ Größe: Größe des Backup-Satzes. ■ Gerätename: Name des Geräts.
Auftragsstatistiken	<p>Details zum Validierungsauftrag.</p> <ul style="list-style-type: none"> ■ Auftragsname: Name des Validierungsauftrags. ■ Startzeit: Wann der Validierungsauftrag gestartet wurde.
Backup-Satz-Überprüfung	<p>Der Status der auf den Backup-Satz ausgeführten Tests und Prüfungen.</p> <ul style="list-style-type: none"> ■ VM registrieren: Status des Tests "VM registrieren". ■ Einschalten: Status des Tests "Einschalten". ■ Heartbeat-Prüfung: Status der Heartbeat-Prüfung.

Element	Beschreibung
Validierungsstatus	<p>Der endgültige Validierungsstatus des Backup-Satzes.</p> <ul style="list-style-type: none"> ■ Validierung bestanden ■ Validierung fehlgeschlagen ■ Validierung nicht möglich

Der Validierungsstatus und der Bereich des Berichts, den Sie ausgewählt haben, werden in der Validierungsübersicht "Wiederherstellung bereit" angezeigt.

Wenn Sie keinen Bereich auswählen, wird der Bericht für die letzten 30 Tage angezeigt. Wenn Sie denselben Validierungsauftrag mehrmals für den gleichen Backup-Satz ausführen, enthält der Bericht Informationen zur letzten Ausführung.

Bericht "Kürzlich geschützte Ressourcen"

Der Bericht zu kürzlich geschützten Ressourcen enthält eine Liste mit allen Auftragsdetailstatistiken und Ausnahmen, die auf einem Backup Exec-Server aufgetreten sind, für den Sie diesen Bericht ausführen.

Tabelle 16-34 Bericht "Kürzlich geschützte Ressourcen"

Element	Beschreibung
Startzeit	Zeitpunkt (Datum und Uhrzeit), an dem der Backup-Auftrag gestartet wurde.
Geschäftskritisch	Gibt an, ob das Element als geschäftskritische Ressource gekennzeichnet wurde.
Dauer	Erforderliche Dauer zum Abschließen des Auftrags.
Größe	Menge der gesicherten Daten.
Dateien	Anzahl der gesicherten Dateien.
Verzeichnisse	Anzahl der gesicherten Verzeichnisse.
Größe pro Min.	Menge der gesicherten Daten pro Minute.
Übersprungen	Anzahl der Dateien, die während des Backups übersprungen wurden.
Beschädigte Dateien	Anzahl der während des Backups erkannten beschädigten Dateien.

Element	Beschreibung
Dateien in Gebrauch	Anzahl der Dateien, die während des Backups verwendet wurden.
Status	Status des Backup-Auftrags.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Ressourcenrisikoanalyse"

Im Bericht "Ressourcenrisikoanalyse" sind die Auftragsinformationen für Ressourcen angezeigt, auf denen der letzte Backup-Auftrag fehlgeschlagen ist.

Tabelle 16-35 Bericht "Ressourcenrisikoanalyse"

Element	Beschreibung
Ressource	Das System, auf dem der Auftrag ausgeführt wurde.
Fehlertext	Beschreibt das Ereignis, das zum Fehlschlagen des Auftrags geführt hat.
Startzeit	Zeitpunkt, zu dem der Vorgang gestartet wurde.
Auftrag	Name des fehlgeschlagenen Auftrags.
Geschäftskritisch	Gibt an, ob das Element als geschäftskritische Ressource gekennzeichnet wurde.
Fehlerkategorie	Die Kategorie des fehlgeschlagenen Auftrags, der auf einen System-, Auftrags-, Medien- oder Gerätefehler zurückzuführen ist.
Backup Exec-Server	Name des Backup Exec-Servers, auf dem der Auftrag ausführte.
Gerätename	Der Name des Geräts, auf dem der Auftrag ausgeführt wurde.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Wiederherstellungssatz-Details nach Ressource"

Im Bericht "Wiederherstellungssatz-Details nach Ressource" sind alle Wiederherstellungsaufträge aufgeführt, die im angegebenen Zeitraum auf dem

ausgewählten Server ausgeführt wurden. Die Aufträge werden nach Server und Ressourcen sortiert.

Tabelle 16-36 Bericht "Ressourcensatz-Details nach Ressource"

Element	Beschreibung
Ressource	Name des Systems, das gesichert wird.
Startzeit	Zeitpunkt (Datum und Uhrzeit), an dem der Vorgang gestartet wurde.
Dauer	Der für den Verarbeitungsvorgang erforderliche Zeitraum.
Größe	Die Menge an verarbeiteten Daten.
Dateien	Anzahl der verarbeiteten Dateien.
Verzeichnisse	Anzahl der verarbeiteten Verzeichnisse.
Daten/Minute	Menge Daten, die pro Minute verarbeitet wurden.
Übersprungen	Anzahl Dateien, die während des Vorgangs übersprungen wurden.
Beschädigte Dateien	Anzahl beschädigter Dateien, die während des Vorgangs angetroffen wurden.
Dateien in Gebrauch	Anzahl der Dateien, die während des Vorgangs verwendet wurden.
Status	Status des Vorgangs, z. B. "Abgeschlossen".

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Medium aus Speicher abrufen"

Im Bericht "Medium aus Speicher abrufen" sind alle wiederverwendbaren Medien aufgeführt, die sich derzeit im angegebenen Medienspeicher befinden.

Tabelle 16-37 Bericht "Medium aus Speicher abrufen"

Element	Beschreibung
Kassettenkennung	<p>Zeigt den Namen der Plattenkassette an. Namen von Plattenkassetten dürfen höchstens 128 Zeichen lang sein.</p> <p>Sie können die Plattenkassette umbenennen.</p> <p>Siehe "Bearbeiten der Eigenschaften von Festplattenkassetten" auf Seite 385.</p>

Element	Beschreibung
Speichername	Zeigt den Namen des Speichers an, in dem die Medien sich befinden.
Mediensatzname	Zeigt den Namen des Mediensatzes an.
Offsite- Rückgabedatum	Zeigt das Datum an, zu dem Medien an den Offsite-Speicher zurückverschoben wurden.
Wiederverwendungsdatum	Zeigt das Datum an, nach dem die Medien überschrieben werden können.
Enddatum für Anhänge	Zeigt das Datum an, von dem an Backup Exec keine Daten mehr an die Medien anfügen kann.
Name der Regel	Zeigt den Namen der Regel für Speichermedien, die für die Medien gilt.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Wechslerinventar"

Im Bericht "Wechslerinventar" wird der Inhalt von Schächten in an Backup Exec-Servern angeschlossenen Wechslern angezeigt. Für alle Medien werden statistische Informationen zur Nutzung angezeigt.

Tabelle 16-38 Bericht "Wechslerinventar"

Element	Beschreibung
Server	Name des Servers, auf dem sich der Wechsler befindet.
Gerätename	Name des Wechslers.
Schacht	Die laufende Nummer des Schachts im Wechsler.
Medienkennung	Medienkennung, die von Backup Exec oder dem Administrator zugewiesen wurde bzw. in einer zuvor zugewiesenen Barcodekennung enthalten ist.
Status	Betriebsstatus des Schachts: angehalten, deaktiviert, aktiviert, offline oder online.
Verändert	Datum, an dem zuletzt auf das Medium im Schacht zugegriffen wurde.

Element	Beschreibung
Geschäftskritisch	Gibt an, ob das Medium einen Backup-Satz enthält, der über eine geschäftskritische Ressource verfügt.
Schreiben	Anzahl der auf dieses Medium geschriebenen Byte.
Vollständiges Backup	Der auf Medien verfügbare Speicherplatz. "1" bedeutet, dass das Medium voll ist. "0" bedeutet, dass auf dem Medium noch Speicherplatz verfügbar ist.
Stunden	Gesamtanzahl der Stunden, die das Medium verwendet wurde.
Geladen	Gibt an, wie oft das Medium insgesamt bereitgestellt wurde.
Anhängen	Die verbleibende Zeit im Anhängezeitraum des Mediums.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Geplante Serverarbeitslast"

Im Bericht "Geplante Serverauslastung" wird die erwartete Arbeitslast für einen Server in den nächsten 24 Stunden oder einem benutzerdefinierten Zeitraum angezeigt. Im Bericht werden nur wiederkehrende Aufträge angezeigt, die bereits mindestens einmal ausgeführt wurden. Aufträge, die nur einmal ausgeführt werden sollen, werden nicht angezeigt.

Tabelle 16-39 Bericht "Geplante Serverarbeitslast"

Element	Beschreibung
Backup Exec-Server	Name des Backup Exec-Servers, der die geplanten Aufträge verarbeiten wird.
Auftrag	Name des Auftrags, der geplant wird.
Nächstes Fälligkeitsdatum	Geplanter Zeitpunkt (Datum und Uhrzeit), an dem der nächste Auftrag ausgeführt werden soll.
Backup-Größe	Geschätzte Menge an Daten, die in den nächsten 24 Stunden verarbeitet wird.
Gesamtgröße	Gesamtmenge der Daten, die in den nächsten 24 Stunden verarbeitet werden soll.
Gesamtgröße	Gesamtmenge der Daten, die auf allen Backup Exec-Servern verarbeitet werden soll.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Verfügbarkeit temporärer Medien"

Im Bericht "Verfügbarkeit temporärer Medien" werden Informationen zur Verfügbarkeit von Medien, zur Anzahl der zum Überschreiben verfügbaren Medien und zu den Zeitpunkten angezeigt, an denen andere Medien zum Überschreiben verfügbar werden.

Tabelle 16-40 Bericht "Verfügbarkeit temporärer Medien"

Element	Beschreibung
Kassettenkennung	Medienkennung, die von Backup Exec oder dem Administrator zugewiesen wurde bzw. die in einer zuvor zugewiesenen Barcodekennung enthalten ist. Sie können das Medium umbenennen. Siehe "Bearbeiten der Eigenschaften von Festplattenkassetten" auf Seite 385.
Name des Medienspeicherorts	Name des Speichergeräts, das die tatsächlichen Medien enthält.
Gesamtkapazität	Gesamte native Kapazität der temporären Medien ohne Komprimierung.
Verbleibende Stunden zum Anhängen	Der zum Anhängen von Daten auf den temporären Medien verfügbare Speicherplatz.
Restliche Kapazität	Gesamte restliche native Kapazität der temporären Medien ohne Komprimierung.
Verbleibende Stunden für Aufbewahrung	Die verbleibende Zeit zum Aufbewahren und zum Schützen der Medien vor dem Überschreiben.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Bericht "Probelaufergebnisse"

Im Bericht "Probelaufergebnisse" werden die Ergebnisse für die Probelaufaufträge angezeigt, die für den ausgewählten Zeitraum festgelegt wurden.

Tabelle 16-41 Bericht "Probelaufergebnisse"

Element	Beschreibung
Backup Exec-Server	Name des Backup Exec-Servers, auf dem der Auftrag ausführte.
Datum und Uhrzeit der Auftragsausführung	Zeitpunkt (Datum und Uhrzeit), an dem der Backup-Auftrag verarbeitet wurde.
Auftragsname	Der Name des Probelaufauftrags.
Backup-Sätze	Name des Backup-Satzes.
Überprüfung der Identifikationsdaten	Zeigt an, ob für das Backup der Ressourcen das entsprechende Backup Exec-Login-Konto vorliegt.
Backup-Größe	Die Backup-Datenmenge in KB, Megabyte oder Gigabyte.
Medientyp	Typ der verwendeten Medien, z. B. "4 MM".
Gerätename	Name des Geräts, z. B. Name des Wechslers.
Maximal benötigt	Platz, der auf den Medien erforderlich ist, um den Auftrag auszuführen.
Online	Speicherplatz der Medien im Gerät, der zum Anhängen von Daten verfügbar ist.
Medien insgesamt	Anzahl der im System insgesamt verfügbaren Medien, auf denen Daten angehängt werden können.
Online	Speicherplatz der Medien im Gerät, der zum Schreiben von Daten verfügbar ist.
Medien insgesamt	Anzahl der im System insgesamt verfügbaren Medien, die überschrieben werden können.

Siehe ["Einen Bericht jetzt ausführen"](#) auf Seite 794.

Siehe ["Erstellen eines benutzerdefinierten Berichts"](#) auf Seite 796.

Sofortwiederherstellung in der Cloud

In diesem Kapitel werden folgende Themen behandelt:

- [Info zur Sofortwiederherstellung in der Cloud](#)
- [Überblick über die Registerkarte "Sofortwiederherstellung in der Cloud" in Backup Exec](#)
- [Anforderungen zum Konfigurieren der Sofortwiederherstellung in der Cloud in Backup Exec](#)
- [Vorkonfigurationen, die im Azure-Portal abgeschlossen werden müssen](#)
- [Konfigurieren von Azure-Ressourcen](#)
- [Anzeigen von Fehlerdetails](#)
- [Anzeigen der Konfigurationsdetails](#)
- [Anzeigen der Details zum virtuellen Computer](#)
- [Manuelles Aktualisieren der Ansicht virtueller Computer](#)
- [Aktivieren der Replikation virtueller Computer](#)
- [Verwalten der Replikation von virtuellen Computern](#)
- [Verwalten des Failover für einen virtuellen Computer](#)
- [Ändern des Abonnements oder des Recovery Services-Tresors](#)
- [Vorbereiten einer neuen Infrastruktur](#)
- [Entfernen einer konfigurierten Azure-Ressource aus Backup Exec](#)

- [Verlängern des Backup Exec-Zertifikats](#)

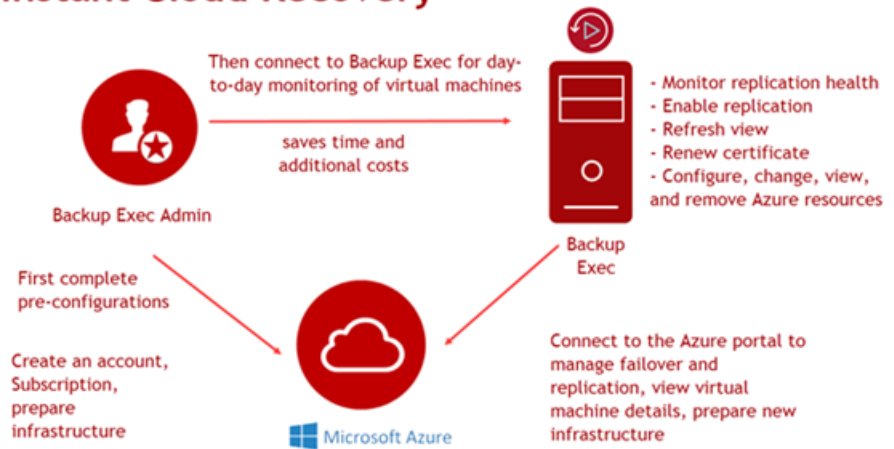
Info zur Sofortwiederherstellung in der Cloud

Backup Exec-Benutzer können die Notfallwiederherstellung von Azure Site Recovery nutzen. Sie können die Microsoft Azure-Infrastruktur in Backup Exec einrichten, mit der Sie Zeit und zusätzlichen Kosten sparen können.

Sie können den Zustand von virtuellen Computern überwachen, die von Azure Site Recovery verwaltet werden. Sie können die virtuellen Computer von der Backup Exec-Konsole aus täglich unabhängig voneinander überwachen.

Die Sofortwiederherstellung in der Cloud hilft beim Aktivieren der Replikation für die lokalen virtuellen Computer (VMware und Hyper-V), deren Hosts mit Azure Site Recovery konfiguriert sind. Wenn ein Ausfall oder Fehler auftritt, ist ein Failover der replizierten virtuellen Computer auf Azure möglich, um sicherzustellen, dass sie für den Geschäftsbetrieb verfügbar sind.

Instant Cloud Recovery



Siehe "[Überblick über die Registerkarte "Sofortwiederherstellung in der Cloud" in Backup Exec](#)" auf Seite 853.

Siehe "[Anforderungen zum Konfigurieren der Sofortwiederherstellung in der Cloud in Backup Exec](#)" auf Seite 856.

Siehe "[Vorkonfigurationen, die im Azure-Portal abgeschlossen werden müssen](#)" auf Seite 856.

Siehe "[Konfigurieren von Azure-Ressourcen](#)" auf Seite 857.

Siehe ["Aktivieren der Replikation virtueller Computer"](#) auf Seite 862.

Siehe ["Verwalten des Failover für einen virtuellen Computer"](#) auf Seite 865.

Siehe ["Verwalten der Replikation von virtuellen Computern"](#) auf Seite 864.

Siehe ["Ändern des Abonnements oder des Recovery Services-Tresors"](#) auf Seite 865.

Siehe ["Anzeigen der Konfigurationsdetails"](#) auf Seite 860.

Siehe ["Verlängern des Backup Exec-Zertifikats"](#) auf Seite 867.

Siehe ["Vorbereiten einer neuen Infrastruktur"](#) auf Seite 866.

Siehe ["Manuelles Aktualisieren der Ansicht virtueller Computer"](#) auf Seite 861.

Siehe ["Entfernen einer konfigurierten Azure-Ressource aus Backup Exec"](#) auf Seite 866.

Siehe ["Anzeigen der Details zum virtuellen Computer"](#) auf Seite 861.

Überblick über die Registerkarte "Sofortwiederherstellung in der Cloud" in Backup Exec

Auf der Registerkarte "Sofortwiederherstellung in der Cloud" können Sie die Notfallwiederherstellung mit Azure Site Recovery verwalten. Sie können den Replikationszustand von virtuellen Computern überwachen und die Replikation von lokalen virtuellen Computern aktivieren, deren Hosts mit Azure Site Recovery konfiguriert sind.

Auf der Registerkarte "Sofortwiederherstellung in der Cloud" können Sie auch die Ansicht der virtuellen Computer in Backup Exec aktualisieren, das Abonnement und den Recovery Services-Tresor ändern, Fehlerdetails anzeigen, das Zertifikat verlängern, Details zu virtuellen Computern im Azure-Portal anzeigen, Failover über das Azure-Portal verwalten, eine neue Infrastruktur im Azure-Portal erstellen und die Azure-Ressourcenkonfiguration aus Backup Exec löschen.

Sie können den Schutzstatus, Replikationszustand und Validierungsfehler für einen virtuellen Computer anzeigen.

Siehe ["Info zur Sofortwiederherstellung in der Cloud"](#) auf Seite 852.

Tabelle 17-1 Registerkarte "Sofortwiederherstellung in der Cloud"

Gruppe	Element	Beschreibung
Verwalten	Failover verwalten	<p>Hiermit können Sie das Failover nur für virtuelle Computer, die repliziert oder geschützt sind, verwalten.</p> <p>Wenn Sie diese Option wählen, wird zum Verwalten des Failover das Azure-Portal geöffnet.</p> <p>Siehe "Verwalten des Failover für einen virtuellen Computer" auf Seite 865.</p>
	Replikation verwalten	<p>Hiermit können Sie die Replikation der virtuellen Computer eines konfigurierten Recovery Services-Tresors über das Azure-Portal verwalten.</p> <p>Wenn Sie diese Option wählen, wird zum Verwalten der Replikation das Azure-Portal geöffnet.</p> <p>Siehe "Verwalten der Replikation von virtuellen Computern" auf Seite 864.</p>
	Fehlerdetails anzeigen	<p>Hier können Sie Fehler für einen virtuellen Computer anzeigen. Bevor Sie einen virtuellen Computer schützen können, müssen Sie eventuell vorhandene Validierungsfehler beheben.</p> <p>Siehe "Anzeigen von Fehlerdetails" auf Seite 860.</p>
Aktuelle Anzeige	Abonnement oder Tresor ändern	<p>Hier können Sie ändern Sie das Azure-Abonnement oder den Recovery Services-Tresor für Backup Exec ändern, um die Azure Site Recovery-Ressourcen zu überwachen und zu verwalten.</p> <p>Siehe "Ändern des Abonnements oder des Recovery Services-Tresors" auf Seite 865.</p>
	Ansicht aktualisieren	<p>Hiermit können Sie die Ansicht der virtuellen Computer basierend auf dem Abonnement und dem Recovery Services-Tresor manuell aktualisieren.</p> <p>Siehe "Manuelles Aktualisieren der Ansicht virtueller Computer" auf Seite 861.</p>
	Zertifikat verlängern	<p>Hiermit können Sie das Backup Exec-Zertifikat verlängern, das den Einsatz im Azure-Portal ermöglicht.</p> <p>Siehe "Verlängern des Backup Exec-Zertifikats" auf Seite 867.</p>

Gruppe	Element	Beschreibung
Konfiguration	Azure-Ressourcen konfigurieren	<p>Hiermit können Sie Azure-Ressourcen konfigurieren, indem Sie ein Abonnement und einen vorhandenen Azure Recovery Services-Tresor auswählen oder einen neuen Tresor erstellen. Anschließend können Sie die virtuellen Computer anzeigen, die im konfigurierten Azure Recovery Services-Tresor verfügbar sind.</p> <p>Siehe "Konfigurieren von Azure-Ressourcen" auf Seite 857.</p>
	Konfigurationsdetails anzeigen	<p>Zeigt die konfigurierten Azure-Ressourcendetails an.</p> <p>Siehe "Anzeigen der Konfigurationsdetails" auf Seite 860.</p>
	Neue Infrastruktur vorbereiten	<p>Hiermit können Sie die neue Infrastruktur für den konfigurierten Recovery Services-Tresor im Azure-Portal vorbereiten.</p> <p>Wenn Sie diese Option wählen, wird zum Vorbereiten der Infrastruktur das Azure-Portal geöffnet.</p> <p>Siehe "Vorbereiten einer neuen Infrastruktur" auf Seite 866.</p>
	Konfiguration entfernen	<p>Entfernt die konfigurierten Azure-Ressourcen und die Ansicht der virtuellen Computer aus Backup Exec.</p> <p>Siehe "Entfernen einer konfigurierten Azure-Ressource aus Backup Exec" auf Seite 866.</p>
	Details zum virtuellen Computer	<p>Zeigt Details zu einem in Backup Exec geschützten virtuellen Computer im Azure-Portal an.</p> <p>Wenn Sie diese Option wählen, wird zum Anzeigen der Details zum virtuellen Computer das Azure-Portal geöffnet.</p> <p>Siehe "Anzeigen der Details zum virtuellen Computer" auf Seite 861.</p>

Anforderungen zum Konfigurieren der Sofortwiederherstellung in der Cloud in Backup Exec

Es gelten folgende Anforderungen in Backup Exec zum Überwachen des Zustands und Aktivieren die Replikation virtueller Computer mithilfe der Sofortwiederherstellung in der Cloud:

- Sie müssen ein Abonnement im Azure-Portal erstellt haben.
- Sie müssen sich bei Microsoft Azure mit einem Benutzerkonto einloggen, das folgende Kriterien erfüllt.
 - Globaler Administrator für den Active Directory-Mandanten des Azure-Abonnements oder Berechtigungen zum Erstellen von Apps im Mandanten.
 - Eigentümer des Azure-Abonnements oder Benutzerzugriffsadministrator
Weitere Informationen finden Sie im Abschnitt "Erforderliche Berechtigungen" in der Microsoft-Dokumentation:
<https://docs.microsoft.com/de-de/azure/azure-resource-manager/resource-group-create-service-principalportal>
- Sie müssen die Infrastruktur im Azure-Portal vorbereitet haben, wenn Sie einen Recovery Services-Tresor in Backup Exec erstellen.

Siehe "[Vorkonfigurationen, die im Azure-Portal abgeschlossen werden müssen](#)" auf Seite 856.

Vorkonfigurationen, die im Azure-Portal abgeschlossen werden müssen

Um den Zustand zu überwachen und die Replikation virtueller Computer in Backup Exec zu aktivieren, müssen Sie bestimmte Konfigurationen im Azure-Portal ausführen.

Siehe "[Vorbereiten der VMware- bzw. Hyper-V-Infrastruktur](#)" auf Seite 857.

Siehe "[Info zur Sofortwiederherstellung in der Cloud](#)" auf Seite 852.

Siehe "[Anforderungen zum Konfigurieren der Sofortwiederherstellung in der Cloud in Backup Exec](#)" auf Seite 856.

Vorbereiten der VMware- bzw. Hyper-V-Infrastruktur

Zum Replizieren von virtuellen VMware- bzw. Hyper-V-Computern in Azure müssen Sie die lokale Infrastruktur vorbereiten.

Weitere Informationen hierzu finden Sie in der Dokumentation zu Microsoft Azure.

<https://docs.microsoft.com/de-de/azure/site-recovery/vmware-azure-tutorial-prepare-on-premises>

<https://docs.microsoft.com/de-de/azure/site-recovery/hyper-v-prepare-on-premises-tutorial>

Konfigurieren von Azure-Ressourcen

Sie können Azure-Ressourcen durch Auswählen eines Abonnements und eines vorhandenen Azure Recovery Services-Tresors bzw. Erstellen eines neuen Tresors konfigurieren. Anschließend können Sie die entsprechenden virtuellen Computer anzeigen. Sie können den Replikationszustand von virtuellen Computern überwachen und die Replikation von lokalen virtuellen Computern aktivieren, deren Hosts mit Azure Site Recovery konfiguriert sind.

Wenn Sie zum ersten Mal die Notfallwiederherstellung in Azure Site Recovery konfigurieren, sind keine virtuellen Computer für die Replikation verfügbar, wenn Sie die Registerkarte "Sofortwiederherstellung in der Cloud" aufrufen.

So konfigurieren Sie Azure-Ressourcen

- 1 Klicken Sie auf der Registerkarte "Sofortwiederherstellung in der Cloud" auf "Azure-Ressourcen konfigurieren".

Im Azure-Portal erhalten Sie weitere Informationen zu Azure Site Recovery.

- 2 Wählen Sie im Assistenten "Azure-Ressourcen konfigurieren" die Cloud-Umgebung aus, die Sie für die Konfiguration verwenden möchten.

Die Cloud-Umgebungen werden angezeigt. Beispiel: Azure, Azure China, Azure Germany, Azure US Government Cloud.

- 3 Klicken Sie auf "Weiter".

Das Microsoft-Dialogfeld zum Einloggen wird geöffnet.

Sie müssen sich bei Microsoft Azure mit einem Benutzerkonto einloggen, das folgende Kriterien erfüllt:

Weitere Informationen finden Sie im Abschnitt "Erforderliche Berechtigungen" in der Microsoft-Dokumentation:

<https://docs.microsoft.com/de-de/azure/azure-resource-manager/resource-group-create-service-principal-portal>

- Globaler Administrator für den Active Directory-Mandanten des Azure-Abonnements oder Berechtigungen zum Erstellen von Apps im Mandanten.

- Eigentümer des Azure-Abonnements oder Benutzerzugriffsadministrator

Nach dem Einloggen wird der Assistent "Azure-Ressourcen konfigurieren" geöffnet.

Basierend auf Ihrem Azure-Konto wird die Liste Ihrer Abonnements aus dem Azure-Portal abgerufen.

- 4 Wählen Sie das gewünschte Azure-Abonnement aus.

Hinweis: Sie müssen ein gültiges Abonnement auswählen.

Wenn für das Azure-Konto keine Abonnements erstellt wurden, wird eine Meldung angezeigt. In diesem Fall müssen Sie das Abonnement im Azure-Portal erstellen. Nachdem das Abonnement erstellt wurde, starten Sie die Konfiguration ab Schritt 1 erneut.

Weitere Informationen zum Erstellen eines Azure-Abonnements finden Sie unter folgendem Link:

<https://azure.microsoft.com/en-in/free/>

- 5 Klicken Sie auf "Weiter".

Je nach ausgewähltem Abonnement wird eine Liste der Recovery Services-Tresore aus Azure abgerufen.

- 6 Sie haben folgende Möglichkeiten:

Verwenden eines vorhandenen Recovery Services-Tresors

Gehen Sie dazu in folgender Reihenfolge vor:

- 1 Wählen Sie den Recovery Services-Tresor aus der Dropdown-Liste.

Die entsprechende Region wird angezeigt. Sie können die Region nicht ändern.

- 2 Klicken Sie auf "Fertigstellen".

Erstellen eines neuen Recovery Services-Tresors

Gehen Sie dazu in folgender Reihenfolge vor:

- 1** Wählen Sie in der Dropdown-Liste die Option "Neuen Tresor erstellen".
- 2** Geben Sie einen Namen für den neuen Recovery Services-Tresor ein.
- 3** Wählen Sie die Region des Tresors aus der Dropdown-Liste.
- 4** Klicken Sie auf "Fertigstellen".
Es wird gemeldet, dass das Azure-Portal aufgerufen wird.
- 5** Klicken Sie auf "OK".

Das Azure-Portal wird geöffnet. Bereiten Sie im Azure-Portal die Infrastruktur für den neuen Tresor vor.

Backup Exec ruft Informationen zum Tresor und die Liste der virtuellen Computer basierend auf der Infrastruktur des Recovery Services-Tresors ab und zeigt die Informationen in der Backup Exec-Konsole an.

Folgende Informationen werden angezeigt:

Name	Zeigt den Namen des virtuellen Computers an, wie er im Azure-Portal aufgeführt ist. Für ESX oder Hyper-V ist dies der Anzeigename des virtuellen Computers.
Replikationszustand	<p>Zeigt den Replikationszustand an, ob der virtuelle Computer repliziert ist und ob Fehler bzw. Warnungen ausgegeben wurden. Der Replikationszustand kann folgende Werte haben:</p> <ul style="list-style-type: none"> ■ Warnung ■ Fehlerfrei ■ Kritisch ■ Nicht repliziert
Schutzstatus	Zeigt den Schutzzustand an und ob der virtuelle Computer geschützt ist. Die gängigsten Werte für den Schutzstatus sind "Geschützt" und "Nicht geschützt".
Konfigurationsprobleme	<p>Zeigt an, ob für einen virtuellen Computer von Azure Konfigurationsprobleme erkannt wurden sowie deren Anzahl.</p> <p>Wählen Sie zum Anzeigen der Konfigurationsprobleme den virtuellen Computer aus und klicken Sie auf "Fehlerdetails anzeigen".</p>
Letzter Failover	Zeigt das Datum und die Uhrzeit des letzten Failover an.

RPO	<p>Recovery Point Objective (RPO, Vorgabe für den Wiederherstellungspunkt)</p> <p>Zeigt das Datum und Uhrzeit der letzten Replikation an.</p>
Validierungsfehler	<p>Zeigt an, ob für einen virtuellen Computer von Azure Validierungsfehler erkannt wurden sowie deren Anzahl. Wählen Sie zum Anzeigen der Validierungsfehler den virtuellen Computer aus und klicken Sie auf "Fehlerdetails anzeigen".</p> <p>Wenn ein virtueller Computer Validierungsfehler aufweist, können Sie ihn nicht schützen. Sie müssen zunächst die Validierungsfehler beheben und anschließend den Computer schützen.</p>

Siehe ["Info zur Sofortwiederherstellung in der Cloud"](#) auf Seite 852.

Anzeigen von Fehlerdetails

Sie können die Fehler für einen virtuellen Computer anzeigen. Sie müssen zunächst die Validierungsfehler beheben und anschließend den virtuellen Computer schützen. Das Aktivieren der Replikation für einen virtuellen Computer, der Validierungsfehler aufweist, ist nicht möglich.

Wählen Sie auf der Registerkarte "Sofortwiederherstellung in der Cloud" den virtuellen Computer aus und klicken Sie in der Gruppe "Verwalten" auf "Fehlerdetails anzeigen".

Im Dialogfeld "Fehlerdetails anzeigen" werden Informationen zum Typ der Fehler auf dem virtuellen Computer angezeigt. Es gibt drei Fehlertypen:

- Validierungsfehler
- Konfigurationsprobleme
- Probleme mit dem Replikationszustand

Für jeden Fehlertyp wird die Fehlermeldung zusammen mit der möglichen Ursache und einem Behebungsvorschlag angezeigt.

Anzeigen der Konfigurationsdetails

Sie können die konfigurierten Azure-Ressourcendetails in der Backup Exec-Konsole anzeigen.

Klicken Sie auf der Registerkarte "Sofortwiederherstellung in der Cloud" in der Gruppe "Konfigurieren" auf "Konfigurationsdetails anzeigen".

Das Dialogfeld "Details zur Azure-Ressourcenkonfiguration" wird geöffnet.

Tabelle 17-2 Details zur Azure-Konfiguration

Element	Beschreibung
Abonnement-ID	Die Abonnement-ID aus dem Azure-Portal.
Abonnementname	Der Name des konfigurierten Abonnements.
Recovery Services-Tresor	Der Name des konfigurierten Recovery Services-Tresors.

Siehe ["Info zur Sofortwiederherstellung in der Cloud"](#) auf Seite 852.

Anzeigen der Details zum virtuellen Computer

Sie können die Details zu einem virtuellen Computer im Azure-Portal anzeigen. Sie können nur die Details von virtuellen Computern anzeigen, die geschützt sind.

Führen Sie auf der Registerkarte "Sofortwiederherstellung in der Cloud" einen der folgenden Schritte aus:

- Wählen Sie den virtuellen Computer aus, dessen Details angezeigt werden sollen, und klicken Sie in der Gruppe "Konfigurieren" auf "Details zum virtuellen Computer".
- Klicken Sie mit der rechten Maustaste auf den virtuellen Computer, dessen Details angezeigt werden sollen, und wählen Sie im Kontextmenü die Option "Details zum virtuellen Computer".

Im Azure-Portal wird die Seite "Eigenschaften" für den ausgewählten virtuellen Computer geöffnet.

Siehe ["Info zur Sofortwiederherstellung in der Cloud"](#) auf Seite 852.

Manuelles Aktualisieren der Ansicht virtueller Computer

Sie können die Ansicht der virtuellen Computer basierend auf dem Abonnement und dem Recovery Services-Tresor, die Sie während der Konfiguration ausgewählt haben, manuell aktualisieren. Da die Ansicht der virtuellen Computer nicht immer auf dem neuesten Stand ist, wird sie in regelmäßigen Abständen automatisch aktualisiert. Standardmäßig wird die Ansicht alle 10 Minuten aktualisiert. Wenn Sie die Ansicht vor der automatischen Aktualisierung manuell aktualisieren möchten, wählen Sie diese Option.

Klicken Sie auf der Registerkarte "Sofortwiederherstellung in der Cloud" in der Gruppe "Aktualisierungsvorgänge" auf "Ansicht aktualisieren".

Die Ansicht der virtuellen Computer wird mit den neuesten Informationen aktualisiert.

Siehe "[Info zur Sofortwiederherstellung in der Cloud](#)" auf Seite 852.

Aktivieren der Replikation virtueller Computer

Sie können die Replikation virtueller Computer in der Backup Exec-Konsole aktivieren. Die Replikation ist ein kontinuierliches Backup der virtuellen Computer in Azure Cloud. Wenn ein Systemausfall eintritt, können Sie ein Failover auf dem virtuellen Zielcomputer ausführen.

Wenn Sie bei Microsoft Azure als globaler Administrator, Eigentümer oder Benutzerzugriffadministrator eingeloggt sind, können Sie die Replikation in Backup Exec aktivieren.

Weitere Informationen finden Sie im Abschnitt "Erforderliche Berechtigungen" in der Microsoft-Dokumentation:

<https://docs.microsoft.com/de-de/azure/azure-resource-manager/resource-group-create-service-principal-portal>

Zum Aktivieren der Replikation in Backup Exec müssen Sie zuerst Replikationsrichtlinien im Azure-Portal erstellen. Wenn Sie die Infrastruktur für Ihren Recovery Services-Tresor vorbereiten, erstellen Sie die Replikationsrichtlinien für die virtuellen Computer.

Sie können die Replikation virtueller VMware- und Hyper-V-Computer aktivieren.

Siehe "[Info zur Sofortwiederherstellung in der Cloud](#)" auf Seite 852.

So aktivieren Sie die Replikation virtueller Computer

- 1 Klicken Sie auf der Registerkarte "Sofortwiederherstellung in der Cloud" mit der rechten Maustaste auf den virtuellen Computers, für den die Replikation aktiviert werden soll, und wählen Sie im Kontextmenü die Option "Replikation aktivieren".

Das Dialogfeld "Replikation aktivieren" wird geöffnet.

Hinweis: Das Aktivieren der Replikation für einen virtuellen Computer, der Validierungsfehler aufweist, ist nicht möglich.

- 2 Wählen Sie die VMware- bzw. Hyper-V-Parameter.

Name des virtuellen Computers	VMware und Hyper-V	Zeigt den Namen des virtuellen VMware- bzw. Hyper-V-Computers an, für den die Replikation aktiviert werden soll.
Name des Zielcomputers	VMware und Hyper-V	<p>Geben Sie den Namen des virtuellen VMware- bzw. Hyper-V-Computers als Ziel an.</p> <p>Der Name des Zielcomputers muss die folgenden Anforderungen erfüllen:</p> <ul style="list-style-type: none"> ■ Er muss angegeben werden. ■ Die Länge darf 63 Zeichen nicht überschreiten. ■ Er muss mit einem Buchstaben beginnen und darf nur Buchstaben, Ziffern und Bindestriche enthalten.
Betriebssystem	Hyper-V	Wählen Sie das Betriebssystem des virtuellen Hyper-V-Computers aus. Der virtuelle Zielcomputer in Azure Cloud wird mit demselben Betriebssystem erstellt.
Prozessserver	VMware	Wählen Sie den Konfigurationsserver, der die Replikation für den virtuellen Zielcomputer verwaltet.
Konfigurationsserver	VMware	Wählen Sie den Konfigurationsserver, der die Replikation für den virtuellen Zielcomputer verwaltet.
Als Konto ausführen	VMware	Wählen Sie das Konto aus, das der virtuelle Zielcomputer nutzt.
Replikationsrichtlinie	VMware und Hyper-V	Wählen Sie die Replikationsrichtlinie, die für den virtuellen VMware- bzw. Hyper-V-Computer verwendet werden soll.
Speicherkonto	VMware und Hyper-V	<p>Wählen Sie das Speicherkonto aus, das der Zielcomputer nutzt.</p> <p>Es gibt zwei Typen von Speicherkonten: Standard und Premium.</p>
Speicherkonto für Replikationsprotokolle	VMware und Hyper-V	<p>Wählen Sie das Speicherkonto für Replikationsprotokolle auf dem Zielcomputer aus.</p> <p>Wenn Sie ein Premium-Speicherkonto auswählen, müssen Sie ein Standardspeicherkonto für Replikationsprotokolle auswählen.</p> <p>Diese Option ist ausgegraut, wenn Sie ein Standardspeicherkonto auswählen. Das Standardspeicherkonto wird als Speicherkonto für Replikationsprotokolle verwendet.</p>

Virtuelles Netzwerk	VMware und Hyper-V	Wählen Sie das virtuelle Netzwerk aus, zu dem der Zielcomputer gehört.
Ressourcengruppe	VMware und Hyper-V	Wählen Sie die Ressourcengruppe aus, zu der der Zielcomputer gehört.

Weitere Informationen zu den erweiterten Eigenschaften zum Aktivieren der Replikation virtueller Computer finden Sie im Azure-Portal.

3 Klicken Sie auf "OK".

Die ausgewählten Replikationsparameter bzw. -einstellungen werden an Azure gesendet und wenn die Parameter korrekt eingegeben wurden, wird eine Meldung angezeigt. Der Replikationsstatus des virtuellen Computers wird alle zehn Minuten aktualisiert. Zum Anzeigen weiterer Informationen wählen Sie einen virtuellen Computer aus und klicken Sie auf "Details zum virtuellen Computer" oder zeigen Sie den Status der Replikation in der Spalte "Schutzstatus" an. Nach Abschluss der Replikation wird der Schutzstatus in "Geschützt" geändert.

Wurde ein falscher Parameter festgelegt, wird eine Popup-Meldung angezeigt. Klicken Sie in diesem Fall auf "Replikation aktivieren" und wählen Sie die Parameter erneut aus.

Wenn die Replikationsaufgabe fehlschlägt, zeigt Backup Exec Replikationsfehler für den entsprechenden virtuellen Computer an. Klicken Sie zum Anzeigen der Fehler auf "Fehlerdetails anzeigen". Sie können auch den virtuellen Computer auswählen und auf "Details zum virtuellen Computer" klicken. Die Replikationsfehler werden dann im Azure-Portal angezeigt.

Siehe ["Info zur Sofortwiederherstellung in der Cloud"](#) auf Seite 852.

Verwalten der Replikation von virtuellen Computern

Sie können die Replikation der virtuellen Computer eines konfigurierten Recovery Services-Tresors über das Azure-Portal verwalten.

Wählen Sie auf der Registerkarte "Sofortwiederherstellung in der Cloud" den virtuellen Computer aus und klicken Sie in der Gruppe "Verwalten" auf "Replikation verwalten".

Im Azure-Portal wird die Seite "Replizierte Elemente" des Recovery Services-Tresors aufgerufen, den Sie in Backup Exec ausgewählt haben.

Sie können jetzt die Replikation der virtuellen Computer in diesem Recovery Services-Tresor über das Azure-Portal verwalten.

Siehe ["Info zur Sofortwiederherstellung in der Cloud"](#) auf Seite 852.

Verwalten des Failover für einen virtuellen Computer

Sie können Failover nur für einen virtuellen Computer verwalten, der über das Azure-Portal geschützt ist.

Führen Sie auf der Registerkarte "Sofortwiederherstellung in der Cloud" einen der folgenden Schritte aus:

- Wählen Sie den virtuellen Computer aus, für den Sie Failover verwalten möchten, und klicken Sie in der Gruppe "Verwalten" auf "Failover verwalten".
- Klicken Sie mit der rechten Maustaste auf den virtuellen Computer, für den Sie Failover verwalten möchten, und klicken Sie auf "Failover verwalten".

Das Azure-Portal wird zum Verwalten des Failover geöffnet.

Siehe ["Info zur Sofortwiederherstellung in der Cloud"](#) auf Seite 852.

Ändern des Abonnements oder des Recovery Services-Tresors

Sie können das Abonnement oder den Recovery Services-Tresor ändern, das bzw. den Sie beim Konfigurieren der Azure-Ressourcen ausgewählt haben.

So ändern Sie das Abonnement oder den Recovery Services-Tresor

- 1 Klicken Sie auf der Registerkarte "Sofortwiederherstellung in der Cloud" in der Gruppe "Aktualisierungen" auf "Abonnement oder Tresor ändern".

Der Assistent "Azure-Ressourcen konfigurieren" wird angezeigt.

- 2 Wählen Sie die zu ändernde Ressource aus:

- Abonnement
- Recovery Services-Tresor

- 3 Klicken Sie auf "Weiter".

- 4 Wenn Sie die Option "Abonnement" ausgewählt haben, wird die Seite "Azure-Umgebung" angezeigt. Wählen Sie die Umgebung aus, loggen Sie sich beim Azure-Portal ein und wählen Sie dann das gewünschte Azure-Abonnement aus, oder erstellen Sie ein neues Abonnement in Azure-Portal.

Weitere Informationen zum Erstellen eines Azure-Abonnements finden Sie unter folgendem Link:

<https://azure.microsoft.com/en-in/free/>

Wenn Sie "Recovery Services-Tresor" ausgewählt haben, wählen Sie den gewünschten Azure-Tresor aus oder erstellen Sie einen neuen Tresor in Backup Exec und bereiten Sie die Infrastruktur im Azure-Portal vor.

Siehe ["Konfigurieren von Azure-Ressourcen"](#) auf Seite 857.

- 5 Klicken Sie auf "Fertigstellen".

Backup Exec ruft Informationen zum Tresor und die Liste der virtuellen Computer basierend auf dem Tresor und dem Abonnement ab und zeigt die Informationen in der Backup Exec-Konsole an.

Siehe ["Info zur Sofortwiederherstellung in der Cloud"](#) auf Seite 852.

Vorbereiten einer neuen Infrastruktur

Sie können im Azure-Portal eine neue Infrastruktur für den Recovery Services-Tresor vorbereiten, der in Backup Exec erstellt wurde.

Klicken Sie auf der Registerkarte "Sofortwiederherstellung in der Cloud" in der Gruppe "Konfigurieren" auf "Neue Infrastruktur vorbereiten".

Im Azure-Portal wird die Seite "Site Recovery" geöffnet. Sie können jetzt eine neue Infrastruktur für den Recovery Services-Tresor vorbereiten, der in Backup Exec erstellt wurde, oder einen anderen Tresor auswählen.

Siehe ["Info zur Sofortwiederherstellung in der Cloud"](#) auf Seite 852.

Entfernen einer konfigurierten Azure-Ressource aus Backup Exec

Sie können die konfigurierten Azure-Ressourcen aus Backup Exec entfernen. Die konfigurierten Informationen zu Abonnement und Recovery Services-Tresor werden dabei aus Backup Exec entfernt.

So eine Sie eine konfigurierten Azure-Ressource

- 1 Klicken Sie auf der Registerkarte "Sofortwiederherstellung in der Cloud" in der Gruppe "Konfigurieren" auf "Konfiguration entfernen".

Das Microsoft-Dialogfeld zum Einloggen wird geöffnet. Sie müssen sich beim Azure-Portal mit Ihren Identifikationsdaten einloggen.

Sie müssen sich bei Microsoft Azure mit einem Benutzerkonto einloggen, das folgende Kriterien erfüllt:

- Globaler Administrator für den Active Directory-Mandanten des Azure-Abonnements oder Berechtigungen zum Erstellen von Apps im Mandanten.
- Eigentümer des Azure-Abonnements oder Benutzerzugriffsadministrator
Weitere Informationen finden Sie im Abschnitt "Erforderliche Berechtigungen" in der Microsoft-Dokumentation:
<https://docs.microsoft.com/de-de/azure/azure-resource-manager/resource-group-create-service-principal-portal>

Eine Bestätigungsmeldung wird angezeigt.

- 2 Klicken Sie auf "Ja".

Die konfigurierten Azure-Ressourcen werden aus Backup Exec entfernt.

Siehe "Info zur Sofortwiederherstellung in der Cloud" auf Seite 852.

Verlängern des Backup Exec-Zertifikats

Das Zertifikat, das beim Installieren von Backup Exec erzeugt wird, wird verwendet, wenn Sie eine Verbindung zum Azure-Portal herstellen. Das Zertifikat ist ein Jahr lang gültig. Ein neues Zertifikat wird automatisch sechs Monate nach dem Startdatum erstellt. Das ältere Zertifikat ist weiterhin ein Jahr lang gültig.

Beispiel: Sie haben am 1. Januar 2018 Backup Exec installiert. Das Zertifikat ist bis zum 31. Dezember 2018 gültig. Am 1. Juli 2018 wird automatisch ein neues Zertifikat erzeugt. Das neue Zertifikat ist vom 1. Januar 2019 bis 31. Dezember 2019 gültig. Das ältere Zertifikat ist weiterhin bis zum 31. Dezember 2018 gültig.

15 Tage vor dem Ablauf des Zertifikats wird jeden Tag eine Warnmeldung angezeigt, die Sie auffordert, das Zertifikat zu verlängern.

So verlängern Sie das Zertifikat

- 1** Klicken Sie auf der Registerkarte "Sofortwiederherstellung in der Cloud" in der Gruppe "Aktualisierungsvorgänge" auf "Zertifikat verlängern".

Hinweis: Die Option "Zertifikat verlängern" ist nur sechs Monate vor dem Ablauf des Zertifikats verfügbar.

Das Microsoft-Dialogfeld zum Einloggen wird geöffnet.

- 2** Loggen Sie sich beim Azure-Portal ein.

Das Zertifikat wird automatisch verlängert.

Wenn Sie das Zertifikat nicht verlängern und es nach einem Jahr abläuft, kann Backup Exec keine Vorgänge im Azure-Portal mehr ausführen. Alle Optionen außer "Zertifikat verlängern" auf der Registerkarte "Sofortwiederherstellung in der Cloud" sind dann nicht verfügbar.

Nachdem Sie das Zertifikat verlängert haben, wird die Verbindung zwischen Backup Exec und Azure wiederhergestellt, und die Optionen auf der Registerkarte "Sofortwiederherstellung in der Cloud" sind wieder verfügbar.

Siehe ["Info zur Sofortwiederherstellung in der Cloud"](#) auf Seite 852.

GDPR Guard

In diesem Kapitel werden folgende Themen behandelt:

- [Info zu GDPR Guard](#)
- [Befehle der Backup Exec-Management-Befehlszeile \(BEMCLI\) zum Importieren und Exportieren](#)
- [Unterstützte Typen gesicherter Daten](#)
- [Blockieren des Zugriffs auf gesicherte Elemente](#)
- [Wiederherstellen blockierter Elemente](#)
- [Best Practices zum Blockieren des Zugriffs auf gesicherte Elemente mit GDPR Guard](#)

Info zu GDPR Guard

Ein Unternehmen kann eventuell anfordern, dass bestimmte gesicherte Elemente aus Datenschutz- und Compliance-Gründen blockiert werden (z. B. Datenschutz-Grundverordnung - DSGVO). Diese Elemente sollten nicht angezeigt oder wiederhergestellt werden.

Backup Exec enthält eine Option zum Importieren der Liste der zu blockierenden Elemente. Sie können GDPR Guard verwenden, um die Liste der gesicherten Elemente anzugeben, deren Zugriff blockiert werden soll.

Ein Unternehmen kann ein beliebiges Tool verwenden, um eine Liste der blockierten Elemente zu erstellen. Backup Exec erstellt diese Liste als CSV-Datei. Das Format der CSV-Datei für Informationen zu blockierten Elementen ist generisch, d. h. Sie können ein beliebiges Tool zum Erzeugen verwenden.

Um die CSV-Datei mit den blockierten Elementen in Backup Exec zu importieren, müssen Sie den BEMCLI-Befehl `Import-BEItemsToBlock` verwenden. Sie können

CSV-Dateien mehrmals in Backup Exec importieren. Jede CSV-Datei kann blockierte Elemente aus mehreren Servern enthalten.

Sie können den Inhalt aller importierten Dateien mithilfe des BEMCLI-Befehls `Export-BEItemsBlocked` in eine CSV-Datei exportieren.

Nachdem die blockierten Elemente importiert wurden, werden sie nicht mehr in der Wiederherstellungs- und Suchansicht angezeigt. Wenn Sie einen Wiederherstellungsauftrag ausführen, sind die blockierten Elemente nicht zum Wiederherstellen verfügbar. Die blockierten Elemente werden weiterhin in Backups aufgenommen und werden nicht aus den Backup-Medien gelöscht.

Backup Exec stellt sicher, dass Informationen zu blockierten Elementen durch Verschlüsselung geschützt und alle Vorgänge im Zusammenhang mit blockierten Elementen im Überwachungsprotokoll für Compliance-Anforderungen aufgezeichnet werden.

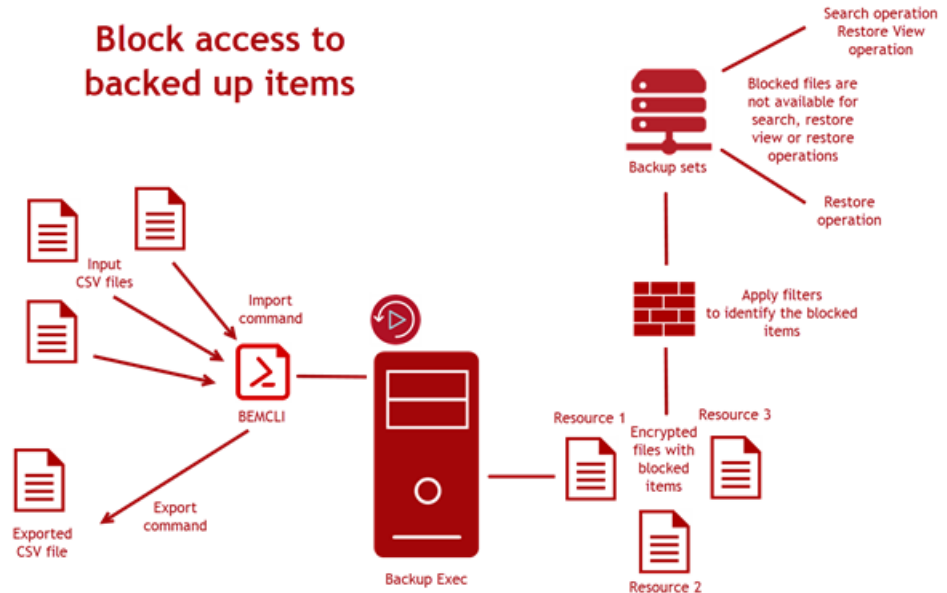
Wenn Sie einen Wiederherstellungsauftrag ausführen, können Sie die Option "Wiederherstellen blockierter Elemente zulassen" verwenden, um blockierten Elemente wiederherzustellen. Wenn Sie diese Option aktivieren, müssen Sie einen Grund zum Wiederherstellen der blockierten Elemente angeben, der dann im Überwachungsprotokoll aufgezeichnet wird. Backup Exec lässt das Wiederherstellen blockierter Elemente nur durch den SLA-Besitzer zu.

Die wichtigsten Funktionen GDPR Guard sind:

- Blockierten Elemente können nicht in der Backup Exec-Konsole angezeigt oder wiederhergestellt werden.
- Backup Exec gewährleistet die Integrität und den Schutz der Informationen zu den blockierten Elementen.
- Das Dateiformat für Vorgänge mit den blockierten Elementen (Import und Export) ist CSV, ein gängiges und benutzerfreundliches Format. CSV-Dateien unterstützen alle Arten von Zeichenkodierung.
- Alle Vorgänge im Zusammenhang mit den blockierten Elementen werden in Überwachungsprotokollen und im Windows-Ereignisprotokoll aufgezeichnet, die zu Compliance-Zwecken verwendet werden können.
- Die importierten blockierten Elemente unter Central Administration Server (CAS) werden automatisch über alle verwalteten Backup Exec-Server (MBES) synchronisiert. Dies gewährleistet die Blockierung in der CAS-MBES-Umgebung, ohne dass die Elemente in jeden Server importiert werden müssen.

Hinweis: Der Importbefehl kann nicht auf MBES ausgeführt werden. Der Exportbefehl kann auf CAS und MBES ausgeführt werden.

Abbildung 18-1 Arbeitsablauf zum Blockieren des Zugriffs auf gesicherte Elemente mit GDPR Guard



Siehe "[Befehle der Backup Exec-Management-Befehlszeile \(BEMCLI\) zum Importieren und Exportieren](#)" auf Seite 871.

Siehe "[Unterstützte Typen gesicherter Daten](#)" auf Seite 873.

Siehe "[Blockieren des Zugriffs auf gesicherte Elemente](#)" auf Seite 874.

Siehe "[Wiederherstellen blockierter Elemente](#)" auf Seite 875.

Siehe "[Best Practices zum Blockieren des Zugriffs auf gesicherte Elemente mit GDPR Guard](#)" auf Seite 876.

Siehe "[Fehlerbehebung beim Blockieren des Zugriffs auf gesicherte Elemente mit GDPR Guard](#)" auf Seite 897.

Befehle der Backup Exec-Management-Befehlszeile (BEMCLI) zum Importieren und Exportieren

Sie können blockierte Elemente mit den folgenden BEMCLI-Befehlen aufrufen und anzeigen:

- `Import-BEItemsToBlock`
- `Export-BEItemsBlocked`

Weitere Informationen zur Backup Exec-Befehlszeilenschnittstelle und den dazugehörigen Befehlen finden Sie in der Hilfedatei "BEMCLI" im Standard-Installationsverzeichnis:

`C:<Backup Exec-Installationsordner>\Backup Exec`

Importieren von blockierten Elemente

Der Befehl `Import-BEItemsToBlock` wird verwendet, um die Liste der blockierten Elemente in Backup Exec bereitzustellen. Beim Ausführen dieses Befehls muss der vollständige Pfad zur CSV-Datei als Parameter angegeben werden.

Die CSV-Datei enthält Informationen zu den zu blockierenden Elementen, insbesondere den Namen des Servers und den vollständigen Pfad. Mit dem Importbefehl können Sie der in Backup Exec vorhandenen Liste blockierter Elemente neue Einträge hinzufügen.

Die Spaltennamen in der CSV-Datei müssen nicht in einer bestimmten Reihenfolge vorliegen, und der Importbefehl akzeptiert CSV-Dateien, die zusätzliche Spalten enthalten. Das Format der CSV-Datei ist daher generisch, d. h. Sie können ein beliebiges Tool zum Erzeugen verwenden.

Im selben Vorgang können Sie blockierte Elemente importieren, die zu verschiedenen Servern gehören und in derselben CSV-Datei enthalten sind.

Bei jedem Ausführen des Importbefehls wird ein Eintrag im Überwachungsprotokoll unter der Kategorie "Compliance" und in der Windows-Ereignisanzeige protokolliert.

Exportieren von blockierten Elementen

Mit dem Befehl `Export-BEItemsBlocked` können Sie Informationen zu allen blockierten Elementen exportieren, die importiert wurden.

Diese Informationen werden in eine CSV-Datei im angegebenen Speicherort exportiert. Sie müssen den Speicherort für die CSV-Datei als Befehlsparameter angeben. Der Exportbefehl erstellt eine CSV-Datei im selben Format wie die Eingabe-CSV-Datei.

Bei jedem Ausführen des Exportbefehls wird ein Eintrag im Überwachungsprotokoll unter der Kategorie "Compliance" und in der Windows-Ereignisanzeige aufgezeichnet.

Es wird empfohlen, die importierten blockierten Elemente regelmäßig zu sichern, indem Sie den BEMCLI-Befehl zum Exportieren ausführen.

Das Verhalten von CAS-MBES beim Ausführen von Import- und Exportbefehlen

Importbefehl - Verhalten:

- Der Importbefehl kann nur unter CAS ausgeführt werden und wird unter MBES blockiert.
- Nach dem Import in CAS werden die Informationen zu den blockierten Elementen zusammen mit dem Verschlüsselungscode an MBES gesendet.
- Wenn ein MBES während des Imports offline ist, werden die Informationen zu den blockierten Elementen an diesen MBES weitergeleitet, wenn er wieder online ist.
- Bei einem rollenden Upgrade werden die blockierten Elemente nicht an den älteren MBES gesendet. Nachdem MBES auf die aktuelle Version von Backup Exec aktualisiert wurde, werden die Informationen zu den blockierten Elementen mit MMS synchronisiert.
- Wenn ein neuer MBES hinzugefügt wird, werden der Verschlüsselungscode und die Informationen zu den blockierten Elementen mit dem MBES synchronisiert.
- Wurden die Vorgänge für die blockierten Elemente oder das Zurücksetzen aktualisiert, werden alle Informationen, einschließlich der CSV-Daten, mit MBES synchronisiert.

Der Exportbefehl wird unter CAS und MBES ausgeführt.

Siehe ["Info zu GDPR Guard"](#) auf Seite 869.

Siehe ["Unterstützte Typen gesicherter Daten"](#) auf Seite 873.

Siehe ["Blockieren des Zugriffs auf gesicherte Elemente"](#) auf Seite 874.

Siehe ["Wiederherstellen blockierter Elemente"](#) auf Seite 875.

Siehe ["Best Practices zum Blockieren des Zugriffs auf gesicherte Elemente mit GDPR Guard"](#) auf Seite 876.

Siehe ["Fehlerbehebung beim Blockieren des Zugriffs auf gesicherte Elemente mit GDPR Guard"](#) auf Seite 897.

Unterstützte Typen gesicherter Daten

Backup Exec unterstützt die folgenden Datentypen zum Sichern:

- Von Backup Exec unterstützte Dateisysteme. Beispiele: NTFS, Linux.

Hinweis: NDMP-Dateiserver werden nicht unterstützt.

- Windows-Freigaben
- Datei- und Ordnerdaten aus Backups virtueller Computer (VMware und Hyper-V).

Siehe ["Info zu GDPR Guard"](#) auf Seite 869.

Siehe ["Befehle der Backup Exec-Management-Befehlszeile \(BEMCLI\) zum Importieren und Exportieren"](#) auf Seite 871.

Siehe ["Blockieren des Zugriffs auf gesicherte Elemente"](#) auf Seite 874.

Siehe ["Wiederherstellen blockierter Elemente"](#) auf Seite 875.

Siehe ["Best Practices zum Blockieren des Zugriffs auf gesicherte Elemente mit GDPR Guard"](#) auf Seite 876.

Siehe ["Fehlerbehebung beim Blockieren des Zugriffs auf gesicherte Elemente mit GDPR Guard"](#) auf Seite 897.

Blockieren des Zugriffs auf gesicherte Elemente

Sie können den Zugriff auf gesicherte Elemente aus Backup Exec blockieren. Backup Exec erwartet als Eingabe die Liste der Elemente, die nicht wiedergestellt werden dürfen. Backup Exec berücksichtigt diese Liste bei der Wiederherstellung und gewährleistet die Integrität und den Schutz der Informationen zu den blockierten Elementen.

Sie benötigen eine Liste der Elemente, die nicht wiederhergestellt werden sollen. Ein Unternehmen kann ein beliebiges Tool verwenden, um diese Liste zu erstellen. Die Liste muss als CSV-Datei gespeichert werden und den Pfad zum Ordner mit den Elementen sowie die Serverinformationen für jedes blockierte Element enthalten.

Alle Import- und Exportvorgänge sowie die ausgeführten Aufträge werden im Überwachungsprotokoll sowie im Windows-Ereignisprotokoll aufgezeichnet.

Das Wiederherstellungsauftragsprotokoll enthält die Informationen zu den blockierten Elementen, die nicht wiederhergestellt werden. Die tatsächlichen Dateinamen sind nicht aufgeführt.

So blockieren Sie den Zugriff auf gesicherte Elemente

- 1 Importieren Sie die CSV-Datei mit der Liste der blockierten Elemente in Backup Exec mit dem BEMCLI-Befehl `Import-BEItemsToBlock`.

Sie können dann die importierte Liste mit dem BEMCLI-Befehl `Export-BEItemsBlocked` in einen anderen Speicherort exportieren. Die exportierte CSV-Datei ist Ihr Backup der blockierten Elemente.

Siehe "[Befehle der Backup Exec-Management-Befehlszeile \(BEMCLI\) zum Importieren und Exportieren](#)" auf Seite 871.

- 2 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" mit der rechten Maustaste auf den Server, aus dem Sie Daten wiederherstellen möchten, und klicken Sie dann auf "Wiederherstellen".
- 3 Wählen Sie "Dateien, Ordner oder Datenträger" und klicken auf "Weiter".
- 4 Aktivieren Sie die Option "Datei- und Ordner-Backups zu einem Zeitpunkt", "Datei- und Ordner-Backups aus einem Backup-Satz" oder "Dateien und Ordner durchsuchen".

Die blockierten Elemente in der importierten Liste sind nicht beim Auswählen von Dateien und Ordnern verfügbar. Wenn die blockierten Elemente wiederhergestellt werden müssen, kann dies nur vom SLA-Besitzer durchgeführt werden. Außerdem wird der Grund im Überwachungsprotokoll aufgezeichnet.

- 5 Folgen Sie im Assistenten für Wiederherstellungsaufträge den Anweisungen zum Wiederherstellen der Daten.

Siehe "[Wiederherstellen von Dateisystemdaten](#)" auf Seite 265.

Siehe "[Info zu GDPR Guard](#)" auf Seite 869.

Siehe "[Befehle der Backup Exec-Management-Befehlszeile \(BEMCLI\) zum Importieren und Exportieren](#)" auf Seite 871.

Siehe "[Unterstützte Typen gesicherter Daten](#)" auf Seite 873.

Siehe "[Wiederherstellen blockierter Elemente](#)" auf Seite 875.

Siehe "[Best Practices zum Blockieren des Zugriffs auf gesicherte Elemente mit GDPR Guard](#)" auf Seite 876.

Siehe "[Fehlerbehebung beim Blockieren des Zugriffs auf gesicherte Elemente mit GDPR Guard](#)" auf Seite 897.

Wiederherstellen blockierter Elemente

Blockierte Elemente werden standardmäßig nicht in der Wiederherstellungs- und Suchansicht angezeigt und können nicht wiederhergestellt werden.

Wenn die blockierten Elemente wiederhergestellt werden müssen, kann dies nur vom SLA-Besitzer durchgeführt werden. Der Grund für die Wiederherstellung wird im Überwachungsprotokoll aufgezeichnet.

Wenn Sie den Besitzer des System-Login-Kontos abrufen möchten, klicken Sie auf die Schaltfläche "Backup Exec" und wählen Sie dann "Konfiguration und Einstellungen > Login-Konten auswählen > Login-Konten verwalten". Im Dialogfeld "Login-Kontenverwaltung" wird in der Spalte "Eigentümer" der Name angezeigt.

So stellen Sie blockierte Elemente wieder her

- 1** Loggen Sie sich als SLA-Besitzer ein.
- 2** Aktivieren Sie im Assistenten für Wiederherstellungsaufträge die Option "Dateien, Ordner oder Datenträger" und klicken Sie auf "Weiter".
- 3** Aktivieren Sie das Kontrollkästchen "Wiederherstellen blockierter Elemente zulassen".
- 4** Geben Sie im Dialogfeld "Blockierte Elemente wiederherstellen" den Grund für die Wiederherstellung ein.
- 5** Klicken Sie im Assistenten für Wiederherstellungsaufträge auf "Weiter", um die blockierten Elemente in der Ansicht "Wiederherstellen" anzuzeigen. Die Ansicht "Wiederherstellen" enthält die Elemente, die zur Wiederherstellung ausgewählt wurden.
- 6** Folgen Sie im Assistenten für Wiederherstellungsaufträge den Anweisungen zum Wiederherstellen der Daten.

Siehe ["Info zu GDPR Guard"](#) auf Seite 869.

Siehe ["Befehle der Backup Exec-Management-Befehlszeile \(BEMCLI\) zum Importieren und Exportieren"](#) auf Seite 871.

Siehe ["Blockieren des Zugriffs auf gesicherte Elemente"](#) auf Seite 874.

Siehe ["Unterstützte Typen gesicherter Daten"](#) auf Seite 873.

Siehe ["Best Practices zum Blockieren des Zugriffs auf gesicherte Elemente mit GDPR Guard"](#) auf Seite 876.

Siehe ["Fehlerbehebung beim Blockieren des Zugriffs auf gesicherte Elemente mit GDPR Guard"](#) auf Seite 897.

Best Practices zum Blockieren des Zugriffs auf gesicherte Elemente mit GDPR Guard

Lesen Sie die folgenden Best Practices, bevor Sie den Zugriff auf gesicherte Elemente blockieren:

- Beim Angeben der blockierten Elemente in der CSV-Datei zum Importieren müssen Sie ein Sternchen (*) als Platzhalter für eine Reihe von Elementen im selben Ordner angeben. Beispiele: "H:\Ordner1*.txt" und "E:*". Das Sternchen kann für den Pfad zu den blockierten Elementen in der CSV-Datei stehen. Beispiel: Im Ordner "H:\Folder1" werden alle Textdateien oder auf dem Laufwerk "E:" werden alle Elemente blockiert.
- Für blockierten Elemente, die sich auf einem Computer mit einem anderen Betriebssystem als Windows befinden, muss beim Dateipfad die Groß- und Kleinschreibung beachtet werden. Gewährleisten Sie, dass die Schreibweise des Pfads korrekt ist.
- Der Name des Servers in der CSV-Datei muss mit dem in der Liste "Server" auf dem Medienserver übereinstimmen (Registerkarte "Backup- und Wiederherstellung" > Spalte "Server"). Wenn dabei der vollständig qualifizierte Domänenname (FQDN) verwendet wird, und der Server in der Liste "Server" einen anderen Namen hat, muss der Remote Agent für diesen Server sich selbst auf dem Medienserver veröffentlichen. Wenn der Servername nicht übereinstimmt, werden die Einträge übersprungen.
- Führen Sie den Exportbefehl nach Abschluss des Imports aus. Die exportierte Datei ist Ihr Backup für alle blockierten Elemente, die importiert wurden.
- Geben Sie den Grund für das Wiederherstellen von blockierten Elemente an, wenn Sie einen Wiederherstellungsauftrag mit der Option "Wiederherstellen blockierter Elemente zulassen" erstellen. Der Grund wird in den Überwachungsprotokollen und -berichten aufgezeichnet. Die Berichte können zu Compliance- und Prüfungszwecken verwendet werden.
- Führen Sie den Importbefehl erneut aus, wenn ein Datenträger auf einen neuen Medienserver verschoben wird und dieser Backup-Sätze mit blockierten Elementen enthält. Wenn Sie dies nicht tun, sind die blockierten Elemente zur Wiederherstellung verfügbar.
- Führen Sie in einer CASO-Umgebung CAS auf allen verwalteten Servern mit Backup Exec 20.3 und höher für Elemente aus, die auf allen Medienservern blockiert werden sollen. Wenn Sie den Importbefehl auf dem CAS ausführen, werden die Informationen automatisch auf dem MBES synchronisiert.
- Führen Sie den Überwachungsprotokollbericht regelmäßig aus, damit alle Vorgänge zu blockierten Elemente aufgezeichnet werden.
- Die CSV-Datei zum Angeben der zu importierenden blockierten Elemente muss folgende Zeichenkodierung aufweisen:
 - Gebietsschemakodierung entsprechend der ANSI- und OEM-Codeseiten
 - UTF-8 mit Bytereihenfolge-Marke (BOM)

- UTF-16 Little Endian mit BOM
- UTF-16 Big Endian mit BOM

Der Importbefehl funktioniert nicht richtig, wenn die Eingabe-CSV-Datei Zeichenfolgen aus mehreren Gebietsschemata enthält.

- Wenn Sie einen virtuellen Computer wiederherstellen oder eine lokale Wiederherstellung des Computers mithilfe von Simplified Disaster Recovery ausführen, müssen Sie die blockierten Elemente manuell löschen oder nach Abschluss der Wiederherstellung ein entsprechendes Skript ausführen. Andernfalls werden die blockierten Elemente wiederhergestellt.

Siehe ["Info zu GDPR Guard"](#) auf Seite 869.

Siehe ["Befehle der Backup Exec-Management-Befehlszeile \(BEMCLI\) zum Importieren und Exportieren"](#) auf Seite 871.

Siehe ["Unterstützte Typen gesicherter Daten"](#) auf Seite 873.

Siehe ["Blockieren des Zugriffs auf gesicherte Elemente"](#) auf Seite 874.

Siehe ["Wiederherstellen blockierter Elemente"](#) auf Seite 875.

Siehe ["Fehlerbehebung beim Blockieren des Zugriffs auf gesicherte Elemente mit GDPR Guard"](#) auf Seite 897.

Fehlerbehebung bei Backup Exec

In diesem Kapitel werden folgende Themen behandelt:

- Fehlerbehebung von Hardware-bezogenen Problemen
- Fehlerbehebung auf Wechslern und Bandlaufwerken
- Weitere Informationen über Warn- und Fehlermeldungen
- Beheben von Fehlern beim Sichern in Backup Exec
- Fehlerbehebung bei ausgefallenen Komponenten in einem SAN
- Beheben von Fehlern mit der Installation von Backup Exec
- Fehlerbehebung beim Blockieren des Zugriffs auf gesicherte Elemente mit GDPR Guard
- Fehlerbehebung bei der Sofortwiederherstellung in der Cloud in Backup Exec
- Verbesserung der Leistung von Backup Exec
- Zugriff auf Veritas Online
- Durchsuchen der Veritas-Supportdatenbank
- Kontaktieren des technischen Support für Backup Exec
- Einsatz des Remote-Support
- Verwalten Ihrer Backup Exec-Support-Fälle
- Infos zu den BackupExec-Diagnosetools
- Ausführen des Hilfe-Tools "Veritas QuickAssist"

- [Generieren einer Diagnosedatei zur Fehlerbehebung von Backup Exec](#)
- [Ausführen des begather-Dienstprogramms, um Fehler bei Backup Exec-Komponenten auf Linux-Servern zu beheben](#)
- [Verwenden von Backup Exec Debug Monitor zur Fehlerbehebung](#)
- [Informationen zum Backup Exec Debug Tool](#)

Fehlerbehebung von Hardware-bezogenen Problemen

Weitere Informationen zu allgemeinen Hardwareproblemen finden Sie in den folgenden häufig gestellten Fragen:

Tabelle 19-1 Fragen zur Hardware

Frage	Antwort
Wie weiß ich, dass mein Speichergerät unterstützt wird?	<p>Die unterstützten Geräte finden Sie in der Liste der mit Backup Exec kompatiblen Hardware.</p> <p>Wenn das Laufwerk in der Liste der kompatiblen Hardware enthalten ist, führen Sie den Assistenten "Speicher konfigurieren" aus und installieren Sie die Gerätetreiber.</p> <p>Siehe "Installieren von Bandgerätetreibern " auf Seite 449.</p> <p>Im Assistenten "Speicher konfigurieren" findet der Assistent für die Installation der Gerätetreiber den geeigneten Treiber für das angeschlossene Bandlaufwerk und installiert ihn.</p>
Wie kann ich eine Fehlerbehebung bei Problemen mit einem Wechsler oder einem Bandlaufwerk durchführen?	<p>Die folgenden Abschnitte enthalten Tipps zur Fehlerbehebung und Konfigurieren von Bandgeräten und Wechslern:</p> <p>Siehe "Fehlerbehebung auf Wechslern und Bandlaufwerken" auf Seite 883.</p> <p>Siehe "Starten und Anhalten von Backup Exec-Diensten" auf Seite 776.</p> <p>Siehe "Löschen von Speichergeräten" auf Seite 546.</p>

Frage	Antwort
<p>Ich erhalte die Fehlermeldung "Speichergerät [Gerät] hat bei folgender Anforderung einen Fehler gemeldet: Lesen/Schreiben von Daten vom/auf Medium. Fehler: Datenfehler (CRC)." Was kann ich tun?</p>	

Frage	Antwort
	<p>Viele Faktoren können den Fehler der zyklischen Redundanzüberprüfung (CRC) verursachen.</p> <p>Die folgende Liste enthält die häufigsten Gründe für diesen Fehler sowie Möglichkeiten zur Behebung:</p> <ul style="list-style-type: none"> ■ Verschmutzte Lese-/Schreibköpfe des Bandgeräts. Informieren Sie sich beim Hardware-Hersteller über geeignete Reinigungstechniken. ■ Fehlerhaftes Medium. Ersetzen Sie das Medium. Verwenden Sie ein neues Band, das vom Hardware-Hersteller zertifiziert wurde. ■ Bandlaufwerk. Laden Sie das entsprechende Backup Exec-Bandlaufwerk. Die unterstützten Geräte finden Sie in der Liste der mit Backup Exec kompatiblen Hardware. ■ Wide-Aushandlung für den SCSI-Controller ist nicht richtig konfiguriert. Wenn es sich um ein Wide-SCSI-Gerät (68 Pins) handelt, sollte die Wide-Aushandlung verwendet werden. Deaktivieren Sie die Wide-Aushandlung, wenn es sich um ein Narrow-SCSI-Gerät (50 Pins) handelt. Verwenden Sie das SCSI-Installationsprogramm des Herstellers, um die Wide-Aushandlung auf der SCSI-Controller-Karte zu deaktivieren. ■ Die Übertragungsrate des SCSI-Controllers ist zu hoch. Verwenden Sie das SCSI-Installationsprogramm des Herstellers, um die SCSI-Übertragungsrate zu verringern. Fragen Sie beim Hersteller des Controllers und des Geräts nach der richtigen Konfiguration für die SCSI-Übertragungsrate. ■ Die synchrone Aushandlung des SCSI-Controllers ist aktiviert. Verwenden Sie das SCSI-Installationsprogramm des Herstellers, um die synchrone Aushandlung auf der SCSI-Controller-Karte zu deaktivieren. Fragen Sie beim Hersteller des Controllers und des Geräts nach der richtigen Konfiguration für synchrone -SCSI-Aushandlung. ■ Falscher Abschluss oder fehlerhafte Kabe. Überprüfen Sie das SCSI-Kabel und dessen ordnungsgemäße Konfiguration des SCSI-Abschlusses. Verwenden Sie nicht gleichzeitig passive und aktive Abschlüsse. ■ Bestätigen Sie, dass das Bandlaufwerk richtig funktioniert. Informieren Sie sich beim Hersteller des Bandlaufwerks über Diagnosesoftware, um den Zustand der Bandlaufwerkshardware zu überprüfen. ■ Allgemeine SCSI-Probleme. Weisen Sie dem Bandlaufwerk eine eigene Controller-Karte zu oder

Frage	Antwort
	versuchen Sie es mit einer anderen SCSI-Karte.
Warum hält mein DLT-Bandlaufwerk an, wenn es einige Bänder katalogisiert?	<p>Das DLT-Bandlaufwerk zeichnet in einem Bandverzeichnisprotokoll interne Informationen über das Band auf. Das Verzeichnisprotokoll wird jedes Mal aktualisiert, bevor das Band aus dem Laufwerk ausgeworfen wird. Wird das Laufwerk jedoch ausgeschaltet, ohne dass das Band zuvor ausgeworfen wurde, gehen die Daten verloren.</p> <p>Die Regenerierung dieser Bandverzeichnisdaten ist sehr langwierig und dauert mehrere Stunden, sodass es den Anschein hat, als wäre das Laufwerk blockiert. Warten Sie, bis der Vorgang abgeschlossen ist und nehmen Sie erst dann das Band aus dem Laufwerk. Der normale Betrieb wird nach der Aktualisierung der Verzeichnisspur wieder aufgenommen.</p>
ein Backup auf mein DLT-Bandlaufwerk hält bei 99-prozentigem Fortschritt an. Was kann ich tun?	<p>Das Backup schlägt möglicherweise fehl, weil die Speicheroption "Medium nach Auftragsabschluss auswerfen" ausgewählt ist und das Bandlaufwerk den Vorgang nicht unterstützt. Bei einigen Bandlaufwerken müssen Sie das Band manuell entfernen, wie z. B. bei den Laufwerken "Digital Linear Tape" (DLT), "Linear Tape-Open" (LTO), "Travon" und "Onstream".</p> <p>Um diese Situation zu beheben, deaktivieren Sie entweder die Speicheroption "Medium nach Auftragsabschluss auswerfen" oder konfigurieren Sie eine automatische Reaktion auf die aktive Warnmeldung.</p> <p>Siehe "Konfigurieren erweiterter Optionen für Backup-Aufträge" auf Seite 223.</p>

Fehlerbehebung auf Wechslern und Bandlaufwerken

Dieser Abschnitt enthält Fehlerbehebungsverfahren, die beim Beheben von Problemen auf Wechslern und Bandlaufwerken helfen können. Führen Sie diese in der angegebenen Reihenfolge durch.

Mehrere dieser Fehlerbehebungsverfahren nutzen Veritas QuickAssist (VQA).

Zuerst prüfen Sie, ob das Betriebssystem das Gerät erkennt. Wiederholen Sie diesen Vorgang, wenn Backup Exec externe Band-Hardware nicht mehr verwalten kann. Befindet sich das Bandlaufwerk in einem Storage Area Network (SAN), müssen Sie dieses aus- und wieder einschalten, damit das Gerät erkannt wird. Es wird empfohlen, das Bandlaufwerk an einer Backup-Stromversorgung mit Überlastungsschutz anzuschließen.

Außerdem muss die neueste Firmware für Bandgerät, Wechsler und Host-Bus-Adapter installiert sein. Die aktuelle Firmware und Gerätetreiber erhalten Sie bei Hersteller.

Gewährleisten Sie, dass Ihre Lizenz und die installierten Funktionen die Anzahl der erforderlichen Laufwerke unterstützen. Abhängig von der Backup Exec-Edition und -Lizenz müssen Sie möglicherweise Unterstützung für zusätzliche Bandlaufwerke in Wechslern erwerben, oder auf eine andere Edition aktualisieren. Weitere Informationen finden Sie im Lizenzierungshandbuch zu Backup Exec.

Prüfen Sie die Liste der mit Backup Exec kompatiblen Hardware.

1. Die die Liste der mit Backup Exec kompatiblen Hardware (HCL) hilft beim Prüfen, ob Backup Exec die Geräte, Abfragezeichenfolgen und Verbindungsmethoden unterstützt. Prüfen Sie in der HCL, ob das Gerät offiziell von Backup Exec unterstützt wird.
2. Prüfen Sie außerdem, ob die Abfragezeichenfolge für das Gerät der in der HCL entspricht.
3. Prüfen Sie weiterhin, ob die Verbindungsmethode zwischen Server und Gerät unterstützt wird. Viele Geräte unterstützen mehrere Verbindungsmethoden. Diese Geräte werden mehrmals in der HCL aufgeführt. Einige Verbindungsmethoden sind möglicherweise für ein bestimmtes Gerät geeignet, aber nicht in der HCL aufgeführt. Ist dies der Fall, wird sie nicht offiziell unterstützt.

Verifizieren der Administratorrechte für das Backup Exec-Dienstkonto

1. Prüfen Sie, ob das Backup Exec-Dienstkonto ein Domänenadministrator- oder ein integriertes Administratorkonto ist.

Sie können dafür das Tool "VQA" verwenden.

- Klicken Sie unter Backup Exec 2012 und höher auf die Backup Exec-Schaltfläche und wählen Sie "Konfiguration und Einstellungen" und dann WBackup Exec Services".
 - Wählen Sie unter Backup Exec 2010 im Menü "Backup Exec-Tools" die Option "Backup Exec Services" und klicken Sie dann auf "Identifikationsdaten".
2. Stellen Sie sicher, dass das Konto die folgenden grundlegenden Rechte und Berechtigungen hat:
 - Einsetzen als Teil des Betriebssystems
 - Sichern von Dateien und Verzeichnissen
 - Erstellen eines Tokenobjekts

- Anmelden als Stapelverarbeitungsauftrag
- Anmelden als Dienst
- Verwalten von Überwachungs- und Sicherheitsprotokollen
- Wiederherstellen von Dateien und Verzeichnissen
- Übernehmen des Besitzes von Dateien und Objekten

Beenden und Deaktivieren des Wechselmediendienstes

1. Dieses Verfahren gilt nur für Windows Server 2003/XP. Wählen Sie in Windows "Start, Systemsteuerung und Verwaltung" und doppelklicken Sie auf "Dienste". Sie können dafür das Tool "VQA" verwenden.
2. Klicken Sie auf "Wechselmediendienst" und dann auf "Beenden" und "Deaktivieren". Wenn ein Fehler angezeigt wird, ignorieren Sie diesen. Nach einem Neustart des Servers sollte dieser Fehler nicht wieder auftreten.
3. Starten Sie den Server neu.

Prüfen der Systemereignisprotokolle auf Hardwarefehler

1. Klicken Sie in Windows mit der rechten Maustaste auf "Arbeitsplatz" und wählen Sie im Kontextmenü die Option "Verwalten".
2. Erweitern Sie "Computerverwaltung > System > Ereignisanzeige" und klicken Sie dann auf "System". Unter bestimmten Windows-Versionen lautet der Pfad "Computerverwaltung > System > Ereignisanzeige > Windows-Protokolle > System".
3. Suchen Sie in den Protokollen nach Hardwarefehlern.

Außerdem müssen die neuesten Gerätetreiber für das Bandgerät installiert sein.

-
1. **Hinweis:** Backup Exec wurde nur mit den Treibern getestet, die in der Liste der kompatiblen Hardware aufgeführt sind.
-

Wenn Sie die neueste Version von Backup Exec installiert haben, sollten die neuesten Treiber bereits vorhanden sein. Wenn die Treiber veraltet sind, finden Sie unter "Backup Exec-Bandgerätetreiber > Treiber" eine Liste der zum Herunterladen verfügbaren Treiber.

2. Verwenden Sie zum Installieren der Treiber `Tapeinst.exe`. Dieses Programm wird auf die Festplatte kopiert, wenn Sie Backup Exec installieren.
3. Prüfen Sie im Windows-Geräte-Manager, ob die Bandgerätetreiber installiert wurden.

- Windows 2008: Klicken Sie mit der rechten Maustaste auf "Computer > Verwalten", erweitern Sie "Server-Manager > Diagnose" und klicken Sie dann auf "Geräte-Manager".
 - Windows 2003: Klicken Sie mit der rechten Maustaste auf "Arbeitsplatz > Verwalten", erweitern Sie "Computerverwaltung" und klicken Sie dann auf "Geräte-Manager".
4. Klicken Sie im Geräte-Manager mit der rechten Maustaste auf den Bandgerätetreiber und wählen Sie im Kontextmenü die Option "Eigenschaften".
 5. Klicken Sie auf die Registerkarte "Treiber" und gewährleisten Sie, dass der Treiberanbieter Veritas ist.

Deinstallieren von Anwendungen anderer Hersteller, die das Bandgerät steuern

1. Backup Exec kommuniziert möglicherweise nicht ordnungsgemäß mit Bandgeräten, wenn eine Backup-Anwendung eines anderen Herstellers installiert ist. Dies kann auftreten, selbst wenn die Dienste für die Anwendung deaktiviert sind. Klicken Sie auf "Start > Systemsteuerung > Software".

Hinweis: Deinstallieren Sie Banddiagnose-Tools nicht, wenn Backup Exec-Dienste ausgeführt werden. Entfernen Sie die Banddiagnose-Tools, wenn die Diagnose abgeschlossen ist.

2. Wählen Sie das Programm aus und klicken Sie auf "Deinstallieren".
3. Wiederholen Sie die Deinstallation für alle Programme anderer Anbieter, die eine ordnungsgemäße Kommunikation mit Backup Exec-Kommunikation verhindern.

Gewährleisten, dass die Microsoft-Standardtreiber für Medienwechsler installiert sind

1. Dieses Verfahren bezieht sich nur auf Wechslergeräte. Rufen Sie den Windows-Geräte-Manager auf:
 - Windows Server 2008: Klicken Sie mit der rechten Maustaste auf "Computer" und wählen Sie im Kontextmenü die Option "Verwalten". Erweitern Sie "Server-Manager > Diagnose" und klicken Sie dann auf "Geräte-Manager".
 - Windows Server 2003: Klicken Sie mit der rechten Maustaste auf "Arbeitsplatz" und wählen Sie im Kontextmenü die Option "Verwalten". Erweitern Sie "Computerverwaltung" und klicken Sie dann auf "Geräte-Manager".

2. Erweitern Sie den Eintrag "Medienwechsler" und prüfen Sie, ob "Unbekannter Medienwechsler" aufgeführt ist. Wenn "Unbekannter Medienwechsler" aufgeführt ist, sind die Microsoft-Standardtreiber installiert.
3. Wenn OEM-Treiber installiert sind, klicken Sie mit der rechten Maustaste auf den OEM-Treiber und wählen Sie im Kontextmenü "Eigenschaften > Treiber aktualisieren". Der Microsoft-Treiber wird installiert und "Unbekannter Medienwechsler" wird angezeigt.

Verwenden Sie das Tool "Discover" zum Beheben von Hardwarefehlern und Reservierungskonflikten

1. Discover zeigt detaillierte Attribute der am Server angeschlossenen Backup-Geräte an. Beenden Sie zuerst die Backup Exec-Dienste.
2. Öffnen Sie den Installationsordner von Backup Exec.
3. Führen Sie den folgenden Befehl in einer Eingabeaufforderung aus, um das Tool zu starten und eine Textausgabe zu erzeugen: `Discover.exe > C:\discover.txt`

Verwenden von `tracer.exe` zum Beheben von Fehlern mit SCSI

1. Verifizieren Sie zuerst, ob der SCSI-Wechslerdienst ausgeführt wird. Klicken Sie auf "Start". Geben Sie im Suchfeld `msinfo32` ein und drücken Sie die Eingabetaste.
 Sie können dafür das Tool "VQA" verwenden.
2. Erweitern Sie im Dialogfeld "Systeminformationen" den Eintrag "Softwareumgebung" und klicken Sie dann auf "Systemtreiber."
3. Suchen Sie das Gerät "SCSIChanger" und prüfen Sie, ob der Status "Wird ausgeführt" ist.
4. Beenden Sie anschließend die Backup Exec-Dienste.
5. Öffnen Sie den Backup Exec-Ordner und starten Sie `tracer.exe`. Tracer beginnt mit der Erfassung von SCSI-Daten.
6. Starten Sie die Backup Exec-Dienste wieder. Um die Dienste neu starten, starten Sie im Backup Exec-Ordner das Programm `Servicesmgr.exe`.
7. Nach dem Starten der Dienste überprüfen Sie des Tracer-Protokoll auf Hardwarefehler und Reservierungskonflikte.

Erkennen und Deinstallieren verwaister Geräte

1. Verwaiste Geräte können im Geräte-Manager vorhanden sein, nachdem Sie Hardware austauschen oder Treiber und Firmware aktualisieren. Öffnen Sie

zuerst den Windows-Geräte-Manager, indem Sie folgenden Befehle in der Eingabeaufforderung eingeben:

```
C:\cd WINDOWS
```

```
C:\WINDOWS>cd system32
```

```
C:\WINDOWS\system32>devmgmt.msc
```

```
C:\Windows\System32>
```

2. Wählen Sie im Geräte-Manager im Menü "Ansicht" die Option "Ausgeblendete Geräte anzeigen". Es werden alle Gerätetreiber angezeigt, auch die derzeit nicht auf dem Computer installierten.
3. Erweitern Sie folgende Geräte: Klicken Sie mit der rechten Maustaste auf die Geräte, die nicht fett angezeigt werden, und wählen Sie im Kontextmenü die Option "Deinstallieren".
 - Medienwechsler
 - Bandlaufwerke
 - SCSI-Karten

Geräte, die nicht fett formatiert sind, sind nicht geladen und können deinstalliert werden.

Warnung: Das Entfernen von Geräten und Treibern, die noch vom Computer benötigt werden, kann dazu führen, dass er instabil wird und nicht mehr gestartet werden kann.

Deaktivieren, Löschen und Aktivieren von Geräten in Backup Exec

1. Klicken Sie in der Backup Exec-Konsole auf die Registerkarte "Geräte/Speicher".
2. Klicken Sie mit der rechten Maustaste auf das Gerät und wählen Sie die Option "Deaktivieren".
 Unter Backup Exec 2010 und niedriger deaktivieren Sie die Option "Aktivieren". Wenn das Kontrollkästchen für diese Option deaktiviert ist, ist das Gerät deaktiviert.
3. Klicken Sie mit der rechten Maustaste auf das Gerät und wählen Sie die Option "Löschen". Sie werden eventuell aufgefordert, Backup-Aufträge auf andere Geräte oder Gerätepools zu verschieben. Unter Backup Exec 2012 wird die Aufforderung "Aufträge umleiten" angezeigt.

4. Notieren Sie sich die betroffenen Aufträge und verschieben Sie diese zurück auf das ursprüngliche Gerät, nachdem Sie das Problem mit dem Gerät behoben haben.
5. Beenden Sie die Backup Exec-Dienste.
6. Öffnen Sie den Backup Exec-Ordner und führen Sie `Tapeinst.exe` aus.
7. Aktivieren Sie im Backup Exec-Gerätetreiber-Installationsprogramm die folgenden Optionen:
 - Bandtreiber für alle unterstützten Bandgeräte verwenden
 - Einträge für nicht verfügbare, entfernte oder ausgeschaltete Bandgeräte löschen
 - Windows 2000 und höher: Plug&Play-Treiber verwenden
8. Starten Sie die Backup Exec-Dienste wieder.

Weitere Informationen über Warn- und Fehlermeldungen

Backup Exec zeigt eine Fehlermeldung an, sobald eine Situation eintritt, die Ihre Aufmerksamkeit oder eine Benutzerreaktion erfordert. Die meisten Warn- und Fehlermeldungen sind selbsterklärend, in manchen Fällen benötigen Sie für die Fehlerbehebung jedoch Zusatzinformationen.

Weitere Informationen zu Backup Exec-Warn- und -Fehlermeldungen erhalten Sie auf folgende Weise:

- In der Warnmeldung klicken Sie auf den Link, um weitere Informationen zu erhalten, oder schauen Sie im Auftragsprotokoll nach und klicken Sie auf den UMI-Link. Dieser Code ist ein Hyperlink zur Website des technischen Supports von Veritas. Hier finden Sie technische Hinweise in direktem Bezug auf die Meldung.
 Siehe "[Verknüpfung des Auftragsprotokolls mit der Website des technischen Supports von Veritas](#)" auf Seite 313.
- Suchen Sie in der technischen Supportdatenbank von Veritas nach dem Fehler.
 Siehe "[Durchsuchen der Veritas-Supportdatenbank](#)" auf Seite 901.

Beheben von Fehlern beim Sichern in Backup Exec

Bei Problemen mit dem Backup von Daten lesen Sie folgende Fragen durch.

Tabelle 19-2 Fragen zu Backups

Frage	Antwort
Es ist nicht möglich, auf meinem System bestimmte Dateien zu sichern, die von anderen Vorgängen verwendet werden. Woran liegt das?	<p>Für Backups ohne Snapshot in Backup Exec-Dateien, die von einem anderen Prozess verwendet werden, überspringt sie entweder die Datei oder wartet darauf, dass die Datei verfügbar wird. Diese Aktionen hängen von den Optionen für Backups ohne Snapshots ab, die Sie beim Erstellen des Backups konfigurieren.</p> <p>Siehe "Konfigurieren von Datei- und Ordneroptionen für Backup-Aufträge" auf Seite 676.</p> <p>Wenn Sie Backup Exec konfigurieren, um geöffnete Dateien mit einer Sperre zu sichern, versucht das Programm, die Dateien in einem anderen Modus zu öffnen. Es sperrt diese Dateien während des Backups, damit andere Prozesse nicht auf diese Dateien schreiben können. Es wird empfohlen, dass Sie die Anwendungen schließen, die Dateien geöffnet lassen, damit die Dateien in einem konsistenten Zustand gesichert werden.</p> <p>Um geöffnete Dateien auf Windows-Computern zu sichern, verwenden Sie die Optionen "Advanced Open File", um die Backups zu konfigurieren, die Snapshot-Technologie verwenden.</p> <p>Siehe "Konfigurieren von Advanced Open File-Optionen für Backup-Aufträge" auf Seite 664.</p>
Warum verfügt die Backup Exec-Administratorkonsole weiterhin über ein Speichergerät, selbst wenn es nicht ausgeführt wird?	<p>Backup Exec ist eine vollwertige Client-/Server-Anwendung, die ständig zum Verarbeiten von Aufträgen lokaler und standortferner Administratorkonsolen verfügbar sein muss.</p> <p>Die Backup Exec Services beanspruchen alle Speichergeräte, die am Backup Exec-Server angeschlossen sind, wenn die Dienste ausgeführt werden. Backup Exec erfordert konstante Kontrolle der Speichergeräte, um Statistiken über Medien und Speichergerätverwendung zu sammeln, und Medienüberschreibschutz, wenn erforderlich, zu bieten.</p>

Frage	Antwort
Wenn ich ein lokales Backup durchführe, entspricht die Gesamtzahl der von Backup Exec gesicherten Byte nicht der in Windows angezeigten Anzahl. Woran liegt das?	<p>Der Typ der Partition, für den das System formatiert wird, verursacht möglicherweise dieses Problem.</p> <p>Wenn Sie eine komprimierte NTFS-Partition von Windows haben, zeigt Backup Exec die nicht komprimierten Byteanzahl der Dateien an, die gesichert werden. Unterdessen zeigt Windows-Explorer die komprimierte Byteanzahl der Dateien auf der Festplatte an. Beispielsweise komprimiert Windows eine NTFS-Partition, die 1 GB von Daten zu 500 MB enthält. Backup Exec zeigt an, dass 1 GB Daten gesichert wurden, während Windows Explorer nur die 500 MB komprimierten Daten auf der Festplatte anzeigt.</p> <p>Wenn Sie über eine FAT-Partition verfügen, gibt Backup Exec die tatsächliche Anzahl der Byte in den gesicherten Dateien an, während der Datei-Manager eine größere Menge an verbrauchtem Speicherplatz angibt. Zum Beispiel besitzt eine FAT-Partition von 2 GB eine Clustergröße von 32 KB und der Datei-Manager zeigt an, dass 1,9 GB der Partition belegt ist. Backup Exec zeigt an, dass nur 1,4 GB Daten gesichert wurden. Auch wenn beispielsweise die Datei "pagefile.sys" mit 50 MB Daten vom Backup ausgeschlossen wurde, ergibt dies eine Differenz von 450 MB bei der Anzahl der Byte.</p> <p>Beim Umwandeln in NTFS, können Sie Speicherplatz sparen, da NTFS effizienter und mit kleineren Standardclustergrößen (wird von Windows automatisch eingestellt) arbeitet als FAT. Unter Windows können Sie auch andere Clustergrößen als die Standardgrößen verwenden, was jedoch die Systemleistung beeinträchtigen kann. Weitere Informationen dazu finden Sie in der Windows-Dokumentation.</p>
Wie kann ich den vorhandenen Datenbankverschlüsselungscode ändern, wenn ich glaube, dass er gefährdet ist, oder um ihn an die Unternehmensrichtlinien anzupassen?	<p>Sie können einen Datenbankverschlüsselungscode jederzeit aktualisieren. Weitere Informationen zum Aktualisieren von Datenbankverschlüsselungscodes finden sie im folgenden Thema:</p> <p>Siehe "Aktualisieren von Backup Exec-Datenbankverschlüsselungscodes" auf Seite 700.</p>

Frage	Antwort
Warum sinkt die Systemleistung beim Sichern von Remote-Datenträgern?	<p>Die lokalen Laufwerke des Backup Exec-Servers können normalerweise schneller gesichert werden als Remote-Server über ein Netzwerk.</p> <p>Die Geschwindigkeit des Backup für einen Remote-Datenträger wird von der Geschwindigkeit der physischen Verbindung begrenzt. Die Geschwindigkeit, mit der die Festplatten eines Remote-Servers gesichert werden können, ist von folgenden Faktoren abhängig:</p> <ul style="list-style-type: none"> ■ Marke/Modell der Netzwerkkarten ■ Konfiguration von Modus/Rahmentyp für den Netzwerkadapter ■ Verbindungsgeräte (Hubs, Switches, Router usw.) ■ Windows-Einstellungen

Fehlerbehebung bei ausgefallenen Komponenten in einem SAN

In einem SAN können unterschiedliche Probleme an verschiedenen Stellen auftreten. Damit Backup Exec richtig funktioniert, muss ein Speichergerät wie folgt erkannt werden:

- Die Brücke oder der Router müssen es als SCSI-Gerät erkennen.
- Das Betriebssystem muss es als Gerät erkennen.
- Backup Exec muss es als unterstütztes Gerät erkennen.

In einigen Fällen müssen Sie sich bei Hardwareproblemen an Ihren Hardwarehersteller wenden.

Sie müssen dann möglicherweise eine Komponente des SAN austauschen, z. B. eine Brücke oder einen Switch. Informationen zu den jeweiligen Schritten zum Austauschen von Geräten finden Sie in der Dokumentation Ihres Hardwareherstellers.

Siehe ["Fehlerbehebung bei Offline-Speichergeräten in einem SAN "](#) auf Seite 892.

Fehlerbehebung bei Offline-Speichergeräten in einem SAN

Wenn ein Gerät im SAN nicht mehr online ist, führen Sie diese Schritte aus, um die Ursache des Problems zu bestimmen.

Bevor Sie mit der Fehlerbehebung beginnen, überprüfen Sie, ob die Speichergeräte in der Liste der von Backup Exec unterstützten Geräte enthalten sind.

Die unterstützten Betriebssysteme, Plattformen und Anwendungen finden Sie in der Liste der mit Backup Exec kompatiblen Software.

Stellen Sie außerdem sicher, dass alle Hardware-Treiber aktuell sind und gestartet wurden. Wenn Ihre Hardware fehlerhaft ist, bitten Sie den Hardwarehersteller um genaue Anweisungen.

Tabelle 19-3 Fehlerbehebung bei Offline-Speichergeräten in einem SAN

Schritt	Aktion
Schritt 1	Überprüfen Sie mithilfe des Windows Geräte-Managers, ob das Betriebssystem das Gerät erkennt. Wenn das Gerät nicht erkannt wird, muss auf dem Gerät möglicherweise eine Fehlerbehebung ausgeführt werden. Siehe "Suchen von Hardwarefehlern in einem SAN" auf Seite 894.
Schritt 2	Stellen Sie bei Wechslern sicher, dass die Wechslerunterstützung installiert ist.
Schritt 3	Überprüfen Sie das Ereignisprotokoll auf die folgenden Fehlermeldungen, durch die SAN-Verbindungsfehler angegeben werden: SCSI-Fehler 9, 11 und 15 oder Zeitüberschreitungsfehler bei der Speicherung. Überprüfen Sie das Anwendungsereignisprotokoll auf das mehrfache Auftreten des Ereignisses 33152. Durch diese Ereignisse werden SAN-Kommunikationsfehler angegeben. Siehe "Suchen von Hardwarefehlern in einem SAN" auf Seite 894. Eventuell müssen Sie sich an Ihren Hardware-Händler wenden.

Schritt	Aktion
Schritt 4	<p>Wenn der Wechsler online ist, einige oder alle Laufwerke jedoch offline sind, initialisieren Sie den Wechsler mit Backup Exec.</p> <p>Siehe "Initialisieren eines Wechslers" auf Seite 553.</p>
Schritt 5	<p>Wenn das Initialisieren der Bibliothek die Speichergeräte nicht in den Onlinezustand versetzt, überprüfen Sie die Bibliothek auf eine Fehleranzeige auf der Vorderseite, auf mechanische Probleme oder auf Bänder, die nicht im Laufwerk sein sollten. Beheben Sie ggf. gefundene Fehler.</p>
Schritt 6	<p>Wenn in der Bibliothek keine Fehler vorhanden sind oder Sie diese behoben haben, die Speichergeräte jedoch noch offline sind, beenden Sie Backup Exec-Dienste und starten Sie sie neu.</p> <p>Siehe "Starten und Anhalten von Backup Exec-Diensten" auf Seite 776.</p>
Schritt 7	<p>Wenn die Speichergeräte durch den Neustart der Dienste nicht online geschaltet werden, starten Sie das Betriebssystem neu. Stellen Sie sicher, dass beim Neustart keine Backup Exec-Aufträge ausgeführt werden.</p>
Schritt 8	<p>Wenn die Geräte durch den Neustart des Betriebssystems nicht online geschaltet werden, setzen Sie das SAN zurück, um den Bandspeicher zu bestimmen, bei dem ein Problem vorliegt. Fibre Channel-Probleme können auch durch ein Recycling des SAN gelöst werden.</p> <p>Siehe "Zurücksetzen des SAN" auf Seite 895.</p>

Suchen von Hardwarefehlern in einem SAN

Mit den folgenden Schritten können Sie nach allgemeinen Hardwarefehlern suchen, die in einem SAN auftreten. Wenn Ihre Hardware fehlerhaft ist, bitten Sie den Hardwarehersteller um genaue Anweisungen.

Tabelle 19-4 Suchen von Hardwarefehlern in einem SAN

Schritt	Aktion
Schritt 1	Überprüfen Sie, ob die richtigen Gerätetreiber installiert sind.
Schritt 2	Überprüfen Sie, ob das Fibre Channel-Kabel fest mit dem HBA und dem Fibre Channel Switch verbunden ist.
Schritt 3	Überprüfen Sie, ob der Wechsler mit dem Fibre Channel Switch über eine Fibre Channel-Verbindung ordnungsgemäß verbunden ist.
Schritt 4	Prüfen Sie auf eine ausgefallene Hardwarekomponente zwischen dem Server und dem Fibre Channel Switch. Manchmal erkennen einige der Server im SAN das Speichergerät, andere Server jedoch nicht. Wenn kein Server im SAN das Speichergerät erkennt, prüfen Sie auf eine ausgefallene Hardwarekomponente zwischen dem Fibre Channel Switch und dem Speichergerät.
Schritt 5	Setzen Sie das SAN zurück. Dadurch werden möglicherweise Hardwarekomponenten, die Probleme aufweisen, erkannt und Fibre Channel-Probleme gelöst. Siehe "Zurücksetzen des SAN" auf Seite 895.

Zurücksetzen des SAN

Beim Zurücksetzen des SAN werden die Komponenten des SAN abgeschaltet und anschließend in einer bestimmten Reihenfolge wieder eingeschaltet.

Tabelle 19-5 Zurücksetzen des SAN

Schritt	Aktion
Schritt 1	Schalten Sie alle Server, Wechsler und Fibre Channel-Brücken im SAN aus. In seltenen Fällen müssen Sie möglicherweise auch den Fibre Channel Switch ausschalten. Wenn Sie den Switch ausschalten müssen, sollten Sie ihn vor allen anderen Komponenten einschalten. Warten Sie, bis alle Prüfungen abgeschlossen sind, bevor Sie die anderen Komponenten einschalten.
Schritt 2	Schalten Sie den Wechsler ein. Siehe "Initialisieren eines Wechslers" auf Seite 553.
Schritt 3	Überprüfen Sie, ob der Fibre Channel Switch den Wechsler erkennt.
Schritt 4	Schalten Sie den zentralen Administrationsserver ein.
Schritt 5	Überprüfen Sie, ob das Betriebssystem den Wechsler und die Laufwerke erkennt.
Schritt 6	Schalten Sie einen der verwalteten Backup Exec-Server ein. Warten Sie, bis der verwaltete Backup Exec-Server gestartet wurde, bevor Sie die anderen verwalteten Backup Exec-Server einschalten.

Onlineschalten von Speichergeräten nach dem unsicheren Entfernen eines Geräts in einem SAN

Wenn ein Speichergerät beim unsicheren Entfernen des Geräts von Backup Exec verwendet wird, wird das Gerät in Backup Exec als offline angezeigt.

Tabelle 19-6 Onlineschalten eines Geräts nach dem unsicheren Entfernen des Geräts

Schritt	Aktion
Schritt 1	Stellen Sie sicher, dass im SAN keine Backup Exec-Aufträge ausgeführt werden.

Schritt	Aktion
Schritt 2	<p>Verwenden Sie Backup Exec, um den Wechsler zu initialisieren, wenn dieser online ist, die Laufwerke jedoch offline sind.</p> <p>Siehe "Initialisieren eines Wechslers" auf Seite 553.</p>
Schritt 3	<p>Beenden Sie alle Backup Exec-Dienste und starten Sie sie dann neu, wenn die Bibliothek oder das Laufwerk nach der Initialisierung offline ist.</p> <p>Wenn das Gerät nicht online ist, muss auf dem Gerät möglicherweise eine Fehlerbehebung ausgeführt werden.</p> <p>Siehe "Suchen von Hardwarefehlern in einem SAN" auf Seite 894.</p>

Beheben von Fehlern mit der Installation von Backup Exec

Lesen Sie folgende Punkte, wenn Sie Probleme mit der Installation von .NET haben.

- Wenn die Installation von .NET 4.6 fehlschlägt, installieren Sie die Software manuell, bevor Sie die Installation von Backup Exec wiederholen. Auf diese Weise können Sie Fehler in Backup Exec von solchen mit dem Installationsprogramm von Microsoft .NET oder in der Umgebung trennen.
- In der Datei "BKUPINST20.htm" werden Fehler protokolliert, die bei der Installation von .NET auftreten. Ausführliche Informationen finden Sie in den Installationsprotokollen von .NET 4.6 im Ordner "%temp%": Microsoft .NET Framework 4.6 Setup_*.html und Dd_NDP46-KB3045557-x86-x64-AllOS-ENU_decompression_log.txt.

Fehlerbehebung beim Blockieren des Zugriffs auf gesicherte Elemente mit GDPR Guard

Lesen Sie folgende Punkte, wenn Sie Probleme beim Blockieren des Zugriffs auf gesicherte Elemente mit GDPR Guard haben.

- Wenn das Importieren zwar abgeschlossen wurde, aber Such- und Wiederherstellungsansicht weiterhin die blockierten Elemente enthalten, prüfen Sie Folgendes:
 - ob der vollständige Pfad eines Elementeintrag in der CSV-Datei ein Komma (,) enthält Wenn der Name der Datei bzw. eines Ordners im Pfad ein Komma enthält, wird der Eintrag nicht ordnungsgemäß importiert. Beispiel: E:\Folder,Delimited\Datei.txt und E:\F1\ab,a.txt sind ungültige Einträge für blockierte Elemente.
 - Bestimmte Einträge werden möglicherweise blockiert, wenn der vollständige Pfad einen Platzhalter in einem Ordner enthält, der auch für die Elemente dieses Ordners und seiner Unterordner gilt. Beispiel: E:\F1*.txt blockiert alle Textdateien in den Ordnern "E:\F1" und "E:\F1\F2", die mit "a" beginnen. Um sicherzustellen, dass Elemente in Unterordnern nicht blockiert wird, müssen Sie jeden Eintrag separat hinzufügen und dürfen in diesem Fall keine Platzhalter verwenden.
 - Wenn derselbe Server mit unterschiedlichen Namen Backup Exec hinzugefügt wird (z. B. NetBIOS-Name, FQDN oder IP-Adresse), werden die Elemente werden nur für den Servernamen blockiert, der in der CSV-Datei steht. Um dieses Problem zu beheben, fügen Sie in der CSV-Datei zum Importieren einen separaten Eintrag für jeden Servernamen ein.
- Wenn einige blockierte Elemente aufgrund eines ungültigen Elementpfads beim Importieren übersprungen werden, prüfen Sie Folgendes:
 - Der vollständige Pfad für das übersprungene Element darf nicht mit dem Namen des Datenträger oder der Freigabe, sondern muss mit dem Servernamen beginnen. Beispiel: "E:\folder1*.txt" und "TestShare\F1\b.txt" sind gültige Einträge für den vollständigen Pfad.
 - Nur der Dateiname im Elementpfad darf den Platzhalter "*" enthalten. Wenn der Ordnerpfad den Platzhalter enthält, wird der Eintrag übersprungen. Beispiel: G:\Test2*\CatTrans.xml und G:*\results.txt sind ungültige Einträge.
- Wenn Importvorgänge mit der folgenden Fehlermeldung fehlschlagen: "Fehler beim Verarbeiten eines blockierten Elements. Die interne Liste blockierter Elemente ist nicht verfügbar.":
Prüfen Sie, ob der Pfad der Eingabe-CSV-Datei auf ein ungültiges Laufwerk oder einen ungültigen Netzwerkspeicherort verweist.
- Wenn Exportvorgänge mit folgender Fehlermeldung beendet wird: "Fehler beim Öffnen der internen Liste blockierter Elemente":
Gewährleisten Sie, dass der Ausgabepfad auf ein gültiges Laufwerk bzw. einen gültigen Netzwerkspeicherort verweist.

- Wenn blockierte Elemente in der Such- oder Wiederherstellungsansicht angezeigt werden, kann dies folgende Ursachen haben:
 - Die CSV-Datei mit einigen blockierten Elemente derselben Ressource wird importiert.
 - Die interne Liste der blockierten Elemente für diese Ressource hat die Integritätsprüfung nicht bestanden oder beim Lesen der internen Liste für die Wiederherstellungs- oder Suchansicht ist ein Problem aufgetreten.
Wenn der Wiederherstellungsauftrag ausgeführt wird, wird im Protokoll nicht der Grund für den Fehler beim Lesen der internen Liste blockierter Elemente angezeigt.
- Wenn in der CSV-Datei ein weicher oder harter Verknüpfungspfad angegeben ist, wird nur die Verknüpfung blockiert. Um den Ordner zu blockieren, auf den die Verknüpfung verweist, geben Sie den tatsächlichen Pfad zum Ordner in die CSV-Datei ein.
- Wenn Sie einen Eintrag für ein blockiertes Element aus einer bereits importierten CSV-Datei entfernen möchten, gehen Sie dazu in folgender Reihenfolge vor:
 - Führen Sie den Exportbefehl aus.
 - Entfernen Sie den Eintrag aus der erzeugten CSV-Datei.
 - Löschen Sie die interne Datei mit der Liste der blockierten Elemente für die Ressource, deren Eintrag entfernt wurde, aus dem folgenden Speicherort:
Backup Exec-Installationsordner\data\BLFileInfo
 - Führen Sie den Importbefehl erneut mit dem Parameter `ResetIfCorrupted` aus:


```
Import-BEItemsToBlock - RESETIfCorrupted - CsvFilePath <Pfad zur CSV-Datei> - ColumnNameForServerName <Name der ersten Spalte> - ColumnNameForBlockedItemPath <Name der zweiten Spalte>
```
- Wenn die Wiederherstellungs- und Suchansichten lange Zeit keine Ergebnisse anzeigen, wird eventuell eine große Anzahl von blockierten Elemente für diese Ressource hinzugefügt. In diesem Fall kann der Wiederherstellungsauftrag weiterhin auf Ordner- oder Datenträgerebene ausgeführt werden, um die Elemente anzuzeigen, die wiederhergestellt und angezeigt werden.
- Wenn ein eigenständiger Medienserver mit blockierten Elementen in einen MBES konvertiert werden muss, führen Sie die folgenden Schritte in der angegebenen Reihenfolge aus:
 - Exportieren Sie die Datei mit den blockierten Elementen.
 - Löschen Sie die Bin-Dateien aus dem Ordner `Data\BLFileInfo` im Backup Exec-Installationsordner.

- Konvertieren Sie den eigenständigen Server in einen MBES.
- Importieren Sie die blockierten Elemente in CAS mit der exportierten Datei, die Sie erstellt haben.

Siehe ["Info zu GDPR Guard"](#) auf Seite 869.

Fehlerbehebung bei der Sofortwiederherstellung in der Cloud in Backup Exec

Lesen Sie folgende Punkte, wenn Probleme mit der Funktion "Sofortwiederherstellung in der Cloud" von Backup Exec auftreten:

- Wenn beim Herstellen der ersten Verbindung zu Azure Site Recovery (Azure-Portal) Fehler auftreten, stellen Sie sicher, dass die Mindestanforderungen für Internet Explorer erfüllt sind. Unter dem folgenden Link finden eine Liste der unterstützten Browser:
<https://docs.microsoft.com/en-us/azure/azure-preview-portal-supported-browsers-devices>
Das Portal muss im Browser verfügbar sein, bevor Sie versuchen, Verbindungsprobleme zu beheben.
- Die Systemuhr muss mit der Internetzeit übereinstimmen. Ein Unterschied führt dazu, dass Zertifikatsfehler bei der Verbindung zu Azure Site Recovery auftreten.

Verbesserung der Leistung von Backup Exec

Um die beste Leistung von Backup Exec zu erhalten, sollten Sie einige Faktoren überprüfen:

- Datenübertragungspfad
- Backup Exec-Agentleistung
- Netzwerkleistung
- Backup Exec-Server-Leistung
- Speichergeräteleistung

Weitere Informationen zum Messen und Optimieren der Leistung dieser Elemente finden Sie unter folgender URL:

Siehe ["Verbessern von Backups in Backup Exec"](#) auf Seite 156.

Siehe ["Fehlerbehebung bei der Backup-Leistung"](#) auf Seite 160.

Zugriff auf Veritas Online

Sie können auf Veritas-Community-Foren zugreifen, sich über Schulungen informieren und Veritas-Websites aufrufen.

Tabelle 19-7 Einträge im Menü "Veritas Online"

Element	Beschreibung
Teilen Sie Ihre Ideen mit	Stellt eine Verbindung zum Veritas Connect-Forum her, in dem Sie Ihre Ideen zur Verbesserung von Backup Exec veröffentlichen können.
Schulungsangebote	Stellt Links zu allen Veritas Education-Diensten für Schulungen und benutzerdefinierten Lernoptionen zur Verfügung.
Backup Exec Tech Center	Enthält Links zu Backup Exec-Schulungen.
Backup Exec-Seite	Hier finden Sie Links zu den Ressourcen für Backup Exec.
Veritas Startseite	Ruft die Veritas-Website auf.

So greifen Sie auf Veritas Online zu

- ◆ Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "VeritasVeritas Online" und dann den entsprechenden Menüeintrag aus.

Siehe ["Durchsuchen der Veritas-Supportdatenbank"](#) auf Seite 901.

Durchsuchen der Veritas-Supportdatenbank

Die Supportdatenbank von Veritas enthält Informationen zu Veritas-Produkten. Sie enthält Informationen zum Installieren, Aktualisieren, Konfigurieren und Einsetzen von Veritas-Produkten. Sie enthält auch Informationen zu Anforderungen, empfohlene Verfahren und Fehlerbehebung. Die Veritas-Supportdatenbank ist von Backup Exec aus einfach zugänglich.

Hinweis: Zum Zugriff auf die Veritas-Supportdatenbank ist eine aktive Internetverbindung erforderlich.

Die Supportdatenbank verwendet eine schlüsselwortbasierte Suchfunktion. Sie konzentriert sich auf die wichtigen Schlüsselwörter in einer Suche und vergleicht

sie mit anderen Suchsätzen, um die bestmöglichen Ergebnisse zur Verfügung zu stellen. Sie können boolesche Suchfunktionen und Ausdruckabfragen verwenden, um Suchparameter zur Verfügung zu stellen. Konzentrieren Sie sich für bestmögliche Ergebnisse auf wenige Schlüsselwörter, die Ihre Frage am besten darstellen.

Wenn Sie die Supportdatenbank durchsuchen, wird ein neues Browser-Fenster gestartet, das die Suchergebnisse anzeigt.

So durchsuchen Sie die Veritas-Supportdatenbank

- 1** Sie haben folgende Möglichkeiten:
 - Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Technischer Support", und wählen Sie dann "Supportdatenbank durchsuchen" aus.
 - Aktivieren Sie auf der Registerkarte "Startseite" in der Gruppe "Support" die Option "Technischer Support". Klicken Sie dann im Fenster "Technischer Support" auf "Technischer Support von Veritas".
- 2** Geben Sie ein Schlüsselwort oder eine Phrase ein und klicken Sie dann auf das Suchsymbol.

Kontaktieren des technischen Support für Backup Exec

Wenn Sie versucht haben, ein Problem selbst zu lösen, aber noch Hilfe benötigen, können Sie sich über das Internet oder telefonisch an den technischen Support von Veritas für Backup Exec wenden.

So können Sie die Unterstützung durch den technischen Support beschleunigen:

- Halten Sie die Versions- und Revisionsnummer von Backup Exec bereit.
- Verwenden Sie eines der in Backup Exec enthaltenen Diagnoseprogramme, um Informationen zu sammeln, die für den technischen Support zur Diagnose Ihres Problems nützlich sind.

So kontaktieren Sie den technischen Support für Backup Exec

- ◆ Klicken Sie auf die Schaltfläche "Backup Exec", wählen Sie "Technischer Support" und dann "Backup Exec Technischer Support".

Siehe ["Anzeigen der Versionshinweise für Backup Exec"](#) auf Seite 134.

Siehe ["Infos zu den BackupExec-Diagnosetools"](#) auf Seite 903.

Siehe ["Zugriff auf Veritas Online"](#) auf Seite 901.

Einsatz des Remote-Support

Remote-Support startet eine WebEx-Sitzung im Internet, über die Sie an einer Support-Sitzung teilnehmen oder eine solche starten können.

So nehmen Sie den Remote-Support in Anspruch:

- ◆ Klicken Sie auf die Schaltfläche "Backup Exec" wählen Sie "Technischer Support" und dann "Remote-Support".

Verwalten Ihrer Backup Exec-Support-Fälle

Von Backup Exec aus können Sie die Website "My Veritas" aufrufen, auf der Sie Support-Fälle im Bereich des technischen Produkt-Supports erstellen, prüfen und verwalten können.

So verwalten Sie Ihre Backup Exec-Support-Fälle

- ◆ Klicken Sie auf die Schaltfläche "Backup Exec" wählen Sie "Technischer Support" und dann "Support-Fälle verwalten".

Infos zu den BackupExec-Diagnosetools

Die folgenden Diagnosetools helfen bei der Problemlösung in Backup Exec:

Tabelle 19-8 BackupExec-Diagnosetools

Element	Beschreibung
Veritas QuickAssist (VQA)	Scannt den lokalen Computer und erstellt einen Bericht über häufige Probleme in der Backup Exec-Umgebung. Siehe " Ausführen des Hilfe-Tools "Veritas QuickAssist" " auf Seite 904.
Backup Exec-Diagnoseanwendung	Sammelt wichtige Informationen über einen Windows-Computer zur Problemlösung. Siehe " Generieren einer Diagnosedatei zur Fehlerbehebung von Backup Exec" auf Seite 904.

Element	Beschreibung
Gather Utility für Linux-Server	<p>Erstellt und kompiliert eine Packet-Datei. Diese Datei enthält ausführliche Informationen über Installation, Diagnoseergebnisse und Fehlerberichte.</p> <p>Siehe "Ausführen des begather-Dienstprogramms, um Fehler bei Backup Exec-Komponenten auf Linux-Servern zu beheben" auf Seite 909.</p>
Backup Exec Debug Monitor	<p>Erfasst die Debugging-Ausgabe von Backup Exec und speichert sie in Debug-Protokollen.</p> <p>Siehe "Verwenden von Backup Exec Debug Monitor zur Fehlerbehebung" auf Seite 910.</p>

Ausführen des Hilfe-Tools "Veritas QuickAssist"

Das Hilfe-Tool "Veritas QuickAssist" ist ein programmübergreifendes Diagnoseprogramm zum Identifizieren von gängigen Problemen, Erfassen von Daten für die vom Support unterstützte Fehlerbehebung und Bereitstellen von Links für andere Support- und Selbsthilfe-Ressourcen. Veritas QuickAssist erfasst zum Ausführen von Prüfungen Information auf dem lokalen Computer und analysiert sie. Veritas QuickAssist nimmt keine permanente Änderungen an Dateien auf dem Computer vor, es sei denn, Sie aktivieren die entsprechende Option. Veritas QuickAssist installiert während der Ausführung nichts permanent auf dem Computer.

So führen Sie das Hilfe-Tool "Veritas QuickAssist" aus

- 1 Klicken Sie auf die Schaltfläche "Backup Exec" wählen Sie "Technischer Support" und dann "QuickAssist".
- 2 Folgen Sie den Anweisungen auf dem Bildschirm.

Generieren einer Diagnosedatei zur Fehlerbehebung von Backup Exec

Backup Exec enthält eine Diagnoseanwendung (Bediag.exe), die zum Zweck der Fehlerbehebung Informationen über einen Windows-Computer sammelt. Sie kann innerhalb von Backup Exec oder in einer Befehlszeile ausgeführt werden. Diese Anwendung kann für einen lokalen oder einen Remote-Server ausgeführt werden. Sie können Diagnoseprogramme auf einem standortfernen Backup Exec-Server

ausführen, wenn Backup Exec auf dem Remote-Server installiert wird und die Backup Exec-Dienste ausgeführt werden.

Die Anwendung "Bediag" sammelt die folgenden Informationen:

- Kontogruppen, Kontoberechtigungen und Umgebungseinstellungen
- Informationen zur Backup Exec-Softwareversion und Registrierungsinformationen, eine Liste der Backup Exec Agents, Windows-Versionsinformationen, SCSI-Hardwarekonfiguration sowie Informationen zu SQL Server, Treiberdiensten und den Windows-Diensten.
- Serverinformationen, unterstützte gemeinsam genutzte Verzeichnisse und Informationen zu Windows-Sockets

So generieren Sie eine Diagnosedatei aus Backup Exec

- 1** Klicken Sie auf die Schaltfläche "Backup Exec", wählen Sie "Technischer Support" und dann "Backup Exec-Diagnoseprogramm".
- 2** Wählen Sie in der Dropdown-Liste den Server.

Wenn der Server, den Sie auswählen möchten, nicht in der Dropdown-Liste ist, klicken Sie auf "Durchsuchen", um ihn aus der Liste verfügbarer Server auszuwählen.
- 3** Geben Sie die Login-Daten für den Server ein, den Sie auswählen.
- 4** Klicken Sie auf "Diagnoseprogramm ausführen".
- 5** Klicken Sie auf "Schließen".
- 6** Öffnen Sie die Datei "Bediag.txt" in dem Ordner, das die Datei "Bediag.exe" enthält (standardmäßig <Backup Exec-Installationsordner>\Backup Exec).

So generieren Sie eine Diagnosedatei von einer Befehlszeile

- 1 Öffnen Sie die Befehlszeilenanweisung.
- 2 Sie haben folgende Möglichkeiten:

So generieren Sie eine Diagnosedatei für einen Backup Exec-Server

Geben Sie im Ordner *<Backup Exec-Installationsordner>\Backup Exec* die Anweisung **"bediag [Parameter] Servername** ein.

Siehe ["Befehlszeilenparameter für eine Diagnosedatei"](#) auf Seite 906.

So erzeugen Sie eine Diagnosedatei für einen Remote-Computer

Geben Sie im Ordner *<Backup Exec-Installationsordner>\Backup Exec* folgenden Befehl ein: **bediag [Parameter] Name der Arbeitsstation**.

Siehe ["Befehlszeilenparameter für eine Diagnosedatei"](#) auf Seite 906.

- 3 Öffnen Sie die Datei "Bediag.txt" in dem Ordner, das die Datei "Bediag.exe" enthält (standardmäßig *<Backup Exec-Installationsordner>\Backup Exec*).

Befehlszeilenparameter für eine Diagnosedatei

Sie können die folgenden Parameter hinzufügen, um beim Generieren einer Diagnosedatei für die Fehlerbehebung zusätzliche Informationen zu sammeln.

Siehe ["Generieren einer Diagnosedatei zur Fehlerbehebung von Backup Exec"](#) auf Seite 904.

Tabelle 19-9 Befehlszeilenparameter für eine Diagnosedatei

Parameter	Beschreibung
/a	Gibt die Agent-Liste aus.
/ad	Gibt Active Directory-Informationen aus.
/adamm	Hängt Informationen zu ADAMM-Dateien an.
/agents	Gibt Agentinformationen für die bevorzugten Ressourcen aus.
/all	Gibt alles aus.
/app	Gibt das Anwendungsereignisprotokoll aus.
/b2d	Gibt Backup-to-Disk-Daten von Backup Exec aus.

Parameter	Beschreibung
/basicscsi	Gibt den grundlegenden SCSI-Hardwareunterschlüssel von der Registrierung aus.
/beallfiles	Gibt alle Backup Exec-Dateien und -Verzeichnisse aus.
/bedb	Gibt Informationen der Backup Exec-Datenbank aus.
/befiles	Gibt alle Dateiinformationen der Backup Exec-Datenbank aus.
/bereg	Gibt die in der Registrierung gespeicherte Backup Exec-Softwarekonfiguration aus.
/beupdate	Gibt Update-Informationen zu Backup Exec aus.
/bex	Gibt nur die Backup Exec-Einträge aus, die sich im Anwendungs-Ereignisprotokoll befinden.
/c	Gibt die in der Registrierung gespeicherte Backup Exec-Softwarekonfiguration aus.
/caso	Gibt Informationen über den zentralen Administrationsserver und die verwalteten Backup Exec-Server aus.
/cluster	Gibt Clusterinformationen aus
/cps	Gibt CPS-Registrierungsinformationen aus.
/detailnic	Gibt die ausführlichen Daten zur Netzwerkkarte des Servers aus.
/detailscsi	Gibt die ausführlichen SCSI-Adapterinformationen des Servers aus.
/dirsvc	Gibt das Ereignisprotokoll des Verzeichnisdienstes aus.
/dlo	Gibt die DLO-INI-Datei aus.
/dns	Gibt das DNS-Ereignisprotokoll aus.
/err	Gibt nur Fehlerereignisse in den Ereignisprotokollen aus.
/evdb	Gibt Datenbankinformationen von Veritas Enterprise Vault aus.
/evevents	Gibt die Ereignisprotokolle des Veritas Enterprise Vault aus.
/evreg	Gibt Veritas Enterprise Vault-Registrierungsinformationen aus.
/frs	Gibt das Ereignisprotokoll des Dateireplikationsdienstes aus.
/o:[Datei]	Legt das Ausgabeauftragsprotokoll für den Anhang fest. Das Auslassen [Datei] schickt Ausgabe zum Bildschirm.

Parameter	Beschreibung
/h	Gibt den in der Registrierung gespeicherten SCSI-Hardwareunterschlüssel aus.
/instapp	Gibt Informationen über installierte Anwendungen aus.
/lic	Gibt Lizenzinformationen zum Backup Exec-Server aus.
/liveupdate	Gibt Informationen zu Veritas Update aus.
/n	Gibt das Windows Socket-Netzwerkprotokoll aus.
/networkinformation	Gibt Informationen zu TCP/IP-Einstellungen, WinSock und Windows-Firewall aus.
/oracle	Gibt Oracle-Informationen aus.
/p	Gibt die Benutzerrechte aus.
/power	Gibt das PowerShell-Ereignisprotokoll aus.
/recs:n	Gibt nur die neuesten Einträge in den ausgewählten Ereignisprotokollen aus. Die Parameter "bex", "err" und "recs" müssen mit dem App-Parameter und dem Sys-Parameter verwendet werden.
/s	Gibt die Informationen zu Dienstleistungen aus.
/sec	Gibt das Sicherheitsereignisprotokoll aus.
/server	Gibt Serverinformationen, wie zum Beispiel CPU, Arbeitsspeicher, Datenträgerinformationen und mehr aus.
/services	Gibt Informationen über Dienste aus.
/sql	Gibt die Microsoft SQL Server-Informationen aus.
/symreginfo	Gibt die Backup Exec-Registrierungsinformationen aus.
/sys	Gibt das Systemereignisprotokoll aus.
/sys32info	Gibt Treiberinformationen des Ordners "system32\drivers" aus.
/svccact	Gibt die Benutzernamen aus, die für Backup Exec-Dienste verwendet werden.
/u	Gibt Microsoft-Aktualisierungsinformationen aus.
/userinfo	Gibt Informationen über Benutzerrechte und Gruppen aus.

Ausführen des begather-Dienstprogramms, um Fehler bei Backup Exec-Komponenten auf Linux-Servern zu beheben

Parameter	Beschreibung
/v	Gibt Serverinformationen aus.
/w	Gibt Windows-Versionsinformationen aus.
/winpower	Gibt das Ereignisprotokoll von Windows PowerShell aus.
/winupdate	Gibt Microsoft-Aktualisierungsinformationen aus.
/x	Gibt Microsoft Exchange-Serverinformationen aus.
/?	Zeigt Hinweise zur Verwendung an.

Ausführen des begather-Dienstprogramms, um Fehler bei Backup Exec-Komponenten auf Linux-Servern zu beheben

Das begather-Dienstprogramm stellt jene Dateien bereit, mit denen Sie Probleme bei Backup Exec-Komponenten auf Linux-Servern erkennen können. Nach dem Ausführen zeigt das begather-Dienstprogramm den Namen der von ihm erstellten Paketdatei an. Die gesammelten Dateien enthalten genaue Informationen über die Installation, die Diagnoseergebnisse und die Fehlerberichte. Bevor Sie den technischen Support kontaktieren, können Sie durch Überprüfen dieser Dateien unter Umständen die Fehlerquelle entdecken. Ist eine Lösung auf Grundlage der gesammelten Dateien nicht offensichtlich, sollten Sie die Paketdatei bereithalten, wenn Sie den Support kontaktieren. Möglicherweise bittet Sie der Supporttechniker um eine E-Mail mit der Paketdatei.

Führen Sie das begather-Dienstprogramm aus, um Fehler bei Backup Exec-Komponenten auf Linux-Servern zu beheben.

- 1 Loggen Sie sich als Root am Linux-Server ein, auf dem die Backup Exec-Komponenten installiert sind.
- 2 Navigieren Sie zum folgenden Verzeichnis:

/opt/VRTSralus/bin

Beispiel:

```
cd /opt/VRTSralus/bin
```

- 3 Starten Sie das begather-Dienstprogramm.

Beispiel:

```
./begather
```

- 4 Beachten Sie den Speicherort der Paketdatei, die auf dem Bildschirm angezeigt wird.

Verwenden von Backup Exec Debug Monitor zur Fehlerbehebung

Backup Exec Debug Monitor oder SGMon ist ein Diagnosetool, das die Debug-Leistung von Backup Exec erfasst und diese in den Debug-Protokollen speichert. Mithilfe der Debug-Protokolle von SGMon können Sie Backup-Probleme beheben. Darüber hinaus können Debug-Protokolle den technischen Support dabei unterstützen, Probleme zu diagnostizieren und zu beheben.

Wenn Sie SGMon öffnen, erfasst es automatisch Debug-Daten von Backup Exec-Diensten. Um Debug-Informationen bei nicht aktivem SGMon zu sammeln, aktivieren Sie die Erstellung des Debug-Protokolls außerhalb von SGMon, und geben Sie ein Verzeichnis an, in dem die Protokolle gespeichert werden sollen.

Weitere Informationen zur Konfiguration des Debug-Monitors und zum Lesen von Protokolldateien finden Sie in der Hilfe des Debug-Monitors.

So verwenden Sie Backup Exec Debug Monitor zur Fehlerbehebung

- ◆ Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Technischer Support" und dann "Debug-Ausgabe abrufen".

Informationen zum Backup Exec Debug Tool

Backup Exec enthält ein Debugging-Tool (BEDBG), das Diagnoseinformationen über Backup Exec-Prozesse enthält, die unerwartet beendet wurden. Anhand dieser Informationen kann der technische Support Probleme diagnostizieren und beheben. Das Backup Exec-Debug-Tool wird standardmäßig in Backup Exec ausgeführt. Die vom Tool erfassten Daten werden in den Ordner "BEDBG" in "<Backup Exec-Installationsordner>\Backup Exec" kopiert.

Verwenden von Backup Exec in Clusterumgebungen

In diesem Kapitel werden folgende Themen behandelt:

- Über Backup Exec und Cluster
- Anforderungen zum Erstellen von Clustern für Backup Exec in einer Microsoft Cluster Server-Umgebung
- Funktionsweise von Backup Exec in einer Microsoft Cluster Server-Umgebung
- Voraussetzungen für die Installation von Backup Exec auf einem Microsoft Cluster Server
- Installieren von Backup Exec auf einem Microsoft Cluster Server
- Aktualisieren von Backup Exec in einem Microsoft-Cluster
- Installieren zusätzlicher Backup Exec-Funktionen in einem Microsoft-Cluster
- Deinstallieren von Backup Exec aus einem Microsoft-Cluster
- Erstellen von Speichergerätepools für Microsoft Cluster Server
- Festlegen eines anderen Failover-Knotens
- Festlegen eines neuen zentralen Administrationsservers in einer Microsoft Cluster Server-Umgebung
- Konfigurationen für Backup Exec und Microsoft Cluster Server

- [Verwenden von Central Admin Server Feature mit Microsoft-Clustern und einem SAN](#)
- [Info zur Sicherung von Microsoft Cluster Servern](#)
- [Wiederherstellen von Daten in einem Microsoft Cluster](#)
- [Notfallwiederherstellung eines Clusters](#)
- [Wiederherstellen der Datendateien des Microsoft Clusters Servers](#)
- [Wiederherstellen von Backup Exec in einem Microsoft-Cluster](#)
- [Manuelles Verbinden zweier Cluster-Datenträgergruppen und Neusynchronisierung der Datenträger](#)
- [Fehlerbehebungs-Cluster](#)

Über Backup Exec und Cluster

In einem Servercluster können mit Backup Exec Daten auf lokalen und gemeinsam genutzten Festplatten, sowie Microsoft SQL Server- und Exchange Server-Datenbanken geschützt werden, die als virtuelle Serveranwendungen konfiguriert wurden. Virtuelle Serveranwendungen enthalten eine IP-Adressenressource und eine Netzwerknamenressource. Sie werden im Netzwerk mit einem eindeutigen Servernamen, dem virtuellen Servernamen, angezeigt. Servercluster stellen den Benutzern Hochverfügbarkeit von Anwendungen und Daten bereit. Für einen Servercluster werden mehrere Server (so genannte Knoten) in einem Netzwerk miteinander verknüpft. Auf diesen Servern wird eine Clustersoftware ausgeführt, die jedem Knoten Zugriff auf die gemeinsam genutzten Festplatten gewährt. Fällt ein Knoten aus, werden die Clusterressourcen zu einem anderen verfügbaren Knoten (so genannter Failover) verlagert. Die gemeinsam verwendeten Festplatten und der virtuelle Server bleiben verfügbar. Ein Failover macht sich bei den Benutzern nur durch eine kurze Unterbrechung der Dienste bemerkbar.

Informationen zu den Best Practices zum Einsatz von Backup Exec in Cluster-Umgebungen finden Sie unter *Best Practices für Backup Exec*.

Siehe "[Installieren von Backup Exec auf einem Microsoft Cluster Server](#)" auf Seite 916.

Siehe "[Konfigurationen für Backup Exec und Microsoft Cluster Server](#)" auf Seite 923.

Siehe "[Info zur Sicherung von Microsoft Cluster Servern](#)" auf Seite 932.

Siehe "[Wiederherstellen von Daten in einem Microsoft Cluster](#)" auf Seite 933.

Siehe "[Anforderungen zum Erstellen von Clustern für Backup Exec in einer Microsoft Cluster Server-Umgebung](#)" auf Seite 913.

Siehe "[Notfallwiederherstellung eines Clusters](#)" auf Seite 933.

Anforderungen zum Erstellen von Clustern für Backup Exec in einer Microsoft Cluster Server-Umgebung

Im Folgenden sehen Sie Anforderungen für das Clustering von Backup Exec:

- Es wird dringend empfohlen, dass Sie zur Erstellung von Backup Exec-Clustern die Standard-Datenbankinstanz (MSDE) verwenden, die zusammen mit Backup Exec installiert wird.
- Sie können eine Remote-SQL Server-Instanz zum Hosten der Backup Exec-Datenbank verwenden.
Nur eine installierte Instanz von Backup Exec kann in der standortfernen SQL Server-Instanz auf einem Clusterknoten installiert werden. Alle weiteren installierten Instanzen von Backup Exec im Cluster müssen die Backup Exec-Standarddatenbankinstanz MSDE verwenden.

Hinweis: Sie müssen den Backup Exec-Clusterassistenten auf dem Clusterknoten ausführen, der die Remote-SQL Server-Instanz verwendet.

- Bei Backups auf einem anderen Host, die den Hardwareanbieter in einer Microsoft Cluster Server-Umgebung verwenden, müssen sich der Backup Exec-Server und der Remote-Computer in unterschiedlichen Clustergruppen befinden. Die Clusteranwendungen können die LUNs (Logical Unit Numbers, Nummern der logischen Einheit), die doppelte Signaturen und Partitions-Layouts haben, nicht unterstützen. Deshalb müssen die Snapshots, die das LUNs enthalten, zu einem Host oder zu einem Remote-Computer transportiert werden, der außerhalb des Cluster ist.
- Für Windows Server 2008 und höher, müssen Sie die gleiche Stufe des Betriebssystems auf dem Backup Exec-Server und auf dem Computer verwenden, der die Remote-SQL Server-Instanz in den folgenden Szenarien hostet:
 - So verwenden Sie ein Remote-SQL Server-Instanz zum Hosten der Backup Exec-Datenbank

- So verwenden Sie Backup Exec Utility zum Konfigurieren der geclusterten Backup Exec-Installation oder der geclusterten Remote- SQL Server-Instanz

Unter Windows Server 2012 und höher unterstützt Backup Exec parallele Backups über freigegebene Clustervolumes (CSV) und Cluster-Knoten hinweg.

Backup Exec unterstützt keine virtuellen Computer, die Daten auf CSVFS und NTFS-Datenträgern speichern.

Anforderungen an das jeweilige Betriebssystem finden Sie in der Liste der mit Backup Exec kompatiblen Software.

Siehe ["Installieren von Backup Exec auf einem Microsoft Cluster Server "](#) auf Seite 916.

Siehe ["Info zur Sicherung von Microsoft Cluster Servern"](#) auf Seite 932.

Funktionsweise von Backup Exec in einer Microsoft Cluster Server-Umgebung

Wenn Sie Backup Exec in einem Microsoft-Cluster installieren, installieren Sie ihn als eine virtuelle Serveranwendung. Sie weisen Backup Exec eine IP-Adressenressource, eine Netzwerknamenressource (den virtuellen Servernamen) und eine Plattenressource zu.

Bei einem Failover werden bereits laufende Backup-Aufträge neu geplant. Die Backup Exec-Dienste werden auf einem vorher festgelegten Failover-Knoten neu gestartet, und die Backup-Aufträge werden standardmäßig neu gestartet. Backup Exec stellt eine zusätzliche Regel für den Cluster-Failover-Neustart zur Verfügung: Auftragswiederaufnahme. Die Option "Auftragswiederaufnahme" ermöglicht die Wiederaufnahme von Backup-Aufträgen ab dem Punkt, an dem sie unterbrochen wurden. Das Backup muss also nicht vollständig neu gestartet werden. Wenn die Regel zur Auftragswiederholung bei einem Cluster-Failover aktiviert ist, kann eine zusätzliche Option festgelegt werden, um bei Fortsetzung der Auftragsausführung eine Auftragswiederaufnahme auszuführen. Die Option "Auftragswiederaufnahme" ist die einzige Eigenschaft, die für die Cluster-Failover-Regel zur Verfügung steht. Sie können die Standardvorgabe ändern, sodass Aufträge nicht erneut gestartet werden.

Sobald der ausgefallene Server wieder online ist, kann der Microsoft-Cluster automatisch die Arbeitslast in einem Cluster ausgleichen (so genanntes Failback), indem Clustergruppen wieder zu dem sich wieder im Cluster befindlichen Server zurückverlagert werden. Backup Exec wurde jedoch absichtlich nicht mit einer Failback-Funktion ausgestattet. Die Backup-Aufträge werden auf dem festgelegten Failover-Knoten fortgesetzt. Durch diese Fortsetzung auf dem festgelegten Failover-Knoten wird vermieden, dass die Aufträge neu gestartet werden müssen,

sobald der ausgefallene Server wieder in den Cluster aufgenommen wird. Die Backup Exec-Clustergruppe kann anschließend zu einem beliebigen Zeitpunkt zum steuernden Knoten zurückverlagert werden.

Wie die Ausführung von Backup Exec in einem Cluster genau abläuft, ist von der im Cluster verwendeten Konfiguration abhängig.

Siehe ["Konfigurieren der Auftragswiederaufnahme"](#) auf Seite 667.

Siehe ["Konfigurationen für Backup Exec und Microsoft Cluster Server"](#) auf Seite 923.

Siehe ["Installieren von Backup Exec auf einem Microsoft Cluster Server "](#) auf Seite 916.

Voraussetzungen für die Installation von Backup Exec auf einem Microsoft Cluster Server

Anforderungen an das jeweilige Betriebssystem finden Sie in der Liste der mit Backup Exec kompatiblen Software.

Folgende Elemente müssen zur Installation von Backup Exec auf einem Microsoft-Cluster vorhanden sein:

- Backup Exec-Cluster können unter Windows Server 2008 R2 SP1 mit Hauptknotenkonfiguration installiert werden. In der Konfiguration muss jedoch eine gemeinsam verwendete Festplatte zur Verfügung stehen, damit Backup Exec die Datenbankdateien zwischen den Knoten aufteilen kann. Wenn bei diesem Konfigurationstyp die Mehrheit der Clusterknoten ausfällt, führt dies zum Ausfall des gesamten Clusters. Für diese Konfiguration werden in der Regel mehr als zwei Knoten im Cluster verwendet.
- Der steuernde Knoten und der festgelegte Failover-Knoten müssen bei der Installation von Backup Exec im Cluster online geschaltet sein.
- Bei der Installation wird für den virtuellen Backup Exec-Server eine eindeutige IP-Adresse und ein eindeutiger Netzwerkname abgefragt.
- Bei der Installation eines Backup Exec-Clusters muss der Knoten, der die Installation ausführt, Besitzer der gemeinsam verwendeten Festplatte sein. Wenn Sie eine physische Festplattenressource verwenden, die zu einer anderen Anwendung gehört, verschiebt der Backup Exec-Clusterassistent alle Ressourcen, die zur anderen Anwendung gehören, in die Backup Exec-Gruppe. Es wird empfohlen, Backup Exec nicht auf dem Clusterquorum zu installieren.
- Wie im Endbenutzerlizenzvertrag angegeben, wird für jeden aktiven Knoten im Cluster ein eigenes, lizenziertes Exemplar von Backup Exec sowie aller gegebenenfalls erforderlichen Agents und Optionen benötigt. Wenn Sie eine

Probeversion von Backup Exec installieren, wird eine Clusterumgebung automatisch erkannt. Lizenzen sind nicht erforderlich.

- Wenn Sie Backup Exec-Cluster in einer Central Admin Server Feature(CAS)-Konfiguration installieren, müssen alle Backup Exec-Installationen über die gleiche Serverkonfiguration verfügen. Alle Knoten sollten entweder Datenbankserver oder verwaltete Backup Exec-Server sein, die eine Verbindung mit dem zentralen Administrationsserver herstellen.
- Alle Installationen von Backup Exec in einem Cluster müssen entweder Teil einer einzelnen Clustergruppe oder lokal auf allen Knoten installiert sein. Wenn in einem Cluster sowohl die clusterfähige Version von Backup Exec als auch eine lokale (nicht clusterfähige) Version installiert ist, können Sie sich nicht beim lokal installierten Backup Exec-Server einloggen. Sie können sich nur mit dem Namen des virtuellen Backup Exec-Servers einloggen. Um sich beim lokal installierten Backup Exec-Server einloggen zu können, müssen Sie zuerst mithilfe des Assistenten für die Clusterkonfiguration die clusterfähige Version von Backup Exec von allen Knoten im Cluster deinstallieren.
- Verwenden Sie auf allen Knoten im Cluster dasselbe Login-Konto für Backup Exec-Dienste. Wenn Knoten in einem Cluster Backup Exec verwenden und über unterschiedliche Login-Konten verfügen, ändern Sie die Dienste so, dass der Zugriff über dasselbe Login-Konto erfolgt.

Siehe ["Installieren von Backup Exec auf einem Microsoft Cluster Server "](#) auf Seite 916.

Siehe ["Konfigurationen für Backup Exec und Microsoft Cluster Server"](#) auf Seite 923.

Installieren von Backup Exec auf einem Microsoft Cluster Server

Das Installieren von Backup Exec auf demselben Datenträger, auf dem auch das Clusterquorum installiert ist, wird nicht empfohlen. Wenn Sie bei einer Wiederherstellung einen neuen Laufwerksbuchstaben für das Clusterquorum angeben müssen, erkennt Backup Exec das neue Laufwerk nicht und kann nicht gestartet werden.

Hinweis: Standardmäßig wird ein Failover vom steuernden Knoten zu einem festgelegten Failover-Knoten in alphabetischer Reihenfolge nach dem Computernamen jedes Knotens durchgeführt. Um die Reihenfolge zu ändern, mit der das Failover auf dem festgelegten Knoten durchgeführt wird, müssen Sie die Computer umbenennen.

Backup Exec Agent for Windows wird automatisch auf allen Knoten im Cluster installiert. Falls diese Installation von Backup Exec zum Sichern von Remote-Servern außerhalb des Clusters verwendet werden soll, müssen Sie Agent for Windows auch auf den Remote-Servern installieren.

So installieren Sie Backup Exec auf einem Microsoft Cluster Server

- 1** Installieren Sie Backup Exec auf allen Knoten, die zum Cluster gehören. Verwenden Sie für jeden Knoten denselben Installationspfad.
- 2** Starten Sie Backup Exec von dem Knoten aus, der als aktiver Knoten agieren soll.
- 3** Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und dann "Assistent für die Clusterkonfiguration".
- 4** Befolgen Sie die Anweisungen auf dem Bildschirm.

Im Fenster "Informationen zum virtuellen Server" wird von Backup Exec automatisch der Standardname des virtuellen Servers (BKUPEXECVRS) angezeigt. Wenn Sie einen anderen Standardnamen verwenden möchten, geben Sie diesen in das entsprechende Feld ein.

- 5** Erstellen Sie nach Beendigung des Assistenten für die Clusterkonfiguration einen Speichergerätepool, der alle lokal angeschlossenen Speichergeräte für alle Knoten enthält, die bei einem Failover verwendet werden sollen. Dadurch wird gewährleistet, dass auf den an Failover-Knoten angeschlossenen Speichergeräten Aufträge ausgeführt werden können.

Siehe ["Erstellen von Speichergerätepools für Microsoft Cluster Server"](#) auf Seite 920.

- 6** Wiederholen Sie Schritt 5 für alle Knoten.

Siehe ["Konfigurationen für Backup Exec und Microsoft Cluster Server"](#) auf Seite 923.

Siehe ["Festlegen eines anderen Failover-Knotens"](#) auf Seite 920.

Aktualisieren von Backup Exec in einem Microsoft-Cluster

Sie können Backup Exec Version auf den Knoten in einem Cluster aktualisieren, ohne die Knoten aus dem Cluster zu entfernen.

Tabelle 20-1 Aktualisieren von Backup Exec in einem Microsoft-Cluster

Schritt	Aktion
Schritt 1	Wählen Sie einen zu aktualisierenden Knoten aus und verwenden Sie diesen als aktiven Backup Exec-Clusterknoten.
Schritt 2	Führen Sie das Backup Exec-Installationsprogramm auf dem aktiven Knoten aus.
Schritt 3	Verschieben Sie die Clustergruppe zum nächsten zu aktualisierenden Knoten und führen Sie anschließend auf diesem Knoten das Backup Exec-Installationsprogramm aus. Mit Ausnahme des Datenträgers sollten alle Ressourcen offline sein, wenn sie zum Aktualisieren an die einzelnen Knoten verschoben werden.
Schritt 4	Wiederholen Sie Schritt 3 für jeden Knoten im Cluster.

Siehe ["Installieren zusätzlicher Agents und Funktionen auf dem lokalen Backup Exec-Server"](#) auf Seite 66.

Installieren zusätzlicher Backup Exec-Funktionen in einem Microsoft-Cluster

Installieren Sie zusätzliche Backup Exec-Funktionen auf jedem Knoten im Cluster. Nähere Erläuterungen zur Installation der einzelnen Funktionen finden Sie in den entsprechenden Abschnitten in diesem Handbuch bzw. in der Online-Hilfe.

So installieren Sie zusätzliche Backup Exec-Funktionen

- 1 Stellen Sie vor der Installation zusätzlicher Funktionen auf dem steuernden Knoten sicher, dass die Backup Exec-Gruppe online geschaltet ist.
- 2 Installieren Sie die zusätzlichen Funktionen.

Siehe ["Installieren zusätzlicher Agents und Funktionen auf dem lokalen Backup Exec-Server"](#) auf Seite 66.

- 3 Nachdem die Installation auf dem steuernden Knoten abgeschlossen ist, können Sie die Clusterverwaltungssoftware verwenden, um die Backup Exec-Gruppe zum nächsten geeigneten Knoten zu verschieben. Wiederholen Sie dann Schritt 2.

Stellen Sie sicher, dass Sie für jeden Knoten im Cluster dieselben Funktionen mit denselben Einstellungen installieren.

- 4 Um den Agent for Oracle auf Windows- oder Linux-Servern auf anderen Knoten zu installieren, ordnen Sie ein Laufwerk den freigegebenen Datenträgern zu, auf denen Backup Exec im Cluster installiert ist, und führen Sie das Setup aus.

Siehe ["Deinstallieren von Backup Exec aus einem Microsoft-Cluster"](#) auf Seite 919.

Deinstallieren von Backup Exec aus einem Microsoft-Cluster

Zum Entfernen von Backup Exec verwenden Sie den Assistenten für die Clusterkonfiguration.

Deinstallieren von Backup Exec aus einem Cluster:

- 1 Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und dann "Assistent für die Clusterkonfiguration".
- 2 Verwenden Sie den Assistenten, um die clusterfähige Version von Backup Exec von allen ausgewählten Servern zu entfernen.

Wenn Sie den aktiven Knoten aus dem Cluster entfernen, können Sie die Backup Exec-Daten auf dem gemeinsam verwendeten Laufwerk belassen oder sie löschen. Wenn Sie die Daten löschen, können Sie sie auf dem aktiven Knoten verfügbar machen.

- 3 Deinstallieren Sie Backup Exec von allen Knoten.
- 4 Nachdem Backup Exec deinstalliert wurde, sollten Sie sämtliche Ressourcenfestplatten aus der Backup Exec-Clustergruppe in eine andere Gruppe verlagern und anschließend die Backup Exec-Clustergruppe löschen.
- 5 Klicken Sie zum Deinstallieren von Backup Exec auf einem beliebigen Knoten auf "Start", wählen Sie "Einstellungen" und klicken Sie anschließend auf "Systemsteuerung".
- 6 Doppelklicken Sie auf "Software", wählen Sie in der Liste der aktuell installierten Programme "Backup Exec" und klicken Sie auf "Ändern/Entfernen".
- 7 Wiederholen Sie Schritt 5 für alle Knoten.

Siehe ["Erstellen von Speichergerätepools für Microsoft Cluster Server"](#) auf Seite 920.

Erstellen von Speichergerätepools für Microsoft Cluster Server

Wenn Backup Exec in einem Cluster installiert wird, erstellt es einen Satz Standardspeicherpools für jeden Knoten im Cluster. Falls ein Knoten über Speichergeräte verfügt, werden diese automatisch einem entsprechenden Gerätepool zugeordnet, der zudem das Standardzielgerät auf diesem Knoten für das Erstellen von Backup- oder Wiederherstellungsaufträgen ist. Damit Aufträge bei einem Failover auf den Speichergeräten ausgeführt werden können, die am festgelegten Failover-Knoten angeschlossen sind, müssen Sie einen Speicherpool erstellen, der die Speichergeräte aller Knoten enthält. Wenn der Cluster außerdem mit Bandgeräten an einem gemeinsam genutzten SCSI-Bus konfiguriert wurde, fügen Sie den von jedem Knoten verwendeten Bandgerätenamen dem Speicherpool hinzu. Sie müssen diesen Speicherpool auch als Zielgerät für alle Aufträge auswählen, die neu gestartet werden sollen.

Sie können entweder einen einzelnen Speicherpool oder Speicherpools für Geräte- oder Medientypen erstellen, sodass Aufträge bei einem Failover auf ähnlichen Geräten und Medien neu gestartet werden können.

So erstellen Sie einen Speicherpool für einen Cluster

- 1 Öffnen Sie Backup Exec vom steuernden Knoten aus.
- 2 Erstellen Sie einen neuen Speichergerätepool und fügen Sie Speichergeräte hinzu.

Siehe ["Erstellen von Speichergerätepools"](#) auf Seite 512.
- 3 Beenden Sie Backup Exec. Fügen Sie den von jedem Knoten verwendeten Bandgerätenamen hinzu, wenn sich Bandgeräte an einem gemeinsam genutzten SCSI-Bus befinden.
- 4 Verwenden Sie die Cluster-Administratorsoftware um die Backup Exec-Ressourcengruppe zum nächsten geeigneten Knoten zu verschieben.
- 5 Öffnen Sie Backup Exec, fügen Sie dem vorherigen Speicherpool Speichergeräte für diesen Knoten hinzu und beenden Sie Backup Exec. Fügen Sie den von jedem Knoten verwendeten Bandgerätenamen hinzu, wenn sich Bandgeräte an einem gemeinsam genutzten SCSI-Bus befinden.
- 6 Wiederholen Sie Schritt 4 und 5 für jeden Knoten im Cluster.

Festlegen eines anderen Failover-Knotens

Gehen Sie folgendermaßen vor:

- Ändern Sie die Reihenfolge, in der die Knoten ein Failover durchführen.
- Fügen Sie einen Failover-Knoten zum Cluster hinzu.
- Entfernen Sie einen Failover-Knoten aus dem Cluster.

Hinweis: Standardmäßig erfolgt das Failover in einem MSCS-Cluster vom steuernden Knoten zu einem festgelegten Knoten in alphabetischer Reihenfolge gemäß des Computernamens jedes Knotens. Um die Reihenfolge der festgelegten Knoten zu ändern, sollten Sie die Computer in der Reihenfolge umbenennen, in der das Failover erfolgen soll.

Bevor Sie einen Knoten zur Backup Exec-Clusterkonfiguration hinzufügen können, müssen Sie Backup Exec auf dem Knoten installieren. Clusterdienste für einen Knoten sollten online sein, bevor Sie den Knoten hinzufügen bzw. entfernen.

Wenn Sie einen Knoten entfernen, darf der Assistent für die Clusterkonfiguration dazu nicht auf diesem Knoten gestartet werden.

So fügen Sie einen Failover-Knoten hinzu bzw. entfernen ihn

- 1** Klicken Sie auf dem steuernden Knoten auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und dann "Assistent für die Clusterkonfiguration".
- 2** Befolgen Sie die Anweisungen auf dem Bildschirm, um einen Knoten hinzuzufügen oder zu entfernen.
- 3** Nach dem Hinzufügen eines Failover-Knotens müssen Sie dem Speicherpool des Clusters alle lokal angeschlossenen Speichergeräte hinzufügen, die beim Auftreten eines Failovers verwendet werden sollen. Dadurch wird gewährleistet, dass auf den an Failover-Knoten angeschlossenen Speichergeräten Aufträge ausgeführt werden können.

Wenn Sie einige, jedoch nicht alle Knoten aus einem Cluster entfernen, wird beim Deinstallieren von Backup Exec ein Kennwort für den virtuellen Server und die Dienste angefordert, die weiterhin ausgeführt werden. Sie müssen Backup Exec aus allen Knoten im Cluster entfernen.

Siehe ["Deinstallieren von Backup Exec aus einem Microsoft-Cluster"](#) auf Seite 919.

Siehe ["Festlegen eines anderen Failover-Knotens"](#) auf Seite 920.

Siehe ["Konfigurationen für Backup Exec und Microsoft Cluster Server"](#) auf Seite 923.

Festlegen eines neuen zentralen Administrationsservers in einer Microsoft Cluster Server-Umgebung

Um einen neuen zentralen Administrationsserver für eine Clusterumgebung festzulegen, verwenden Sie BEUtility.exe. Mit BEUtility können Sie verschiedene Typen von Konfigurations- und Wartungsvorgängen auf Ihren Backup Exec-Servern ausführen.

Hinweis: Verwenden Sie die Option "Dienstkonto ändern" von BEUtility.exe nicht in Clusterumgebungen.

So ändern Sie einen Backup Exec-Cluster von einem Datenbankserver in einen Mitgliedsserver:

- 1** Installieren Sie den neuen Server als verwalteten Backup Exec-Server mit installierter Library Expansion Feature.

Vergewissern Sie sich, dass die Verbindungen zum Backup Exec-Cluster und anderen Mitgliedsservern ordnungsgemäß funktionieren.
- 2** Fahren Sie die Backup Exec-Clusterdienste mithilfe der Clusteradministrator-Software herunter.

Stellen Sie sicher, dass die Festplattenressource online geschaltet bleibt.
- 3** Verschieben Sie die Katalogdateien vom Pfad der Backup Exec-Clusterinstallation zu den entsprechenden Installationspfaden auf dem neuen Datenbankserver.
- 4** Verwenden Sie BEUtility.exe, um alle Backup Exec-Server mit dem neuen Datenbankserver zu verbinden, und starten Sie alle Backup Exec-Dienste neu.
- 5** Beenden Sie die Backup Exec-Dienste auf dem neuen Datenbankserver und starten Sie sie erneut.
- 6** Verschieben Sie die Backup Exec-Ressourcengruppe mithilfe der Clusteradministrator-Software zum Failover-Knoten und vergewissern Sie sich, dass die Dienste auf diesem Knoten gestartet werden.
- 7** Verwenden Sie BEUtility.exe, um die Backup Exec-Dienste auf allen Mitgliedsservern des SAN zu beenden und neu zu starten, damit Verbindungen mit dem neuen Datenbankserver hergestellt werden.

So wandeln Sie einen Backup Exec-Cluster von einem zentralen Administrationsserver in einen verwalteten Backup Exec-Server um

- 1** Installieren Sie den neuen Server als verwalteten Backup Exec-Server.
Vergewissern Sie sich, dass die Verbindungen zum Backup Exec-Cluster und anderen verwalteten Backup Exec-Servern ordnungsgemäß funktionieren.
- 2** Fahren Sie die Backup Exec-Clusterdienste mithilfe der Clusteradministrator-Software herunter.
Stellen Sie sicher, dass die Festplattenressource online geschaltet bleibt.
- 3** Verschieben Sie die Katalogdateien vom Pfad der Backup Exec-Clusterinstallation zu den entsprechenden Installationspfaden auf dem neuen zentralen Administrationsserver.
- 4** Verwenden Sie BEUtility.exe, um alle Backup Exec-Server mit dem neuen zentralen Administrationsserver zu verbinden und alle Backup Exec-Dienste zu starten.
- 5** Beenden Sie die Backup Exec-Dienste auf dem zentralen Administrationsserver und starten Sie sie neu.
- 6** Verschieben Sie die Backup Exec-Ressourcengruppe mithilfe der Clusteradministrator-Software zum Failover-Knoten und vergewissern Sie sich, dass die Dienste auf diesem Knoten gestartet werden.
- 7** Verwenden Sie BEUtility.exe, um die Backup Exec-Dienste auf allen verwalteten Backup Exec-Servern zu beenden und neu zu starten, damit Verbindungen mit dem neuen zentralen Administrationsserver hergestellt werden.

Siehe ["Cluster mit mehreren Knoten in einem Fibre Channel-SAN mit Central Admin Server Feature"](#) auf Seite 929.

Konfigurationen für Backup Exec und Microsoft Cluster Server

Backup Exec unterstützt verschiedene Clusterkonfigurationen zwischen zwei und acht Knoten in einem Fibre Channel-SAN mit lokal angeschlossenen Speichergeräten oder mit Speichergeräten an einem gemeinsamen SCSI-Bus. Sie können diese Konfigurationen beliebig miteinander kombinieren.

Hinweis: Wenn Sie den Cluster in einem privaten Netzwerk installieren, verwenden Sie die Clusterverwaltungssoftware, um bei Bedarf eine öffentliche Kommunikation zu ermöglichen.

Wenn Sie einen Cluster auf einem Fibre Channel-SAN oder mit Speichergeräten auf einem freigegebenen SCSI-Bus verwenden und ein Failover auftritt, wird in Abhängigkeit vom Funktionsumfang Ihrer verschiedenen SAN-Komponenten das Medium u. U. im Bandlaufwerk belassen, bis der fehlgeschlagene Knoten wieder aktiv ist.

Wurden die Markierungen für das Auftragsende vor dem Failover nicht auf das Medium geschrieben, wird das Medium von Backup Exec bei der Ausführung des nächsten Anhängauftrags eventuell als nicht anhängefähig gekennzeichnet. Das Medium bleibt in diesem Zustand, bis es überschrieben wird (der Überschreibschutzzeitraum abgelaufen ist oder es gelöscht wird usw.).

Wenn es sich bei dem Speichergerät um einen Wechsler handelt, können Sie den Wechsler-Inventarisierungsbericht anzeigen, um festzustellen, ob das Medium von Backup Exec als nicht anhängefähig gekennzeichnet wurde. Wenn in der Spalte "Vollständig" die Ziffer 3 eingetragen ist, bedeutet dies, dass Backup Exec das Medium als nicht anhängefähig gekennzeichnet hat.

Führen Sie den Assistenten für Hot Swap-Geräte an allen Backup Exec-Clusterknoten aus, um einem Cluster Hot Swap-Geräte hinzuzufügen oder aus diesem zu entfernen. Ein Server muss zum Erkennen von neuen Geräten aktualisiert werden, sonst schlagen alle Aufträge fehl, die auf diesen Geräten ausgeführt werden sollen.

Siehe ["Hinzufügen oder Ersetzend von Geräten durch den Assistent für Hot Swap-Geräte"](#) auf Seite 447.

Die folgenden Beispiele veranschaulichen verschiedene Clusterkonfigurationen:

- Siehe ["Cluster mit zwei Knoten und lokal angeschlossenen Speichergeräten"](#) auf Seite 924.
- Siehe ["Cluster mit zwei Knoten und Bandgeräten an einem gemeinsamen SCSI-Bus"](#) auf Seite 925.
- Siehe ["Konfigurieren eines gemeinsam genutzten SCSI-Busses für Bandgeräte"](#) auf Seite 927.
- Siehe ["Cluster mit mehreren Knoten in einem Fibre Channel-SAN mit Central Admin Server Feature"](#) auf Seite 929.

Cluster mit zwei Knoten und lokal angeschlossenen Speichergeräten

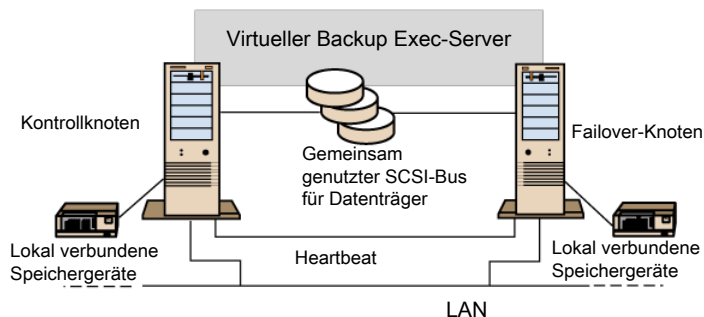
Bei dieser Konfiguration wird eine clustergerechte Backup Exec-Version auf dem steuernden Knoten installiert. Es wird ein bestimmter Knoten im Cluster als Failover-Knoten festgelegt und die Speichergeräte sind lokal an jeden Knoten angeschlossen.

Die lokal angeschlossenen Speichergeräte aller Knoten werden je nach Typ des Speichergeräts automatisch einem entsprechenden Speichergerätepool zugeordnet, den Backup Exec erstellt. Diese Speichergerätepools fungieren bei der Erstellung von Backup- oder Wiederherstellungsaufträgen auch als Standardzielgeräte auf diesem Knoten. Erstellen Sie einen Speicherpool, der Speichergeräte auf dem steuernden Knoten und dem Failover-Knoten enthält, sodass Aufträge bei einem Failover darauf ausgeführt werden können.

Siehe ["Erstellen von Speichergerätepools für Microsoft Cluster Server"](#) auf Seite 920.

Bevor eine Wiederherstellung von Daten dieser Konfiguration durchgeführt werden kann, müssen die Medien zum lokal angeschlossenen Speichergerät des Failover-Knotens verschoben und das Gerät erneut inventarisiert werden.

Abbildung 20-1 Cluster mit zwei Knoten und lokal angeschlossenen Speichergeräten



Siehe ["Cluster mit mehreren Knoten in einem Fibre Channel-SAN mit Central Admin Server Feature"](#) auf Seite 929.

Cluster mit zwei Knoten und Bandgeräten an einem gemeinsamen SCSI-Bus

Bei dieser Konfiguration ist die clusterfähige Backup Exec-Version auf dem steuernden Knoten installiert. Es wird ein bestimmter Knoten im Cluster als Failover-Knoten festgelegt und die Bandgeräte werden an einen gemeinsamen SCSI-Bus angeschlossen, der von anderen gemeinsamen SCSI-Bussen für Festplatten unabhängig ist.

Da jeder Knoten für dasselbe Gerät einen eigenen eindeutigen Bandgerätenamen erstellt, müssen Sie beim Verwenden eines nicht serialisierten Laufwerks für diese Konfiguration einen Speicherpool erstellen. Der Speicherpool muss die von allen Knoten verwendeten Bandgerätenamen enthalten, damit Aufträge bei einem Failover ausgeführt werden können.

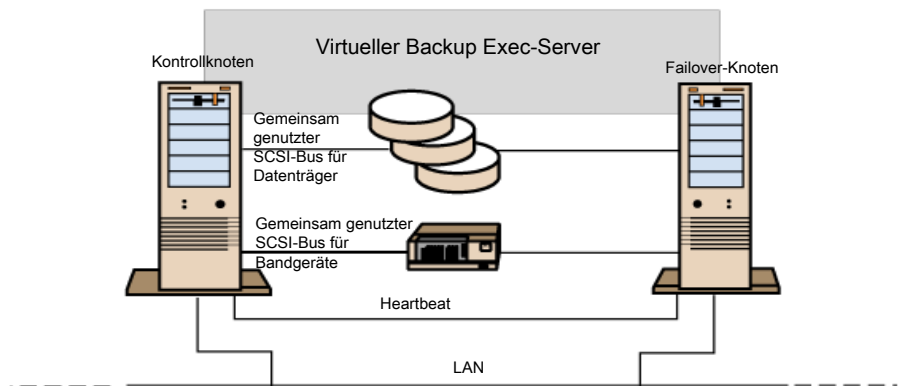
Siehe ["Erstellen von Speichergerätepools für Microsoft Cluster Server"](#) auf Seite 920.

Bei einem Failover wird der SCSI-Bus zurückgesetzt. Deshalb sollten Bandgeräte und gemeinsam verwendete Laufwerke nicht an denselben SCSI-Bus angeschlossen sein.

Siehe ["Konfigurieren eines gemeinsam genutzten SCSI-Busses für Bandgeräte"](#) auf Seite 927.

Hinweis: Bei Verwendung eines serialisierten Medienlaufwerks in einer gemeinsamen SCSI-Clusterkonfiguration werden alle Medien, die auf Grund eines Failover in einem Gerät verbleiben, aus dem Medienlaufwerk ausgeworfen. Wenn Sie ein nicht serialisiertes Bandgerät verwenden, müssen Sie die Medien manuell aus dem Gerät entfernen oder das Gerät neu starten.

Abbildung 20-2 Cluster mit zwei Knoten und Bandgeräten an einem gemeinsamen SCSI-Bus



Siehe ["Cluster mit mehreren Knoten in einem Fibre Channel-SAN mit Central Admin Server Feature"](#) auf Seite 929.

Konfigurieren eines gemeinsam genutzten SCSI-Busses für Bandgeräte

Zur Konfiguration von Bandgeräten an einem gemeinsam genutzten SCSI-Bus benötigen Sie für jeden Clusterknoten SCSI-Kabel, SCSI-Abschlusswiderstände, einen SCSI-Adapter (um einen gemeinsam genutzten externen Bus zwischen den Knoten bereitzustellen) sowie mindestens ein Bandgerät am gemeinsam genutzten Bus.

Die Bandgeräte müssen an einen Bus angeschlossen sein, der die gleiche Übertragungsmethode wie das Gerät verwendet (Single-Ended oder Differential). An einem einzelnen SCSI-Bus kann nur eine Übertragungsmethode verwendet werden. Es können jedoch zwischen den Geräten Signalkonverter installiert werden, wenn die Geräte verschiedene Übertragungsmethoden verwenden. Ein Signalkonverter wandelt Single-Ended-SCSI-Signale in Differential-SCSI-Signale um.

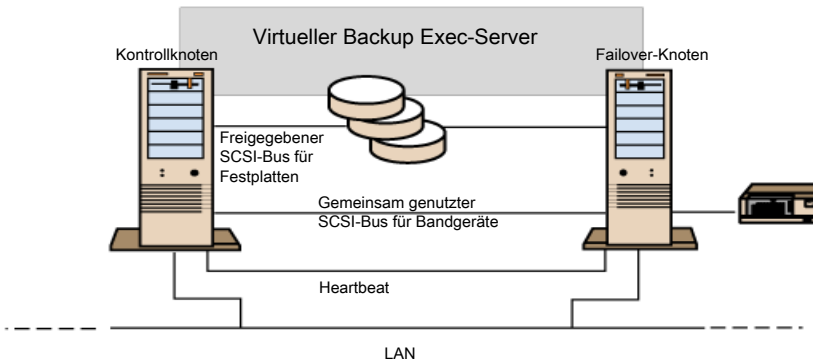
Hinweis: Zum Verbinden von Single-Ended- und Differential-Geräten müssen Signalkonverter verwendet werden, um Beschädigungen der Hardware zu verhindern.

Der SCSI-Bus muss an beiden Enden abgeschlossen werden, damit Befehle und Daten von und zu allen Geräten am Bus übertragen werden können. Jeder SCSI-Bus benötigt zwei Abschlusswiderstände, die sich jeweils am Ende des Segments befinden müssen.

Wenn sich ein Bandgerät in der Mitte eines Busses befindet, entfernen Sie jeden internen Abschlusswiderstand in diesem Gerät.

Befindet sich das Bandgerät am Ende des Busses und verfügt über einen internen Abschlusswiderstand, so können Sie diesen internen Abschlusswiderstand verwenden, um den Bus abzuschließen.

Abbildung 20-3 Beispiel eines gemeinsam genutzten SCSI-Busses mit Bandgeräten am Ende des Busses



Ein Bus kann mit den folgenden Methoden abgeschlossen werden:

- **SCSI-Adapter:** Diese Methode wird nicht empfohlen. Wenn der Server nicht mit dem gemeinsam genutzten Bus verbunden ist oder falls es zu einem Stromausfall kommt, kann der Bus eventuell nicht richtig abgeschlossen und dadurch funktionsunfähig werden.
- **Pass-Through- (oder Feed-Through-) SCSI-Abschlusswiderstände:** Diese können mit SCSI-Adaptern und mit einigen Bandgeräten verwendet werden. Wenn sich das Gerät am Ende des Busses befindet, können Sie einen Pass-Through-SCSI-Abschlusswiderstand anschließen, um den Bus abzuschließen. Interne Abschlusswiderstände im Bandgerät müssen deaktiviert werden. Diese Methode wird empfohlen.

Hinweis: Um sicherzustellen, dass der Abschluss bei einem Stromausfall funktioniert, schalten Sie Abschlusswiderstände am SCSI-Controller aus (benutzen Sie dazu die vom Hersteller des Hostadapters empfohlene Methode) und schließen Sie den Controller physisch mit einem Abschlusswiderstand ab.

- **Y-Kabel:** Diese können mit einigen Bandgeräten verwendet werden. Wenn sich das Bandgerät am Ende des Busses befindet, können Sie einen Abschlusswiderstand an einem Zweig des Y-Kabels anschließen, um den Bus abzuschließen. Interne Abschlusswiderstände im Bandgerät müssen deaktiviert werden. Diese Methode wird empfohlen.
- **Dreifachstecker:** Diese können mit einigen Bandgeräten verwendet werden. Wenn sich das Bandgerät am Ende des Busses befindet, können Sie einen

Abschlusswiderstand an einem Anschluss des Dreifachsteckers anschließen, um den Bus abzuschließen. Interne Abschlusswiderstände im Bandgerät müssen deaktiviert werden. Diese Methode wird empfohlen.

Y-Kabel und Dreifachstecker ermöglichen zudem die Isolierung der Geräte von einem gemeinsam genutzten Bus, ohne dass sich dies auf den Abschlusswiderstand des Busses auswirkt. Sie können dieses Gerät weiterhin verwenden oder entfernen, ohne dass sich dies auf die anderen Geräte am gemeinsam genutzten SCSI-Bus auswirkt.

So konfigurieren Sie einen gemeinsam genutzten SCSI-Bus für Bandgeräte:

- 1 Installieren Sie die SCSI-Controller für den gemeinsam genutzten SCSI-Bus.

Stellen Sie sicher, dass die SCSI-Controller für den gemeinsam genutzten SCSI-Bus unterschiedliche SCSI-IDs verwenden. Setzen Sie die SCSI-Controller-ID am steuernden Knoten beispielsweise auf 6 und am Failover-Knoten auf 7.

- 2 Bereiten Sie die SCSI-Controller für den gemeinsamen SCSI-Bus vor. Einzelheiten hierzu finden Sie in der Herstellerdokumentation zum SCSI-Hostadapter.

Während der Konfiguration des Computers sollten beide Knoten keinen Strom führen. Lässt sich dies jedoch nicht vermeiden, sollten die gemeinsam genutzten SCSI-Busse nicht an beide Knoten angeschlossen sein.

- 3 Schließen Sie die gemeinsam genutzten SCSI-Bandgeräte an das Kabel an, verbinden Sie das Kabel mit beiden Knoten und schließen Sie das Bussegment mit einer der im oben stehenden Abschnitt erläuterten Methoden ab.

Siehe "[Cluster mit zwei Knoten und Bandgeräten an einem gemeinsamen SCSI-Bus](#)" auf Seite 925.

Cluster mit mehreren Knoten in einem Fibre Channel-SAN mit Central Admin Server Feature

Bei dieser Konfiguration sind ein oder mehrere Cluster an ein Fibre Channel-SAN angeschlossen, wobei auf dem steuernden Knoten jedes Clusters die clusterfähige Backup Exec-Version und Central Admin Server Feature (CAS) installiert sind. Gemeinsam verwendete sekundäre Speichergeräte sind an den Fibre Channel angeschlossen, obwohl ein einzelnes Speichergerät von einem oder mehreren Clustern verwendet werden kann. Das Failover erfolgt in alphabetischer Reihenfolge des Computernamens auf anderen, als Failover-Knoten festgelegten Knoten im Cluster.

Hinweis: Es wird dringend empfohlen, die Clusterknoten über einen Fibre Switch mit den Speichergeräten zu verbinden, wenn Sie mehrere Cluster in einer CAS-Umgebung verwenden. Wenn Sie anstelle eines Fibre Switch einen Hub verwenden, wird der Hub während eines Failovers zurückgesetzt. Alle anderen an den Hub angeschlossenen Komponenten werden daraufhin getrennt. Sie können jeden Server in dem Fibre Channel-SAN als zentralen Administrationsserver festlegen.

Richten Sie im Cluster einen Speicherpool für Failover ein.

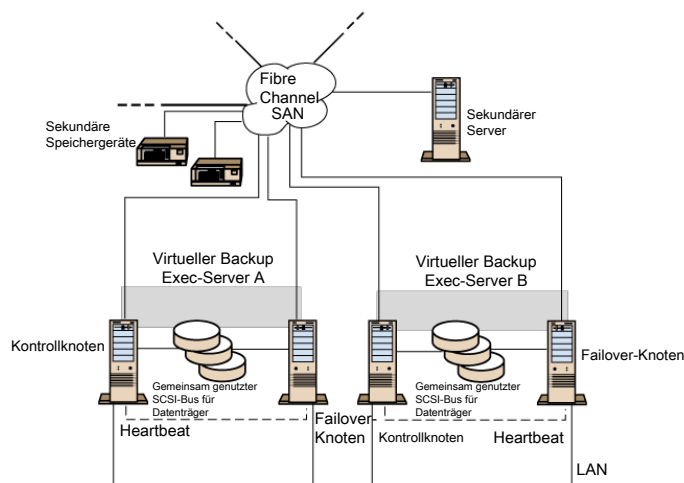
Siehe ["Erstellen von Speichergerätepools für Microsoft Cluster Server"](#) auf Seite 920.

Diese Konfiguration zeichnet sich durch eine verbesserte Leistungsfähigkeit aus, da Backups lokal anstatt über ein Netzwerk vorgenommen werden. Zusätzlich stehen zentralisierte Medienkataloge zur Verfügung. Da CAS eine gemeinsame Katalogdatenbank verwendet, kann ein bereits katalogisiertes Band ohne erneute Katalogisierung physisch von einem Gerät zum anderen verschoben werden.

Hinweis: CAS muss auf jedem Failover-Knoten mit denselben Einstellungen wie auf dem primären Knoten installiert sein. Alle Knoten sollten entweder Datenbankserver oder verwaltete Backup Exec-Server sein.

Im Folgenden finden Sie Beispiele für Cluster mit mehreren Knoten:

Abbildung 20-4 Zwei Cluster mit zwei Knoten in einem Fibre Channel-SAN mit Central Admin Server Feature



Sie können einen Cluster mit vier Knoten haben.

Siehe "[Verwenden von Central Admin Server Feature mit Microsoft-Clustern und einem SAN](#)" auf Seite 931.

Verwenden von Central Admin Server Feature mit Microsoft-Clustern und einem SAN

Verwaltete Backup Exec-Server können gruppiert werden. Jedoch wird diese Konfiguration nicht empfohlen, da der zentrale Administrationsserver alle fehlgeschlagenen Aufträge in einer verteilten Auftragsumgebung wiederherstellt.

Folgende Konfigurationen können bei der Installation von Backup Exec-Clustern mit Central Admin Server Feature (CAS) verwendet werden.

- Backup Exec-Cluster mit CAS
- Backup Exec-Cluster mit Konfiguration für verwaltete Backup Exec-Server

So installieren Sie Backup Exec in einem Microsoft-Cluster mit CAS

- 1** Installieren Sie Backup Exec mit CASO und zusätzlichen Funktionen auf den Microsoft-Clusterknoten.
- 2** Starten Sie Backup Exec von dem Knoten aus, den Sie als aktiven Knoten festlegen möchten.
- 3** Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und dann "Assistent für die Clusterkonfiguration".
- 4** Befolgen Sie die Anweisungen auf dem Bildschirm.
- 5** Installieren Sie nach Beendigung des Assistenten für die Clusterkonfiguration den verwalteten Backup Exec-Server. Verwenden Sie für den zentralen Administrationsserver den Namen des virtuellen Backup Exec-Clusters, wenn Sie dazu aufgefordert werden.

So installieren Sie Backup Exec in einem Microsoft-Cluster mit der Konfiguration für verwaltete Backup Exec-Server

- 1 Installieren Sie Backup Exec mit der Funktion für verwaltete Backup Exec-Server und zusätzlichen Funktionen auf den Microsoft-Clusterknoten.

Achten Sie darauf, dass alle Knoten, die Backup Exec in der Microsoft-Clusterkonfiguration ausführen, auf denselben zentralen Administrationsserver zugreifen. Greifen die Knoten nicht auf denselben zentralen Administrationsserver zu, können Failover nicht ordnungsgemäß ausgeführt werden.
- 2 Starten Sie Backup Exec von dem Knoten aus, den Sie als aktiven Knoten festlegen möchten.
- 3 Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und dann "Assistent für die Clusterkonfiguration".
- 4 Befolgen Sie die Anweisungen auf dem Bildschirm.

Siehe ["Info zur Sicherung von Microsoft Cluster Servern"](#) auf Seite 932.

Info zur Sicherung von Microsoft Cluster Servern

Um alle Daten im Cluster (einschließlich Dateifreigaben, Datenbanken und Clusterquorum) zu schützen, muss Folgendes gesichert werden:

- Lokale Festplatten, Schattenkopie-Komponenten und der Systemstatus auf allen Knoten. Das Clusterquorum, das Wiederherstellungsdaten für den Cluster sowie Informationen zu den Änderungen der Clusterkonfiguration enthält, ist beim Systemstatus-Backup enthalten.
- Alle gemeinsam verwendeten Festplatten einschließlich der Daten im Microsoft Cluster Server-Ordner auf der Quorum-Festplatte.
- Virtuelle Server, die möglicherweise Daten oder Anwendungen wie Microsoft SQL Server oder Exchange Server enthalten. Verwenden Sie Backup Exec-Datenbank-Agents zum Sichern von Datenbanken.

Hinweis: Bei Backup-Aufträgen auf einem anderen Host unter Verwendung des Hardwareanbieters müssen sich der Backup Exec-Server und der Remote-Computer in unterschiedlichen Clustergruppen befinden. Clusteranwendungen unterstützen keine LUNs (Logical Unit Numbers, Nummern der logischen Einheit) von Geräten, die über doppelte Signaturen und Partitionslayouts verfügen. Snapshots, die LUNs enthalten, müssen auf einen Host oder Remote-Computer übertragen werden, der sich außerhalb des Clusters befindet.

Sie können die Backup Exec-Befehlszeilenschnittstelle (BEMCLI) verwenden, wenn Backup Exec in einem Cluster installiert ist. Die einzige Beschränkung ist, dass Sie BEMCLI nicht verwenden können, um ein zu sicherndes Gerät anzugeben. Sie können BEMCLI zur Auswahl eines Speicherpools, jedoch nicht zur Auswahl eines bestimmten Geräts in diesem Pool verwenden.

Siehe ["Sichern von Daten"](#) auf Seite 174.

Siehe ["Bearbeiten von Backup-Definitionen"](#) auf Seite 226.

Siehe ["Hinzufügen einer Stufe zu einer Backup-Definition"](#) auf Seite 244.

Wiederherstellen von Daten in einem Microsoft Cluster

Bei allen Dateiwiederherstellungsvorgängen (einschließlich des Umleitens von Wiederherstellungen) gilt der normale Ablauf.

Leiten Sie beim Wiederherstellen von Dateien auf gemeinsam verwendete Laufwerke die Dateien zum virtuellen Server oder zum steuernden Knoten der Ressource weiter. Beim Wiederherstellen einzelner Datenbankdateien (z. B. Microsoft SQL Server oder Exchange Server) sollten Sie diese Dateien zum virtuellen Server einer spezifischen Installation der SQL- oder Exchange-Datenbank weiterleiten.

Siehe ["Methoden für das Wiederherstellen von Daten in Backup Exec"](#) auf Seite 258.

Notfallwiederherstellung eines Clusters

Bereiten Sie die Notfallwiederherstellung durch Erstellung eines Plans für die Notfallwiederherstellung vor.

Bereiten Sie die Wiederherstellung von SQL- und Exchange-Datenbanken in einem Cluster nach einem Systemausfall vor, indem Sie die Abschnitte zum Vorbereiten von Notfallwiederherstellungen in den entsprechenden Kapiteln lesen.

Zusätzlich sind weitere Schritte notwendig, um Microsoft-Cluster vollständig zu schützen.

In einem Notfall werden folgende Daten benötigt, um den Cluster erfolgreich wiederherzustellen:

- Allgemeine Informationen zum Cluster
 - Clustername
 - IP-Adresse und Subnetzmaske des Clusters
 - Clusterknotennamen

- IP-Adressen der Knoten
- Lokale und gemeinsam verwendete Laufwerksbuchstaben und das Partitionsschema
- Datenträgersignaturen
- Clustergruppen
 - Gruppenname
 - Bevorzugte Knoten
 - Failover-/Failback-Richtlinien
- Clusterressourcen
 - Ressourcenname
 - Ressourcentyp
 - Gruppenmitgliedschaft
 - Mögliche Besitzer
 - Ressourcenabhängigkeiten
 - Eigenschaften für Neustart und Looks Alive/Is Alive
 - Ressourcenbezogene Parameter
 - Anwendungsspezifische Konfiguration (SQL-Datenbankzeichensatz)

Siehe ["Erstellen eines Plans für die Notfallwiederherstellung \(DPP\)"](#) auf Seite 148.

Siehe ["Notfallwiederherstellung für Exchange-Server"](#) auf Seite 1316.

Verwenden von Simplified Disaster Recovery zum Vorbereiten einer Notfallwiederherstellung eines Clusters

In Backup Exec steht eine vollautomatische Lösung für die Notfallwiederherstellung mit der Bezeichnung Simplified Disaster Recovery (SDR) zur Verfügung, mit der Sie Knoten in einem Servercluster im Notfall schnell und problemlos wiederherstellen können. Oracle-Server können nicht mithilfe von Simplified Disaster Recovery wiederhergestellt werden. Weitere Informationen zur Notfallwiederherstellung für diese Optionen finden Sie in den entsprechenden Kapiteln.

Siehe ["Vorbereiten von Computern für die Verwendung mit Simplified Disaster Recovery"](#) auf Seite 946.

Hinweis: Wenn Sie das Setup ändern oder von der ursprünglichen Konfiguration abweichende Hardware bzw. Hardwarekonfigurationen verwenden möchten, müssen Sie eine manuelle Wiederherstellung vornehmen.

Wiederherstellen von Knoten im Cluster mithilfe von Simplified Disaster Recovery

Wenn Sie zur Vorbereitung auf einen Notfall Simplified Disaster Recovery von Backup Exec verwendet haben, können Sie die Knoten mithilfe von SDR wiederherstellen.

Wenn Sie beide Knoten in einem Cluster wiederherstellen, müssen die Laufwerksbuchstaben mit der ursprünglichen Clusterkonfiguration übereinstimmen. Die minimierte Windows-Version, unter der der Assistent für die IDR-Notfallwiederherstellung ausgeführt wird, erkennt die Festplatten möglicherweise in einer anderen Reihenfolge als in der ursprünglichen Konfiguration unter der zuvor verwendeten Windows-Version.

Wenn die ursprüngliche Konfiguration nicht übereinstimmt, können Sie die von Windows vorgenommene Festplattennummerierung bis zu einem gewissen Grad beeinflussen.

Kann der Assistent "Computer wiederherstellen" die Reihenfolge der Festplatten nicht erkennen, können Sie Festplattenpartitionen manuell mit Hilfe der Option "Erweiterte Datenträgerkonfiguration" des Assistenten "Computer wiederherstellen" einrichten. Anschließend können Sie mit der automatisierten Wiederherstellung des Backup-Mediums fortfahren.

Hinweis: Der Laufwerksbuchstabe des Systemlaufwerks kann nach der Installation von Windows nicht mehr geändert werden. Das System muss zu dem Laufwerksbuchstaben wiederhergestellt werden, von dem es gesichert wurde.

So stellen Sie Knoten im Cluster mithilfe von Simplified Disaster Recovery wieder her

- 1 Wenn Sie mehrere Knoten wiederherstellen, sollten Sie die Verbindung der gemeinsam verwendeten Festplatten trennen. Dies ist nicht notwendig, wenn Sie nur einen Knoten wiederherstellen.

Wenn kein Knoten im Cluster verfügbar ist und alle Knoten wiederhergestellt werden müssen, kann im Cluster kein Failover erfolgen. Trennen Sie die Verbindung der gemeinsam verwendeten Festplatten vor dem Start der Wiederherstellung.

- 2 Stellen Sie die Knoten wieder her.

Siehe ["Methoden für das Wiederherstellen von Daten in Backup Exec"](#) auf Seite 258.

- 3 Stellen Sie die Verbindung der gemeinsam verwendeten Laufwerke wieder her und schalten Sie die Knoten online.
- 4 Verwenden Sie zum Wiederherstellen einer Datenbank auf den gemeinsam verwendeten Laufwerken den entsprechenden Backup Exec Agent.

Siehe ["Info zu Simplified Disaster Recovery"](#) auf Seite 941.

Wiederherstellen von Backup Exec in einem Microsoft-Cluster mithilfe von Simplified Disaster Recovery

Um einen Cluster, in dem Backup Exec installiert ist, vollständig wiederherzustellen, können Sie den Clusterknoten und alle gemeinsam verwendeten Datenträger mit Simplified Disaster Recovery wiederherstellen oder den Cluster neu erstellen. Um den Cluster standortfern wiederherzustellen, katalogisieren Sie die Medien, die die Backup-Sätze der Clusterknoten und die gemeinsam verwendeten Festplatten enthalten.

So stellen Sie Backup Exec in einem Microsoft-Cluster mit Simplified Disaster Recovery wieder her

- 1 Ersetzen Sie bei Bedarf alle gemeinsam verwendeten Festplatten.
- 2 Führen Sie den Assistenten "Computer wiederherstellen" auf einem der Knoten aus. Verwenden Sie "Erweiterte Datenträgerkonfiguration", um die Partitionen aller gemeinsam verwendeten Festplatten auf ihre ursprüngliche Konfiguration zurückzusetzen. Speichern Sie den lokalen Datenträger, Systemstatus und die Datendateien auf der gemeinsam verwendeten Festplatte.

- 3 Starten Sie den Server neu.

Der Clusterdienst und alle anderen Clusteranwendungen sind nun online.

- 4 Führen Sie den Assistenten "Computer wiederherstellen" auf allen weiteren Knoten aus. Stellen Sie nur den lokalen Datenträger und den Systemstatus wieder her.

Siehe ["Info zu Simplified Disaster Recovery"](#) auf Seite 941.

Wiederherstellen des gesamten Clusters mithilfe der manuellen Notfallwiederherstellung

Im Zuge der manuellen Wiederherstellung müssen Sie Windows einschließlich des Service Pack, das vor dem Ausfall installiert war, neu installieren.

Siehe ["Wiederherstellen von Oracle-Ressourcen"](#) auf Seite 1368.

So stellen Sie den gesamten Cluster manuell wieder her

- 1 Installieren Sie Windows auf dem ersten wiederherzustellenden Knoten neu (einschließlich des Service Packs, das vor dem Ausfall installiert war).
- 2 Installieren Sie Windows auf den anderen wiederherzustellenden Knoten neu (einschließlich des Service Packs, das vor dem Ausfall installiert war).
- 3 Installieren Sie die Clusterdienste neu und schalten Sie den Cluster online.

Gehen Sie wie folgt vor:

- Wenn Sie einen Microsoft Cluster Server wiederherstellen, stellen Sie nach dem Hochfahren der Knoten in einem Cluster sicher, dass die Laufwerksbuchstaben mit der ursprünglichen Clusterkonfiguration übereinstimmen. Wenn die ursprüngliche Konfiguration nicht übereinstimmt, können Sie die von Windows vorgenommene Festplattennumerierung bis zu einem gewissen Grad beeinflussen. Verwenden Sie hierzu den Festplatten-Manager.
- Wenn Sie einen Microsoft Cluster Server wiederherstellen möchten, verwenden Sie den Assistenten für die Clusterkonfiguration, um Backup Exec im Cluster neu zu installieren. Achten Sie darauf, dass Sie dieselben Einstellungen wie bei der ursprünglichen Installation verwenden.
Siehe ["Installieren von Backup Exec auf einem Microsoft Cluster Server"](#) auf Seite 916.

- 4 Katalogisieren Sie die Medien im Cluster.
- 5 Auf der Registerkarte "Backup und Wiederherstellung auf dem aktiven Knoten, klicken Sie auf "Wiederherstellen".

- 6 Stellen Sie die neuesten vollständigen Backup-Sätze vom aktiven Knoten wieder her und stellen Sie anschließend den Systemstatus wieder her.
- 7 Wenn Sie Microsoft Cluster Server wiederherstellen, wählen Sie die Option "Clusterquorum wiederherstellen" im "Assistent für Wiederherstellungsaufträge" aus.
- 8 Starten Sie die Wiederherstellung.
- 9 Starten Sie den aktiven Knoten nach Abschluss der Wiederherstellung neu.
- 10 Wiederholen Sie für jeden wiederherzustellenden Knoten Schritt 5 bis 9.
- 11 Stellen Sie nach der Wiederherstellung aller Knoten die Backup Exec-Datendateien und alle anderen Datendateien auf den gemeinsam verwendeten Festplatten wieder her.
- 12 Verwenden Sie zum Wiederherstellen einer Datenbank auf den gemeinsam verwendeten Festplatten den entsprechenden Backup Exec Agent.

Wiederherstellen der Datendateien des Microsoft Clusters Servers

Um den Cluster vollständig wiederherzustellen, müssen u. U. die Clusterdateien im MSCS-Ordner wiederhergestellt werden. Wenn der Quorumdatenträger noch verfügbar ist und nicht geändert wurde, müssen Sie die Datendateien nicht wiederherstellen.

Für Windows-Versionen vor Windows Server 2008, wenn der Quorumdatenträger neu ist, müssen Sie die Datendateien auf dem neuen Quorumdatenträger wiederherstellen. Deaktivieren Sie den Treiber des Clusterdatenträgers, bevor Sie die Datendateien wiederherstellen.

Siehe ["Methoden für das Wiederherstellen von Daten in Backup Exec"](#) auf Seite 258.

Wiederherstellen von Backup Exec in einem Microsoft-Cluster

Falls Sie mithilfe des "Assistenten zum Erstellen eines SDR-Datenträgers" die Notfallwiederherstellungsmedien für die gemeinsam verwendeten Festplatten vorbereitet haben, müssen Sie Backup Exec auf einer gemeinsam genutzten Festplatte manuell wiederherstellen.

So stellen Sie Backup Exec auf einer gemeinsam verwendeten Festplatte manuell wieder her

- 1 Ersetzen Sie bei Bedarf die gemeinsam verwendete Festplatte und fügen Sie dem Cluster diese Festplatte als Festplattenressource hinzu.
- 2 Installieren Sie die clusterfähige Version von Backup Exec auf dem Cluster neu. Verwenden Sie dazu dieselben Angaben wie bei der ursprünglichen Installation.
- 3 Verwenden Sie Backup Exec, um Daten aus den Katalogen wiederherzustellen.

Siehe ["Methoden für das Wiederherstellen von Daten in Backup Exec"](#) auf Seite 258.

Manuelles Verbinden zweier Cluster-Datenträgergruppen und Neusynchronisierung der Datenträger

Wenn ein Advanced Disk-based-Backup wegen des virtuellen Server-Failovers der Anwendung fehlgeschlagen ist, müssen Sie die Cluster-Datenträgergruppen möglicherweise manuell miteinander verbinden.

So verbinden Sie erneut zwei Cluster-Datenträgergruppen und synchronisieren die Datenträger:

- 1 Importieren Sie die Cluster-Datenträgergruppe in den Knoten, wenn nicht bereits die ursprüngliche Cluster-Datenträgergruppe in den Knoten importiert wurde, auf dem derzeit der virtuelle Produktivserver ausgeführt wird.
- 2 Verbinden Sie die neue Cluster-Datenträgergruppe erneut mit der ursprünglichen Cluster-Datenträgergruppe.
- 3 Übertragen Sie die Snapshot-Datenträger auf die ursprünglichen Datenträger zurück. Vergewissern Sie sich, dass die Option zum Synchronisieren mit den ursprünglichen Datenträgern ausgewählt ist.

Wenn es nicht möglich ist, die neue Cluster-Datenträgergruppe in den Knoten zu importieren, in dem sich die ursprüngliche Cluster-Datenträgergruppe derzeit befindet, führen Sie ein Failover der virtuellen Serveranwendung zu ihren ursprünglichen Knoten aus, bevor Sie die beiden Cluster-Datenträgergruppen erneut verbinden.

Siehe ["Fehlerbehebungs-Cluster"](#) auf Seite 940.

Fehlerbehebungs-Cluster

Wenn beim Einsatz von Backup Exec in einer Clusterumgebung Probleme auftreten, sehen Sie in diesem Abschnitt nach.

Tabelle 20-2 Fragen und Antworten zur Cluster-Fehlerbehebung

Frage	Antwort
Ich habe die Option "Auftragswiederaufnahme" für meine Backups verwendet. Bei einem Backup-Vorgang trat ein Microsoft Cluster-Failover auf. Mehrere Backup-Sätze wurden erstellt. Bei Verwendung dieser Backup-Sätze zum Verifizieren oder Wiederherstellen wird die Fehlermeldung "Unerwartetes Datenende" für den Backup-Satz mit den Daten angezeigt, die vor dem Failover gespeichert wurden. Wie kommt es zu dieser Fehlermeldung? Sind die Daten sicher?	Diese Fehlermeldung wird angezeigt, da das Failover während des Ressourcen-Backup auftrat und der Backup-Satz aus diesem Grund auf dem Medium nicht geschlossen werden konnte. Die im ersten Backup-Satz teilweise gesicherten Objekte wurden nach dem Neustart erneut vollständig gesichert, damit die Datenintegrität gewährleistet ist. Aus diesem Grund sollten alle Objekte eines bestimmten Backup-Satzes wiederhergestellt und verifiziert werden.
Ich habe einen zentralen Administrationsserver mit einem verwalteten Backup Exec-Server gruppiert. Jetzt schlägt der Geräte- und Mediendienst auf dem verwalteten Backup Exec-Server fehl. Woran liegt das?	Dies ist der Fall, wenn der verwaltete Backup Exec-Server der aktive Knoten ist und versucht, mit der Backup Exec-Datenbank auf dem zentralen Administrationsserver zu verbinden, der nicht mehr verfügbar ist. Verwenden Sie die Backup Exec Utility (BEUTILITY.EXE) oder installieren Sie den verwalteten Backup Exec-Server erneut als zentralen Administrationsserver, um das Problem zu beheben.

Siehe ["Über Backup Exec und Cluster"](#) auf Seite 912.

Simplified Disaster Recovery

In diesem Kapitel werden folgende Themen behandelt:

- [Info zu Simplified Disaster Recovery](#)
- [Anforderungen für die Anwendung von Simplified Disaster Recovery](#)
- [Vorbereiten von Computern für die Verwendung mit Simplified Disaster Recovery](#)
- [Sicherstellen, dass Simplified Disaster Recovery für Backups aktiviert ist](#)
- [Verwendung der Notfallwiederherstellungs-Informationsdateien durch Simplified Disaster Recovery](#)
- [Festlegen oder Ändern des alternativen Speicherorts für die Notfallwiederherstellungs-Informationsdatei](#)
- [Erstellen eines SDR-Datenträger-Image](#)
- [Sich vorbereiten, um sich von einem Systemausfall durch die Anwendung von Simplified Disaster Recovery zu erholen](#)
- [Wiederherstellen eines Computers mithilfe von Simplified Disaster Recovery](#)
- [Erweiterte Datenträgerkonfiguration in Verbindung mit dem Assistenten "Computer wiederherstellen"](#)
- [Manuelles Ausführen der Notfallwiederherstellung](#)

Info zu Simplified Disaster Recovery

Simplified Disaster Recovery (SDR) wird automatisch mit Backup Exec installiert, damit Sie Notfallwiederherstellung auf Windows-Computern durchführen können,

auf denen der Agent for Windows installiert wird. Standardmäßig ist Backup Exec so konfiguriert, dass alle kritischen Systemkomponenten gesichert werden, die Sie zum Wiederherstellen eines Computers benötigen.

Verwenden Sie den Assistent zum Erstellen eines SDR-Datenträgers, um eine SDR-Datenträger-Image zu erstellen. Verwenden Sie den Wiederherstellungsdatenträger, um eine Notfallwiederherstellung der Computer durchzuführen, die gesichert werden.

Wenn Sie SDR verwenden, um eine Wiederherstellung durchzuführen, verwendet Backup Exec die Systemstufeninformationen vom SDR-Backup, um den Server umzubauen und in einen Funktionszustand wiederherzustellen. Eine Wiederherstellung umfasst eine Bare Metal- oder eine unähnliche Hardwarewiederherstellung.

Durch Integration mit Microsoft Volume Shadow Copy Service (VSS) enthalten die SDR-Backups alle ausgewählten Elemente, auch wenn sie Komponenten des aktiven Betriebssystems oder in einem geöffneten Zustand sind. VSS-Integration stellt sicher, dass die Backups in einem konsistenten Status sind und in einen Ruhezustand versetzt worden sind, wenn das Backup auftritt.

Simplified Disaster Recovery ist nur für Server verfügbar, auf denen der Agent for Windows installiert ist und die durch den Agent for Windows gesichert werden. Sie müssen Agent for Windows separat erwerben. Installieren Sie ihn anschließend auf den Remote-Computern, die Sie schützen möchten.

Die Simplified Disaster Recovery-Funktion erfordert jetzt das Microsoft Assessment and Deployment Kit (ADK), um ein Simplified Disaster Recovery-Datenträger-Image (.iso) zu erstellen.

Hinweis: Nachdem Backup Exec aktualisiert wurde, müssen Kunden die vorhandenen SDR-ISO-Dateien anpassen, damit diese mit der neuen Backup Exec-Version kompatibel sind.

Informationen zu den Best Practices zum Einsatz von Backup Exec Simplified Disaster Recovery (SDR) finden Sie unter *Best Practices für Backup Exec*.

Siehe ["Vorbereiten von Computern für die Verwendung mit Simplified Disaster Recovery"](#) auf Seite 946.

Siehe ["Sicherstellen, dass Simplified Disaster Recovery für Backups aktiviert ist"](#) auf Seite 950.

Siehe ["Anforderungen für die Anwendung von Simplified Disaster Recovery"](#) auf Seite 943.

Siehe ["Erstellen eines SDR-Datenträger-Image"](#) auf Seite 957.

Siehe ["Wiederherstellen eines Computers mithilfe von Simplified Disaster Recovery"](#) auf Seite 987.

Anforderungen für die Anwendung von Simplified Disaster Recovery

Sie benötigen die folgenden Produkte für Simplified Disaster Recovery (SDR):

- Backup Exec oder der Backup Exec Agent for Windows muss auf jedem Computer, den Sie mit SDR schützen möchten, installiert sein.

Hinweis: Der Assistent zum Erstellen eines SDR-Datenträgers wird unter 32-Bit-Betriebssystemen nicht unterstützt.

- Verschlüsselungsdateien müssen für alle Datenträger, die mithilfe der Windows-BitLocker-Laufwerkverschlüsselung verschlüsselt werden, vorhanden sein.
- Eine ISO 9660-kompatible CD- oder DVD-Brennanwendung eines Drittanbieters, um das mit SDR erstellte startfähige Image auf eine CD oder DVD zu brennen.
- Ein Laufwerk für beschreibbare bzw. wiederbeschreibbare CDs oder DVDs muss verfügbar sein.
- Eine Internetverbindung, sodass Sie das Assessment and Deployment Kit von Microsoft herunterladen können.
- Die Option "Speicherbasierte Kataloge verwenden" muss aktiviert sein. Wenn Sie diese Option deaktivieren, können die Backup-Sätze, die Sie für den Einsatz mit SDR erstellt haben, nicht während eines SDR-Wiederherstellungsvorgangs wiederhergestellt werden. SDR kann den beschädigten Computer daher nicht wiederherstellen. Um sicherzustellen, dass diese Option aktiviert ist, klicken Sie auf die Backup Exec-Schaltfläche und dann auf "Konfiguration und Einstellungen" > "Backup-Einstellungen" > "Katalog".

Hinweis: Wenn Sie Deduplizierungs-Plattenspeichergeräte verwenden, beachten Sie, dass es Beschränkungen in ihrer Verwendung mit SDR gibt.

Siehe ["Hinweise zum Einsatz von Simplified Disaster Recovery mit Exchange, SQL, SharePoint, CAS, Hyper-V-Hosts und Deduplication Feature"](#) auf Seite 999.

Es gibt zusätzliche Anforderungen, wenn Sie ein Simplified Disaster Recovery-Datenträger-Image erstellen und wenn Sie den Assistenten "Computer wiederherstellen" wie in den folgenden Abschnitten beschrieben wiederherstellen.

Anforderungen zum Erstellen eines Simplified Disaster Recovery-Datenträger-Image

Sie benötigen die folgenden Produkte zum Erstellen des SDR-Datenträger-Image:

- Das Simplified Disaster Recovery-Datenträger-Image muss dieselbe Version von Backup Exec sein wie der Backup Exec-Server. Sie können SDR nicht zum Wiederherstellen von Backups verwenden, die mit vorherigen Versionen von Backup Exec erstellt wurden.
- Das Microsoft Windows Assessment and Deployment Kit (8.1 und 8.1 Update 1) wird nur unter Windows Server 2008 SP2 unterstützt. Unter Windows Server 2008 R2 bis Windows Server 2016 können SDR-Datenträger nur mit ADK 10 erstellt werden. Unter Windows Server 2019 müssen Sie Windows ADK 1809 verwenden, um einen SDR-Datenträger zu erstellen. Wenn der Backup Exec-Server unter Windows Server 2008 SP2 oder höher nicht ausgeführt wird oder wenn der Server keine Internetverbindung hat, werden Methoden bereitgestellt, mit denen Sie den SDR-Datenträger erstellen können.

Hinweis: Der Wiederherstellungsdatenträger, der mit Windows ADK 8.1 erstellt wurde, erkennt den Backup Exec-Speicherordner (\BEData) nicht, wenn dieser in den Speicherpools und -plätzen auf dem Backup Exec-Server konfiguriert ist. Dieses Problem tritt nur auf, wenn der Backup Exec-Server (unter Windows Server 2016) nicht verfügbar ist und eine lokale SDR-Wiederherstellung aus dem Ordner "BEData" ausgeführt werden soll.

Wiederherstellungsdatenträger, die mit Windows ADK 8.1 oder 10 erstellt wurden, erkennen den Backup Exec-Speicherordner (\BEData) nicht, wenn dieser in den Speicherpools und -plätzen auf dem Backup Exec-Server konfiguriert ist. Dieses Problem tritt nur auf, wenn der Backup Exec-Server (unter Windows Server 2019) nicht verfügbar ist und eine lokale SDR-Wiederherstellung aus dem Ordner "BEData" ausgeführt werden soll.

Wenn Sie die Speicherpools und Speicherplätze unter Verwendung des Wiederherstellungsdatenträgers erstellen, der mit Windows ADK 10 erstellt wurde, dann erkennt Windows Server 2012 (R2) nach der Systemwiederherstellung die Speicherpools und die Speicherplätze nicht.

Wenn Sie die Speicherpools und -plätze mit einem Wiederherstellungsdatenträger erstellen, der mit Windows ADK 1809 erstellt wurde, werden diese unter Windows Server 2016 und niedriger nach der Systemwiederherstellung nicht erkannt.

- 5 GB Speicherplatz zum Herunterladen und Installieren des ADK.

- 1 GB Speicherplatz zum Speichern der erforderlichen Dateien und Ordner zum Erstellen des ISO-Image.

Anforderungen zum Ausführen des Assistenten "Computer wiederherstellen"

Zum Ausführen des Assistenten "Computer wiederherstellen" wiederherzustellen, sind folgende Elemente erforderlich:

- Das Simplified Disaster Recovery-Datenträger-Image muss dieselbe Version von Backup Exec sein wie der Backup Exec-Server.
- Wenn der wiederherzustellende Computer auf ein Bandgerät, einen Deduplizierungsspeicher oder einen virtuellen Datenträger gesichert wurde, kann SDR die Notfallwiederherstellungs-Informationsdatei nicht mit den Backup-Sätzen speichern. Stattdessen müssen Sie den Pfad zum Standardspeicherort oder dem alternativen Speicherort angeben, wenn Sie vom Assistenten "Computer wiederherstellen" dazu aufgefordert werden. Der Standardordner ist `C:\<Backup Exec-Installationsordner>\Backup Exec\sdr\Data`. Wenn die Datei nicht verfügbar ist, können Sie den Computer nicht mit SDR wiederherstellen.
- Der Backup-Satz, der alle kritischen Systemkomponenten für den zu wiederherstellenden Computer enthält.
- Das Startlaufwerk auf dem zu wiederherstellenden Computer muss je nach Betriebssystem und Konfiguration zwischen 3 und 5 GB freien Speicherplatz haben.

Wenn ein leerer Bildschirm angezeigt wird und der Computer nach dem Verwenden des SDR-Datenträgers nicht neu gestartet wird, vergewissern Sie sich, dass das Startlaufwerk genügend freien Speicherplatz verfügbar hat. Starten Sie anschließend den Computer neu.
- Der zu wiederherstellende Zielcomputer muss eine Menge von RAM haben, die größer oder gleich dem für das wiederhergestellte Betriebssystem mindestens erforderlichen Speicherplatz ist.
- Der zu wiederherstellende Zielcomputer muss Datenträger mit genügend freiem Speicher für die Daten haben, die Sie vom Backup von kritischen Datenträgern wiederherstellen. Ein Datenträger wird als kritisch betrachtet, wenn er für einen erfolgreichen Start des Computers erforderlich ist.
- Wenn Sie einen Windows-Computer wiederherstellen, bei dem BitLocker-Verschlüsselung aktiviert ist, muss diese nach der Wiederherstellung aktiviert werden. Weitere Informationen zur BitLocker-Laufwerkverschlüsselung finden Sie in der Microsoft-Dokumentation.

- Wenn der Computer, den Sie wiederherstellen, ein RAID-Setup enthält, müssen Sie möglicherweise zuerst das RAID konfigurieren, bevor Sie ihn mit dem SDR-Datenträger starten. Verwenden Sie die RAID-Software des Computerherstellers, um das RAID-System zu konfigurieren.
- Wenn Sie Windows mit Speicherpools und Speicherplätzen wiederherstellen, sollten Sie die möglichen Wiederherstellungsszenarien kennen.
Siehe ["Wiederherstellungshinweise für die Anwendung von Simplified Disaster Recovery in Verbindung mit Speicherpools und Speicherplätzen"](#) auf Seite 995.

Siehe ["Erstellen eines SDR-Datenträger-Image"](#) auf Seite 957.

Siehe ["Wiederherstellen eines Computers mithilfe von Simplified Disaster Recovery"](#) auf Seite 987.

Vorbereiten von Computern für die Verwendung mit Simplified Disaster Recovery

Bereiten Sie Computer für Verwendung mit Simplified Disaster Recovery (SDR) vor, indem Sie die folgenden Schritte durchführen:

Tabelle 21-1 Vorbereiten von Computern für die Verwendung mit Simplified Disaster Recovery

Schritt	Beschreibung	Weitere Informationen
Schritt 1	Geben Sie einen alternativen Speicherort für Kopien der Notfallwiederstellungs-Informationsdateien an.	<p>Backup Exec erstellt die Notfallwiederherstellungs-Informationsdatei, nachdem ein Backup-Auftrag, der alle kritischen Systemkomponenten umfasst, erfolgreich abgeschlossen wurde. Backup Exec speichert dann die Datei im Standardspeicherort mit dem Backup-Satz auf einem Plattenspeicher oder einem Plattenkassettengerät und in den alternativen Speicherorten. Katalogeinträge aus späteren Backups werden automatisch der Notfallwiederherstellungs-Informationsdatei hinzugefügt.</p> <p>Warnung: Wenn Sie einen Computer auf ein Bandgerät, einen Deduplizierungsspeicher oder einen virtuellen Datenträger sichern, kann Backup Exec keine Notfallwiederherstellungs-Informationsdatei mit dem Backup-Satz speichern. Sie benötigen eine Notfallwiederherstellungs-Informationsdatei in einem alternativen Speicherort, damit Sie den Computer mit SDR wiederherstellen können.</p> <p>Siehe "Festlegen oder Ändern des alternativen Speicherorts für die Notfallwiederherstellungs-Informationsdatei" auf Seite 954.</p>

Schritt	Beschreibung	Weitere Informationen
Schritt 2	<p>Führen Sie die Backup-Aufträge aus, die alle kritischen Systemkomponenten für die Computer umfassen, die Sie schützen möchten, enthalten. Dies sind die Backups, für die die Simplified Disaster Recovery-Anzeige auf "Ein" steht.</p> <p>Hinweis: Für Umgebungen, die Central Admin Server Feature ausführen, führen Sie einen Datenbankwartungsauftrag aus, bevor Sie Backups mit aktivierter SDR ausführen. Andernfalls verweigert der zentrale Administrationsserver Kommunikationsversuche der verwalteten Backup Exec-Servern.</p> <p>Siehe "Konfigurieren der Datenbankverwaltung und -sicherheit" auf Seite 694.</p>	<p>Standardmäßig wählt Backup Exec alle kritischen Systemkomponenten für Sie aus, wenn Sie einen Computer zum Sichern auswählen. Wenn alle kritischen Systemkomponenten in die Backup-Auftrag-Auswahl eingeschlossen werden, steht die Simplified Disaster Recovery-Anzeige in der Backup-Auswahl auf "Ein".</p> <p>Wenn Sie die Auswahl einer oder mehrerer kritischer Systemkomponentendateien aufheben, wechselt die Anzeige in "Aus". Es wird empfohlen, den gesamten Computer zum Sichern auswählen; da sonst Backup Exec die systemspezifische Notfallwiederherstellungs-Informationsdatei nicht erstellen kann.</p> <p>Dies sind die kritischen Systemkomponenten:</p> <ul style="list-style-type: none"> ■ Systemdatenträger (einschließlich EFI und Dienstprogrammpartitionen) ■ Startdatenträger (führt das Betriebssystem aus) ■ Dienst-Anwendungsdatenträger (Boot, System und automatischer Systemstart) ■ Systemstatusgeräte und -Datenträger (einschließlich Active Directory, Systemdateien, und so weiter) <p>Siehe "Sicherstellen, dass Simplified Disaster Recovery für Backups aktiviert ist" auf Seite 950.</p>

Schritt	Beschreibung	Weitere Informationen
Schritt 3	Erstellen Sie zusätzliche Kopien der Notfallwiederherstellungs-Informationsdateien und speichern Sie sie an einem sicheren Ort.	<p>Backup Exec speichert die wichtigen Notfallwiederherstellungs-Informationsdateien im Standardpfad, dem alternativen Speicherort und mit dem Backup-Satz, wenn Festplatten oder Plattenkassettengeräte als Zielspeicher verwendet werden. Es wird empfohlen, dass Sie zusätzliche Kopien der Dateien erstellen und sie an einem sicheren Ort speichern. Ohne die Notfallwiederherstellungs-Informationsdateien können Sie Backup Exec-Server mithilfe von Simplified Disaster Recovery (SDR) nicht wiederherstellen. Indem Sie mehrere Kopien der Notfallwiederherstellungs-Informationsdateien erstellen, stellen Sie sicher, dass Sie Backup Exec-Server mit SDR erfolgreich wiederherstellen können.</p> <p>Standardmäßig befinden sich die Notfallwiederherstellungs-Informationsdateien auf dem Backup Exec-Server im Ordner <i><Backup Exec-Installationsordner>\Backup Exec\SDR\Data</i>. Verwenden Sie Windows-Explorer oder ein anderes Programm, um die Notfallwiederherstellungs-Informationsdateien aus dem Standard- in einen anderen Speicherort Ihrer Wahl zu kopieren. Backup Exec aktualisiert diese Kopien nicht automatisch, aber Sie können einen Computer auf einen älteren Zeitpunkt wiederherstellen, wenn die anderen Notfallwiederherstellungsdateien nicht verfügbar sind.</p>

Schritt	Beschreibung	Weitere Informationen
Schritt 4	Verwenden Sie den Assistent zum Erstellen eines SDR-Datenträgers, um ein Image und daraus eine startfähige CD bzw. DVD zu erstellen.	<p>Backup Exec erzeugt Warnmeldungen nach jedem Backup-Auftrag, bis Sie das Simplified Disaster Recovery-Datenträger-Image erstellen. Sie können diese Warnmeldungen deaktivieren, sollten aber das SDR-Datenträger-Image erstellen.</p> <p>Siehe "Erstellen eines SDR-Datenträger-Image" auf Seite 957.</p> <p>Wenn Sie den Assistenten zum Erstellen eines SDR-Datenträgers auf einen eigenständigen Server installieren, können Sie ihn nicht verwenden, um Veritas Update auszuführen.</p>

Sicherstellen, dass Simplified Disaster Recovery für Backups aktiviert ist

Standardmäßig ist Backup Exec so konfiguriert, dass alle kritischen Systemkomponenten gesichert werden, die Sie benötigen, um zum Wiederherstellen eines Computers die Simplified Disaster Recovery zu verwenden.

Wenn die Simplified Disaster Recovery-Anzeige für die Backup-Auswahl grün ist bzw. auf "Ein" steht, sind die kritischen Systemkomponenten zum Sichern ausgewählt. Es handelt sich um ein SDR-Backup. Wenn die Anzeige grau ist oder auf "Aus" steht, ist SDR nicht aktiviert. Sie können auf das Symbol klicken, um alle notwendigen Komponenten für die Notfallwiederherstellung auszuwählen bzw. für die Backups zu deaktivieren, die von diesem Auftrag erstellt werden.

Um sicherzustellen, dass Simplified Disaster Recovery für ein Backup für aktiviert ist, können Sie die Backup-Auswahl anzeigen, die angezeigt wird, wenn Sie einen Backup-Auftrag erstellen oder bearbeiten.

So stellen Sie sicher, dass Simplified Disaster Recovery für Backups aktiviert ist

- 1 Erstellen Sie einen neuen Backup-Auftrag oder bearbeiten Sie einen vorhandenen auf der Registerkarte "Backup und Wiederherstellung".
- 2 Im Dialogfeld "Eigenschaften der Backup-Definition" im Teilfenster "Auswahl" haben Sie folgende Möglichkeiten:

Sicherstellen, dass Simplified Disaster Recovery für Backups aktiviert ist

- Stellen Sie sicher, dass das Symbol links neben dem Computernamen grün ist.
- Klicken Sie auf "Bearbeiten" und stellen Sie sicher, dass das Symbol auf der rechten Seite grün ist und dass der Text darauf hinweist, dass Simplified Disaster Recovery aktiviert ist.

Hinweis: Wenn Sie mit der Maus auf das Symbol zeigen, wird angezeigt, ob Simplified Disaster Recovery aktiviert ist.

- 3 Wenn das Symbol nicht grün ist oder gemeldet wird, dass Simplified Disaster Recovery deaktiviert ist, klicken Sie auf das Symbol und wählen Sie dann die Option "Alle notwendigen Komponenten für Notfallwiederherstellung auswählen".

Abbildung 21-1 Im Dialogfeld "Eigenschaften der Backup-Definition" ist die Simplified Disaster Recovery aktiviert.

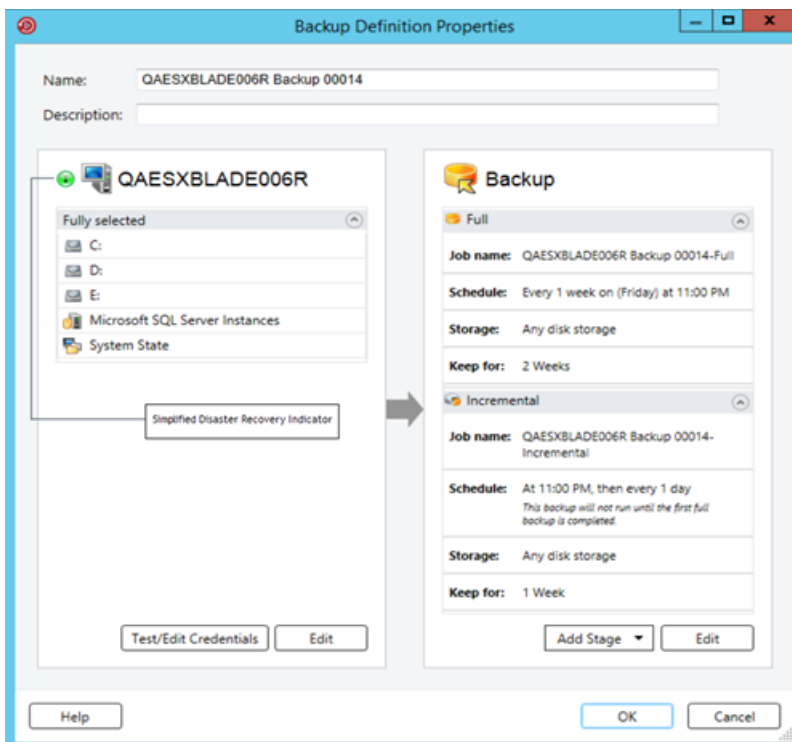
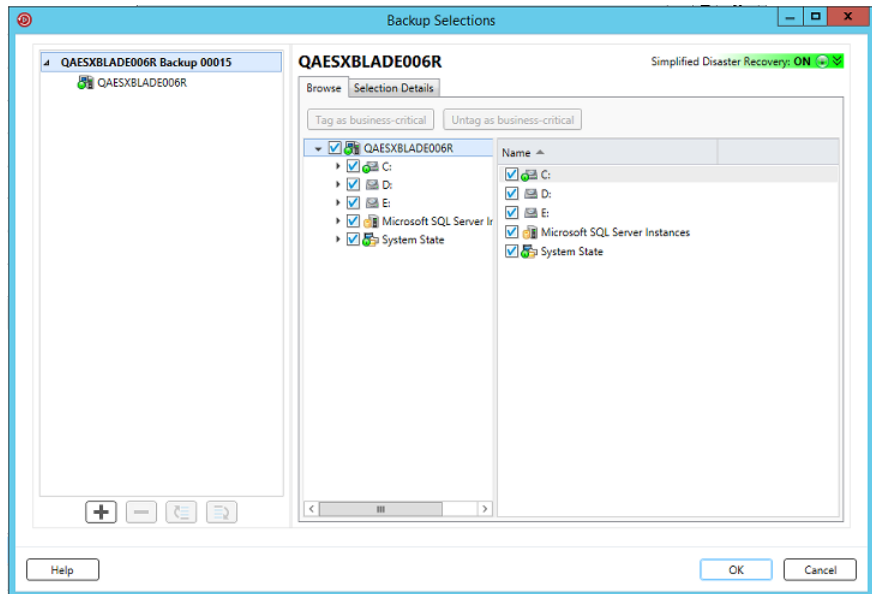


Abbildung 21-2 Im Dialogfeld "Backup-Auswahl" ist die Simplified Disaster Recovery aktiviert.



Siehe ["Vorbereiten von Computern für die Verwendung mit Simplified Disaster Recovery"](#) auf Seite 946.

Verwendung der Notfallwiederherstellungs-Informationsdateien durch Simplified Disaster Recovery

Für jeden Computer, den Sie sichern und für den die Simplified Disaster Recovery-Anzeige auf "EIN" eingestellt ist, erstellt Backup Exec eine Notfallwiederherstellungs-Informationsdatei. Eine Notfallwiederherstellungs-Informationsdatei enthält computerspezifische Informationen für den zu sichernden Computer. Jedes Mal, wenn ein Backup aller kritischen Systemkomponenten ausgeführt wird, werden die Notfallwiederherstellungs-Informationsdateien automatisch aktualisiert. Eine Notfallwiederherstellungs-Informationsdatei hat immer den Dateinamen <Computernamen>.DR. SDR verwendet die in der Datei enthaltenen computerspezifischen Informationen, wenn Sie den Assistenten "Computer wiederherstellen" ausführen. Ohne eine Notfallwiederherstellungs-Informationsdatei ist keine Wiederherstellung des Computers mit SDR möglich.

Hinweis: Backup Exec unterstützt standardmäßig die neuesten drei vollen SDR-Backup-Ketten, die für die Systemwiederherstellung mit SDR erforderlich sind. Jede Backup-Kette enthält einen vollständigen Backup-Satz, ihre abhängigen inkrementellen und differenziellen Backups und deren doppelten Backup-Sätze.

Eine Notfallwiederherstellungs-Informationsdatei enthält die folgenden Informationen für den zu sichernden Computer:

- Hardwarespezifische Informationen, z. B. Informationen zu den Festplattenpartitionen, zu Massenspeichercontrollern und zur Netzwerkkarte
- Eine Liste von Katalogeinträgen, die die Backup-Sätze und die Speichermedien identifizieren, die für die Wiederherstellung des Computers erforderlich sind
- Die Konfigurationsdatei für die automatische Systemwiederherstellung (asr.xml) ist zum Wiederherstellen erforderlich.

Backup Exec speichert dann die Notfallwiederherstellungs-Informationsdatei in den folgenden Speicherorten:

- Bei den Backup-Sätzen, wenn der Backup-Speicher ein Festplattenspeicher- oder Plattenkassettengerät ist.
- Auf der Festplatte des Backup Exec-Servers unter folgendem Pfad:

`C:<Backup Exec install path>\Backup Exec\sdr\Data\`

- In einem von Ihnen festgelegten alternativen Speicherort auf einem anderen Computer als der Backup Exec-Server.

Hinweis: Es wird empfohlen, einen Pfad zu dem alternativen Speicherort anzugeben. Wenn der Backup Exec-Server abstürzt, können Sie die Notfallwiederherstellungs-Informationsdatei nicht vom Standardspeicherort abrufen. Jedoch können Sie sie vom alternativen Speicherort abrufen. Sie sollten auch zusätzliche Kopien der Notfallwiederherstellungs-Informationsdateien erstellen und sie an einem sicheren Ort speichern. Verwenden Sie Windows-Explorer oder ein anderes Programm, um die Notfallwiederherstellungs-Informationsdateien aus dem Standard- in einen anderen Speicherort Ihrer Wahl zu kopieren. Backup Exec aktualisiert diese Kopien nicht automatisch, aber Sie können einen Computer auf einen älteren Zeitpunkt wiederherstellen, wenn die anderen Notfallwiederherstellungsdateien nicht verfügbar sind.

Wenn die Notfallwiederherstellungs-Informationsdatei bei den Backup-Sätzen gespeichert wird, verwendet SDR automatisch diese Datei für die Wiederherstellung. Wenn die Backup-Sätze auf einem Bandgerät, einem Deduplizierungsspeicher oder einem virtuellen Datenträger gesichert wurden, kann SDR die Datei nicht bei

den Backup-Sätzen speichern. Stattdessen müssen Sie den Pfad zum Standardspeicherort oder dem alternativen Speicherort der Notfallwiederherstellungsdatei angeben, wenn Sie vom Assistenten "Computer wiederherstellen" dazu aufgefordert werden.

Siehe ["Festlegen oder Ändern des alternativen Speicherorts für die Notfallwiederherstellungs-Informationsdatei"](#) auf Seite 954.

Siehe ["Ändern des Standardpfads für die Notfallwiederherstellungs-Informationsdateien"](#) auf Seite 955.

Festlegen oder Ändern des alternativen Speicherorts für die Notfallwiederherstellungs-Informationsdatei

Es wird empfohlen, dass Sie einen alternativen Ort für die Notfallwiederherstellungs-Informationsdateien angeben, die Backup Exec erstellt. Diese Dateien enthalten computerspezifische Informationen für jeden Computer, den Sie mit Simplified Disaster Recovery (SDR) schützen. Um einen Backup Exec-Server nach einem Systemausfall wiederherzustellen, benötigen Sie die Notfallwiederherstellungs-Informationsdatei des Backup Exec-Servers. Ohne sie kann SDR den Backup Exec-Server nicht wiederherstellen.

Es wird empfohlen, dass sich der alternative Ort im Gegensatz zum Standort auf einem anderen Computer oder einem anderen physischen Laufwerk befindet. Wenn die Festplatte des Backup Exec-Servers beschädigt ist, können Sie auf eine Kopie der Notfallwiederherstellungs-Informationsdatei an einem alternativen Speicherort zugreifen. Sie können einen Laufwerksbuchstaben angeben, der einer Netzwerkfreigabe als alternativem Ort zugeordnet ist.

Zur Verwendung der Festplatte eines Remote-Computers als alternativen Pfad benötigen Sie eine gültige Verbindung zum Remote-Computer. Geben Sie als alternativen Pfad einen UNC-Pfad an und überprüfen Sie anschließend, ob die Notfallwiederherstellungs-Informationsdateien kopiert wurden.

Für einen Backup Exec-Server oder Remote Backup Exec-Server in einem Cluster geben Sie einen alternativen Ort auf einem freigegebenen Laufwerk oder auf einem Laufwerk an, das sich außerhalb des Cluster befindet.

Sie sollten auch zusätzliche Kopien der Notfallwiederherstellungs-Informationsdateien erstellen und sie an einem sicheren Ort speichern.

Siehe ["Verwendung der Notfallwiederherstellungs-Informationsdateien durch Simplified Disaster Recovery"](#) auf Seite 952.

So legen Sie den alternativen Speicherort für die Notfallwiederherstellungs-Informationsdatei fest oder ändern ihn

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Backup Exec-Einstellungen".
- 2 Wählen Sie im linken Teilfenster die Option "Simplified Disaster Recovery".
- 3 Geben Sie im Feld "Alternativer Pfad" den alternativen Speicherort ein, an dem eine Kopie der Notfallwiederherstellungs-Informationsdatei gespeichert werden soll, oder klicken Sie auf Durchsuchen, um zum Speicherort zu navigieren.
- 4 Geben Sie das für den Zugriff auf das Deduplizierungsspeichergerät zu verwendende Login-Konto an.
- 5 Klicken Sie auf "OK".

Siehe ["Ändern des Standardpfads für die Notfallwiederherstellungs-Informationsdateien"](#) auf Seite 955.

Ändern des Standardpfads für die Notfallwiederherstellungs-Informationsdateien

Sie können den Standardpfad für die Notfallwiederherstellungs-Informationsdateien ändern. Es empfiehlt sich jedoch nicht, den Standardpfad zu ändern.

Kopien der Notfallwiederherstellungs-Informationsdateien sind notwendig, um die Wiederherstellung eines Backup Exec-Servers zu automatisieren.

Backup Exec erstellt während eines Backups automatisch die Notfallwiederherstellungs-Informationsdatei und speichert eine Kopie davon im folgenden Verzeichnis:

```
C:<Backup Exec install path>\Backup Exec\sdr\Data\
```

Wenn Sie den Pfad für die Notfallwiederherstellung ändern, müssen Sie die vorhandenen Informationsdateien in den neuen Pfad kopieren. Mit den Kopien können Sie einen Computer mit den vorherigen SDR-Backups wiederherstellen.

Siehe ["Verwendung der Notfallwiederherstellungs-Informationsdateien durch Simplified Disaster Recovery"](#) auf Seite 952.

So ändern Sie den Standardpfad für die Notfallwiederherstellungs-Informationsdateien

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Backup Exec-Einstellungen".
- 2 Wählen Sie im linken Teilfenster die Option "Simplified Disaster Recovery".

Festlegen oder Ändern des alternativen Speicherorts für die Notfallwiederherstellungs-Informationsdatei

- 3 Ändern Sie im Feld "Pfad" den Pfad zum Speicherort, an dem die Notfallwiederherstellungs-Informationsdateien gespeichert werden sollen, oder klicken Sie auf "Durchsuchen", um zu einem Speicherort zu navigieren.
- 4 Klicken Sie auf "OK".

Siehe ["Festlegen oder Ändern des alternativen Speicherorts für die Notfallwiederherstellungs-Informationsdatei"](#) auf Seite 954.

Pfad zur Notfallwiederherstellung-Informationsdatei

Simplified Disaster Recovery (SDR) erstellt Notfallwiederherstellung-Informationsdateien, die für die Wiederherstellung erforderlich sind.

Siehe ["Verwendung der Notfallwiederherstellungs-Informationsdateien durch Simplified Disaster Recovery"](#) auf Seite 952.

Tabelle 21-2 Speicherorte für die Notfallwiederherstellung-Informationsdatei

Element	Beschreibung
Pfad	<p>Gibt den Pfad zu den Notfallwiederherstellung-Informationsdateien für die zu sichernden Computer an. Backup Exec erstellt automatisch die Dateien, nachdem ein Backup-Auftrag ausgeführt wurde, für den alle kritischen Systemkomponenten ausgewählt wurden. Backup Exec legt dann die Notfallwiederherstellung-Informationensdateien im folgenden Speicherort ab:</p> <p><i>C:<Backup Exec-Installationsordner>\Backup Exec\sdr\Data\<Computername>.dr.</i></p> <p>Hinweis: Es wird empfohlen, den Standardpfad nicht zu ändern.</p>

Element	Beschreibung
Alternativer Pfad	<p>Gibt einen alternativen Pfad zum Ablegen von Kopien der Notfallwiederherstellung-Informationsdateien für die zu sichernden Computer an. Backup Exec erstellt bzw. aktualisiert automatisch die Dateien, nachdem ein Backup-Auftrag ausgeführt wurde, für den alle kritischen Systemkomponenten ausgewählt wurden. Backup Exec legt dann Kopien der Notfallwiederherstellung-Informationsdateien in diesem Speicherort ab.</p> <p>Es wird empfohlen, dass Sie einen alternativen Pfad angeben, der sich nicht auf dem Backup Exec-Server oder auf einem anderen physischen Laufwerk als der Standardspeicherort befindet. Sie können einen Laufwerksbuchstaben angeben, der mit einer Netzwerkfreigabe verbunden ist. Wenn die Festplatte des Backup Exec-Servers während einer Wiederherstellung nicht verfügbar ist, können Sie die Notfallwiederherstellung-Informationsdatei vom alternativen Pfad in einen beliebigen Speicherort kopieren, um den ausgefallenen Computer wiederherzustellen.</p> <p>Zur Verwendung der Festplatte eines Remote-Computers als alternativen Pfad benötigen Sie eine gültige Verbindung zum Remote-Computer. Geben Sie als alternativen Pfad einen UNC-Pfad an und überprüfen Sie anschließend, ob die Notfallwiederherstellungs-Informationsdateien kopiert wurden.</p>

Erstellen eines SDR-Datenträger-Image

Der Assistent zum Erstellen eines SDR-Datenträgers führt Sie durch den Prozess der Erstellung eines Startdatenträgers, mit dem Sie gesicherte Computer wiederherstellen.

Sie benötigen die folgenden Produkte zum Erstellen des SDR-Datenträger-Image:

- 5 GB Speicherplatz zum Herunterladen und Installieren des ADK.
- 1 GB Speicherplatz zum Speichern der erforderlichen Dateien und Ordner zum Erstellen des ISO-Image.

Warnung: Der ADK-Download dauert je nach Netzwerkgeschwindigkeit möglicherweise wenige Stunden.

Nach dem Ausführen von Simplified Disaster Recovery-aktivierten Backups auf den zu schützenden Computern, führen Sie zum Erstellen des Simplified Disaster Recovery-Datenträger-Image den Assistenten zum Erstellen eines SDR-Datenträgers aus. Simplified Disaster Recovery-aktivierte Backups sind jene Backups, bei denen im Teilfenster "Backup-Eigenschaften" ein grünes Symbol angezeigt wird, das die kritischen Systemkomponenten auf dem ausgewählten Computer kennzeichnet.

Siehe ["Sicherstellen, dass Simplified Disaster Recovery für Backups aktiviert ist"](#) auf Seite 950.

Unter Windows Server 2008 SP2 bis Windows Server 2016 installiert der Assistent das ADK. Unter Windows Server 2019 müssen Sie das ADK manuell herunterladen und installieren.

Der Assistent verwendet die erforderlichen Dateien und die Ordner aus dem ADK, um ein Wiederherstellungsdatenträger-Start-Image im Format "ISO" zu erstellen. Sie können das Image auf eine CD oder DVD brennen, indem Sie eine entsprechende Anwendung eines Drittanbieters verwenden. Für die Notfallwiederherstellung eines Computers verwenden Sie den Simplified Disaster Recovery-Datenträger, um den Computer zu starten und wiederherzustellen.

Während Sie den Wiederherstellungsdatenträger erstellen, können Sie Auswahlen für Sprache und Zeitzone hinzufügen. Sie können auch die Computer auswählen, für die Sie Netzwerk- und Speichertreiber hinzufügen möchten. Sie können weiterhin den Wiederherstellungsdatenträger anpassen, indem Sie neue OEM-Treiber hinzufügen.

Hinweis: Wenn Sie das Simplified Disaster Recovery-Datenträger-Image erstellen, bevor Sie Backups ausführen, sind die Treiber für die unterstützten Computer nicht auf dem Wiederherstellungsdatenträger enthalten. Sie müssen einen neuen Wiederherstellungsdatenträger erstellen, wenn Sie die Treiber der unterstützten Computer auf dem Wiederherstellungsdatenträger speichern möchten. Sie können dabei den vorhandenen Wiederherstellungsdatenträger als Quelle angeben. Dann wählen Sie die Computer aus, deren Treiber Sie dem Wiederherstellungsdatenträger hinzufügen möchten.

Abhängig von Ihrer Umgebung sind verschiedene Methoden für das Erstellen eines Simplified Disaster Recovery-Datenträger-Image verfügbar.

Tabelle 21-3 Methoden zum Erstellen eines SDR-Datenträger-Image

Umgebung	Methode
Wenn der Backup Exec-Server unter Windows Server 2019 ausgeführt wird	Siehe „Erstellen eines SDR-Datenträger-Image, wenn der Backup Exec-Server unter Windows Server 2019 ausgeführt wird“ auf Seite 959.
Wenn der Backup Exec-Server unter Windows Server 2008 R2 bis Windows Server 2016 ausgeführt wird	Siehe „Erstellen eines SDR-Datenträger-Image, wenn der Backup Exec-Server unter Windows Server 2008 R2 bis Windows Server 2016 ausgeführt wird“ auf Seite 963.
Wenn der Backup Exec-Server unter Windows Server 2008 SP2 ausgeführt wird	Siehe „Erstellen eines SDR-Datenträger-Image, wenn der Backup Exec-Server unter Windows Server 2008 SP2 ausgeführt wird“ auf Seite 966.
Der Backup Exec-Server nicht verfügbar ist	Siehe „Erstellen eines SDR-Datenträger-Image, wenn der Backup Exec-Server nicht verfügbar ist“ auf Seite 970.
Wenn der Backup Exec-Server, auf dem Sie das Simplified Disaster Recovery-Datenträger-Image erstellen möchten, keine Internetverbindung und kein ADK installiert hat	Siehe „Erstellen eines SDR-Datenträger-Image auf einem Backup Exec-Server, der keine Internetverbindung hat und auf dem ADK bzw. Windows Preinstallation Environment nicht installiert sind“ auf Seite 973.

Erstellen eines SDR-Datenträger-Image, wenn der Backup Exec-Server unter Windows Server 2019 ausgeführt wird

Ist das Windows ADK noch nicht auf dem Server installiert, müssen Sie Windows ADK 1809 manuell über den folgenden Link herunterladen und installieren:

<https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install?ocid=tia-235208000>

Es wird empfohlen, dass Sie Windows ADK 1809 herunterladen und installieren, bevor Sie den Assistenten zum Erstellen eines SDR-Datenträgers starten.

Wenn Windows ADK 1809 bereits installiert ist, erkennt der Assistent zum Erstellen eines SDR-Datenträgers das installierte ADK und erstellt den Datenträger.

So erstellen Sie ein Simplified Disaster Recovery-Datenträger-Image, wenn der Backup Exec-Server unter Windows Server 2019 ausgeführt wird

- 1 Sie haben folgende Möglichkeiten:
 - Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" unter "Wiederherstellungen" auf "SDR-Datenträger erstellen".
 - Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie auf "SDR-Datenträger erstellen".
 - Klicken Sie auf der Registerkarte "Startseite" im Bereich Simplified Disaster Recovery auf "SDR-Datenträger erstellen".
 - Klicken Sie auf die Schaltfläche "Start" und auf "SDR-Datenträger erstellen".
- 2 Überprüfen Sie den Bereich "Willkommen" des Assistenten zum Erstellen eines SDR-Datenträgers und klicken Sie auf "Weiter".

- 3 Sie haben folgende Möglichkeiten:

So erstellen Sie ein SDR-Datenträger-Image zum ersten Mal	Klicken Sie auf "Neues SDR-Datenträger-Image (.iso) erstellen".
---	---

So wählen Sie Netzwerk- und Speichertreiber von einer vorhandenen SDR-Datenträger-CD oder -DVD oder aus einem Ordner	Gehen Sie dazu wie folgt vor: <ul style="list-style-type: none"> ■ Klicken Sie auf "Von einer vorherigen CD oder DVD oder aus einem Ordner". ■ Geben Sie den Speicherort des vorherigen SDR-Datenträgers an oder den Pfad zu einem Ordner, der von einem Wiederherstellungsdatenträger extrahierte Dateien enthält.
--	---

So wählen Sie Netzwerk- und Speichertreiber aus einer vorhandenen Image-Datei (.iso)	Gehen Sie dazu wie folgt vor: <ul style="list-style-type: none"> ■ Klicken Sie auf "Aus einer Image-Datei (.iso)". ■ Geben Sie den Speicherort der Wiederherstellungs-Image-Datei ein.
--	--

- 4 Klicken Sie auf "Weiter".

5 Sie haben folgende Möglichkeiten:

Wenn ADK 1809 bereits auf dem Computer installiert ist	<p>Der Assistent zum Erstellen eines SDR-Datenträgers erkennt die installierte Version des ADK und setzt den Vorgang fort.</p> <p>Hinweis: Wenn Sie einen SDR-Datenträger mit ADK 10.0 erstellt haben, können Sie den Datenträger auch dann anpassen, wenn Windows ADK 1809 unter Windows Server 2019 installiert ist.</p>
Wenn Windows ADK 1809 bereits auf dem Computer installiert ist	<p>Der Assistent zum Erstellen eines SDR-Datenträgers zeigt folgenden Link zum Herunterladen und Installieren von Windows ADK 1809 an:</p> <p>https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install#id=1a235208000</p> <p>Installieren Sie die Komponenten "Windows ADK Insider " und "Windows Preinstallation Environment".</p> <p>Folgen Sie den Eingabeaufforderungen des Assistenten zum Installieren der Komponente Windows ADK Insider. Auf der Seite "Select the features you want to install" (Wählen Sie die zu installierenden Funktionen) aktivieren Sie nur das Kontrollkästchen "Deployment Tools" (Bereitstellungs-Tools).</p> <p>Nachdem das ADK installiert wurde, installieren Sie Windows Preinstallation Environment, indem Sie im Assistent die empfohlenen Standardwerte akzeptieren.</p> <p>Nachdem beide Komponenten installiert sind, starten Sie den Assistenten zum Erstellen von SDR-Datenträgern erneut.</p>
Wenn ADK 10.0 nicht auf dem Computer installiert ist	<p>Der Assistent zum Erstellen eines SDR-Datenträgers erkennt, dass ADK 10.0 installiert ist und zeigt die Seite zum Installieren des ADK an.</p> <p>Der Assistent meldet zwar, dass die neueste verfügbare Version des ADK nicht installiert ist, aber Sie können trotzdem das Erstellen des SDR-Datenträgers fortsetzen. Bestätigen Sie, dass Sie weiterhin ADK 10 nutzen möchten. Wenn Sie den Vorgang fortsetzen, werden eventuell nicht alle Funktionen von Windows Server 2019 unterstützt.</p> <p>Nachdem Sie das Kontrollkästchen aktiviert und auf "Weiter" geklickt haben, wird der Assistent zum Erstellen der SDR-Datenträgers fortgesetzt.</p>

6 Geben Sie die Startoptionen an, die beim Wiederherstellen des Computer verwendet werden sollen, und klicken Sie auf "Weiter".

7 Sie haben folgende Möglichkeiten:

So fügen Sie Netzwerk- und Speichertreiber für Computer hinzu, für die Sie SDR-Backups ausgeführt haben

Wählen Sie die Computer aus, deren Treiber Sie dem Wiederherstellungsdatenträger hinzufügen möchten, und klicken Sie auf "Weiter".

So fügen Sie erkannte Netzwerk- und Speichertreiber für Computer hinzu, für die Sie SDR-Backups ausgeführt haben, wenn die Treiber nicht im Quell-Image enthalten sind

Gehen Sie dazu wie folgt vor:

- Klicken Sie im Bereich "Computer für Verwendung der Treiber auswählen" auf "Weiter".
- Wählen Sie im Bereich "Einzuschließende Treiber" die Treiber aus, die auf dem benutzerdefinierten SDR-Datenträger enthalten sein sollen, und klicken Sie auf "Weiter".

So fügen Sie Netzwerktreiber und Speichertreiber aus OEM-Medien hinzu

Gehen Sie dazu wie folgt vor:

- Klicken Sie im Bereich "Computer für Verwendung der Treiber auswählen" auf "Weiter".
- Klicken Sie im Bereich "Einzuschließen Treiber" auf "Treiber hinzufügen", navigieren Sie zum Speicherort der Medien, wählen Sie ihn aus und klicken Sie auf "Öffnen".
- Wenn die Treiber im Bereich "Computer für Verwendung der Treiber auswählen" angezeigt werden, klicken Sie auf "Weiter".

- 8 Geben Sie die Datenträgerbezeichnung und den Pfad für das Image der Startdatei (.iso) ein und klicken Sie auf "Weiter".

Hinweis: Wenn Sie andere als englische Zeichen in der Datenträgerbezeichnung verwenden, werden diese Zeichen nicht richtig angezeigt, wenn Sie das ISO-Image bereitstellen.

Hinweis: Es wird empfohlen, dass Sie das zu brennende Image auf dem Computer speichern, auf dem die Anwendung zum Brennen des CD- oder DVD-Image installiert ist. Der standardmäßige Speicherort lautet: `C:\<Backup Exec-Installationsordner>\Backup Exec\sdr\CustomSDRImage.iso`

- 9 Lesen Sie die Übersicht und klicken Sie auf "Image erstellen".

- 10 Nachdem das SDR-CD- oder DVD-Image erstellt wurde, klicken Sie auf "Weiter" und auf "Fertigstellen".
- 11 Brennen Sie das ISO 9660-Image auf eine CD oder DVD, indem Sie eine entsprechende Anwendung eines Drittanbieters verwenden.

Erstellen eines SDR-Datenträger-Image, wenn der Backup Exec-Server unter Windows Server 2008 R2 bis Windows Server 2016 ausgeführt wird

Wenn Microsoft Assessment and Deployment Kit (ADK) nicht bereits auf diesem Server installiert ist, fordert Sie der Assistent zum Erstellen eines SDR-Datenträgers zum Herunterladen und Installieren des ADK auf. Die ADK-Installationsstandards sind bereits ausgewählt. Es wird empfohlen, dass Sie diese Standardeinstellungen verwenden.

Hinweis: Backup Exec unterstützt ADK 10 nur unter Windows Server 2008 R2 bis Windows Server 2016. Ist Windows ADK nicht installiert, lädt der Assistent zum Erstellen eines SDR-Datenträgers Windows ADK 10 herunter und installiert es.

So erstellen Sie ein Simplified Disaster Recovery-Datenträger-Image, wenn der Backup Exec-Server unter Windows Server 2008 R2 oder höher ausgeführt wird

- 1 Sie haben folgende Möglichkeiten:
 - Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" unter "Wiederherstellungen" auf "SDR-Datenträger erstellen".
 - Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie auf "SDR-Datenträger erstellen".
 - Klicken Sie auf der Registerkarte "Startseite" im Bereich Simplified Disaster Recovery auf "SDR-Datenträger erstellen".
 - Klicken Sie auf die Schaltfläche "Start" und auf "SDR-Datenträger erstellen".
- 2 Überprüfen Sie den Bereich "Willkommen" des Assistenten zum Erstellen eines SDR-Datenträgers und klicken Sie auf "Weiter".
- 3 Sie haben folgende Möglichkeiten:

So erstellen Sie ein	Klicken Sie auf "Neues
SDR-Datenträger-Image zum ersten Mal	SDR-Datenträger-Image (.iso) erstellen".

So wählen Sie Netzwerk- und Speichertreiber von einer vorhandenen SDR-Datenträger-CD oder -DVD oder aus einem Ordner

Gehen Sie dazu wie folgt vor:

- Klicken sie auf "Von einer vorherigen CD oder DVD oder aus einem Ordner".
- Geben Sie den Speicherort des vorherigen SDR-Datenträgers an oder den Pfad zu einem Ordner, der von einem Wiederherstellungsdatenträger extrahierte Dateien enthält.

So wählen Sie Netzwerk- und Speichertreiber aus einer vorhandenen Image-Datei (.iso)

Gehen Sie dazu wie folgt vor:

- Klicken Sie auf "Aus einer Image-Datei (.iso)".
- Geben Sie den Speicherort der Wiederherstellungs-Image-Datei ein.

4 Klicken Sie auf "Weiter".

5 Sie haben folgende Möglichkeiten:

Wenn das ADK bereits auf dem Computer installiert ist

Wenn bereits eine andere Windows ADK-Version als 10 installiert ist, erkennt der Assistent zum Erstellen eines SDR-Datenträgers die Version und informiert den Benutzer, dass kein neuer SDR-Datenträger mit der installierten ADK-Version erstellt werden kann.

Wenn ADK 10 installiert ist, meldet der Assistent zwar, dass es nicht die neueste verfügbare Version des ADK ist, aber Sie können trotzdem das Erstellen des SDR-Datenträgers fortsetzen. Bestätigen Sie, dass Sie weiterhin ADK 10 nutzen möchten.

Nachdem Sie das Kontrollkästchen aktiviert und auf "Weiter" geklickt haben, wird der Assistent zum Erstellen der SDR-Datenträgers fortgesetzt.

Fahren Sie mit Schritt **6** fort.

Wenn das ADK nicht auf dem Computer installiert ist

Ist Windows ADK nicht installiert, lädt der Assistent zum Erstellen eines SDR-Datenträgers Windows ADK 10 herunter und installiert es.

Gehen Sie dazu wie folgt vor:

- Klicken Sie auf "Weiter", um mit dem Assistenten für ADK-Download und Installation fortzusetzen.
- Klicken Sie in den Bereichen des ADK-Assistenten auf "Weiter", um die empfohlenen Standards zu akzeptieren.

Hinweis: Der ADK-Download dauert je nach Bandbreite möglicherweise wenige Stunden.

- Nachdem das ADK installiert wurde, klicken Sie auf "Schließen", um mit dem Assistenten zum Erstellen eines SDR-Datenträgers fortzufahren.

6 Geben Sie die Startoptionen an, die beim Wiederherstellen des Computer verwendet werden sollen, und klicken Sie auf "Weiter".

7 Sie haben folgende Möglichkeiten:

So fügen Sie Netzwerk- und Speichertreiber für Computer hinzu, für die Sie SDR-Backups ausgeführt haben

Wählen Sie die Computer aus, deren Treiber Sie dem Wiederherstellungsdatenträger hinzufügen möchten, und klicken Sie auf "Weiter".

So fügen Sie erkannte Netzwerk- und Speichertreiber für Computer hinzu, für die Sie SDR-Backups ausgeführt haben, wenn die Treiber nicht im Quell-Image enthalten sind

Gehen Sie dazu wie folgt vor:

- Klicken Sie im Bereich "Computer für Verwendung der Treiber auswählen" auf "Weiter".
- Wählen Sie im Bereich "Einzuschließende Treiber" die Treiber aus, die auf dem benutzerdefinierten SDR-Datenträger enthalten sein sollen, und klicken Sie auf "Weiter".

So fügen Sie Netzwerktreiber und Speichertreiber aus OEM-Medien hinzu

Gehen Sie dazu wie folgt vor:

- Klicken Sie im Bereich "Computer für Verwendung der Treiber auswählen" auf "Weiter".
- Klicken Sie im Bereich "Einzuschließen Treiber" auf "Treiber hinzufügen", navigieren Sie zum Speicherort der Medien, wählen Sie ihn aus und klicken Sie auf "Öffnen".
- Wenn die Treiber im Bereich "Computer für Verwendung der Treiber auswählen" angezeigt werden, klicken Sie auf "Weiter".

- 8 Geben Sie die Datenträgerbezeichnung und den Pfad für das Image der Startdatei (.iso) ein und klicken Sie auf "Weiter".

Hinweis: Wenn Sie andere als englische Zeichen in der Datenträgerbezeichnung verwenden, werden diese Zeichen nicht richtig angezeigt, wenn Sie das ISO-Image bereitstellen.

Hinweis: Es wird empfohlen, dass Sie das zu brennende Image auf dem Computer speichern, auf dem die Anwendung zum Brennen des CD- oder DVD-Image installiert ist. Der standardmäßige Speicherort lautet: `C:\<Backup Exec-Installationsordner>\Backup Exec\sdr\CustomSDRImage.iso`

- 9 Lesen Sie die Übersicht und klicken Sie auf "Image erstellen".
- 10 Nachdem das SDR-CD- oder DVD-Image erstellt wurde, klicken Sie auf "Weiter" und auf "Fertigstellen".
- 11 Brennen Sie das ISO 9660-Image auf eine CD oder DVD, indem Sie eine entsprechende Anwendung eines Drittanbieters verwenden.

Erstellen eines SDR-Datenträger-Image, wenn der Backup Exec-Server unter Windows Server 2008 SP2 ausgeführt wird

Wenn Microsoft Assessment and Deployment Kit (ADK) nicht bereits auf diesem Server installiert ist, fordert Sie der Assistent zum Erstellen eines SDR-Datenträgers zum Herunterladen und Installieren des ADK auf. Die ADK-Installationsstandards sind bereits ausgewählt. Es wird empfohlen, dass Sie diese Standardeinstellungen verwenden.

Hinweis: Backup Exec unterstützt Windows ADK 8.1 unter Windows 2008 SP2. Ist Windows ADK nicht unter Windows Server 2008 SP2 installiert, lädt der Assistent zum Erstellen eines SDR-Datenträgers Windows ADK 8.1 herunter und installiert es.

So erstellen Sie ein Simplified Disaster Recovery-Datenträger-Image, wenn der Backup Exec-Server unter Windows Server 2008 SP2 ausgeführt wird

- 1 Sie haben folgende Möglichkeiten:
 - Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" unter "Wiederherstellungen" auf "SDR-Datenträger erstellen".
 - Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie auf "SDR-Datenträger erstellen".
 - Klicken Sie auf der Registerkarte "Startseite" im Bereich Simplified Disaster Recovery auf "SDR-Datenträger erstellen".
 - Klicken Sie auf die Schaltfläche "Start" und auf "SDR-Datenträger erstellen".
- 2 Überprüfen Sie den Bereich "Willkommen" des Assistenten zum Erstellen eines SDR-Datenträgers und klicken Sie auf "Weiter".
- 3 Sie haben folgende Möglichkeiten:

So erstellen Sie ein SDR-Datenträger-Image zum ersten Mal

Klicken Sie auf "Neues SDR-Datenträger-Image (.iso) erstellen".

So wählen Sie Netzwerk- und Speichertreiber von einer vorhandenen SDR-Datenträger-CD oder -DVD oder aus einem Ordner

Gehen Sie dazu wie folgt vor:

- Klicken Sie auf "Von einer vorherigen CD oder DVD oder aus einem Ordner".
- Geben Sie den Speicherort des vorherigen SDR-Datenträgers an oder den Pfad zu einem Ordner, der von einem Wiederherstellungsdatenträger extrahierte Dateien enthält.

So wählen Sie Netzwerk- und Speichertreiber aus einer vorhandenen Image-Datei (.iso)

Gehen Sie dazu wie folgt vor:

- Klicken Sie auf "Aus einer Image-Datei (.iso)".
- Geben Sie den Speicherort der Wiederherstellungs-Image-Datei ein.

- 4 Klicken Sie auf "Weiter".
- 5 Sie haben folgende Möglichkeiten:

Wenn das ADK bereits auf dem Computer installiert ist

Wenn Windows ADK 8.0 bereits installiert ist, meldet der Assistent für den Wiederherstellungsdatenträger, dass mit dieser ADK-Version keine neue SDR-Version erstellt werden kann. Der Wiederherstellungsdatenträger kann jedoch angepasst werden. Der Benutzer kann den Assistenten beenden oder ADK 8.1 herunterladen und den Datenträger anpassen.

Ist Windows ADK 8.1 bereits installiert, warnt der Assistent zuerst den Benutzer über die Version von Windows ADK. Will der Benutzer den Vorgang fortsetzen, setzt der Assistent das Erstellen des SDR-Datenträgers fort.

Fahren Sie mit Schritt 6 fort.

Wenn das ADK nicht auf dem Computer installiert ist

Ist Windows ADK nicht installiert, lädt der Assistent zum Erstellen eines SDR-Datenträgers Windows ADK 8.1 herunter und installiert es.

Gehen Sie dazu wie folgt vor:

- Klicken Sie auf "Weiter", um mit dem Assistenten für ADK-Download und Installation fortzusetzen.
- Klicken Sie in den Bereichen des ADK-Assistenten auf "Weiter", um die empfohlenen Standards zu akzeptieren.

Hinweis: Der ADK-Download dauert je nach Bandbreite möglicherweise wenige Stunden.

- Nachdem das ADK installiert wurde, klicken Sie auf "Schließen", um mit dem Assistenten zum Erstellen eines SDR-Datenträgers fortzufahren.

- 6 Geben Sie die Startoptionen an, die beim Wiederherstellen des Computer verwendet werden sollen, und klicken Sie auf "Weiter".
- 7 Sie haben folgende Möglichkeiten:

So fügen Sie Netzwerk- und Speichertreiber für Computer hinzu, für die Sie SDR-Backups ausgeführt haben

Wählen Sie die Computer aus, deren Treiber Sie dem Wiederherstellungsdatenträger hinzufügen möchten, und klicken Sie auf "Weiter".

So fügen Sie erkannte Netzwerk- und Speichertreiber für Computer hinzu, für die Sie SDR-Backups ausgeführt haben, wenn die Treiber nicht im Quell-Image enthalten sind

Gehen Sie dazu wie folgt vor:

- Klicken Sie im Bereich "Computer für Verwendung der Treiber auswählen" auf "Weiter".
- Wählen Sie im Bereich "Einzuschließende Treiber" die Treiber aus, die auf dem benutzerdefinierten SDR-Datenträger enthalten sein sollen, und klicken Sie auf "Weiter".

So fügen Sie Netzwerktreiber und Speichertreiber aus OEM-Medien hinzu

Gehen Sie dazu wie folgt vor:

- Klicken Sie im Bereich "Computer für Verwendung der Treiber auswählen" auf "Weiter".
- Klicken Sie im Bereich "Einzuschließen Treiber" auf "Treiber hinzufügen", navigieren Sie zum Speicherort der Medien, wählen Sie ihn aus und klicken Sie auf "Öffnen".
- Wenn die Treiber im Bereich "Computer für Verwendung der Treiber auswählen" angezeigt werden, klicken Sie auf "Weiter".

- 8** Geben Sie die Datenträgerbezeichnung und den Pfad für das Image der Startdatei (.iso) ein und klicken Sie auf "Weiter".

Hinweis: Wenn Sie andere als englische Zeichen in der Datenträgerbezeichnung verwenden, werden diese Zeichen nicht richtig angezeigt, wenn Sie das ISO-Image bereitstellen.

Hinweis: Es wird empfohlen, dass Sie das zu brennende Image auf dem Computer speichern, auf dem die Anwendung zum Brennen des CD- oder DVD-Image installiert ist. Der standardmäßige Speicherort lautet:

```
C:<Backup_Exec-Installationsordner>\Backup  
Exec\sdr\CustomSDRImage.iso
```

- 9 Lesen Sie die Übersicht und klicken Sie auf "Image erstellen".
- 10 Nachdem das SDR-CD- oder DVD-Image erstellt wurde, klicken Sie auf "Weiter" und auf "Fertigstellen".
- 11 Brennen Sie das ISO 9660-Image auf eine CD oder DVD, indem Sie eine entsprechende Anwendung eines Drittanbieters verwenden.

Erstellen eines SDR-Datenträger-Image, wenn der Backup Exec-Server nicht verfügbar ist

Microsoft Windows Assessment and Deployment Kit (ADK) kann nur unter Windows Server 2008 SP2 und höher installiert werden. Wenn der Backup Exec-Server nicht unter Windows Server 2008 SP2 oder höher ausgeführt wird oder nicht verfügbar ist, können Sie die Backup Exec-Installationsdatenträger verwenden, um den Assistenten zum Erstellen eines SDR-Datenträgers und die Remote-Administratorkonsole auf einem eigenständigen Server zu installieren, auf dem Windows Server 2008 SP2 oder höher ausgeführt wird.

Der Assistent zum Erstellen eines SDR-Datenträgers führt Sie durch den Download und die Installation des ADK. Die ADK-Installationsstandards sind bereits ausgewählt. Es wird empfohlen, dass Sie diese Standardeinstellungen verwenden. Sie können den Wiederherstellungsdatenträger erstellen, indem Sie gemäß Anleitung durch den Assistenten eine Verbindung zu einem Remote-Backup Exec-Server herstellen.

So erstellen Sie ein SDR-Datenträger-Image, wenn der Backup Exec-Server nicht verfügbar ist

- 1 Legen Sie den Backup Exec-Installationsdatenträger auf einem Server ein, auf dem Windows Server 2008 SP2 oder höher ausgeführt wird.
- 2 Klicken Sie im Installationsmedien-Browser auf "Installation".
- 3 Klicken Sie auf den Assistenten zum Erstellen eines SDR-Datenträgers und auf "Weiter".

Hinweis: Der Assistent zum Erstellen eines SDR-Datenträgers und die Backup Exec-Remote-Administratorkonsole werden installiert.

- 4 Akzeptieren Sie die Bedingungen der Lizenzvereinbarung und klicken Sie auf "Weiter".
- 5 Akzeptieren Sie den Standard-Installationsort oder geben Sie einen neuen Speicherort an, und klicken Sie auf "Weiter".

- 6 Standardmäßig wird der Assistent zum Erstellen eines SDR-Datenträgers gestartet, nachdem der Computer neu gestartet wurde. Falls Sie diese Standardeinstellung deaktiviert haben, klicken Sie zum Starten des Assistenten auf "Start > Programme > Veritas Backup Exec > SDR-Datenträger erstellen".
- 7 Klicken Sie im Bereich "Willkommen" des Assistenten zum Erstellen eines SDR-Datenträgers auf "Verbindung zu einem Backup Exec-Server herstellen".
- 8 Geben Sie Name oder IP-Adresse des Backup Exec-Servers, Ihre Identifikationsdaten und die Domäne ein und klicken Sie auf "Weiter".
- 9 Sie haben folgende Möglichkeiten:

So erstellen Sie ein SDR-Datenträger-Image zum ersten Mal

Klicken Sie auf "Neues SDR-Datenträger-Image (.iso) erstellen".

So wählen Sie Netzwerk- und Speichertreiber von einer vorhandenen SDR-Datenträger-CD oder -DVD oder aus einem Ordner

Gehen Sie dazu wie folgt vor:

- Klicken Sie auf "Von einer vorherigen CD oder DVD oder aus einem Ordner".
- Geben Sie den Speicherort des vorherigen SDR-Datenträgers an oder den Pfad zu einem Ordner, der von einem Wiederherstellungsdatenträger extrahierte Dateien enthält.

So wählen Sie Netzwerk- und Speichertreiber aus einer vorhandenen Image-Datei (.iso)

Gehen Sie dazu wie folgt vor:

- Klicken Sie auf "Aus einer Image-Datei (.iso)".
- Geben Sie den Speicherort der Wiederherstellungs-Image-Datei ein.

- 10 Klicken Sie auf "Weiter".
- 11 Sie haben folgende Möglichkeiten:

Wenn das ADK bereits auf diesem Computer installiert ist

Fahren Sie mit Schritt [12](#) fort.

Wenn das ADK nicht auf diesem Computer installiert ist Gehen Sie dazu wie folgt vor:

- Klicken Sie auf "Weiter", um mit dem Assistenten für ADK-Download und Installation fortzusetzen.
- Klicken Sie in den Bereichen des ADK-Assistenten auf "Weiter", um die empfohlenen Standards zu akzeptieren.

Hinweis: Der ADK-Download dauert je nach Netzwerkgeschwindigkeit möglicherweise wenige Stunden.

- Nachdem das ADK installiert wurde, klicken Sie auf "Schließen", um mit dem Assistenten zum Erstellen eines SDR-Datenträgers fortzufahren.

12 Geben Sie die Startoptionen an, die beim Wiederherstellen des Computer verwendet werden sollen, und klicken Sie auf "Weiter".

13 Sie haben folgende Möglichkeiten:

So fügen Sie Netzwerk- und Speichertreiber für Computer hinzu, für die Sie SDR-Backups ausgeführt haben

Wählen Sie die Computer aus, deren Treiber Sie dem Wiederherstellungsdatenträger hinzufügen möchten, und klicken Sie auf "Weiter".

So fügen Sie erkannte Netzwerk- und Speichertreiber für Computer hinzu, für die Sie SDR-Backups ausgeführt haben, wenn die Treiber nicht im Quell-Image enthalten sind

Gehen Sie dazu wie folgt vor:

- Klicken Sie im Bereich "Computer für Verwendung der Treiber auswählen" auf "Weiter".
- Wählen Sie im Bereich "Einzuschließende Treiber" die Treiber aus, die auf dem benutzerdefinierten SDR-Datenträger enthalten sein sollen, und klicken Sie auf "Weiter".

So fügen Sie Netzwerktreiber und Speichertreiber aus OEM-Medien hinzu

Gehen Sie dazu wie folgt vor:

- Klicken Sie im Bereich "Computer für Verwendung der Treiber auswählen" auf "Weiter".
- Klicken Sie im Bereich "Einzuschließen Treiber" auf "Treiber hinzufügen", navigieren Sie zum Speicherort der Medien, wählen Sie ihn aus und klicken Sie auf "Öffnen".
- Wenn die Treiber im Bereich "Computer für Verwendung der Treiber auswählen" angezeigt werden, klicken Sie auf "Weiter".

So fügen Sie der Liste einen Computer hinzu

Gehen Sie dazu wie folgt vor:

- Klicken Sie auf "DR-Datei hinzufügen".
- Navigieren Sie zum Speicherort der DR-Datei, wählen Sie sie aus und klicken Sie auf "OK".
- Wählen Sie im Bereich "Computer für Verwendung der Treiber auswählen" den Computer aus, den Sie hinzufügen möchten, und klicken Sie auf "Weiter".

- 14** Geben Sie die Datenträgerbezeichnung und den Pfad für das Image der Startdatei (.iso) ein und klicken Sie auf "Weiter".

Hinweis: Es wird empfohlen, dass Sie das zu brennende Image auf dem Computer speichern, auf dem die Anwendung zum Brennen des CD- oder DVD-Image installiert ist. Der standardmäßige Speicherort lautet:

```
C:<Backup Exec-Installationsordner>\Backup  
Exec\sdr\CustomSDRImage.iso
```

- 15** Lesen Sie die Übersicht und klicken Sie auf "Image erstellen".
- 16** Nachdem das SDR-CD- oder DVD-Image erstellt wurde, klicken Sie auf "Weiter" und auf "Fertigstellen".
- 17** Brennen Sie das ISO 9660-Image auf eine CD oder DVD, indem Sie eine entsprechende Anwendung eines Drittanbieters verwenden.

Erstellen eines SDR-Datenträger-Image auf einem Backup Exec-Server, der keine Internetverbindung hat und auf

dem ADK bzw. Windows Preinstallation Environment nicht installiert sind

Für Windows ADK 10 und 8.1 können Sie die ausführbare Datei auf einem Computer mit Internetzugang herunterladen und dann auf den Computer kopieren, auf dem ADK installiert werden soll. Dann können Sie den Assistenten zum Erstellen eines SDR-Datenträgers verwenden, um den Wiederherstellungsdatenträger zu erstellen.

Für Windows ADK 1809 und Windows Preinstallation Environment können Sie die Dateien auf einem Computer mit Internetzugang herunterladen und dann auf den Computer kopieren, auf dem sie installiert werden sollen. Dann können Sie den Assistenten zum Erstellen eines SDR-Datenträgers verwenden, um den Wiederherstellungsdatenträger zu erstellen.

Erstellen eines SDR-Datenträger-Image auf einem Backup Exec-Server mit Windows Server 2019, der keine Internetverbindung hat und auf dem ADK 1809 und Windows Preinstallation Environment nicht installiert sind

- 1 Laden Sie für einen Computer, der eine Internetverbindung hat, manuell Windows ADK 1809 herunter und installieren es. Verwenden Sie dazu den folgenden Link:
<https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install?ocid=fa-235208000>
- 2 Nachdem der Download abgeschlossen ist, vergewissern Sie sich, dass die adksetup.exe-Datei und der Installationsprogrammordner auf den Computer heruntergeladen wurden.
- 3 Kopieren Sie die heruntergeladenen Dateien und den Ordner auf dem Computer, auf dem Sie ADK installieren möchten.
- 4 Starten Sie "adksetup.exe" im kopierten Ordner.
- 5 Klicken Sie im ADK-Bereich "Speicherort angeben" auf "Assessment and Deployment Kit zur Installation auf einem separaten Computer herunterladen", geben Sie den Pfad zum Backup Exec-Server ein, auf dem Sie ADK installieren möchten, und klicken auf "Weiter".
- 6 Klicken Sie auf "Akzeptieren", um die Bedingungen der Lizenzvereinbarung zu akzeptieren.
- 7 Klicken Sie im ADK im Bereich "Select the features you want to install" (Zu installierende Funktionen auswählen) auf "Deployment Tools" (Bereitstellungs-Tools) und dann auf "Install".
Schließen Sie die Installation von ADK ab.
- 8 Vergewissern Sie sich, dass die adksetup.exe-Datei und der Installationsprogrammordner auf den Computer heruntergeladen wurden.

- 9 Kopieren Sie die heruntergeladenen Dateien und den Ordner auf dem Computer, auf dem WinPE installiert werden soll.
- 10 Starten Sie "adkwinpesetup.exe" im kopierten Ordner.
- 11 Klicken Sie im ADK im Bereich "Specify Location" (Speicherort angeben) auf "Install the Assessment and Deployment Kit Windows Preinstallation Environment Add-ons to this computer" (Add-Ons für ADK und WinPE auf diesem Computer installieren), geben Sie den Pfad, in dem Sie die Komponenten installieren möchten, und klicken Sie auf "Weiter".
- 12 Klicken Sie auf "Akzeptieren", um die Bedingungen der Lizenzvereinbarung zu akzeptieren.
- 13 Klicken Sie im ADK im Bereich "Select the features you want to install" (Zu installierende Funktionen auswählen) auf "Windows Preinstallation Environment (WinPE)" und dann auf "Install".
- 14 Nachdem die Installation auf dem Backup Exec-Server abgeschlossen ist, führen Sie beliebige folgende Vorgänge aus:
 - Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" unter "Wiederherstellungen" auf "SDR-Datenträger erstellen".
 - Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie auf "SDR-Datenträger erstellen".
 - Klicken Sie auf der Registerkarte "Startseite" im Bereich Simplified Disaster Recovery auf "SDR-Datenträger erstellen".
 - Klicken Sie auf die Schaltfläche "Start" und auf "SDR-Datenträger erstellen".
- 15 Überprüfen Sie den Bereich "Willkommen" des Assistenten zum Erstellen eines SDR-Datenträgers und klicken Sie auf "Weiter".
- 16 Sie haben folgende Möglichkeiten:

So erstellen Sie ein SDR-Datenträger-Image zum ersten Mal

Klicken Sie auf "Neues SDR-Datenträger-Image (.iso) erstellen".

So wählen Sie Netzwerk- und Speichertreiber von einer vorhandenen SDR-Datenträger-CD oder -DVD oder aus einem Ordner

Gehen Sie dazu wie folgt vor:

- Klicken Sie auf "Von einer vorherigen CD oder DVD oder aus einem Ordner".
- Geben Sie den Speicherort des vorherigen SDR-Datenträgers an oder den Pfad zu einem Ordner, der von einem Wiederherstellungsdatenträger extrahierte Dateien enthält.

So wählen Sie Netzwerk- und Speichertreiber aus einer vorhandenen Image-Datei (.iso)

Gehen Sie dazu wie folgt vor:

- Klicken Sie auf "Aus einer Image-Datei (.iso)".
- Geben Sie den Speicherort der Wiederherstellungs-Image-Datei ein.

17 Klicken Sie auf "Weiter".

18 Geben Sie die Startoptionen an, die beim Wiederherstellen des Computer verwendet werden sollen, und klicken Sie auf "Weiter".

19 Sie haben folgende Möglichkeiten:

So fügen Sie Netzwerk- und Speichertreiber für Computer hinzu, für die Sie SDR-Backups ausgeführt haben

Wählen Sie die Computer aus, deren Treiber Sie dem Wiederherstellungsdatenträger hinzufügen möchten, und klicken Sie auf "Weiter".

So fügen Sie erkannte Netzwerk- und Speichertreiber für Computer hinzu, für die Sie SDR-Backups ausgeführt haben, wenn die Treiber nicht im Quell-Image enthalten sind

Gehen Sie dazu wie folgt vor:

- Klicken Sie im Bereich "Computer für Verwendung der Treiber auswählen" auf "Weiter".
- Wählen Sie im Bereich "Einzuschließende Treiber" die Treiber aus, die auf dem benutzerdefinierten SDR-Datenträger enthalten sein sollen, und klicken Sie auf "Weiter".

So fügen Sie Netzwerktreiber und Speichertreiber aus OEM-Medien hinzu

Gehen Sie dazu wie folgt vor:

- Klicken Sie im Bereich "Computer für Verwendung der Treiber auswählen" auf "Weiter".
- Klicken Sie im Bereich "Einzuschließen Treiber" auf "Treiber hinzufügen", navigieren Sie zum Speicherort der Medien, wählen Sie ihn aus und klicken Sie auf "Öffnen".
- Wenn die Treiber in dem Bereich angezeigt werden, klicken Sie auf "Weiter".

- 20 Geben Sie die Datenträgerbezeichnung und den Pfad für das Image der Startdatei (.iso) ein und klicken Sie auf "Weiter".

Hinweis: Es wird empfohlen, dass Sie das zu brennende Image auf dem Computer speichern, auf dem die Anwendung zum Brennen des CD- oder DVD-Image installiert ist. Der standardmäßige Speicherort lautet: `C:\<Backup Exec-Installationsordner>\Backup Exec\sdr\CustomSDRImage.iso`.

- 21 Lesen Sie die Übersicht und klicken Sie auf "Image erstellen".
- 22 Nachdem das SDR-CD- oder DVD-Image erstellt wurde, klicken Sie auf "Weiter" und auf "Fertigstellen".
- 23 Brennen Sie das ISO 9660-Image auf eine CD oder DVD, indem Sie eine entsprechende Anwendung eines Drittanbieters verwenden.

So erstellen Sie ein SDR-Datenträger-Image auf einem Backup Exec-Server, der keine Internetverbindung hat und auf dem ADK 10 oder ADK 8.1 nicht installiert sind

- 1 Auf einem Computer, der eine Internetverbindung hat, klicken Sie auf den folgenden Link, um die Datei "adksetup.exe" herunterzuladen:
- Windows ADK 10: <https://go.microsoft.com/fwlink/p/?LinkId=526740> (ADK 10.1.14393.0)
- Windows ADK 8.1: <http://go.microsoft.com/fwlink/?LinkId=293840> (ADK 8.100.26866.0)
- 2 Führen Sie "adksetup.exe" aus
- 3 Klicken Sie im ADK-Bereich "Speicherort angeben" auf "Assessment and Deployment Kit zur Installation auf einem separaten Computer herunterladen", geben Sie den Pfad zum Backup Exec-Server ein, auf dem Sie die ADK-Komponenten installieren möchten, und klicken auf "Weiter".
- 4 Klicken Sie auf "Ja" bzw. "Nein", um dem Microsoft-Programm zur Verbesserung der Benutzerfreundlichkeit (nicht) beizutreten, und klicken Sie auf "Weiter".
- 5 Klicken Sie auf "Akzeptieren", um die Bedingungen der Lizenzvereinbarung zu akzeptieren und ADK herunterzuladen.
- 6 Nachdem der Download abgeschlossen ist, vergewissern Sie sich, dass die adksetup.exe-Datei und der Installationsprogrammordner auf den Computer heruntergeladen wurden.

- 7 Kopieren Sie die heruntergeladenen Dateien und den Ordner auf dem Computer, auf dem Sie ADK installieren möchten.

Hinweis: ADK kann nur unter Windows Server 2008 SP2 und höher installiert werden.

- 8 Starten Sie "adksetup.exe" im kopierten Ordner.
- 9 Klicken Sie im ADK-Bereich "Speicherort angeben" auf "Assessment and Deployment Kit zur Installation auf einem separaten Computer herunterladen", geben Sie den Pfad zum Backup Exec-Server ein, auf dem Sie ADK installieren möchten, und klicken auf "Weiter".
- 10 Klicken Sie auf "Akzeptieren", um die Bedingungen der Lizenzvereinbarung zu akzeptieren.
- 11 Klicken Sie im ADK im Bereich "Select the features you want to install" (Zu installierende Funktionen auswählen) auf "Deployment Tools" (Bereitstellungs-Tools) und "Windows Preinstallation Environment (WinPE)" und dann auf "Install".
- 12 Nachdem die Installation auf dem Backup Exec-Server abgeschlossen ist, führen Sie auf diesem Server wahlweise folgende Vorgänge aus:
 - Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" unter "Wiederherstellungen" auf "SDR-Datenträger erstellen".
 - Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie auf "SDR-Datenträger erstellen".
 - Klicken Sie auf der Registerkarte "Startseite" im Bereich Simplified Disaster Recovery auf "SDR-Datenträger erstellen".
 - Klicken Sie auf die Schaltfläche "Start" und auf "SDR-Datenträger erstellen".
- 13 Überprüfen Sie den Bereich "Willkommen" des Assistenten zum Erstellen eines SDR-Datenträgers und klicken Sie auf "Weiter".
- 14 Sie haben folgende Möglichkeiten:

So erstellen Sie ein	Klicken Sie auf "Neues
SDR-Datenträger-Image zum ersten Mal	SDR-Datenträger-Image (.iso) erstellen".

So wählen Sie Netzwerk- und Speichertreiber von einer vorhandenen SDR-Datenträger-CD oder -DVD oder aus einem Ordner

Gehen Sie dazu wie folgt vor:

- Klicken Sie auf "Von einer vorherigen CD oder DVD oder aus einem Ordner".
- Geben Sie den Speicherort des vorherigen SDR-Datenträgers an oder den Pfad zu einem Ordner, der von einem Wiederherstellungsdatenträger extrahierte Dateien enthält.

So wählen Sie Netzwerk- und Speichertreiber aus einer vorhandenen Image-Datei (.iso)

Gehen Sie dazu wie folgt vor:

- Klicken Sie auf "Aus einer Image-Datei (.iso)".
- Geben Sie den Speicherort der Wiederherstellungs-Image-Datei ein.

15 Klicken Sie auf "Weiter".

16 Geben Sie die Startoptionen an, die beim Wiederherstellen des Computer verwendet werden sollen, und klicken Sie auf "Weiter".

17 Sie haben folgende Möglichkeiten:

So fügen Sie Netzwerk- und Speichertreiber für Computer hinzu, für die Sie SDR-Backups ausgeführt haben

Wählen Sie die Computer aus, deren Treiber Sie dem Wiederherstellungsdatenträger hinzufügen möchten, und klicken Sie auf "Weiter".

So fügen Sie erkannte Netzwerk- und Speichertreiber für Computer hinzu, für die Sie SDR-Backups ausgeführt haben, wenn die Treiber nicht im Quell-Image enthalten sind

Gehen Sie dazu wie folgt vor:

- Klicken Sie im Bereich "Computer für Verwendung der Treiber auswählen" auf "Weiter".
- Wählen Sie im Bereich "Einzuschließende Treiber" die Treiber aus, die auf dem benutzerdefinierten SDR-Datenträger enthalten sein sollen, und klicken Sie auf "Weiter".

So fügen Sie Netzwerktreiber und Speichertreiber aus OEM-Medien hinzu

Gehen Sie dazu wie folgt vor:

- Klicken Sie im Bereich "Computer für Verwendung der Treiber auswählen" auf "Weiter".
- Klicken Sie im Bereich "Einzuschließen Treiber" auf "Treiber hinzufügen", navigieren Sie zum Speicherort der Medien, wählen Sie ihn aus und klicken Sie auf "Öffnen".
- Wenn die Treiber in dem Bereich angezeigt werden, klicken Sie auf "Weiter".

- 18** Geben Sie die Datenträgerbezeichnung und den Pfad für das Image der Startdatei (.iso) ein und klicken Sie auf "Weiter".

Hinweis: Es wird empfohlen, dass Sie das zu brennende Image auf dem Computer speichern, auf dem die Anwendung zum Brennen des CD- oder DVD-Image installiert ist. Der standardmäßige Speicherort lautet: `C : <Backup Exec-Installationsordner>\Backup Exec\sdr\CustomSDRImage.iso`

- 19** Lesen Sie die Übersicht und klicken Sie auf "Image erstellen".
- 20** Nachdem das SDR-CD- oder DVD-Image erstellt wurde, klicken Sie auf "Weiter" und auf "Fertigstellen".
- 21** Brennen Sie das ISO 9660-Image auf eine CD oder DVD, indem Sie eine entsprechende Anwendung eines Drittanbieters verwenden.

Inhalt des Simplified Disaster Recovery-Datenträger-Image

Das SDR-Datenträger-Image stellt den Assistenten "Diesen Computer wiederherstellen" zum Wiederherstellen eines Computers zur Verfügung.

Das SDR-Datenträger-Image enthält auch die Tools, die Sie zum Verwalten der Netzwerkkonfiguration des Servers in der Wiederherstellungsumgebung verwenden können. Außerdem sind Dienstprogramme für zusätzliche Wiederherstellungsumgebungsvorgänge, wie zum Beispiel dynamisches Laden von Treibern und Aufrufen einer Eingabeaufforderung, enthalten.

Netzwerk-Tools im Menü:

- Netzwerkdienste starten
- Netzlaufwerk zuordnen

- Einstellungen für Netzwerkverbindung konfigurieren
- IP-Config-Dienstprogramm ausführen
- Ping-Befehl an Remote-Computer senden

Dienstprogramme im Menü:

- Protokolldateien für den technischen Support erfassen
- Protokolldatei anzeigen
- PowerShell starten
- Eingabeaufforderung aufrufen
- Windows boot.ini bearbeiten
- Treiber laden
- Tastatur auswählen

Simplified Disaster Recovery stellt auch ein Festplattenkonfigurations-Tool "Erweiterte Datenträgerkonfiguration" zur Verfügung. Mit "Erweiterte Datenträgerkonfiguration" können Sie erweiterte Festplattenvorgänge auf dem wiederherzustellenden Computer ausführen.

Dazu gehören z. B. Aufgaben wie:

- Erstellen oder Löschen von Datenträgern
- Ändern der Größe eines Datenträgers
- Konvertieren einer einfachen in eine dynamische Festplatte
- Ändern Zuweisen von Laufwerksbuchstaben
- Erstellen von übergreifenden, Stripeset- und gespiegelten Datenträgern

Siehe ["Erweiterte Datenträgerkonfiguration in Verbindung mit dem Assistenten "Computer wiederherstellen""](#) auf Seite 1001.

Siehe ["Anforderungen für die Anwendung von Simplified Disaster Recovery "](#) auf Seite 943.

Benutzerszenarien, wenn ein Benutzer den Assistenten zum Erstellen eines SDR-Datenträgers startet

Wenn ein Benutzer den Assistenten zum Erstellen eines SDR-Datenträgers startet, prüft dieser zuerst, ob Windows ADK bereits installiert ist. In der Tabelle finden Sie den Ablauf.

Tabelle 21-4 Benutzerszenarien, wenn ein Benutzer den Assistenten zum Erstellen eines SDR-Datenträgers startet

Windows Server-Version	Ist Windows ADK nicht installiert	Ist Windows ADK installiert
Windows Server 2008 SP2	Ist Windows ADK nicht installiert, lädt der Assistent Windows ADK 8.1 von der Microsoft-Website herunter. Nachdem Windows ADK 8.1 heruntergeladen und installiert wurde, erstellt der Assistent den SDR-Datenträger.	<p>Ist Windows ADK installiert, prüft der Assistent zum Erstellen von SDR-Datenträgern, ob die Version von Windows ADK "8.1" ist. Ist dies der Fall, wird gemeldet, dass dies zwar nicht die neueste Version ist, aber der Vorgang fortgesetzt werden kann.</p> <p>Wenn die Version von Windows ADK niedriger als 8.1 ist, fordert der Assistent den Benutzer auf, Windows ADK 8.1 von der Microsoft-Website herunterzuladen. Das Erstellen eines neuen SDR-Datenträgers mit ADK 8.0 wird nicht unterstützt.</p>
Windows Server 2008 R2	Ist Windows ADK nicht installiert, lädt der Assistent Windows ADK 10 von der Microsoft-Website herunter. Nachdem Windows ADK 10 heruntergeladen und installiert wurde, erstellt der Assistent den SDR-Datenträger.	<p>Wenn Windows ADK installiert ist, prüft der Assistent zum Erstellen eines SDR-Datenträgers, ob die Version "10" ist. Ist ADK 10 installiert, meldet der Assistent, dass die installierte Version von Windows ADK nicht aktuell ist. Der Vorgang kann trotzdem fortgesetzt werden.</p> <p>Wenn die Version von Windows ADK niedriger als 10 ist, fordert der Assistent den Benutzer auf, Windows ADK 10 von der Microsoft-Website herunterzuladen. Das Erstellen eines neuen SDR-Datenträgers mit ADK 8.0 oder 8.1 wird nicht unterstützt.</p>
Windows Server 2012	Wie bei Windows Server 2008 R2	Wie bei Windows Server 2008 R2
Windows Server 2012 R2	Wie bei Windows Server 2008 R2	Wie bei Windows Server 2008 R2

Sich vorbereiten, um sich von einem Systemausfall durch die Anwendung von Simplified Disaster Recovery zu erholen

Windows Server-Version	Ist Windows ADK nicht installiert	Ist Windows ADK installiert
Windows Server 2016	Wie bei Windows Server 2008 R2	Wie bei Windows Server 2008 R2
Windows Server 2019	<p>Ist Windows ADK 1809 nicht installiert, müssen Sie Windows ADK 1809 manuell herunterladen und installieren.</p> <p>Beim Installieren von ADK 1809 müssen Sie die Komponenten "Windows ADK Insider " und "Windows Preinstallation Environment" installieren.</p> <p>Nachdem die Komponenten installiert sind, starten Sie den Assistenten zum Erstellen von SDR-Datenträgern erneut.</p>	<p>Wenn Windows ADK 1809 installiert ist, erkennt der Assistent zum Erstellen eines SDR-Datenträgers die installierte Version des ADK und setzt den Vorgang fort.</p> <p>Wenn Windows ADK 10 installiert ist, erkennt der Assistent zum Erstellen eines SDR-Datenträgers, dass ADK 10.0 installiert ist und zeigt die Seite zum Installieren des ADK an. Der Assistent meldet zwar, dass die neueste verfügbare Version des ADK nicht installiert ist, aber Sie können trotzdem das Erstellen des SDR-Datenträgers fortsetzen. Bestätigen Sie, dass Sie weiterhin ADK 10 nutzen möchten. Wenn Sie den Vorgang fortsetzen, werden eventuell nicht alle Funktionen von Windows Server 2019 unterstützt.</p>

Sich vorbereiten, um sich von einem Systemausfall durch die Anwendung von Simplified Disaster Recovery zu erholen

Bei einem Systemausfall können Sie mithilfe von Simplified Disaster Recovery (SDR) den Zustand des Computers vor dem Systemausfall wiederherstellen.

Gehen Sie wie folgt vor, um die Wiederherstellung eines Computers vorzubereiten:

Tabelle 21-5

Sich vorbereiten, um sich von einem Systemausfall durch die Anwendung von Simplified Disaster Recovery zu erholen

Schritt	Beschreibung
Schritt 1	<p>Trennen Sie alle Verbindungen des wiederherzustellenden Computers mit einem Storage Area Network oder einem Cluster. Andernfalls werden möglicherweise auch die Festplatten der angeschlossenen Computer neu partitioniert oder formatiert.</p>
Schritt 2	<p>Planen Sie die Wiederherstellung aller am Computer vorgenommenen Hardwareänderungen.</p> <p>Siehe "Austauschen von Hardware während der Notfallwiederherstellung" auf Seite 985.</p>
Schritt 3	<p>Überprüfen Sie die zusätzlichen Voraussetzungen für IBM-Computer, wenn der wiederherzustellende Computer ein IBM-Computer ist.</p> <p>Siehe "Vorbereiten der Wiederherstellung von IBM-Computern mit Simplified Disaster Recovery" auf Seite 986.</p>
Schritt 4	<p>Lesen Sie die Wiederherstellungshinweise, wenn Sie einen SQL-Server, Exchange-Server, SharePoint-Server oder eine Umgebung, in der das Central Admin Server Feature installiert ist, wiederherstellen.</p> <p>Siehe "Hinweise zum Einsatz von Simplified Disaster Recovery mit Exchange, SQL, SharePoint, CAS, Hyper-V-Hosts und Deduplication Feature" auf Seite 999.</p> <p>Lesen Sie die Wiederherstellungshinweise, wenn Sie Windows mit Speicherpools und Speicherplätzen wiederherstellen.</p> <p>Siehe "Wiederherstellungshinweise für die Anwendung von Simplified Disaster Recovery in Verbindung mit Speicherpools und Speicherplätzen" auf Seite 995.</p>

Anschließend können Sie die Wiederherstellung starten.

Siehe ["Wiederherstellen eines Computers mithilfe von Simplified Disaster Recovery"](#) auf Seite 987.

Austauschen von Hardware während der Notfallwiederherstellung

Sie können Simplified Disaster Recovery (SDR) zur Wiederherstellung eines Computers verwenden, der nicht mehr funktioniert. Beispielsweise wenn die Hauptplatine des Computers ausfällt, können Sie die Daten des Computers wiederherstellen, nachdem Sie sie ersetzen. Sie können die Daten auch wiederherstellen, selbst wenn die neue Hauptplatine ein anderes Modell ist oder mehrere Prozessoren enthält.

Wenn Sie planen, die Hardware im wiederherzustellenden Computer auszutauschen, berücksichtigen Sie die folgenden Informationen, bevor Sie SDR zur Wiederherstellung des Computers verwenden.

Tabelle 21-6 Erwägungen bezüglich Hardware beim Wiederherstellen ausgefallener Computer

Element	Beschreibung
Festplatten	Die auszutauschenden Festplatten sollten dieselbe Größe wie die ursprünglichen haben oder größer sein.
Systemplatinen	Nachdem Sie die defekte Systemplatine ausgetauscht und SDR zur Wiederherstellung des Computers verwendet haben, müssen Sie die Treiber-CD des Systemplatinenherstellers einlegen, um zusätzliche Funktionen wie z. B. Onboard-Sound und Video neu zu installieren.

Element	Beschreibung
Netzwerkkarten	<p>Wenn Sie die Netzwerkkarte im Computer auswechseln, müssen Sie die notwendigen Netzwerktreiber installieren. Ohne Netzwerktreiber können Sie nicht auf das Netzwerk zugreifen, um einen Remote-Medienserver oder Remote-Backup-to-Disk-Ordner zur Wiederherstellung des Computers zu verwenden. Nach erfolgter Wiederherstellung müssen Sie geeignete neue Treiber für die neue Netzwerkkarte installieren.</p> <p>In den meisten Fällen ist es nicht notwendig, die Treiber manuell zu installieren. Die meisten Treiber sind auf dem Simplified Disaster Recovery-Datenträger-Image verfügbar. Wenn Sie das Simplified Disaster Recovery-Datenträger-Image erstellen, können Sie es so anpassen, dass es alle erforderlichen Treiber enthält.</p>

Siehe ["Wiederherstellen eines Computers mithilfe von Simplified Disaster Recovery"](#) auf Seite 987.

Vorbereiten der Wiederherstellung von IBM-Computern mit Simplified Disaster Recovery

Gehen Sie zum Wiederherstellen eines IBM-Computers mit einer IBM ServeRAID-Karte unter Verwendung von Simplified Disaster Recovery wie folgt vor:

Tabelle 21-7 Vorbereiten der Wiederherstellung eines IBM-Computers

Schritt	Beschreibung
Schritt 1	<p>Installieren und konfigurieren Sie die IBM ServeRAID-Karte und die ServeRAID-Software so, dass ein Startdatenträger vom Windows-Betriebssystem erkannt werden kann.</p>

Schritt	Beschreibung
Schritt 2	Starten Sie den Server unter Verwendung der CD "ServeRAID Configuration and Management" des IBM-Servers im CD-ROM-Laufwerk, bevor Sie die startfähigen SDR-Medien verwenden. Dadurch wird die Konfiguration und Installation der IBM ServeRAID-Dienstprogramme gestartet, und die aktuellen BIOS- und Firmware-Ebenen werden überprüft und aktualisiert.

Umfassende Informationen zur Installation von Windows auf einem IBM-Server mit dem ServeRAID-Controller finden Sie in der Dokumentation zu IBM ServeRAID. Erstellen und initialisieren Sie die ServeRAID-Datenträger, sodass die Datenträger vom Windows-Betriebssystem erkannt werden können.

Siehe ["Wiederherstellen eines Computers mithilfe von Simplified Disaster Recovery"](#) auf Seite 987.

Wiederherstellen eines Computers mithilfe von Simplified Disaster Recovery

Mit dem Assistenten "Computer wiederherstellen" für Simplified Disaster Recovery können Sie eine lokale oder Remote-Wiederherstellung eines Backup Exec-Servers oder eines Windows-Computers ausführen.

Sie können eine lokale Wiederherstellung durchführen, wenn alle folgenden Bedingungen erfüllt sind:

- Sie möchten einen Backup Exec-Server oder einen Windows-Computer wiederherstellen.
- Die Backup-Daten für den Computer befinden sich auf den Geräten, die Sie lokal an den Computer anschließen können und auf denen Sie den Assistenten "Computer wiederherstellen" ausführen können.
- Sie können die Notfallwiederherstellungs-Informationsdatei für den zu wiederherstellenden Backup Exec-Server oder Windows-Computer bereitstellen.

Hinweis: Wenn der wiederherzustellende Computer auf einem Bandgerät, Deduplizierungsspeicher oder virtuellen Datenträger gesichert wurde, konnte SDR die Notfallwiederherstellungs-Informationsdatei nicht mit den Backup-Sätzen speichern. Sie müssen den Pfad zum Standardspeicherort oder dem alternativen Speicherort für die Notfallwiederherstellungs-Informationsdatei angeben, wenn Sie vom Assistenten "Computer wiederherstellen" dazu aufgefordert werden. Wenn Sie keine Notfallwiederherstellungs-Informationsdatei bereitstellen können, müssen Sie eine manuelle Notfallwiederherstellung durchführen. Weitere Informationen zum Ausführen einer manuellen Notfallwiederherstellung finden Sie in folgenden Abschnitten:

Siehe ["Durchführen einer manuellen Notfallwiederherstellung eines lokalen Backup Exec-Servers auf einem Windows-Computer"](#) auf Seite 1006.

Siehe ["Manuelles Ausführen der Notfallwiederherstellung eines Remote-Backup Exec-Servers oder Remote-Agent auf einem Windows-Computer"](#) auf Seite 1011.

Hinweis: Wenn Sie Daten auf demselben Computer wiederherstellen und dabei die Option Festplatten löschen und oben gezeigtes Datenträgerlayout erneut erstellen nicht aktivieren, werden die WindowsApps-Ordner unter Windows 8 und höher nicht wiederhergestellt. Der Wiederherstellungsauftrag ist aber dennoch erfolgreich. Microsoft empfiehlt, die WindowsApps-Ordner in den Einstellungen mit der Option "Gerät - Zurücksetzen" wiederherzustellen.

Bei der Wiederherstellung werden möglicherweise die folgenden WindowsApps-Ordner ignoriert:

Der in

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Appx\PackageRoot`
erwähnte Ordner

Der in

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Appx\PackageRepositoryRoot`
erwähnte Ordner

`%SystemRoot%\InfusedApps`

Sie können eine Remote-Wiederherstellung durchführen, wenn alle folgenden Bedingungen erfüllt sind:

- Sie möchten einen Backup Exec-Server oder einen Windows-Computer wiederherstellen.
- Die Backup-Daten für den Computer befinden sich auf den Geräten, die an einen Backup Exec-Remote-Server angeschlossen sind.

- Sie haben Netzwerkzugriff auf den Backup Exec-Remote-Server.

Bevor Sie beginnen, überprüfen Sie die Schritte zur Vorbereitung der Wiederherstellung.

Siehe ["Sich vorbereiten, um sich von einem Systemausfall durch die Anwendung von Simplified Disaster Recovery zu erholen"](#) auf Seite 983.

Während der Wiederherstellungsvorgänge können Sie den Computer vom aktuellen Backup wiederherstellen. Alternativ dazu können Sie auch ein älteres Point-In-Time-Backup wiederherstellen.

Der Assistent "Computer wiederherstellen" unterstützt die Wiederherstellung von Computern mit verschlüsselten Backup-Sätzen. Wenn die Simplified Disaster Recovery (SDR)-Backups während des Backups verschlüsselt werden, fordert der Assistent Sie auf, für jeden verschlüsselten Backup-Satz, der für die Wiederherstellung erforderlich ist, die Passphrase einzugeben.

Siehe ["Verwaltung von Verschlüsselungscodes"](#) auf Seite 731.

Um Daten mithilfe des Assistenten "Computer wiederherstellen" wiederherzustellen, sind folgende Elemente erforderlich:

- Das Simplified Disaster Recovery-Datenträger-Image, das dieselbe Version von Backup Exec haben muss wie der Backup Exec-Server.
- Wenn der wiederherzustellende Computer auf ein Bandgerät, einen Deduplizierungsspeicher oder einen virtuellen Datenträger gesichert wurde, wird die Notfallwiederherstellungs-Informationsdatei nicht mit den Backup-Sätzen gespeichert. Stattdessen müssen Sie den Pfad zum Standardspeicherort oder dem alternativen Speicherort angeben, wenn Sie vom Assistenten "Computer wiederherstellen" dazu aufgefordert werden. Der Standardordner ist "C:<Backup Exec-Installationsordner>\Backup Exec\sdr\Data". Wenn die Datei nicht verfügbar ist, können Sie den Computer nicht mit SDR wiederherstellen.
- Der Backup-Satz, der alle kritischen Systemkomponenten für den zu wiederherstellenden Computer enthält.
- Das Startlaufwerk auf dem zu wiederherstellenden Computer muss je nach Betriebssystem und Konfiguration zwischen 3 und 5 GB freien Speicherplatz haben.

Hinweis: Wenn ein leerer Bildschirm angezeigt wird und der Computer nach dem Ausführen von SDR nicht neu gestartet wird, vergewissern Sie sich, dass das Startlaufwerk genügend freien Speicherplatz verfügbar hat. Starten Sie anschließend den Computer neu.

- Der zu wiederherstellende Computer muss eine Menge von RAM haben, die größer oder gleich dem für das wiederhergestellte Betriebssystem mindestens erforderlichen Speicherplatz ist.
- Der zu wiederherstellende Computer muss Datenträger mit genügend freiem Speicher für die Daten haben, die Sie vom Backup von kritischen Datenträgern wiederherstellen. Ein Datenträger wird als kritisch betrachtet, wenn er für einen erfolgreichen Start des Computers erforderlich ist.
- Wenn Sie einen Windows-Computer wiederherstellen, bei dem BitLocker-Verschlüsselung aktiviert ist, muss diese nach der Wiederherstellung aktiviert werden. Weitere Informationen zur BitLocker-Laufwerkverschlüsselung finden Sie in der Microsoft-Dokumentation.
- Wenn der Computer, den Sie wiederherstellen möchten, ein RAID-Setup enthält, müssen Sie möglicherweise zuerst das RAID konfigurieren, bevor Sie ihn mit dem SDR-Datenträger starten. Verwenden Sie die RAID-Software des Computerherstellers, um das RAID-System zu konfigurieren.
- Lesen Sie gegebenenfalls die folgenden Wiederherstellungshinweise:
 - Siehe ["Wiederherstellungshinweise für die Anwendung von Simplified Disaster Recovery in Verbindung mit Speicherpools und Speicherplätzen"](#) auf Seite 995.
 - Siehe ["Hinweise zum Einsatz von Simplified Disaster Recovery mit Exchange, SQL, SharePoint, CAS, Hyper-V-Hosts und Deduplication Feature"](#) auf Seite 999.

Hinweis: Boot-Manager, z. B. System Commander oder OS/2 Boot Manager, können mit SDR nicht wiederhergestellt werden. Boot-Manager werden normalerweise auf einer sehr niedrigen Ebene installiert, die Backup Exec nicht schützen kann. Der OS/2 Boot Manager befindet sich beispielsweise auf einer separaten Festplatte, auf die Backup Exec nicht zugreifen kann. Angesichts der Vielzahl verfügbarer Boot-Manager kann der Computer bei einer SDR-Wiederherstellung möglicherweise selbst dann nicht mehr gestartet werden, wenn das Betriebssystem wiederhergestellt wurde. Um dieses Problem zu lösen, können Sie den Boot-Manager erneut installieren.

So stellen Sie einen Computer mithilfe des Assistenten "Computer wiederherstellen" wieder her

- 1 Legen Sie den startfähigen Simplified Disaster Recovery-Datenträger ins CD- oder DVD-Laufwerk des wiederherzustellenden Computers ein, und starten Sie den Computer.
- 2 Klicken Sie im Bildschirm "Endbenutzerlizenzvereinbarung" auf "Akzeptieren".

- 3** Klicken Sie im Begrüßungsbildschirm von Simplified Disaster Recovery auf **"Computer wiederherstellen"**.
- 4** Klicken Sie links auf "Netzwerk" und dann auf "Einstellungen für Netzwerkverbindung konfigurieren".
- 5** Wählen Sie die entsprechende Netzwerkadapterkonfiguration und klicken Sie auf "OK".
- 6** Sie haben folgende Möglichkeiten:

Die Backup-Daten für diesen Computer befinden sich auf den Geräten, die an einen Backup Exec-Remote-Server angeschlossen sind (Remote-Wiederherstellung).

Gehen Sie dazu in folgender Reihenfolge vor:

- Klicken Sie auf "Die Daten befinden sich auf Geräten, die an einen Backup Exec-Remote-Server angeschlossen sind".
- Geben Sie den Namen und die Domäne des Backup Exec-Remote-Servers ein, auf dem sich die Backup-Daten befinden, sowie gültige Administrator- oder entsprechende Identifikationsdaten ein.
- (Optional) Zum Konfigurieren der Netzwerkadapter-Einstellungen klicken Sie auf "Netzwerkadapter-Einstellungen konfigurieren", und führen Sie dann einen der folgenden Schritte durch:
 - Um jedem erkannten Netzwerkadapter eine statische IP-Adresse zuzuweisen, wählen Sie die entsprechenden Optionen aus und klicken Sie auf "OK".
 - Klicken Sie zum Konfigurieren eines IPv6-Netzwerkcontrollers auf "IPv6 konfigurieren", wählen Sie die entsprechenden Optionen aus, und klicken Sie dann auf "OK".
- (Optional) Klicken Sie zum Laden der Netzwerkadaptertreiber auf "Netzwerkadaptertreiber laden". Klicken Sie dann für jeden deaktivierten Netzwerkcontroller, den der Assistent erkennt, auf "Treiber installieren". Navigieren Sie zu dem Gerät, das den Netzwerkcontroller-Treiber enthält, und klicken Sie auf "Öffnen". Wählen Sie den Treiber aus und klicken Sie erneut auf "Öffnen".
- Klicken Sie auf "Weiter".

<p>Wenn der wiederherzustellende Computer auf lokal angeschlossenen Geräten, z. B. Bandlaufwerken, Wechslern, Plattenspeichergeräten oder Plattenkassettengeräten, gesichert wurde (lokale Wiederherstellung)</p>	<p>Gehen Sie dazu in folgender Reihenfolge vor:</p> <ul style="list-style-type: none"> ■ Klicken Sie auf "Die Daten befinden sich auf Geräten, die lokal an diesen Computer angeschlossen sind". ■ Geben Sie gültige Administrator- oder entsprechende Identifikationsdaten ein, wenn Sie dazu aufgefordert werden, und klicken Sie dann auf "Weiter".
---	--

- 7** Wählen Sie die Notfallwiederherstellungs-Informationsdatei, die Sie verwenden möchten, und klicken Sie dann auf "Weiter".

Hinweis: Backup Exec unterstützt standardmäßig die neuesten drei vollen SDR-Backup-Ketten, die für die Systemwiederherstellung mit SDR erforderlich sind. Jede Backup-Kette enthält einen vollständigen Backup-Satz, ihre abhängigen inkrementellen und differenziellen Backups und deren doppelten Backup-Sätze.

- 8** Wählen Sie die Backup-Sätze aus, die Sie zur Wiederherstellung des Computers verwenden möchten, und klicken Sie auf "Weiter".
- 9** Wählen Sie das Speichergerät mit den Backup-Daten für den Computer aus und klicken Sie auf "Weiter".
- 10** Sie haben folgende Möglichkeiten:

<p>Verwenden des Datenträgerlayouts wie gezeigt</p>	<p>Klicken Sie auf "Weiter".</p>
---	----------------------------------

<p>Anzeigen der Datenträgergeometrie in ihrem aktuellen Zustand oder einer grafischen Darstellung der vorgeschlagenen Änderungen</p>	<p>Klicken Sie auf "Vorschau".</p>
--	------------------------------------

Installieren der erforderlichen SCSI- oder RAID-Controller-Treiber Gehen Sie dazu in folgender Reihenfolge vor:

- Klicken Sie auf "Speichercontroller-Treiber laden".
- Klicken Sie für jeden deaktivierten Netzwerkcontroller, den der Assistent erkennt, auf "Treiber installieren".
- Navigieren Sie zu dem Gerät, das den Netzwerkcontroller-Treiber enthält, und klicken Sie auf "Öffnen".
- Wählen Sie den Treiber aus und klicken Sie erneut auf "Öffnen".

Automatisches Erstellen eines Datenträgerlayouts auf den verfügbaren Festplatten, wenn in der vereinfachten Ansicht des Datenträgerlayouts nicht übereinstimmende Datenträger angezeigt werden Aktivieren Sie die Option "Festplatten löschen und oben gezeigtes Datenträgerlayout erneut erstellen". Die vorhandenen Daten auf diesen Datenträgern gehen verloren.

Ändern der Datenträgergrößen oder andere Datenträgervorgänge Klicken Sie auf "Erweiterte Datenträgerkonfiguration".

Siehe ["Erweiterte Datenträgerkonfiguration in Verbindung mit dem Assistenten"](#) auf Seite 1001.

- 11** Lesen Sie die "Wiederherstellungsübersicht" und klicken Sie auf "Zurück", um Änderungen vorzunehmen, oder auf "Wiederherstellung", um die Wiederherstellung zu starten.

- 12** Wenn Sie einen Backup Exec-Server wiederherstellen, auf dem Backup Exec 15 oder höher ausgeführt wird, wählen Sie den entsprechenden Datenbankverschlüsselungscode aus und klicken Sie dann auf "Weiter".

Hinweis: Unter Backup Exec 15 und höher ist ein Datenbankverschlüsselungscode zum Zugreifen auf die Backup Exec-Datenbank erforderlich. Wenn Sie fortfahren, ohne den Datenbankverschlüsselungscode einzugeben, werden Sie aufgefordert, ihn einzugeben, wenn Sie Backup Exec neu starten.

- 13** Wenn die Wiederherstellung abgeschlossen ist, können Sie beliebige oder alle folgenden Aktionen durchführen:

Fehlerbehebung für Probleme, die während der Hardware-Erkennung aufgetreten sind	Klicken Sie auf "Hardware-Erkennungsprotokoll anzeigen".
Fehlerbehebung für Probleme, die während der Wiederherstellung aufgetreten sind	Klicken Sie auf "Computer wiederherstellen-Protokoll anzeigen".
Neustarten dieses Computers nach dem Klicken auf "Fertigstellen"	Wählen Sie "Diesen Computer neu starten".
Abschließen der Wiederherstellung und Beenden des Assistenten	Klicken Sie auf "Fertigstellen".

Hinweis: Wenn der wiederhergestellte Computer mehrere Festplatten enthält, stellen Sie sicher, dass im Computer-BIOS der Start des Computers über die Festplatte mit dem Windows-Betriebssystem konfiguriert ist. Das BIOS-Menü können Sie auf vielen Computern durch Drücken der Taste F2 oder Entf auf der Computertastatur aufrufen.

Wiederherstellungshinweise für die Anwendung von Simplified Disaster Recovery in Verbindung mit Speicherpools und Speicherplätzen

Sie können Simplified Disaster Recovery (SDR) für Windows mit Speicherplätzen und Speicherpools anhand der in der folgenden Tabelle beschriebenen Szenarien durchführen:

Tabelle 21-8 Szenarien für SDR für Speicherpools und Speicherplätze

Szenario	Beschreibung
Wiederherstellen von Windows Speicherpools und Speicherplätzen auf demselben Computer	

Szenario	Beschreibung
	<p>In diesem Szenario fordert Sie der Assistent "Computer wiederherstellen" dazu auf, die Speicherpools und Speicherplätze neu zu konfigurieren, zu entfernen oder im aktuellen Zustand wiederherzustellen.</p> <p>Klicken Sie zum Neukonfigurieren oder Entfernen der Speicherpools und Speicherplätze in dem angezeigten Meldungsdialogfeld auf die Schaltfläche "PowerShell", um ein PowerShell-Fenster zu öffnen.</p> <p>Hinweis: Der Wiederherstellungsdatenträger, der mit Windows ADK 8.1 erstellt wurde, erkennt den Backup Exec-Speicherordner (\BEData) nicht, wenn dieser in den Speicherpools und -plätzen auf dem Backup Exec-Server konfiguriert ist. Dieses Problem tritt nur auf, wenn der Backup Exec-Server (unter Windows Server 2016) nicht verfügbar ist und eine lokale SDR-Wiederherstellung aus dem Ordner "BEData" ausgeführt werden soll.</p> <p>Wiederherstellungsdatenträger, die mit Windows ADK 8.1 oder 10 erstellt wurden, erkennen den Backup Exec-Speicherordner (\BEData) nicht, wenn dieser in den Speicherpools und -plätzen auf dem Backup Exec-Server konfiguriert ist. Dieses Problem tritt nur auf, wenn der Backup Exec-Server (unter Windows Server 2019) nicht verfügbar ist und eine lokale SDR-Wiederherstellung aus dem Ordner "BEData" ausgeführt werden soll.</p> <p>Wenn Sie die Speicherpools und Speicherplätze unter Verwendung des Wiederherstellungsdatenträgers erstellen, der mit Windows ADK 10 erstellt wurde, erkennt Windows Server 2012 (R2) nach der Systemwiederherstellung keine Speicherpools und Speicherplätze.</p> <p>Wenn Sie die Speicherpools und -plätze mit einem Wiederherstellungsdatenträger</p>

Szenario	Beschreibung
	<p>erstellen, der mit Windows ADK 1809 erstellt wurde, werden diese unter Windows Server 2016 und niedriger nach der Systemwiederherstellung nicht erkannt.</p> <p>Weitere Informationen über Speicherbefehle in PowerShell finden Sie unter folgender URL: http://technet.microsoft.com/library/hh848705.aspx</p>
<p>Wiederherstellen einer Version von Windows (Version vor Windows 8/Windows Server 2012) auf einem Computer, auf dem Speicherpools und Speicherplätze oder virtuelle Datenträger bereits konfiguriert sind.</p>	<p>In diesem Szenario führen Sie die Wiederherstellung auf einem Computer aus, der konfigurierte Speicherpools und Speicherplätze enthält. Das Betriebssystem, das Sie wiederherstellen, erkennt Speicherpools und Speicherplätze jedoch nicht.</p> <p>Der Assistent "Computer wiederherstellen" fordert Sie auf, einen der folgenden Schritte auszuführen.</p> <ul style="list-style-type: none"> ■ Klicken Sie zum Entfernen der Speicherpools und Speicherplätze in dem angezeigten Meldungsdialogfeld auf die Schaltfläche "PowerShell", um ein PowerShell-Fenster zu öffnen. Weitere Informationen über Speicherbefehle in PowerShell finden Sie unter folgender URL: http://technet.microsoft.com/library/hh848705.aspx ■ Klicken Sie zum Fortsetzen der Wiederherstellung der Speicherpools und Speicherplätze in dem angezeigten Meldungsdialogfeld auf "Weiter". Der Assistent "Computer wiederherstellen" blockiert alle Datenträgervorgänge auf dem virtuellen Datenträger, wie etwa das Erstellen eines Datenträgers, Löschen eines Datenträgers, Zuweisen eines Laufwerksbuchstaben usw.

Einschränkungen für die Wiederherstellung von Speicherpools und Speicherplätzen

Der Assistent "Computer wiederherstellen" ordnet Datenträger automatisch ihren ursprünglichen virtuellen Datenträgern oder Speicherplätzen zu, wenn Sie die Wiederherstellung auf demselben Computer ausführen. Führen Sie die Wiederherstellung nicht auf demselben Computer durch, müssen Sie PowerShell und die erweiterte Datenträgerkonfiguration für SDR verwenden, um die Datenträger manuell den virtuellen Datenträgern oder Speicherplätzen zuzuordnen.

Der Assistent "Computer wiederherstellen" lässt das Zuordnen von Start-, System- und Wiederherstellungsdatenträgern zu virtuellen Datenträgern nicht zu.

Siehe ["Erweiterte Datenträgerkonfiguration in Verbindung mit dem Assistenten "Computer wiederherstellen""](#) auf Seite 1001.

Hinweise zum Einsatz von Simplified Disaster Recovery mit Exchange, SQL, SharePoint, CAS, Hyper-V-Hosts und Deduplication Feature

Lesen Sie die folgenden Wiederherstellungshinweise, wenn Sie einen SQL-Server, Exchange-Server, SharePoint-Server oder eine Umgebung, in der Central Admin Server Feature installiert ist, wiederherstellen.

Microsoft SQL Server: Hinweise zur Wiederherstellung

Nachdem der Windows-Server unter Verwendung von Simplified Disaster Recovery (SDR) wiederhergestellt wurde, ersetzt SDR die beschädigten Master- und Modelldatenbanken automatisch durch Kopien der Master- und Modell-Datenbanken. Nachdem SQL neu gestartet wurde und das neueste Master-Datenbank-Backup sowie alle anderen Systemdatenbanken wiederhergestellt wurden, müssen Sie noch alle Benutzerdatenbanken wiederherstellen. Sie können den Backup Exec-Wiederherstellungsassistenten verwenden, um die letzten Backups wiederherzustellen.

Microsoft Exchange: Hinweise zur Wiederherstellung

Nachdem Sie den Windows-Server mit Simplified Disaster Recovery (SDR) wiederhergestellt haben, verwenden Sie den Backup Exec-Wiederherstellungsassistenten, um die Exchange Server-Datenbanken aus den neuesten Exchange Server-Datenbank-Backups wiederherzustellen.

SharePoint Portal Server: Hinweise zur Wiederherstellung

Sie können Simplified Disaster Recovery (SDR) zur Wiederherstellung eines Windows-Servers verwenden, auf dem SharePoint Portal-Server installiert ist. Nachdem Sie den Windows-Computer wiederhergestellt haben, müssen Sie ihn

neu starten. Nach dem Neustart des Computers ist die SharePoint Portal Server zwar installiert, ist aber nicht funktionsfähig. Sie müssen SharePoint Portal-Server entfernen und erneut installieren, bevor die SharePoint-Daten wiederhergestellt werden können.

Central Admin Server Feature (CAS) – Wiederherstellungshinweise

Wenn Sie SDR zum Wiederherstellen eines Computers in einer CAS-Umgebung verwenden, können Sie den Remote-Wiederherstellungsauftrag an eines der beiden folgenden Ziele senden:

- Den zentralen Administrationsserver.
- Den verwalteten Backup Exec-Server, der den ursprünglichen Backup-Auftrag ausführte.

Microsoft Hyper-V-Hosts

Nachdem Sie SDR verwenden, um den Windows-Server wiederherzustellen, verwenden Sie den Backup- Exec-Wiederherstellungsassistenten, um den Microsoft Hyper-V-Host aus den neuesten Backups wiederherzustellen.

Backup Exec Deduplication Feature - Wiederherstellungshinweise

Wenn Backup Exec Deduplication Feature installiert ist und Sie Deduplizierungsspeichergeräte verwenden, beachten Sie die folgenden Punkte:

- Wenn Sie auf den lokalen Backup Exec-Server sichern, wählen Sie kein Deduplizierungsspeichergerät auf dem Server als Zielspeichergerät aus. Der Assistent "Diesen Computer wiederherstellen" kann Daten aus einem lokalen Deduplizierungsspeichergerät nicht wiederherstellen.
- Simplified Disaster Recovery (SDR) kann kein Deduplizierungsspeichergerät wiederherstellen.
- Bevor Sie mithilfe von SDR einen Remote-Computer wiederherstellen können, der unter Verwendung der Client-seitigen Deduplizierung gesichert wurde, müssen Sie zuerst das Gerät für den Direktzugriff löschen.
Siehe "[Wählen von Speichergeräten für die gemeinsame Nutzung über Direktzugriff](#)" auf Seite 1073.

Wenn Sie SDR verwenden, um einen Backup Exec-Server wiederherzustellen, der einen Deduplizierungsspeichergerät enthält, müssen Sie Folgendes beachten:

- Vorhandene Backup-Sätze, die zum Deduplizierungsspeichergerät geschickt wurden, nachdem es gesichert wurde, können nicht wiederhergestellt werden.

- Das Deduplizierungsspeichergerät ist möglicherweise nach der Wiederherstellung nicht verwendbar.

Sie können eine manuelle Notfallwiederherstellung auch dann verwenden, um Deduplizierungsspeicher und OpenStorage-Geräte wiederherzustellen.

Siehe ["Methoden für das Wiederherstellen von Daten in Backup Exec"](#) auf Seite 258.

Siehe ["Notfallwiederherstellung des Deduplizierungsspeichergeräts"](#) auf Seite 1085.

Siehe ["Pfad zur Notfallwiederherstellung-Informationsdatei"](#) auf Seite 956.

Siehe ["Festlegen oder Ändern des alternativen Speicherorts für die Notfallwiederherstellungs-Informationsdatei"](#) auf Seite 954.

Siehe ["Infos zu Central Admin Server Feature"](#) auf Seite 1450.

Erweiterte Datenträgerkonfiguration in Verbindung mit dem Assistenten "Computer wiederherstellen"

Der Assistent "Computer wiederherstellen" stellt die Festplatten mit derselben Größe wieder her, die sie vor dem Systemausfall hatten. Wenn die Festplatte im ausgefallenen Computer größer als die Festplatte vor dem Systemausfall ist, führt dies möglicherweise zu ungenutztem und nicht zugewiesenem Speicherplatz. Sie können die erweiterte Datenträgerkonfiguration ausführen, um die Datenträgergrößen zu ändern, um die größere Festplattengröße zu berücksichtigen.

Im Folgenden finden Sie ein Beispiel dafür, warum die Größe von Festplatten angepasst werden sollte:

Die Hardware des Computers vor dem Notfall enthielt eine 40-GB-Festplatte mit zwei Datenträgern mit jeweils 20 GB. Sie ersetzen die Festplatte durch ein 90-GB-Modell. SDR verwendet dann die Notfallwiederherstellungs-Informationsdatei, um die Festplattenpartitionstabelle auf der Grundlage der Partitionsinformationen von der ursprünglichen 40-GB-Festplatte neu zu erstellen. Dadurch werden auf der neuen 90-GB-Festplatte nur 40 GB Speicherplatz zugewiesen und die Partitionszuweisung besteht aus zwei Partitionen von je 20 GB.

Sie können auf "Erweiterte Datenträgerkonfiguration" über den Assistenten "Computer wiederherstellen" zugreifen.

Hinweis: Sie sollten mit dem Konzept der Microsoft-Datenträgerverwaltung vertraut sein, bevor Sie "Erweiterte Datenträgerkonfiguration" ausführen.

Die folgende Tabelle enthält Informationen zu den zusätzlichen Datenträgervorgängen, die Sie mit "Erweiterte Datenträgerkonfiguration" ausführen können.

Tabelle 21-9 Aufgaben von "Erweiterte Datenträgerkonfiguration"

Aufgabe	Beschreibung
Einfachen Datenträger erstellen	Ein einfacher Datenträger ist eine Partition auf einem Datenträger, der ein Dateisystem enthält.
Datenträger formatieren	Datenträger müssen formatiert werden, bevor Daten auf ihnen gespeichert werden können.
Größe eines Datenträgers erweitern	Wenn ein Datenträger nicht zugewiesenen Speicherplatz enthält, der sich neben einem funktionsfähigen Datenträger befindet, können Sie den Datenträger erweitern, um den freien Speicherplatz einzuschließen. Um den Datenträger zu erweitern, muss er entweder unkomprimiert oder mit dem Windows-NTFS-Dateisystem formatiert sein.
Größe eines Datenträgers reduzieren	<p>Sie können die Größe eines Datenträgers verringern, indem Sie den Datenträger auf den zusammenhängenden, nicht zugewiesenen Speicherplatz verkleinern, der sich auf demselben Datenträger befindet.</p> <p>Wenn Sie einen Datenträger verkleinern, müssen Sie ihn nicht neu formatieren. Gewöhnliche Dateien werden automatisch auf dem Datenträger verschoben, um den neuen, nicht zugewiesenen Speicherplatz zu erstellen.</p>

Aufgabe	Beschreibung
Übergreifenden Datenträger erstellen	<p>Ein übergreifender Datenträger umfasst mehr als einen physischen Datenträger. Sie können einen übergreifenden Datenträger erstellen, indem Sie mehrere physische Datenträger einschließen oder den Datenträger um nicht zugewiesenen Speicherplatz erweitern.</p> <p>Um einen übergreifenden Datenträger zu erstellen, benötigen Sie einen Datenträger für den Systemstart und mindestens zwei dynamische Datenträger.</p> <p>Hinweis: Übergreifende Datenträger sind nicht fehlertolerant.</p>
Stripeset-Datenträger erstellen	<p>Stripeset-Datenträger speichern Daten in Blöcken auf zwei oder mehr physischen Datenträgern. Obwohl Stripeset-Datenträger nicht fehlertolerant sind, bieten sie die beste Leistung aller Datenträger unter Windows.</p>
Gespiegelten Datenträger erstellen	<p>Ein gespiegelter Datenträger liefert eine Kopie der Daten, die auf einen ausgewählten Datenträger geschrieben werden. Da alle Daten auf den gespiegelten Datenträger sowie auf den ausgewählten Datenträger geschrieben werden, wird durch die Spiegelung die Kapazität beider Datenträger um 50 % reduziert.</p>
Datenträgereigenschaften anzeigen	<p>Sie können die Eigenschaften für jeden Datenträger in der Ansicht "Aktuelles Datenträgerlayout" oder "Ursprüngliches Datenträgerlayout" anzeigen.</p>
Zugewiesenen Laufwerksbuchstaben ändern	<p>Sie können zugewiesene Laufwerksbuchstaben für alle Datenträger ändern, wenn Sie die Laufwerksbuchstaben auf eine bestimmte Art organisieren möchten.</p>
Datenträger löschen	<p>Bei diesem Vorgang werden alle Daten gelöscht. Daher sollte diese Option nicht unüberlegt verwendet werden.</p>

Aufgabe	Beschreibung
Basisdatenträger in einen dynamischen Datenträger konvertieren	Durch die Konvertierung von Basisdatenträgern in dynamische Datenträger können Sie Datenträger erstellen, die mehrere Datenträger umfassen. Mithilfe von dynamischen Datenträgern können Sie auch fehlertolerante Datenträger wie gespiegelte und RAID-5-Datenträger erstellen. Alle Datenträger auf dynamischen Datenträgern werden als dynamische Datenträger bezeichnet.
MBR-Datenträger (Master-Bootsektor) in einen GPT-Datenträger (GUID-Partitionstabelle) konvertieren	<p>MBR-Datenträger (Master-Bootsektor) verwenden die Standard-BIOS-Schnittstelle. GPT-Datenträger verwenden das Extensible Firmware Interface (EFI).</p> <p>Sie können MBR-Datenträger in GPT-Datenträger konvertieren, wenn der Datenträger keine Partitionen oder Datenträger enthält.</p>
GPT-Datenträger (GUID-Partitionstabelle) in einen MBR-Datenträger (Master-Bootsektor) konvertieren	<p>GPT-Datenträger verwenden das Extensible Firmware Interface (EFI). MBR-Datenträger verwenden die Standard-BIOS-Schnittstelle.</p> <p>GPT-Datenträger können in MBR-Datenträger konvertiert werden, wenn der Datenträger keine Partitionen oder Datenträger enthält.</p>

Aufgabe	Beschreibung
Ursprüngliches Datenträger-Layout anzeigen	<p>Das ursprüngliche Datenträger-Layout zeigt das Datenträger-Layout, das zum Zeitpunkt der Ausführung des Backup-Auftrags bestand. In der vereinfachten Layoutansicht können Sie die Datenträgergeometrie akzeptieren, wie sie vor dem Systemausfall bestand, oder Sie können die Geometrie ändern, indem Sie die Datenträgergrößen ändern. Abhängig von der Größe der vorhandenen Datenträger können Sie die Datenträgergrößen in Megabyte, Gigabyte oder Terabyte ändern.</p> <p>Die vereinfachte Layoutansicht enthält die Registerkarte "Vorschau", auf der Sie die Datenträgergeometrie in ihrem aktuellen Zustand anzeigen können. Wenn Sie die Datenträgergeometrie und Datenträgergrößen ändern, klicken Sie auf die Registerkarte "Vorschau", um Ihre Änderungsvorschläge grafisch anzuzeigen.</p> <p>Wenn schlecht zusammengestellte Datenträger in der vereinfachten Volumendesignansicht angezeigt werden, können Sie mithilfe der Option Festplatten löschen und oben gezeigtes Datenträgerlayout erneut erstellen automatisch ein Layout auf den verfügbaren Festplatten erstellen. Sie können ein Volumendesign auch manuell mithilfe der Option "Erweiterte Datenträgerkonfiguration" erstellen.</p>

Manuelles Ausführen der Notfallwiederherstellung

Sie sollten die Notfallwiederherstellung in folgenden Situationen manuell ausführen:

- Simplified Disaster Recovery ist nicht verfügbar oder schlug fehl
- Windows wurde beschädigt und kann nicht mit den EDR-Datenträgern wiederhergestellt werden.
- Auf der Festplatte, auf der sich Windows befindet, ist ein nicht behebbarer Fehler aufgetreten, der eine Neuformatierung des Datenträgers erfordert.

- Die Festplatte, auf der sich Windows befindet, muss ausgetauscht werden.

Informationen zum manuellen Ausführen der Notfallwiederherstellung eines lokalen Backup Exec-Servers auf einem Windows-Computer finden Sie im folgenden Abschnitt:

Siehe ["Durchführen einer manuellen Notfallwiederherstellung eines lokalen Backup Exec-Servers auf einem Windows-Computer"](#) auf Seite 1006.

Informationen zum manuellen Ausführen der Notfallwiederherstellung eines Remote-Backup Exec-Servers oder Remote-Agent auf einem Windows-Computer finden Sie im folgenden Abschnitt:

Siehe ["Manuelles Ausführen der Notfallwiederherstellung eines Remote-Backup Exec-Servers oder Remote-Agent auf einem Windows-Computer"](#) auf Seite 1011.

Durchführen einer manuellen Notfallwiederherstellung eines lokalen Backup Exec-Servers auf einem Windows-Computer

Dieses Verfahren stellt das Betriebssystem des Computers auf den Zustand vor dem Notfall wieder her. Dabei werden auch Ihre Datendateien wiederhergestellt, mit Ausnahme derjenigen, die durch einen Backup Exec-Agent, wie zum Beispiel den Agent for Microsoft Exchange Server, geschützt werden. Wenn Daten von Backup Exec-Agents geschützt werden, lesen Sie im Backup Exec-Administratorhandbuch den Abschnitt zum Wiederherstellen der vom Agent geschützten Daten, bevor Sie die Notfallwiederherstellung starten. Stellen Sie die vom Agent geschützten Daten wieder her, wenn die Systemwiederherstellung abgeschlossen ist. Dieses Verfahren enthält die (nicht) autoritative Wiederherstellung von Active Directory für einen Domänencontroller.

Diese Schritte sind nur für die manuelle Notfallwiederherstellung gedacht. Wenn Simplified Disaster Recovery (SDR) für den Computer aktiviert ist, sollten Sie SDR für die Notfallwiederherstellung verwenden.

Die folgenden Elemente sind für die manuelle Notfallwiederherstellung eines lokalen Computers erforderlich:

- Ein aktuelles vollständiges Backup des Computers, dessen Betriebsfähigkeit wiederhergestellt werden soll, und alle nachfolgenden inkrementellen bzw. Differenzial-Backups.
- Das Windows-Installationsmedium
- Backup Exec-Installationsmedium.
- Der Datenbankverschlüsselungscode, der zum Schützen der Backup Exec-Datenbank verwendet wurde. Sie müssen den Code in einen sicheren Speicherort exportieren und dann abrufen, um die Wiederherstellung abzuschließen.

- Ein Speichergerät (z. B. Bandlaufwerk oder Wechsler) muss an den Computer angeschlossen werden, der wiederhergestellt werden soll.
- Wenn Sie eine autoritative Wiederherstellung auf einem Domänencontroller durchführen möchten, müssen Sie die DSRM-Identifikationsdaten angeben.

Hinweis: Wenn Sie einen Windows-Computer wiederherstellen, bei dem BitLocker-Verschlüsselung aktiviert ist, muss diese nach der Wiederherstellung erneut aktiviert werden. Weitere Informationen zur BitLocker-Laufwerksverschlüsselung finden Sie in der Microsoft-Dokumentation.

Während dieses Verfahrens sollten Sie sich immer mit dem Administratorkonto oder einem äquivalenten Konto bei Windows einloggen.

So führen Sie eine manuelle Notfallwiederherstellung eines lokalen Backup Exec-Servers auf einen Windows-Computer aus

1. Installieren Sie die ursprüngliche Version von Windows. Installieren Sie anschließend dieselben Service Packs und Patches, die vorher installiert waren.

Beachten Sie Folgendes:

- Soll der Computer nach einem vollständigen Festplattenausfall wiederhergestellt werden, verwenden Sie das Windows-Setup, um den neuen Datenträger während der Installation zu partitionieren und zu formatieren. Diese Installation von Windows ist notwendig, damit Backup Exec ein Ziel für die Wiederherstellung des Systems hat. Der Computernamen, das Windows-Verzeichnis und das Dateisystem (z. B. NTFS) müssen mit denen der vorherigen Windows-Installation übereinstimmen. Diese Grundinstallation wird durch die gesicherte Version überschrieben, die die Systemkonfiguration, die Anwendungseinstellungen und die Sicherheitseinstellungen wiederherstellt.

- Wenn der Computer ein Domänencontroller in einer bestimmten Domäne oder Arbeitsgruppe war, treten Sie der Domäne oder Arbeitsgruppe nicht bei. Klicken Sie im Dialogfeld "Computernamen ändern" auf "Mehr...", um manuell ein Domänensuffix an den Computernamen anzuhängen, das dem ursprünglichen Domänen- oder Arbeitsgruppensuffix entspricht.

Ändern Sie den neuen Computernamen in den ursprünglichen Namen, indem Sie folgende Schritte in der angegebenen Reihenfolge ausführen:

- Klicken Sie unter "Systemeigenschaften" auf der Registerkarte "Computernamen" auf "Ändern".

Hinweis: Wenn die Domäne oder Arbeitsgruppe verbunden ist, müssen Sie die Vertrauensbeziehung nach der Wiederherstellung und dem Neustart wiederherstellen.

- Klicken Sie im Dialogfeld "Computernamen- bzw. -domänenänderungen" auf "Mehr".
 - Bei Bedarf aktivieren Sie das Kontrollkästchen "Primäres DNS-Suffix bei Domänenmitgliedschaftsänderung ändern" und klicken Sie dann auf "OK".
 - Starten Sie den Computer neu.
2. Installieren Sie Backup Exec in einem anderen Verzeichnis als dem ursprünglichen (eine temporäre Installation). Während dieses Verfahrens sollten Sie sich immer mit dem Administratorkonto oder einem äquivalenten Konto bei Windows einloggen.

Hinweis: Nach Abschluss der Wiederherstellung kann diese Installation von Backup Exec entfernt werden.

3. Starten Sie Backup Exec, und fügen Sie das erforderliche Speichergerät hinzu, indem Sie auf die Registerkarte "Speicher" und dann auf "Speicher konfigurieren" klicken.

Dieses Speichergerät ist das Band, auf dem sich der Backup-Satz befindet, oder der Datenträgerpfad, in dem sich die Backup-Dateien befinden.

Hinweis: Wenn Sie ein Festplattenspeichergerät verwenden, um den lokalen Backup Exec-Server wiederherzustellen, schließen Sie das ursprüngliche Festplattenspeichergerät nicht ein. Sorgen Sie dabei dafür, dass zwischen dem Speichergerät für die Wiederherstellung und dem ursprünglichen Speichergerät kein Konflikt verursacht wird.

4. Klicken Sie auf der Registerkarte "Speicher" auf "Inventar und Katalog", um Medien zu inventarisieren und zu katalogisieren, die die neuesten vollständigen, inkrementellen und differenziellen Backups des wiederherzustellenden Computers enthalten.
5. Wählen Sie die Registerkarte "Backup und Wiederherstellung" und klicken Sie dann auf "Wiederherstellen".
6. Sie haben folgende Möglichkeiten:

- Wenn die Wiederherstellungsmethode "Vollständige Online-Wiederherstellung eines Computers oder Wiederherstellen von Systemkomponenten" verfügbar ist, führen Sie folgende Schritte in der angegebenen Reihenfolge durch:
 - Klicken Sie auf "Vollständige Online-Wiederherstellung eines Computers oder Wiederherstellen von Systemkomponenten" und dann auf "Weiter".
 - Klicken Sie auf "Ein Windows-Computer, der vollständig für ein Backup ausgewählt wurde" und anschließend auf "Weiter".
 - Wählen Sie die Backup-Sätze aus, die Sie wiederherstellen möchten, und klicken Sie dann auf "Weiter".
 - Stellen Sie sicher, dass Sie die Auswahl des Speicherorts für die Wiederherstellung aufheben, in dem sich die Backup-Dateien des Festplattenspeichergeräts befanden, da sie ansonsten überschrieben werden. Anwendungen und Datenlaufwerke können später wiederhergestellt werden, sobald die Serverwiederherstellung abgeschlossen ist.
 - Vergewissern Sie sich, dass die Option "Vorhandene Dateien überschreiben" aktiviert ist. Akzeptieren Sie die dann die Standardeinstellungen im Bereich "Wie sollen die Dateiintegrität, -hierarchie und -sicherheit für wiederhergestellte Daten beibehalten werden".
 - Klicken Sie auf "Weiter".
 - Klicken Sie im Bereich "Wie sollen die Betriebssystemkomponenten wiederhergestellt werden?" auf "Weiter".
 - Für eine autoritative Wiederherstellung eines Domänencontrollers aktivieren Sie im Bereich "Wie sollen die Systemstatusdaten wiederhergestellt werden?" die Option "Bei Wiederherstellung von SYSVOL im Systemstatus diesen Server zum primären Vermittler für die Replikation bestimmen".
 - Aktivieren Sie im Bereich "Welche zusätzlichen Aufgaben möchten Sie vor und/oder nach einer Wiederherstellung ausführen?" die gewünschten Aufgaben und klicken Sie dann auf "Weiter".
 - Erstellen Sie einen Zeitplan zum Ausführen des Auftrags und klicken Sie auf "Weiter".
 - Klicken Sie im Bereich "Wiederherstellungsübersicht" auf "Fertigstellen".
 - Starten Sie den Computer nach Abschluss der Wiederherstellung nicht neu.

- Wenn die Wiederherstellungsmethode "Vollständige Online-Wiederherstellung eines Computers oder Wiederherstellen von Systemkomponenten" nicht verfügbar ist, erstellen Sie einen Wiederherstellungsauftrag und wählen Sie die wiederherzustellenden Systemkomponenten manuell aus. Starten Sie den Computer nach Abschluss der Wiederherstellung nicht neu.
7. Das Betriebssystem des Computers befindet sich jetzt zwar in dem Zustand vor dem Notfall, starten Sie ihn aber noch nicht neu. Die Datendateien, mit Ausnahme jener, die von Backup Exec-Datenbank-Agents geschützt werden, wurden wiederhergestellt.
- Führen Sie dann eine der folgenden Aufgaben aus:
- Wenn Sie eine autoritative Wiederherstellung eines Domänencontrollers ausführen möchten, springen Sie zu Schritt 8.
 - Wenn Sie einen eigenständigen Server wiederherstellen oder eine nicht autoritative Wiederherstellung eines Domänencontrollers ausführen möchten, ist die Wiederherstellung abgeschlossen. Starten Sie den Computer nach Abschluss des Wiederherstellungsauftrags neu. Wenn Sie die Dateien des Festplattenspeichergeräts zum Wiederherstellen in einen anderen Speicherort kopiert haben, können Sie sie entfernen. Springen Sie zu Schritt 9, um dieses Vorgang abzuschließen.
8. So führen Sie eine autoritative Wiederherstellung eines Domänencontrollers aus

Hinweis: Stellen Sie sicher, dass der Computer nach der Wiederherstellung im Modus "Verzeichnisdienstwiederherstellung" neu gestartet wird. Andernfalls wird eventuell das Active Directory repliziert, sobald die Active Directory-Dienste online sind. Um diese Replizierung zu verhindern, können Sie den Computer vorübergehend vom Netzwerk trennen.

- Drücken Sie F8 während des Starts. Ein Menü mit einer Auswahl möglicher Anmeldeverfahren wird angezeigt, mit dem die Startprobleme diagnostiziert und behoben werden können.
- Wählen Sie "Verzeichnisdienstwiederherstellung".
- Loggen Sie sich mit Ihren DSRM-Identifikationsdaten ein.
- Öffnen Sie eine Eingabeaufforderung.
- Geben Sie "NTDSUTIL" ein und drücken Sie die Eingabetaste. Weitere Informationen zum Ausführen von NTDSUTIL für Windows-Server finden Sie in der Microsoft-Dokumentation.

- Geben Sie `Activate Instance NTDS` ein und drücken Sie die Eingabetaste.
- Geben Sie `"Authoritative Restore"` ein und drücken Sie die Eingabetaste.
- Geben Sie den folgenden Befehl ein und drücken Sie die Eingabetaste :
`restore subtree ou=OE_Name,dc=Domänenname,dc=xxx`
Dabei ist `<OE_Name>` der Name der wiederherzustellenden Organisationseinheit, `<Domänenname>` die Domäne, in der sich die Organisationseinheit befindet und `<xxx>` ist der Top-Level-Domänenname des Domänencontrollers (z. B. `.com`, `.org` oder `.net`).
- Wiederholen Sie diese Schritte für die restlichen Objekte, die Sie wiederherstellen müssen.
- Beenden Sie NTDSUTIL, nachdem Sie die Wiederherstellung von Active Directory-Daten abgeschlossen haben.
- Starten Sie den Computer neu.

Hinweis: Wenn Sie die Dateien des Festplattenspeichergeräts zum Wiederherstellen in einen anderen Speicherort kopiert haben, können Sie sie entfernen.

9. Wenn Sie Backup Exec starten, werden Sie aufgefordert, die Datei mit dem Datenbankverschlüsselungscode anzugeben. So importieren Sie die Datei mit dem Datenbankverschlüsselungscode
 - Suchen Sie die Datei mit dem Datenbankverschlüsselungscode in dem Speicherort, in dem Sie er gesichert wurde. Backup Exec gibt den Namen des Schlüssels an, der wiederhergestellt werden muss.
 - Kopieren Sie die Datei und fügen Sie sie im Unterordner "Data" des Installationsordners von Backup Exec ein.
 - Loggen Sie sich bei Backup Exec ein.

Manuelles Ausführen der Notfallwiederherstellung eines Remote-Backup Exec-Servers oder Remote-Agent auf einem Windows-Computer

Dieses Verfahren stellt das Betriebssystem des Computers auf den Zustand vor dem Notfall wieder her. Dabei werden auch Ihre Datendateien wiederhergestellt, mit Ausnahme derjenigen, die durch einen Backup Exec-Agent, wie zum Beispiel den Agent for Microsoft Exchange Server, geschützt werden. Wenn Daten von

Backup Exec-Agents geschützt werden, lesen Sie im Backup Exec-Administratorhandbuch den Abschnitt zum Wiederherstellen der vom Agent geschützten Daten, bevor Sie die Notfallwiederherstellung starten. Stellen Sie die vom Agent geschützten Daten wieder her, wenn die Systemwiederherstellung abgeschlossen ist. Dieses Verfahren enthält die (nicht) autoritative Wiederherstellung von Active Directory für einen Domänencontroller.

Diese Schritte sind nur für die manuelle Notfallwiederherstellung gedacht. Wenn Simplified Disaster Recovery (SDR) für den Computer aktiviert ist, sollten Sie SDR für die Notfallwiederherstellung verwenden.

Die folgenden Elemente sind für die manuelle Notfallwiederherstellung eines Remote-Computers erforderlich:

- Ein aktuelles vollständiges Backup des Computers, dessen Betriebsfähigkeit wiederhergestellt werden soll, und alle nachfolgenden inkrementellen bzw. Differenzial-Backups.
- Das Windows-Installationsmedium
- Der Datenbankverschlüsselungscode, der zum Schützen der Backup Exec-Datenbank verwendet wurde. Sie müssen den Code in einen sicheren Speicherort exportieren und dann abrufen, um die Wiederherstellung abzuschließen.
- Wenn Sie eine autoritative Wiederherstellung auf einem Domänencontroller durchführen möchten, benötigen Sie DSRM-Identifikationsdaten.

Hinweis: Wenn Sie einen Windows-Computer wiederherstellen, bei dem BitLocker-Verschlüsselung aktiviert ist, muss diese nach der Wiederherstellung erneut aktiviert werden. Weitere Informationen zur BitLocker-Laufwerksverschlüsselung finden Sie in der Microsoft-Dokumentation.

Während dieses Verfahrens sollten Sie sich immer mit einem Konto mit Administrator- oder äquivalenten Rechten bei Windows einloggen.

So führen Sie die Notfallwiederherstellung eines Remote-Backup Exec-Servers oder Remote-Agent auf einem Windows-Computer manuell aus

1. Auf dem Remote-Computer installieren Sie die ursprüngliche Windows-Version. Installieren Sie anschließend dieselben Service Packs und Patches, die vorher installiert waren. Beachten Sie Folgendes:
 - Soll der Computer nach einem vollständigen Festplattenausfall wiederhergestellt werden, verwenden Sie das Windows-Setup, um den neuen Datenträger während der Installation zu partitionieren und zu formatieren. Diese Installation von Windows ist notwendig, damit Backup

Exec ein Ziel für die Wiederherstellung des Systems hat. Der Computernamen, das Windows-Verzeichnis und das Dateisystem (z. B. NTFS) müssen mit denen der vorherigen Windows-Installation übereinstimmen. Diese Grundinstallation wird durch die gesicherte Version überschrieben, die die Systemkonfiguration, die Anwendungseinstellungen und die Sicherheitseinstellungen wiederherstellt.

- Wenn der Computer ein Domänencontroller in einer bestimmten Domäne oder Arbeitsgruppe war, treten Sie der Domäne oder Arbeitsgruppe nicht bei. Klicken Sie im Dialogfeld "Computernamen ändern" auf "Mehr...", um manuell ein Domänensuffix an den Computernamen anzuhängen, das dem ursprünglichen Domänen- oder Arbeitsgruppensuffix entspricht.

Ändern Sie den neuen Computernamen in den ursprünglichen Namen, indem Sie folgende Schritte in der angegebenen Reihenfolge ausführen:

- Klicken Sie unter "Systemeigenschaften" auf der Registerkarte "Computernamen" auf "Ändern".

Hinweis: Wenn die Domäne oder Arbeitsgruppe verbunden ist, müssen Sie die Vertrauensbeziehung nach der Wiederherstellung und dem Neustart wiederherstellen.

- Klicken Sie im Dialogfeld "Computernamen- bzw. -domänenänderungen" auf "Mehr".
 - Bei Bedarf aktivieren Sie das Kontrollkästchen "Primäres DNS-Suffix bei Domänenmitgliedschaftsänderung ändern" und klicken Sie dann auf "OK".
 - Starten Sie den Computer neu.
2. Installieren Sie auf dem Backup Exec-Server den Backup Exec Agent for Windows auf dem Remote-Computer.

Hinweis: Nach der Wiederherstellung muss das Backup Exec-Login-Konto aktualisiert werden und das Vertrauen von Backup Exec muss für den wiederhergestellten Remote-Server wieder aufgebaut werden.

3. Wählen Sie auf der Registerkarte "Backup und Wiederherstellung" den Namen des Computers aus und klicken Sie dann auf "Wiederherstellen".
4. Sie haben folgende Möglichkeiten:

Wenn die Wiederherstellungsmethode "Vollständige Online-Wiederherstellung eines Computers oder Wiederherstellen von Systemkomponenten" verfügbar ist, führen Sie folgende Schritte in der angegebenen Reihenfolge durch:

- Klicken Sie auf "Vollständige Online-Wiederherstellung eines Computers oder Wiederherstellen von Systemkomponenten" und dann auf "Weiter".
 - Klicken Sie auf "Ein Windows-Computer, der vollständig für ein Backup ausgewählt wurde" und anschließend auf "Weiter".
 - Wählen Sie den Zeitpunkt aus, um sicherzustellen, dass nur der kritische Satz ausgewählt wird, und klicken Sie dann auf "Weiter".
 - Aktivieren Sie die Option "Am ursprünglichen Speicherort" und klicken Sie auf "Weiter".
 - Vergewissern Sie sich, dass die Option "Vorhandene Dateien überschreiben" aktiviert ist. Akzeptieren Sie die dann die Standardeinstellungen im Bereich "Wie sollen die Dateintegrität, -hierarchie und -sicherheit für wiederhergestellte Daten beibehalten werden".
 - Klicken Sie auf "Weiter".
 - Für eine autoritative Wiederherstellung eines Domänencontrollers aktivieren Sie im Bereich "Wie sollen die Systemstatusdaten wiederhergestellt werden?" die Option "Bei Wiederherstellung von SYSVOL im Systemstatus diesen Server zum primären Vermittler für die Replikation bestimmen".
 - Wählen Sie im Fenster "Welche zusätzlichen Aufgaben möchten Sie vor und/oder nach einer Wiederherstellung durchführen?" auf alle zusätzlichen Aufgaben, die vor oder nach einer Wiederherstellung ausgeführt werden sollen, und anschließend auf "Weiter".
 - Erstellen Sie einen Zeitplan zum Ausführen des Auftrags und klicken Sie auf "Weiter".
 - Klicken Sie im Bereich "Wiederherstellungsübersicht" auf "Fertigstellen".
 - Starten Sie den Computer nicht neu.
Wenn die Wiederherstellungsmethode "Vollständige Online-Wiederherstellung eines Computers oder Wiederherstellen von Systemkomponenten" nicht verfügbar ist, erstellen Sie einen Wiederherstellungsauftrag und wählen Sie die wiederherzustellenden Systemkomponenten manuell aus. Starten Sie den Computer nicht neu.
5. Das Betriebssystem des Computers befindet sich jetzt zwar in dem Zustand vor dem Notfall, starten Sie ihn aber noch nicht neu. Die Datendateien, mit Ausnahme jener, die von Backup Exec-Datenbank-Agents geschützt werden, wurden wiederhergestellt.

Führen Sie dann eine der folgenden Aufgaben aus:

- Wenn Sie eine autoritative Wiederherstellung eines Domänencontrollers ausführen möchten, springen Sie zu Schritt 6.
 - Wenn Sie einen eigenständigen Server wiederherstellen oder eine nicht autoritative Wiederherstellung eines Domänencontrollers ausführen möchten, ist die Wiederherstellung abgeschlossen. Starten Sie den Computer nach Abschluss des Wiederherstellungsauftrags neu. Springen Sie zu Schritt 7, um dieses Vorgang abzuschließen.
6. So führen Sie eine autoritative Wiederherstellung eines Domänencontrollers aus

Hinweis: Stellen Sie sicher, dass der Computer nach der Wiederherstellung im Modus "Verzeichnisdienstwiederherstellung" neu gestartet wird. Andernfalls wird eventuell das Active Directory repliziert, sobald die Active Directory-Dienste online sind. Um diese Replizierung zu verhindern, können Sie den Computer vorübergehend vom Netzwerk trennen.

- Drücken Sie F8 während des Starts. Ein Menü mit einer Auswahl möglicher Anmeldeverfahren wird angezeigt, mit dem die Startprobleme diagnostiziert und behoben werden können.
- Wählen Sie "Verzeichnisdienst-Wiederherstellungsmodus".
- Loggen Sie sich mit Ihren DSRM-Identifikationsdaten ein.
- Öffnen Sie eine Eingabeaufforderung.
- Geben Sie `"NTDSUTIL"` ein und drücken Sie die Eingabetaste. Weitere Informationen zum Ausführen von NTDSUTIL für Windows-Server finden Sie in der Microsoft-Dokumentation.
- Geben Sie `Activate Instance NTDS` ein und drücken Sie die Eingabetaste.
- Geben Sie `"Authoritative Restore"` ein und drücken Sie die Eingabetaste.
- Geben Sie den folgenden Befehl ein und drücken Sie die Eingabetaste :

```
restore subtree ou=OE_Name,dc=Domänenname,dc=xxx
```

Dabei ist `<OE_Name>` der Name der wiederherzustellenden Organisationseinheit, `<Domänenname>` die Domäne, in der sich die Organisationseinheit befindet und `<xxx>` ist der Top-Level-Domänenname des Domänencontrollers (z. B. `.com`, `.org` oder `.net`).
- Wiederholen Sie diese Schritte für die restlichen Objekte, die Sie wiederherstellen müssen.

- Beenden Sie NTDSUTIL, nachdem Sie die Wiederherstellung von Active Directory-Daten abgeschlossen haben.
 - Starten Sie den Computer neu.
7. Wenn Sie Backup Exec starten, werden Sie aufgefordert, die Datei mit dem Datenbankverschlüsselungscode anzugeben.
- So importieren Sie die Datei mit dem Datenbankverschlüsselungscode
- Suchen Sie die Datei mit dem Datenbankverschlüsselungscode in dem Speicherort, in dem Sie er gesichert wurde. Backup Exec gibt den Namen des Schlüssels an, der wiederhergestellt werden muss.
 - Kopieren Sie die Datei und fügen Sie sie im Unterordner "Data" des Installationsordners von Backup Exec ein.
8. Loggen Sie sich bei Backup Exec ein.

Integration in Veritas™ Information Map

In diesem Kapitel werden folgende Themen behandelt:

- [Info zu Veritas™ Information Map](#)
- [Zusammenarbeit von Backup Exec und Veritas™ Information Map](#)
- [Anforderungen für die Integration in Veritas™ Information Map](#)
- [Integration von Backup Exec in Veritas™ Information Map](#)
- [Unterstützte Datenquellen bei der Integration in Veritas™ Information Map](#)
- [Best Practices für die Integration in Veritas™ Information Map](#)
- [Tipps zur Fehlerbehebung bei der Integration in Veritas™ Information Map](#)
- [Einschränkungen für die Integration in Veritas™ Information Map](#)

Info zu Veritas™ Information Map

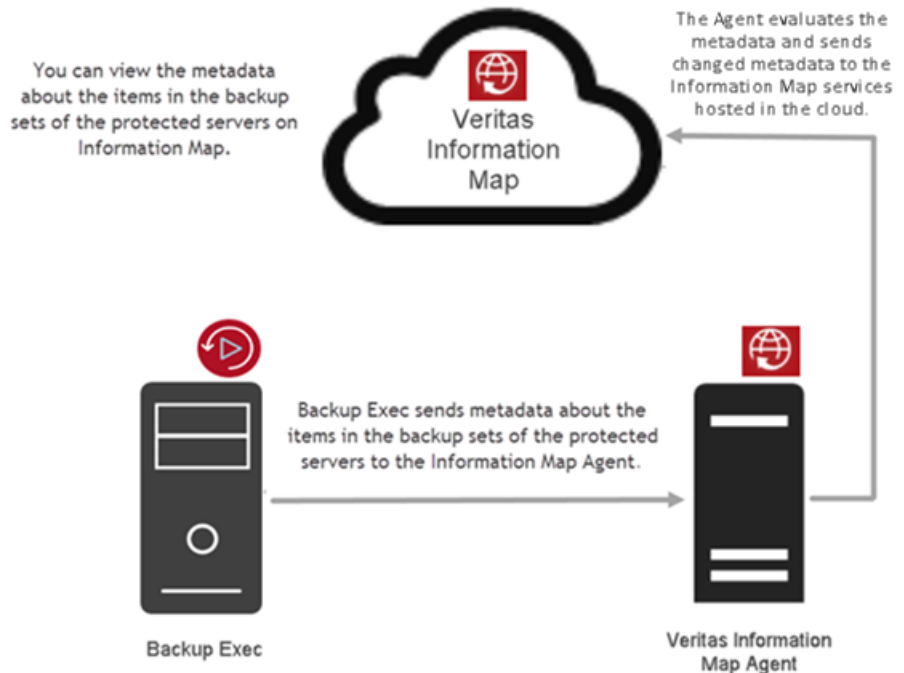
Veritas™ Information Map stellt Ihre unstrukturierten Daten in einem visuellen Kontext dar und hilft Benutzern, objektive, auf Daten beruhende Entscheidungen zu treffen. Mithilfe der dynamischen Navigationsfunktion in Information Map können Kunden Risiko-, Wertschöpfungs- und Verschwendungsbereiche in ihrer Umgebung identifizieren und Entscheidungen treffen, die Datenrisiken mindern und Datenspeicher optimieren.

Weitere Informationen finden Sie in der Dokumentation zu Veritas™ Information Map.

http://veritashelpsupport.com/Welcome?locale=EN_US&context=INFOMAP1.0

Zusammenarbeit von Backup Exec und Veritas™ Information Map

Backup Exec sendet Metadaten zu Elementen in den Backup-Sätzen der geschützten Server an den Information Map-Agent. Der Agent bewertet die Metadaten, die von Backup Exec gesendet werden, und sendet geänderte Metadaten an die Information Map-Dienste in der Cloud.



Anforderungen für die Integration in Veritas™ Information Map

Folgende Anforderungen gelten für das Integrieren von Backup Exec in Veritas™ Information Map.

- Information Map zeigt Metadaten nur für die Server an, die in einer Domäne konfiguriert sind.

- Server, die mit CIFS-Backups geschützt werden (es ist kein Remote-Agent auf dem Server installiert, z. B. eine NAS-Box): Gewährleisten Sie, dass der Server mit seinem FQDN in Backup Exec hinzugefügt wird.
- Bei Servern, auf denen der Remote-Agent installiert ist, kann Backup Exec den FQDN bestimmen, unabhängig davon, wie der Server in Backup Exec hinzugefügt wurde.
- Wenn bei der CAS-MMS-Bereitstellung der CAS-Server beim Information Map-Agent registriert ist, muss der Verschlüsselungscode für Backup-Sätze auf dem CAS-Server verfügbar sein, damit Metadaten über solche Backup-Sätze gesendet werden.
- Informationen zu Betriebssystemanforderungen zum Installieren von Information Map finden Sie in der Dokumentation zu Information Map.
http://veritashelpsupport.com/Welcome?locale=EN_US&context=INFOMAP1.0
- Für das Bereitstellen von CAS-MMS müssen Sie die Registrierung beim Information Map-Agent über den CAS-Server ausführen. Backup Exec sendet Metadaten auf Elementebene aus allen Servern in der CAS-MMS-Bereitstellung. Die Registrierung beim Information Map-Agent über die MMS-Server ist nicht erforderlich.
- Wenn die CAS-MMS im Modus "Verteilter Katalog" konfiguriert ist und sich der Backup-Satz auf MMS befindet und Backup-Satz aus CAS gescannt wird, wird auf dem CAS-Server eine temporäre Datei mit Scanaufgabeninformationen erstellt.
Stellen Sie sicher, dass auf C: des CAS-Servers ausreichend Speicherplatz verfügbar ist. Die erforderliche Größe ist abhängig von der Anzahl der Elemente im Backup-Satz. Beispiel: Der Speicherbedarf für 6 Millionen Elemente im Backup-Satz beträgt ca. 100 GB auf dem Laufwerk C: des CAS-Servers.

Integration von Backup Exec in Veritas™ Information Map

Zur Integration in Backup Exec müssen Sie die folgenden Schritte durchführen:

So integrieren Sie Information Map

- 1 Bereiten Sie die Information Map-Bereitstellung mit einem Mandanten vor. Wenden Sie sich an Veritas, wenn ein Mandant in Information Map bereitgestellt werden soll. Weitere Informationen finden Sie in der Dokumentation zu Information Map.

http://veritashelpsupport.com/Welcome?locale=EN_US&context=INFOMAP1.0

- 2 Installieren und Konfigurieren des Information Map-Agent

Lesen Sie die Systemanforderungen zum Installieren des Information Map-Agent.

Wenn Sie den Information Map-Agent installieren, notieren Sie sich die Port-Nummer, damit Sie diese für die Konfiguration der Installation Map-Einstellungen in Backup Exec verwenden können.

Stellen Sie beim Installieren des Information Map-Agent sicher, dass in der Option "Freigegebener Datenspeicherort" eine Netzwerkfreigabe angegeben ist. Wenn der Information Map-Agent deinstalliert oder erneut installiert wird, gehen die Cache-Informationen aus der vorherigen Installation nicht verloren und können wieder verwendet werden.

Der Information Map-Agent wird lokal installiert und ist für das Senden von Daten an Information Map verantwortlich. Backup Exec kommuniziert mit dem Information Map-Agent.

Ausführliche Informationen finden Sie in der Dokumentation zu Information Map.

http://veritashelpsupport.com/Welcome?locale=EN_US&context=INFOMAP1.0

- 3 Konfigurieren von Backup Exec für die Integration in Information Map.

Gehen Sie dazu in folgender Reihenfolge vor:

- Installieren und konfigurieren Sie Backup Exec.
- Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie "Konfiguration und Einstellungen > Backup Exec-Einstellungen > Veritas Information Map".
- Konfigurieren Sie die Einstellungen für Information Map in der Backup Exec-Konsole.
Siehe "[Konfigurieren der Einstellungen für Veritas™ Information Map](#)" auf Seite 759.

Nachdem Sie diese Schritte ausgeführt haben, ist Backup Exec beim Information Map-Agent registriert.

4 Verwalten Sie Information Map-Einstellungen in der Veritas™ Information Map.

Die von Backup Exec geschützten Server sind in der Information Map-Konsole verfügbar. Aktivieren Sie die Server, deren Element-Metadaten in Information Map angezeigt werden sollen. Es dauert möglicherweise eine Weile, bis die Daten für die aktivierten Server in der Information Map-Konsole angezeigt werden.

Wenn Sie eine große Anzahl von Servern haben, für die Metadaten auf Elementebene an Information Map gesendet werden sollen, wird empfohlen, dass Sie nicht alle Server auf einmal sondern in Gruppen aktivieren. Aktivieren Sie die Server, nachdem ein vollständiges Backup ausgeführt wurde. Beispiel: Wenn Sie zehn Server haben, können Sie zuerst drei Server aktivieren, dann weitere drei usw.

Im Veritas Connection Center (VCC) konfigurieren Sie die Einstellungen für den Backup Exec-Server auf der Registerkarte "Verbindungen". Aktualisieren Sie den Zeitplan in Information Map, um festzulegen, wie häufig Backup Exec Metadaten zu Elementen in den Backup-Sätzen an Information Map senden soll.

Konfigurieren Sie den Scan-Zeitplan im Veritas Connection Center so, dass er außerhalb des Backup-Zeitfensters liegt.

Backup Exec sendet Metadaten zu Elementen in den Backup-Sätzen der geschützten Server an Information Map. Sie können in Information Map die Einstellungen an Ihre Anforderungen anpassen. Wählen Sie "Information Map > Verwaltung > Globale Einstellungen" und legen Sie veraltete Daten, Elementtypen, Erweiterungen usw. fest. Ausführliche Informationen finden Sie in der Dokumentation zu Information Map.

http://veritashelpsupport.com/Welcome?locale=EN_US&context=INFOMAP1.0

5 Basierend auf dem in VCC konfigurierten Zeitplan ruft Backup Exec regelmäßig Erkennungs- und Scanaufgaben vom Information Map-Agent ab.

Die Standardhäufigkeit dafür beträgt 30 Minuten.

- Im Rahmen einer Erkennungsaufgabe sendet Backup Exec Informationen dazu, wie viele Server und Ressourcen geschützt werden.
- Im Rahmen einer Scanaufgabe sendet Backup Exec Metadaten zu Elementen in den Backup-Sätzen der geschützten und aktivierten Server an Information Map.

Ist eine Kette von Backup-Sätzen (ein Satz für das vollständige Backup und mindestens einer für inkrementelle/differenzielle Backups) für einen geschützten Server vorhanden, sendet Backup Exec zuerst Metadaten auf Elementebene im Satz für das vollständige Backup. Die Sätze für

inkrementelle bzw. differenzielle Backups werden gemeinsam beim nächsten Scan verarbeitet.

Backup Exec zeigt Informations- und Fehlermeldungen in der Konsole für die Erkennungs- und Scanaufgabe. Weitere Informationen zu den Erkennungs- und Scanaufgaben von Information Map finden Sie in den Information Map-Warnmeldungen in der Konsole. Diese Warnmeldungen enthalten auch Informationen dazu, wie viele Server erkannt wurden, und welche Backup-Sätze von Backup Exec gescannt wurden.

Weitere Informationen finden Sie in der Dokumentation zu Information Map.

http://veritashelpsupport.com/Welcome?locale=EN_US&context=INFOMAP1.0

Unterstützte Datenquellen bei der Integration in Veritas™ Information Map

Folgende Datenquellen werden bei der Integration in Veritas™ Information Map unterstützt

- Dateisysteme, die von Backup Exec unterstützt werden. Beispiele: NTFS, ext2, ext3.
- NDMP-Dateiserver
- Windows-Freigaben

Best Practices für die Integration in Veritas™ Information Map

Best Practices sind Tipps und Empfehlungen, die Ihnen helfen können, Backup Exec mit Information Map richtig zu verwenden.

- Stellen Sie beim Installieren des Information Map-Agent sicher, dass in der Option "Freigegebener Datenspeicherort" eine standortferne Freigabe angegeben ist. Wenn der Information Map-Agent deinstalliert oder erneut installiert wird, gehen die Cache-Informationen aus der vorherigen Installation nicht verloren und können wieder verwendet werden.

Weitere Informationen zum Installieren und Konfigurieren des Information Map-Agent finden Sie in der Dokumentation zu Veritas™ Information Map.

http://veritashelpsupport.com/Welcome?locale=EN_US&context=INFOMAP1.0

- Um die Last auf dem Backup Exec-Server zu beschränken und den Information Map-Agent für unterschiedliche Information Map-Datenspeicher verwenden zu

können, wird empfohlen, dass Sie den Information Map-Agent auf einem anderen Computer installieren.

- Wenn Sie Metadaten zu geschützten Daten eines virtuellen Agent senden möchten, müssen die Backup-Aufträge mit der entsprechenden Option auf der Registerkarte "Instant GRT" konfiguriert sein. Wählen Sie "Konfiguration und Einstellungen > Auftragsstandardeinstellungen > Backup auf Festplatte > Instant GRT". Wählen Sie auf dieser Registerkarte eine der folgenden Optionen aus:
 - Vollständige Katalogisierung sofort nach Abschluss des Backup-Auftrags als separaten Auftrag ausführen
 - Vollständige Katalogisierung nach Abschluss des Backup-Auftrags als separaten Auftrag planen
- Stellen Sie sicher, dass die im Bereich "Katalog" ausgewählte Dauer länger ist als die Dauer, die Sie für das Senden von Metadaten auf Elementebene über die innerhalb der festgelegten Anzahl von Tagen erstellten Backup-Sätze an Information Map festgelegt haben. Das Ändern der Katalogeinstellung erfolgt in "Konfiguration und Einstellungen > Backup Exec-Einstellungen > Katalog > Kataloge kürzen nach".
 Wenn beispielsweise für die Option "Kataloge kürzen nach" der Wert "60 Tage" angegeben ist, müssen Sie für die Option "Metadaten zu den im angegebenen Zeitraum erstellten Backup-Sätzen senden" eine Dauer von weniger als 60 Tagen auswählen.
- Konfigurieren Sie den Scan-Zeitplan im Veritas Connection Center so, dass er außerhalb des Backup-Zeitfensters liegt.
- Wenn Sie eine große Anzahl von Servern haben, für die Metadaten auf Elementebene an Information Map gesendet werden sollen, wird empfohlen, dass Sie nicht alle Server auf einmal sondern in Gruppen aktivieren. Aktivieren Sie die Server, nachdem ein vollständiges Backup ausgeführt wurde. Beispiel: Wenn Sie zehn Server haben, können Sie zuerst drei Server aktivieren, dann weitere drei usw.

Tipps zur Fehlerbehebung bei der Integration in Veritas™ Information Map

Wenn Sie Probleme mit Veritas™ Information Map in Backup Exec haben, lesen Sie folgende Punkte:

- Wenn Sie Backup Exec deinstallieren, werden Sie gefragt, ob Informationen aus Backup Exec beibehalten oder gelöscht werden sollen. Wenn Sie Informationen beibehalten, werden Servername, Port und Login-Kontoinformationen für den Information Map-Agent gespeichert. Das

Agent-Zertifikat wird auch im Windows-Zertifikatsspeicher beibehalten. Wenn Sie das Löschen von Informationen auswählen, werden alle Daten zum Information Map-Agent entfernt, ebenso das Agent-Zertifikat aus dem Windows-Zertifikatsspeicher.

- Wenn das Information Map-Agent-Zertifikat erneuert oder geändert wird, muss Backup Exec wieder beim Information Map-Agent registriert und die Vertrauenswürdigkeit durch erneute Verifizierung hergestellt werden. Eine Meldung wird angezeigt, dass das Zertifikat geändert wurde. Klicken Sie im Bereich "Konfiguration und Einstellungen > Backup Exec-Einstellungen > Veritas Information Map" auf "Aktualisieren" und verifizieren Sie das Zertifikat, um die Vertrauenswürdigkeit herzustellen.

- Wenn Backup Exec auf einem Windows Server 2008-Server installiert ist, wird eventuell folgender Fehler während der Registrierung beim Information Map-Agent-Server angezeigt:

Es konnte kein geschützter SSL/TLS-Kanal erstellt werden.

Um diesen Fehler zu beheben, aktivieren Sie TLS 1.2. Führen Sie die Schritte im folgenden Artikel in der angegebenen Reihenfolge aus.

<https://support.Microsoft.com/kb/4019276>

- Backup Exec kann keine Verbindung mit dem Information Map-Agent-Connector-Dienst herstellen.
Wenn ein Protokoll, ähnlich dem im folgenden Beispiel, in den Management-Dienstprotokollen auftaucht, konnte Backup Exec keine Verbindung zum Information Map-Agent-Connector-Dienst herstellen. Gewährleisten Sie, dass der Dienst aktiv ist.

Fehler beim Senden von HeartBeat-Daten:

```
MANAGEMENT: [10/26/17 23:07:02] [0029] 10/26
23:07:01.882[InfoMapConne] Sending HeartBeat to InfoMap agent on
10.217.193.169

MANAGEMENT: [10/26/17 23:07:02] [0029] 10/26
23:07:01.978[InfoMapConne] ERROR:Using password to authenticate
during first request

MANAGEMENT: [10/26/17 23:07:03] [0029] 10/26
23:07:03.109[InfoMapConne] ERROR:Exception during sending request.

MANAGEMENT: [10/26/17 23:07:03] [0029] 10/26
23:07:03.109[InfoMapConne] ERROR: Exception Message: Unable to
connect to the remote server

MANAGEMENT: [10/26/17 23:07:03] [0029] 10/26
23:07:03.109[InfoMapConne] ERROR: Exception Status: ConnectFailure

MANAGEMENT: [10/26/17 23:07:03] [0029] 10/26
23:07:03.109[InfoMapConne] ERROR:Retrying after 20000 ms.
```

```

MANAGEMENT: [10/26/17 23:07:23] [0029] 10/26
23:07:23.122[InfoMapConne] ERROR:Using password to authenticate
during retry
MANAGEMENT: [10/26/17 23:07:24] [0029] 10/26
23:07:24.134[InfoMapConne] ERROR:Exception during sending request.
MANAGEMENT: [10/26/17 23:07:24] [0029] 10/26
23:07:24.134[InfoMapConne] ERROR: Exception Message: Unable to
connect to the remote server
MANAGEMENT: [10/26/17 23:07:24] [0029] 10/26
23:07:24.134[InfoMapConne] ERROR: Exception Status: ConnectFailure
MANAGEMENT: [10/26/17 23:07:24] [0029] 10/26
23:07:24.134[InfoMapConne] ERROR:Retrying after 20000 ms.
MANAGEMENT: [10/26/17 23:07:44] [0029] 10/26
23:07:44.149[InfoMapConne] ERROR:Using password to authenticate
during retry
MANAGEMENT: [10/26/17 23:07:45] [0029] 10/26
23:07:45.152[InfoMapConne] ERROR:Exception during sending request.
MANAGEMENT: [10/26/17 23:07:45] [0029] 10/26
23:07:45.152[InfoMapConne] ERROR: Exception Message: Unable to
connect to the remote server
MANAGEMENT: [10/26/17 23:07:45] [0029] 10/26
23:07:45.152[InfoMapConne] ERROR: Exception Status: ConnectFailure
MANAGEMENT: [10/26/17 23:07:45] [0029] 10/26
23:07:45.152[InfoMapConne] ERROR:Retrying after 20000 ms.
MANAGEMENT: [10/26/17 23:08:05] [0029] 10/26
23:08:05.165[InfoMapConne] ERROR:Using password to authenticate
during retry
MANAGEMENT: [10/26/17 23:08:06] [0029] 10/26
23:08:06.185[InfoMapConne] ERROR:Exception during sending request.
MANAGEMENT: [10/26/17 23:08:06] [0029] 10/26
23:08:06.185[InfoMapConne] ERROR: Exception Message: Unable to
connect to the remote server
MANAGEMENT: [10/26/17 23:08:06] [0029] 10/26
23:08:06.185[InfoMapConne] ERROR: Exception Status: ConnectFailure
MANAGEMENT: [10/26/17 23:08:06] [0029] 10/26
23:08:06.189[InfoMapConne] Web Exception in
ConnectorManagerHeartBeatTask: Message: Unable to connect to the
remote server

```

Fehler beim Abrufen von Aufgaben:

```

MANAGEMENT: [10/26/17 22:58:26] [0020] 10/26
22:58:26.828[InfoMapConne] Next Polling Time = 10/8/2018 5:18:27
AM, Poll Now = True, Polling Interval = 30, Task Concurrency Level
= 1, Session Time = 720, Retry Count = 3, Retry Wait = 20000,
HeartBeat Interval = 60, Conn Timeout Secs = 100, Read Write
Timeout Secs = 630
MANAGEMENT: [10/26/17 22:58:31] [0021] 10/26
22:58:31.109[InfoMapConne] Polling for InfoMap jobs, ConnectorId:
8ba84bda-1876-4ca6-92b6-1d6b25a9fc4e
MANAGEMENT: [10/26/17 22:58:31] [0021] 10/26
22:58:31.109[InfoMapConne] GetFileNameForAlert: Current Alert File
Count: 57
MANAGEMENT: [10/26/17 22:58:31] [0021] 10/26
22:58:31.109[InfoMapConne] GetFileNameForAlert: Alert File Name:
C:\Program Files\Veritas\Backup
Exec\Data\BE-WIN2012R2_InfoMap_00058.txt
MANAGEMENT: [10/26/17 22:58:31] [0021] 10/26
22:58:31.109[InfoMapConne] ERROR:The connection time out is 100000
ms.
MANAGEMENT: [10/26/17 22:58:31] [0021] 10/26
22:58:31.109[InfoMapConne] ERROR:The read write time out is 630000
ms.
MANAGEMENT: [10/26/17 22:58:31] [0021] 10/26
22:58:31.125[InfoMapConne] ERROR:Using password to authenticate
during first request
MANAGEMENT: [10/26/17 22:58:32] [0021] 10/26
22:58:32.156[InfoMapConne] ERROR:Exception during sending request.
MANAGEMENT: [10/26/17 22:58:32] [0021] 10/26
22:58:32.156[InfoMapConne] ERROR: Exception Message: Unable to
connect to the remote server
MANAGEMENT: [10/26/17 22:58:32] [0021] 10/26
22:58:32.156[InfoMapConne] ERROR: Exception Status: ConnectFailure
MANAGEMENT: [10/26/17 22:58:32] [0021] 10/26
22:58:32.156[InfoMapConne] ERROR:Retrying after 20000 ms.

```

Eine Warnmeldung mit einer detaillierten Fehlermeldung wird immer erzeugt, wenn ein Fehler beim Ausführen einer Aufgabe auftritt. Sie können auch die Management-Dienstprotokolle mit ausführlicher Protokollierung in der Komponente "InfoMapConnector" und außerdem die Connector-Dienstprotokolle auf dem Information Map-Agent-Server prüfen.

Das Connector-Dienstprotokoll wird standardmäßig im Ordner `C:\<Backup
Exec-Installationsordner>\InformationMapAgent\connectorFramework\connectorService\cfConnectorService.log`
erstellt.

Einschränkungen für die Integration in Veritas™ Information Map

Backup Exec sendet keine Metadaten zu Backup-Sätzen, die mit einem eingeschränkten Code verschlüsselt wurden, an Information Map.

Backup Exec Agent for Windows

Dieser Anhang enthält folgende Themen:

- [Infos zum Agent for Windows](#)
- [Anforderungen für Agent for Windows](#)
- [Beenden und Starten von Agent for Windows](#)
- [Erstellen eines Vertrauensverhältnisses zwischen dem Backup Exec-Server und einem Remote-Computer](#)
- [Info zu Backup Exec Remote Agent Utility for Windows](#)
- [Verwenden des Befehlszeilen-Applet von Backup Exec Agent Utility](#)
- [Parameter für das Befehlszeilen-Applet von Backup Exec Agent Utility](#)

Infos zum Agent for Windows

Agent for Windows ermöglicht Windows-Server-Netzwerkadministratoren, Backup- und Wiederherstellungsvorgänge auf Backup Exec-Agents durchzuführen, die mit dem Netzwerk verbunden sind.

Agent for Windows ist ein Systemdienst, der auf Remote-Windows-Servern und -Arbeitsstationen ausgeführt wird. Agent for Windows ermöglicht ein schnelleres Backup, da Aufgaben, die bei anderen Backup-Technologien intensive Netzwerkinteraktionen erfordern, hier lokal vorgenommen werden. Agent for Windows verarbeitet Backup-Daten zu einem kontinuierlichen Strom, den der Backup Exec-Server dann als einzelne Aufgabe verarbeitet. Diese Methode führt zu besseren Datenübertragungsraten als bei herkömmlichen Technologien, bei

denen mehrere Anforderungen und Bestätigungen zwischen dem Backup Exec-Server und dem Remote-Server erforderlich sind.

Agent for Windows ermöglicht Ihnen Folgendes:

- Backup und Wiederherstellung in Firewall-Umgebungen
- Backup und Wiederherstellung in einem angegebenen lokalen Netzwerk, wenn Backup Exec-Server und Remote-Computer sich im selben Subnetz befinden
- Erzielen einer erheblichen Leistungsverbesserung durch modifizierte Backups (z. B. Differenzial- und inkrementelle Backups). Der Grund dafür ist, dass der Agent for Windows die Dateiauswahl lokal vornimmt und nicht über das Netzwerk, wie es bei traditionellen Backup-Technologien üblich ist.

Hinweis: Die Verarbeitungsgeschwindigkeit hängt maßgeblich von der Netzwerk-Hardware ab. Die Leistungsfähigkeit der Netzwerk-Hardware auf dem Backup Exec-Server und dem Remote-Gerät wirkt sich direkt auf die Leistung der Backup-Software aus. Eine größere Netzwerkbandbreite trägt ebenfalls unterstützend zur Leistungsverbesserung bei.

Siehe ["Anforderungen für Agent for Windows"](#) auf Seite 1029.

Siehe ["Methoden für die Installation von Agent for Windows"](#) auf Seite 77.

Siehe ["Netzwerk- und Sicherheitsoptionen für Backup Exec ändern"](#) auf Seite 713.

Siehe ["Verwendung von Backup Exec mit Firewalls"](#) auf Seite 722.

Siehe ["Shadow Copy-Dateisystemkomponenten von Backup Exec"](#) auf Seite 204.

Siehe ["Info zu Backup Exec Remote Agent Utility for Windows"](#) auf Seite 1031.

Anforderungen für Agent for Windows

Da ein Agent for Windows gleichzeitig eine Clientzugriffslizenz (Client Access License – CAL) darstellt, müssen Sie Agent for Windows auf allen Windows-Remote-Computern installieren, die Sie sichern möchten. Ressourcen auf einem Remote-Server können erst nach der Installation von Agent for Windows vollständig geschützt werden.

Auf dem Backup Exec-Server müssen Sie Agent for Windows-Lizenzen für jeden Remote-Windows-Computer eingeben, den Sie schützen möchten. Zum Sichern eines Windows-Remote-Computers von mehr als einem Backup Exec-Server müssen Sie die gleichen Agent for Windows-Lizenzen auf jedem Backup Exec-Server eingeben.

Backup Exec Agent for Applications and Databases enthält auch einen Agent for Windows, mit dem Sie einen Remote-Windows-Computer schützen können. Die Agent for Windows-Lizenz wird aktiviert, wenn Sie die Datenbank-Agents auf dem Backup Exec-Server installieren.

Um die Arbeitsstationsversionen der unterstützten Windows-Plattformen zu schützen, müssen Sie den Agent for Windows auf jeder Plattform installieren.

Die unterstützten Betriebssysteme, Plattformen und Anwendungen finden Sie in der Liste der mit Backup Exec kompatiblen Software.

Hinweis: Wenn eine vorherige Version von Agent for Windows installiert ist, wird sie automatisch aktualisiert, wenn Sie einen neuen Agent for Windows-Installation initiieren. Vorherige Versionen von Agent for Windows werden automatisch auf den Remote-Computern erkannt und durch die neue Version während der Installation des neuen Agents for Windows ersetzt. Der Name des Systemdiensts kann sich nach Abschluss der Aktualisierung eventuell geändert haben.

Sie können Agent for Windows nach unterschiedlichen Methoden installieren, je nach Ihrer Umgebung.

Siehe "[Methoden für die Installation von Agent for Windows](#)" auf Seite 77.

Beenden und Starten von Agent for Windows

Agent for Windows wird automatisch als Dienst gestartet, wenn Windows auf dem Remote-Computer gestartet wird.

So starten oder beenden Sie Agent for Windows

- 1 Öffnen Sie die Windows-Dienste.
- 2 Klicken Sie im Teilfenster "Ergebnisse" mit der rechten Maustaste auf den Dienst "Backup Exec Remote Agent for Windows".
- 3 Sie haben folgende Möglichkeiten:

So beenden Sie Agent for Windows Klicken Sie auf "Beenden".

Starten von Agent for Windows Klicken Sie auf "Starten".

Siehe "[Infos zum Agent for Windows](#)" auf Seite 1028.

Erstellen eines Vertrauensverhältnisses zwischen dem Backup Exec-Server und einem Remote-Computer

Wenn Sie eine Verbindung zwischen dem Backup Exec-Server und einem Remote-Computer herstellen, müssen Sie ein Vertrauensverhältnis zwischen dem Backup Exec-Server und dem Remote-Computer erstellen, damit die Verbindung sicher ist. Dies ist auch erforderlich, wenn Sie einen Remote-Computer für die clientseitige Deduplizierung konfigurieren möchten. Sie sollten die Identität des Remote-Computers manuell verifizieren, um sicherzustellen, dass der Remote-Computer eine vertrauenswürdige Quelle ist, bevor Sie das Vertrauen herstellen. Nachdem Sie sich vergewissert haben, dass der Remote-Computer eine vertrauenswürdige Ressource ist, können Sie das Vertrauen mit dem Backup Exec erstellen.

Backup Exec stellt ein Sicherheitszertifikat für den Backup Exec-Server und den Remote-Computer aus. Das Sicherheitszertifikat ist ungefähr ein Jahr lang gültig und wird automatisch während des Normalbetriebs verlängert. Wenn das Zertifikat abläuft, müssen Sie die Vertrauenseinstellung erneut festlegen.

Sie können ein Vertrauen zwischen dem Backup Exec-Server und dem Remote-Computer herstellen, indem Sie den Remote-Computer der Liste der Server auf der Registerkarte "Backup und Wiederherstellung" hinzufügen.

Festlegung der Vertrauenseinstellung für einen Remote-Computer

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" unter "Server und virtuelle Hosts" auf "Hinzufügen".
- 2 Klicken Sie auf "Microsoft Windows-Computer und -Server".
- 3 Befolgen Sie die Anweisungen auf dem Bildschirm.

Info zu Backup Exec Remote Agent Utility for Windows

Backup Exec Agent Utility wird installiert, wenn der Agent for Windows auf einem Remote-Windows-Computer installiert wird.

Sie können die folgenden Aufgaben mit Backup Exec Agent Utility durchführen:

- Starten Sie von Backup Exec Agent Utility bei jedem Einloggen
Siehe ["Starten von Backup Exec Agent Utility"](#) auf Seite 1032.
- Anzeigen der aktuellen Aktivität auf dem Remote-Windows-Computer

Siehe ["Anzeigen des Aktivitätsstatus von Remote-Computern in der Taskleiste"](#) auf Seite 1033.

- Konfigurieren des Agent for Windows zum Senden von Informationen (z. B. Version und IP-Adresse) an einen Backup Exec-Server
Siehe ["Info zum Veröffentlichen von Agent for Windows auf den Backup Exec-Servern"](#) auf Seite 1035.
- Konfigurieren von Backup Exec Agent Utility für Backup- und Wiederherstellungsvorgänge von Oracle-Instanzen
Siehe ["Konfigurieren einer Oracle-Instanz auf Linux-Servern"](#) auf Seite 1353.
- Konfigurieren von Backup Exec Agent Utility für Backup Exec-Server-Datenbankzugriff für Oracle-Vorgänge
Siehe ["Konfigurieren des Datenbankzugriffs für Oracle-Vorgänge"](#) auf Seite 1038.
- Entfernen des Sicherheitszertifikats für einen Backup Exec-Server
Siehe ["Entfernen von Backup Exec-Servern, auf denen Agent for Windows Informationen bereitstellen kann"](#) auf Seite 1038.

Starten von Backup Exec Agent Utility

Der Zugriff auf Backup Exec Agent Utility erfolgt über die Windows-Taskleiste.

Siehe ["Anzeigen des Aktivitätsstatus eines Remote-Computers in Backup Exec Agent Utility"](#) auf Seite 1033.

Siehe ["Info zum Veröffentlichen von Agent for Windows auf den Backup Exec-Servern"](#) auf Seite 1035.

So starten Sie Backup Exec Agent Utility

- 1 Klicken Sie auf dem Computer mit dem Agent for Windows in der Taskleiste auf "Start > Alle Programme > Veritas Backup Exec > Backup Exec Agent Utility".

Wenn Backup Exec Agent Utility ausgeführt wird, wird ein Symbol in der Taskleiste eingeblendet. Durch Doppelklicken auf das Symbol können Sie das Dienstprogramm anzeigen.
- 2 Um den Registrierungseditor, das Fenster "Dienste" und die Ereignisanzeige auf dem Remote-Windows-Computer zu öffnen, klicken Sie in der Taskleiste mit der rechten Maustaste auf das Symbol für Backup Exec Agent Utility und wählen Sie die Option "Extras".

Anzeigen des Aktivitätsstatus eines Remote-Computers in Backup Exec Agent Utility

Sie können mit Backup Exec Agent Utility den Aktivitätsstatus des Remote-Windows-Computers anzeigen.

So zeigen Sie den Aktivitätsstatus eines Remote-Computers in Backup Exec Agent Utility an

- 1 Klicken Sie auf dem Computer mit dem Agent for Windows in der Taskleiste auf "Start > Alle Programme > Veritas Backup Exec > Backup Exec Agent Utility".

Wenn Backup Exec Agent Utility bereits ausgeführt wird, können Sie auf das Symbol im Infobereich doppelklicken.

- 2 Klicken Sie auf die Registerkarte "Status".

Sie können eine der folgenden Informationen über den Windows-Remote-Computer ansehen:

Backup Exec-Server	Der Name des Backup Exec-Servers, der den aktuellen Vorgang durchführt.
Quelle	Zeigt die Medien oder die Freigabe an, die verarbeitet werden.
Aktueller Ordner	Zeigt den Namen des gerade verarbeiteten Verzeichnisses, Ordners oder der Datenbank (je nach spezifischem Agent) an.
Aktuelle Datei	Zeigt den Namen der aktuellen Datei an, die verarbeitet wird.

- 3 Klicken Sie auf "OK".

Siehe ["Info zu Backup Exec Remote Agent Utility for Windows"](#) auf Seite 1031.

Anzeigen des Aktivitätsstatus von Remote-Computern in der Taskleiste

Sie können den Aktivitätsstatus für einen Remote-Computer anzeigen.

Folgende Statusangaben sind verfügbar:

- Ein Backup-Auftrag wird ausgeführt.
- Ein Wiederherstellungsauftrag wird ausgeführt.
- Ein Backup-Auftrag und ein Wiederherstellungsauftrag werden ausgeführt.

- Ein Snapshot wird gerade erstellt.
- Der Backup Exec-Clientdienst 'Beremote.exe' wird auf dem Computer nicht ausgeführt.
- Nicht aktiv

So zeigen Sie den Aktivitätsstatus eines Remote-Computers an

- ◆ Positionieren Sie den Mauszeiger über das Symbol für den Agent for Windows in der Taskleiste.

Siehe ["Info zu Backup Exec Remote Agent Utility for Windows"](#) auf Seite 1031.

Automatisches Starten von Backup Exec Agent Utility auf dem Remote-Computer

Sie können festlegen, dass Backup Exec Agent Utility automatisch gestartet wird, wenn Sie sich beim Remote-Computer einloggen.

So legen Sie fest, dass Backup Exec Agent Utility auf dem Remote-Computer automatisch gestartet wird

- 1 Klicken Sie auf dem Computer mit dem Agent for Windows in der Taskleiste auf "Start > Alle Programme > Veritas Backup Exec > Backup Exec Agent Utility".

Wenn Backup Exec Agent Utility bereits ausgeführt wird, können Sie auf das Symbol im Infobereich doppelklicken.

- 2 Klicken Sie auf die Registerkarte "Status".
- 3 Aktivieren Sie das Kontrollkästchen "Backup Exec Agent Utility bei jedem Einloggen starten".
- 4 Klicken Sie auf "OK".

Siehe ["Info zu Backup Exec Remote Agent Utility for Windows"](#) auf Seite 1031.

Festlegen des Aktualisierungsintervalls auf dem Remote-Computer

Sie können die Anzahl der Sekunden anzeigen, die Backup Exec Agent Utility vor der Aktualisierung des Status des Computers warten soll.

So legen Sie das Aktualisierungsintervall auf dem Remote-Computer fest

- 1 Klicken Sie auf dem Computer mit dem Agent for Windows in der Taskleiste auf "Start > Alle Programme > Veritas Backup Exec > Backup Exec Agent Utility".

Wenn Backup Exec Agent Utility bereits ausgeführt wird, können Sie auf das Symbol im Infobereich doppelklicken.
- 2 Klicken Sie auf die Registerkarte "Status".
- 3 Geben Sie im Feld "Aktualisierungsintervall" die Anzahl der Sekunden für die Aktualisierung des Status ein.
- 4 Klicken Sie auf "OK".

Siehe ["Info zu Backup Exec Remote Agent Utility for Windows"](#) auf Seite 1031.

Info zum Veröffentlichen von Agent for Windows auf den Backup Exec-Servern

Verwenden Sie Backup Exec Agent Utility, um die Namen oder IP-Adressen der Backup Exec-Server, auf denen die Informationen dieses Remote-Windows-Computers bereitgestellt werden, hinzuzufügen, zu ändern oder zu löschen. Jeder Backup Exec-Server, den Sie der Liste auf der Registerkarte "Bereitstellen von Informationen" hinzufügen, zeigt diesen Remote-Computer in der Liste der Server auf der Registerkarte "Backup und Wiederherstellung" an. Nachdem der Remote-Computer zur Liste von Servern hinzugefügt ist, können Sie mit der rechten Maustaste auf ihn klicken und dann auf "Vertrauenswürdigkeit herstellen" klicken, um zu prüfen, dass der Remote-Computer eine vertrauenswürdige Ressource ist.

Diese Informationen, die Agent for Windows veröffentlicht, umfassen die Version von Agent for Windows und die IP-Adressen des Remote-Computers. Da die IP-Adresse des Remote-Computers auf dem Backup Exec-Server bereitgestellt wird, kann der Backup Exec-Server eine Verbindung zum Remote-Computer herstellen und diesen anzeigen, auch wenn er sich in einer unbekannten Domäne befindet.

Für jeden Backup Exec-Server, auf dem die Informationen bereit gestellt werden, können Sie ein lokales Backup-Netzwerk für Vorgänge zwischen dem Backup Exec-Server und dem Remote-Computer angeben. Indem Aufträge auf ein bestimmtes lokales Netzwerk, statt auf ein unternehmensweites Netzwerk, geleitet werden, kann der Verkehr an Backup-Daten isoliert werden, sodass andere verbundene Netzwerke von Vorgängen zwischen dem Backup Exec-Server und dem Remote-Computer nicht betroffen sind.

Siehe ["Info zu Backup Exec Remote Agent Utility for Windows"](#) auf Seite 1031.

Siehe ["Backup-Netzwerke"](#) auf Seite 711.

Siehe ["Serverliste auf der Registerkarte "Backup und Wiederherstellung""](#) auf Seite 166.

Siehe ["Hinzufügen von Backup Exec-Servern, auf denen Agent for Windows Informationen bereitstellen kann"](#) auf Seite 1036.

Siehe ["Bearbeiten von Informationen zum Backup Exec-Server, auf den Agent for Windows Informationen bereitstellt"](#) auf Seite 1037.

Siehe ["Entfernen von Backup Exec-Servern, auf denen Agent for Windows Informationen bereitstellen kann"](#) auf Seite 1038.

Hinzufügen von Backup Exec-Servern, auf denen Agent for Windows Informationen bereitstellen kann

Sie können Backup Exec Agent Utility verwenden, um einen Backup Exec-Server hinzuzufügen, auf dem Agent for Windows Informationen bereitstellen kann.

Siehe ["Info zum Veröffentlichen von Agent for Windows auf den Backup Exec-Servern"](#) auf Seite 1035.

Siehe ["Anzeigen des Aktivitätsstatus von Remote-Computern in der Taskleiste"](#) auf Seite 1033.

So fügen Sie Backup Exec-Server hinzu, auf denen Agent for Windows Informationen bereitstellen kann

- 1 Klicken Sie auf dem Computer mit dem Agent for Windows in der Taskleiste auf "Start > Alle Programme > Veritas Backup Exec > Backup Exec Agent Utility".

Wenn Backup Exec Agent Utility ausgeführt wird, wird ein Symbol in der Taskleiste eingeblendet. Durch Doppelklicken auf das Symbol können Sie das Dienstprogramm anzeigen.
- 2 Klicken Sie auf die Registerkarte "Bereitstellen von Informationen".
- 3 (Optional) Klicken Sie beim ersten Starten von Backup Exec Agent Utility auf "Einstellungen ändern", um diese Optionen zu aktivieren.
- 4 Klicken Sie auf "Hinzufügen".

5 Geben Sie die folgenden Informationen ein:

Name oder IP-Adresse des Backup Exec-Servers	Geben Sie den Namen des Backup Exec-Servers oder die IP-Adresse des Backup Exec-Servers ein, auf dem Sie Informationen bereitstellen möchten.
Benutzername	Geben Sie den Benutzernamen für ein Konto ein, das Administratorrechte für den Backup Exec-Server hat.
Kennwort	Geben Sie das Kennwort für ein Konto ein, das Administratorrechte für den Backup Exec-Server hat.

6 Klicken Sie auf "OK".

Bearbeiten von Informationen zum Backup Exec-Server, auf den Agent for Windows Informationen bereitstellt

Sie können Backup Exec Agent Utility verwenden, um den Namen oder die IP-Adresse eines Backup Exec-Servers zu bearbeiten, auf dem Agent for Windows Informationen bereitstellen kann.

Siehe ["Info zum Veröffentlichen von Agent for Windows auf den Backup Exec-Servern"](#) auf Seite 1035.

So bearbeiten Sie die Informationen zu einem Backup Exec-Server

- 1** Klicken Sie auf dem Computer mit dem Agent for Windows in der Taskleiste auf "Start > Alle Programme > Veritas Backup Exec > Backup Exec Agent Utility".

Wenn Backup Exec Agent Utility ausgeführt wird, wird ein Symbol in der Taskleiste eingeblendet. Durch Doppelklicken auf das Symbol können Sie das Dienstprogramm anzeigen.
- 2** Klicken Sie auf die Registerkarte "Bereitstellen von Informationen".
- 3** (Optional) Klicken Sie beim ersten Starten von Backup Exec Agent Utility auf "Einstellungen ändern", um diese Optionen zu aktivieren.
- 4** Wählen Sie in der Liste den Backup Exec-Server aus, den Sie bearbeiten möchten.
- 5** Klicken Sie auf "Bearbeiten".
- 6** Bearbeiten Sie den Namen oder die IP-Adresse des Backup Exec-Servers.
- 7** Klicken Sie auf "OK".

Entfernen von Backup Exec-Servern, auf denen Agent for Windows Informationen bereitstellen kann

Sie können Backup Exec Agent Utility verwenden, um einen Backup Exec-Server zu entfernen, damit Agent for Windows keine Informationen mehr auf ihm bereitstellt.

Siehe ["Info zum Veröffentlichen von Agent for Windows auf den Backup Exec-Servern"](#) auf Seite 1035.

So entfernen Sie Backup Exec-Server, auf denen Agent for Windows Informationen bereitstellen kann

- 1 Klicken Sie auf dem Computer mit dem Agent for Windows in der Taskleiste auf "Start > Alle Programme > Veritas Backup Exec > Backup Exec Agent Utility".

Wenn Backup Exec Agent Utility ausgeführt wird, wird ein Symbol in der Taskleiste eingeblendet. Durch Doppelklicken auf das Symbol können Sie das Dienstprogramm anzeigen.
- 2 Klicken Sie auf die Registerkarte "Bereitstellen von Informationen".
- 3 (Optional) Klicken Sie beim ersten Starten von Backup Exec Agent Utility auf "Einstellungen ändern", um diese Optionen zu aktivieren.
- 4 Wählen Sie den Backup Exec-Server aus, den Sie aus der Liste entfernen möchten.
- 5 Klicken Sie auf "Entfernen".
- 6 Klicken Sie auf "OK".

Konfigurieren des Datenbankzugriffs für Oracle-Vorgänge

Sie können den Datenbankzugriff konfigurieren, damit der Backup Exec-Server Oracle-Vorgänge authentifizieren kann.

Siehe ["Einstellung von Authentifizierungs-Identifikationsdaten auf dem Backup Exec-Server für Oracle-Vorgänge"](#) auf Seite 1360.

So konfigurieren Sie einen Datenbankzugriff für Oracle-Vorgänge

- 1 Klicken Sie auf dem Computer mit dem Agent for Windows in der Taskleiste auf "Start > Alle Programme > Veritas Backup Exec > Backup Exec Agent Utility".
- 2 Klicken Sie auf die Registerkarte "Datenbankzugriff".
- 3 (Optional) Klicken Sie beim ersten Starten von Backup Exec Agent Utility auf "Einstellungen ändern", um diese Optionen zu aktivieren.

4 Legen Sie die gewünschten Optionen fest, um den Datenbankzugriff zu konfigurieren:

Backup Exec-Server kann Oracle-Vorgänge authentifizieren	Aktivieren Sie diese Option, um Oracle-Vorgänge zwischen dem Backup Exec-Server und diesem Computer zu ermöglichen.
Benutzername	<p>Geben Sie einen Benutzernamen an, der Administratorrechte für diesen Computer hat. Dieses Login-Konto wird vom Backup Exec-Server beim Herstellen einer Verbindung zu diesem Computer genutzt.</p> <p>Wenn Sie im Benutzernamen eine IP-Adresse oder einen voll qualifizierten Computernamen angeben, kann Backup Exec Agent Utility das Benutzerkonto möglicherweise nicht verifizieren. Wenn die Login-Daten falsch sind, wird bei der Ausführung eines Backup- oder Wiederherstellungsauftrags möglicherweise die Fehlermeldung "Verbindung zu Ressource nicht möglich..." angezeigt.</p> <p>Sie müssen diesen Computernamen und das Login-Konto der Liste von Authentifizierungsdaten für Oracle-Server auf dem Backup Exec-Server hinzufügen. Wenn bei dem Backup der Oracle-Ressourcen die Authentifizierung fehlschlägt, schlägt auch der Backup-Auftrag fehl. Wenn die Authentifizierung bei der Suche nach den Backup-Sätzen eines Wiederherstellungsauftrags fehlschlägt, sind die Backup-Sätze nicht mehr verfügbar, und Sie müssen einen DBA-initiierten Wiederherstellungsauftrag durchführen, um Daten zu sichern.</p>
Kennwort	<p>Geben Sie das Kennwort für dieses Login-Konto an.</p> <p>Hinweis: Login-Daten werden aus Sicherheitsgründen nicht auf dem Remote-Computer gespeichert.</p>
Kennwort bestätigen	Geben Sie das Kennwort zum Bestätigen erneut ein.

Benutzerdefinierten Port für die Verbindung des Backup Exec-Servers bei Oracle-Vorgängen verwenden	<p>Aktivieren Sie diese Option, um den Port zu ändern, der für die Kommunikation zwischen diesem Computer und dem Backup Exec-Server bei Oracle-Vorgängen genutzt wird. Standardmäßig wird Port 5633 verwendet.</p> <p>Wenn Sie die Port-Nummer auf diesem Computer ändern, müssen Sie sie auch auf dem Backup Exec-Server ändern und anschließend den Backup Exec Job Engine-Dienst auf dem Backup Exec-Server erneut starten.</p>
Port-Nummer	Geben Sie die Port-Nummer ein, die für die Verbindung zwischen diesem Computer und dem Backup Exec-Server verwendet werden soll.

- 5 Klicken Sie auf "OK".
- 6 Fügen Sie auf dem Backup Exec-Server den Namen des Oracle-Servers und den Benutzernamen hinzu, die Sie auf der Registerkarte "Datenbankzugriff" auf der Liste mit den Authentifizierungsdaten des Backup Exec-Servers eingegeben haben.

Siehe ["Info zu Backup Exec Remote Agent Utility for Windows"](#) auf Seite 1031.

Entfernen eines Sicherheitszertifikats für einen Backup Exec-Server, der Vertrauensverhältnis mit Agent for Windows hat

Sie können das Sicherheitszertifikat für einen Backup Exec-Server entfernen, der ein Vertrauensverhältnis mit Agent for Windows hergestellt hat.

So entfernen Sie das Sicherheitszertifikat für einen Backup Exec-Server

- 1 Klicken Sie auf dem Computer mit dem Agent for Windows in der Taskleiste auf "Start > Alle Programme > Veritas Backup Exec > Backup Exec Agent Utility".
- 2 Klicken Sie auf die Registerkarte "Sicherheit".
- 3 (Optional) Klicken Sie beim ersten Starten von Backup Exec Agent Utility auf "Einstellungen ändern", um diese Optionen zu aktivieren.
- 4 Wählen Sie den Backup Exec-Server, für den Sie das Sicherheitszertifikat entfernen möchten aus und klicken Sie dann auf "Entfernen".
- 5 Klicken Sie auf "OK".

Siehe ["Erstellen eines Vertrauensverhältnisses zwischen dem Backup Exec-Server und einem Remote-Computer"](#) auf Seite 1031.

Verwenden des Befehlszeilen-Applet von Backup Exec Agent Utility

Das Befehlszeilen-Applet von Backup Exec Agent Utility kann über eine beliebige Windows-Eingabeaufforderung für den Zugriff auf Backup Exec Agent Utility verwendet werden. Das Befehlszeilen-Applet von Backup Exec Agent Utility wird installiert, wenn Sie Agent for Windows installieren.

Wenn Sie das Befehlszeilendienstprogramm auf einem Computer mit Windows ausführen, müssen Sie eine Eingabeaufforderung mit Administratorrechten verwenden.

Hinweis: Zum Ausführen des Backup Exec Agent Utility-Befehlszeilen-Applet auf einem Windows-Computer müssen Sie Server Core verwenden.

Mit dem Befehlszeilen-Applet von Backup Exec Agent Utility können folgende Funktionen von Backup Exec Agent Utility ausgeführt werden:

- Einstellen des Bereitstellungsintervalls (in Minuten)
- Auflisten der bereitgestellten Namens des Agents
- Auflisten der Backup Exec-Server, auf denen der Agent Informationen bereitstellt
- Hinzufügen eines Backup Exec-Servers zur Bereitstellungsliste
- Entfernen eines Backup Exec-Servers aus der Bereitstellungsliste
- Anzeigen folgender Statusinformationen:
 - Aktivitätsstatus
 - Aktuelle Quelle
 - Aktueller Ordner
 - Aktuelle Datei
 - Derzeit angeschlossener Backup Exec-Server

So verwenden Sie das Befehlszeilen-Applet von Backup Exec Agent Utility

- 1 Öffnen Sie eine Eingabeaufforderung.
- 2 Geben Sie im Backup Exec-Installationsverzeichnis `ramcmd.exe` gefolgt von einer Reihe von Parametern an.

Der Standardinstallationsordner ist "C:<Backup Exec-Installationsordner>\RAWS".

Siehe ["Parameter für das Befehlszeilen-Applet von Backup Exec Agent Utility"](#) auf Seite 1042.

Parameter für das Befehlszeilen-Applet von Backup Exec Agent Utility

Die folgende Tabelle beschreibt die Parameter, die Sie im Befehlszeilen-Applet von Backup Exec Agent Utility verwenden können.

Siehe ["Verwenden des Befehlszeilen-Applet von Backup Exec Agent Utility"](#) auf Seite 1041.

Tabelle A-1

Parameter für das Befehlszeilen-Applet von Backup Exec Agent Utility

Parameter	Beschreibung
status:[n]	<p>Die Statusausgabe wird alle <n> Sekunden wiederholt. Der zulässige Bereich ist 1-86400. Drücken Sie "Q", um die Ausführung der Ausgabe zu beenden.</p> <p><code>ramcmd /status:[n]</code></p> <p>Bei Verwendung von Switch "/status" ohne Zeitangabe wird der Agent for Windows-Status im Befehlsfenster angezeigt und das Applet beendet.</p>

Parameter	Beschreibung
<code>/publish:[on off add remove interval][/ms:<Backup Exec-Server>] [/t:<x>]</code>	<p>Mit "/publish" können folgende Parameter verwendet werden:</p> <ul style="list-style-type: none">■ Keine Parameterangabe – Zeigt den Bereitstellungsstatus an und beendet das Applet.■ [on] – Aktiviert die Bereitstellung. Hiermit kann Agent for Windows eigene Informationen wie Version und IP-Adresse senden.■ [off] - Deaktiviert die Bereitstellung.■ [add], [remove] - verwendet mit /ms. Sie können diesen Parameter verwenden, um Backup Exec-Server der Agent for Windows-Liste hinzuzufügen oder daraus zu entfernen.■ [Intervall] - Verwendet mit /t. Gibt das Zeitintervall an, über das Agent for Windows eigene Informationen an den Backup Exec-Server sendet. <p>Mithilfe des Parameters /t:[<x>] können Sie das Zeitintervall in Minuten festlegen.</p> <p>Hinweis: Der Switch [interval] muss gemeinsam mit dem Parameter "/t:" verwendet werden. Die alleinige Verwendung von [interval] wird nicht unterstützt.</p> <pre>ramcmd /publish:[on off add remove interval] [/ms<Backup Exec-Server>] [/t:<x>]</pre>

Parameter	Beschreibung
<code>/oracle: [new edit delete]</code> <code>/in:[<Instanzname>]</code> <code>/ms:[<Backup Exec-Server IP-Adresse>]</code> <code>/jt:[<Auftragsvorlage>]</code> <code>/user:[<Benutzername>]</code> <code>/password:[<Kennwort> *]</code> <code>/rc: [yes no]</code> <code>/tns:[<TNS-Name>]</code>	<p>Mit "/oracle" können folgende Parameter verwendet werden:</p> <ul style="list-style-type: none">■ Keine Parameterangabe – Zeigt die bestehenden Oracle-Instanzen an und beendet das Applet.■ [new], [edit], [delete] – Gemeinsam verwendet mit /in.■ /in:[<Instanzname>] – Wird zum Hinzufügen, Bearbeiten und Löschen von Oracle-Instanzen aus der Oracle-Instanzenliste verwendet.■ /ms:[<Backup Exec-Server Adresse>] – Legt den Namen oder die IP-Adresse des Backup Exec-Servers fest.■ /jt:[<Auftragsvorlage>] – Legt eine Backup Exec-Auftragsvorlage fest.■ /user:[<Benutzername>] – Legt einen Benutzernamen fest.■ /password:[<Kennwort> *] – Legt ein Kennwort fest, das gemeinsam mit /user:[<Benutzername>] verwendet wird. Wenn Sie kein Kennwort oder ein Sternchen [*] eingeben, muss an der Befehlszeile kein Kennwort angegeben werden. Nach Ausführung des Befehls werden Sie zur Angabe eines Kennworts aufgefordert.■ /rc:[yes no] – Aktiviert bzw. deaktiviert die Einstellung "Verwendung des Wiederherstellungskatalogs". Wenn /rc ohne Parameter angegeben ist, wird der aktuelle Status der betreffenden Instanz angezeigt.■ /tns:[TNS-Name] – Legt in der Oracle-TNSNAMES-Datei den TNS-Namenalias einer verfügbaren Oracle-Datenbank und des zugehörigen Servers fest. <pre>ramcmd.exe /oracle:edit /in:<Instanzname> /rc:[yes no] [/tns:<TNS-Name>] [/user:<Benutzername>] [/password:<password> *]</pre>

Parameter	Beschreibung
/auth:[on off] [/user:<Benutzername>] [/password:<Kennwort> *]	<p>Aktiviert oder deaktiviert die Backup Exec-Server-Authentifizierung für Oracle-Vorgänge.</p> <ul style="list-style-type: none"> ■ /auth:on – Aktiviert den Status. Erfordert den Parameter /user. ■ /auth:off – Deaktiviert den Status. Erfordert den Parameter /user. ■ /user:[<Benutzername>] – Legt einen Benutzernamen fest. ■ /password:<Kennwort> – Legt ein Kennwort fest, das gemeinsam mit /user:<Benutzername> verwendet wird. Wenn Sie kein Kennwort oder ein Sternchen eingeben, werden Sie zur Angabe des Kennworts aufgefordert.
/port:[<Port>]	<p>Zeigt einen benutzerdefinierten Port für die Verbindung zum Backup Exec-Server bei Oracle-Vorgängen an bzw. legt diesen fest.</p> <ul style="list-style-type: none"> ■ /port – Zeigt die aktuelle Port-Nummer an. Wenn dies der Standard-Port ist, wird "(Standard)" angezeigt. ■ /port:<Port> – Legt für die Port-Nummer die Angabe <Port> fest. Zum Ändern der Port-Nummer auf den Standardport geben Sie [/port:0] ein.
/log_path:[<Protokollpfad>]	<p>Zeigt einen benutzerdefinierten Pfad für Debug-Protokolle an oder erstellt ihn.</p> <ul style="list-style-type: none"> ■ /log_path – Zeigt den Protokollverzeichnispfad an und beendet das Applet. ■ /log_path: < "protokolliert Pfad" > - Erstellt das Verzeichnis <"Protokollpfad">. Wenn der Pfad Leerzeichen aufweist, setzen Sie ihn unter Anführungszeichen. Beispiel: "C:\Programme\LogsFolder".

Backup Exec Deduplizierungsfunktion

Dieser Anhang enthält folgende Themen:

- [Info zu Deduplication Feature](#)
- [Deduplizierungsmethoden für Backup Exec Agents](#)
- [Anforderungen für Deduplication Feature](#)
- [Installieren von Deduplication Feature](#)
- [Konvertieren einer älteren Version des Deduplizierungsspeichers in eine neuere Version](#)
- [Konfigurieren eines OpenStorage-Geräts](#)
- [Bearbeiten von Eigenschaften eines OpenStorage-Geräts](#)
- [Angaben eines Backup Exec-Servers mit Näherung zu einem gemeinsam genutzten OpenStorage-Gerät](#)
- [Erstellen oder Importieren des Deduplizierungsspeichers](#)
- [Wählen von Speichergeräten für die gemeinsame Nutzung über Direktzugriff](#)
- [Ändern des Speicherorts für ein Deduplizierungsspeichergerät](#)
- [Gemeinsames Nutzen eines Deduplizierungsgeräts durch mehrere Backup Exec-Server](#)
- [Einsatz der clientseitigen Deduplizierung](#)
- [So werden Backup-Aufträge für die Deduplizierung eingerichtet](#)

- Verwenden der optimierten Duplizierung, um deduplizierte Daten zwischen OpenStorage-Geräten oder Deduplizierungsspeichergeräten zu kopieren
- Kopieren deduplizierter Daten auf Bänder
- Verwendung der Deduplizierung mit Verschlüsselung
- Wiederherstellen eines Deduplizierungs-Plattenspeichergeräts oder von deduplizierten Daten
- Notfallwiederherstellung des Deduplizierungsspeichergeräts
- Notfallwiederherstellung von OpenStorage-Geräten

Info zu Deduplication Feature

Backup Exec Deduplication Feature unterstützt eine Datenreduzierungsstrategie, indem sie Speicher und Netzwerkbandbreite optimiert. Deduplication Feature unterstützt die integrierte Deduplizierung auf dem Backup Exec-Server und auf Remote-Computern, auf denen Agent for Windows oder Agent for Linux installiert ist. Sie ermöglicht auch die Deduplizierung und Speicherung von Daten auf intelligenten Datenträgergeräten von anderen Händlern.

Tabelle B-1 Deduplizierungstypen

Deduplizierungstyp	Deduplizierungsort	Vorteile
Serverseitige Deduplizierung mit Backup Exec	Auf dem Backup Exec-Server.	Reduziert die Größe der Backups, wodurch Speicherbedarf reduziert wird.
Clientseitige Deduplizierung	Auf dem Remote-Computer, auf dem sich die Daten befinden. Hinweis: Agent for Windows ist auf dem Windows-Remote-Computer erforderlich, um eine Windows-Client-seitige Deduplizierung durchzuführen. Agent for Linux ist auf dem Linux-Computer erforderlich, um eine Linux-Client-seitige Deduplizierung durchzuführen.	Reduziert Netzwerkverkehr, weil nur eindeutige Daten über das Netzwerk gesendet werden. Dies reduziert auch den Backup-Zeitrahmen.

Deduplizierungstyp	Deduplizierungsort	Vorteile
Anwendungsdeduplizierung	Auf einem intelligenten Datenträgergerät, wie zum Beispiel Veritas PureDisk oder einem Gerät von einem anderen Hersteller.	Reduziert die Größe der Backups, wodurch Speicherbedarf reduziert wird. Dies reduziert auch den Backup-Zeitrahmen.

Mit nur einem Lizenzschlüssel für Deduplication Feature können Sie zwei Typen von Deduplizierungsgeräten verwenden.

Tabelle B-2 Deduplizierungsgeräte, die mit Deduplication Feature funktionieren

Typ des Geräts	Beschreibung
OpenStorage-Gerät	<p>Backup Exec nutzt Veritas OpenStorage zum Integrieren von intelligenten Datenträgergeräten in Backup Exec. Sie können Daten auf dem Veritas PureDisk-Gerät und Speichergeräten anderer Hersteller sichern.</p> <p>Die unterstützten Speichertypen finden Sie in der Liste der mit Backup Exec kompatiblen Hardware.</p> <p>Siehe "Konfigurieren eines OpenStorage-Geräts" auf Seite 1058.</p>
Deduplizierungsspeicher	<p>Der Deduplizierungsspeicher ermöglicht die integrierte Deduplizierung auf dem Backup Exec-Server. Der Deduplizierungsspeicher ist ein Disk-based Backup-Ordner auf dem Backup Exec-Server.</p> <p>Siehe "Erstellen oder Importieren des Deduplizierungsspeichers" auf Seite 1064.</p>

Zusätzlich zum Reduzieren des Speicherbedarfs und des Netzwerkverkehrs ermöglicht Deduplication Feature Folgendes:

- Kopieren von deduplizierten Daten von einem OpenStorage-Gerät oder einem Deduplizierungsdatenträgerordner auf Band für die langfristige externe Aufbewahrung.
- Verwenden Sie optimierte Duplizierung, anhand der Sie deduplizierte Daten zwischen OpenStorage-Geräten vom gleichen Händler und zwischen Deduplizierungsdatenträgerordnern kopieren können.
- Verwenden Sie Granular Recovery Technology (GRT) bei Aufträgen, die Deduplizierungsgeräte verwenden.
- Geben Sie bei Verwendung der Central Admin Server Feature OpenStorage-Geräte und Deduplizierungsspeichergeräte für mehrere Backup Exec-Server frei.

Informationen zu den Best Practices zum Einsatz der Backup Exec-Deduplizierung mit oder ohne Central Admin Server Option finden Sie unter *Best Practices für Backup Exec*.

Siehe ["Installieren von Deduplication Feature"](#) auf Seite 1056.

Siehe ["Anforderungen für Deduplication Feature"](#) auf Seite 1051.

Siehe ["Gemeinsames Nutzen eines Deduplizierungsgeräts durch mehrere Backup Exec-Server"](#) auf Seite 1077.

Siehe ["Verwenden der optimierten Duplizierung, um deduplizierte Daten zwischen OpenStorage-Geräten oder Deduplizierungsspeichergeräten zu kopieren"](#) auf Seite 1080.

Siehe ["Kopieren deduplizierter Daten auf Bänder"](#) auf Seite 1084.

Deduplizierungsmethoden für Backup Exec Agents

Backup Exec unterstützt die folgenden Deduplizierungsmethoden:

- Client-seitige Dedupli- zierung, entweder auf einem intelligenten Datenträgergerät oder in einen Deduplizierungsspeicherordner.
- Serverseitige Backup Exec-Deduplizierung mit einem Deduplizierungsspeichergerät.
- Anwendungsdeduplizierung auf einem OpenStorage-Gerät.

Die folgende Tabelle listet die Deduplizierungsmethoden auf, die für Backup Exec Agents verfügbar sind.

Tabelle B-3 Deduplizierungsmethoden für Backup Exec Agents

Agent	Client-seitige Deduplizierung (Dateisystem-Backups oder VSS-Snapshot-fähige Backups, je nachdem, welche unterstützt werden)	Client-seitige Deduplizierung (wenn Granular Recovery Technology aktiviert ist)	Serverseitige Deduplizierung mit Backup Exec (Dateisystem-Backups oder VSS-Snapshot-Backups je nach Unterstützung)	Serverseitige Deduplizierung mit Backup Exec (wenn Granular Recovery Technology aktiviert ist)	Anwendung-sdeduplizierung auf einem Open-Storage-Gerät
Agent for Windows	Ja	Nicht anwendbar	Ja	Nicht anwendbar	Ja
Agent for VMware und Hyper-V	Ja (nur für Hyper-V) Hinweis: Agent for Windows muss auf dem Hyper-V-Host installiert sein.	Ja (nur für Hyper-V) Hinweis: Agent for Windows muss auf dem Hyper-V-Host installiert sein.	Ja	Ja	Ja
Agent for Linux	Ja	Nein	Ja	Nicht anwendbar	Ja
Agent for Enterprise Vault	Nein	Nein	Ja	Nein	Nein
Exchange Agent	Ja	Ja	Ja	Ja	Ja
SQL Agent	Ja	Nicht anwendbar	Ja	Nicht anwendbar	Ja
SharePoint Agent	Ja	Ja	Ja	Ja	Ja

Agent	Client-seitige Deduplizierung (Dateisystem-Backups oder VSS-Snapshot-fähige Backups, je nachdem, welche unterstützt werden)	Client-seitige Deduplizierung (wenn Granular Recovery Technology aktiviert ist)	Serverseitige Deduplizierung mit Backup Exec (Dateisystem-Backups oder VSS-Snapshot-Backups je nach Unterstützung)	Serverseitige Deduplizierung mit Backup Exec (wenn Granular Recovery Technology aktiviert ist)	Anwendungsdeduplizierung auf einem Open-Storage-Gerät
Active Directory Agent	Ja	Ja	Ja	Ja	Ja
Agent for Oracle	Linux: Ja Windows: Ja	Nein	Ja	Nein	Ja

Siehe ["Info zu Deduplication Feature"](#) auf Seite 1047.

Anforderungen für Deduplication Feature

Die Anforderungen für die Deduplication Feature hängen vom Speichergerät- und Deduplizierungstyp ab, den Sie verwenden möchten. Sie sollten vor der Installation der Deduplication Feature festlegen, welche Speichergeräte- und Deduplizierungstypen verwendet werden sollen. Dann überprüfen Sie, dass Ihr System die Bedingungen für die Speichergeräte erfüllt, die Sie benutzen möchten.

Warnung: Es wird dringend empfohlen, das Deduplizierungsspeichergerät aus allen Antivirusscans auszuschließen. Wenn ein Antivirusscan die Dateien vom Deduplizierungsspeichergerät löscht oder sie in Quarantäne verschiebt, kann der Zugriff auf dieses Gerät deaktiviert werden.

Tabelle B-4 Anforderungen und Empfehlungen für Deduplication Feature

Element	Voraussetzungen und Empfehlungen
Deduplizierungsspeichergröße	

Element	Voraussetzungen und Empfehlungen
	<p>Die folgenden Komponenten sind erforderlich:</p> <ul style="list-style-type: none"> ■ Ein 64-Bit-Backup Exec-Server. ■ Ein Backup Exec-Server mit mindestens 4 Kernen. Acht Kerne werden empfohlen. ■ Für 64 TB von gespeicherten deduplizierten Daten sind 8 Kerne erforderlich. ■ Ein dedizierter Datenträger, der als Speicherort für den Deduplizierungsspeicher verwendet wird. Der entsprechende Datenträger muss über 20 % freien Speicherplatz verfügen (insgesamt mind. 5 GB freier Speicherplatz). ■ Das Deduplizierungsspeichergerät muss von Antivirusscans ausgeschlossen werden. Wenn ein Antivirusscan die Dateien vom Deduplizierungsspeichergerät löscht oder sie in Quarantäne verschiebt, kann der Zugriff auf dieses Speichergerät deaktiviert werden. ■ Für den Deduplizierungsspeicher sind 4 GB physischer Arbeitsspeicher für bis zu 4 TB Speicherplatz erforderlich. Weiterhin ist 1 GB physischer Arbeitsspeicher pro 1 TB Deduplizierungsspeicherplatz (maximal 32 TB) erforderlich. Beispiel: 5 GB physischer Arbeitsspeicher für 5 TB Speicherplatz. Für Deduplizierungsspeicher zwischen 32 und 64 TB werden mindestens 32 GB physischer Arbeitsspeicher empfohlen. ■ Folgende minimale Festplattenzugriffszeit pro individuellem Schreib-, Lese- oder Prüfvorgang wird empfohlen: <ul style="list-style-type: none"> ■ Bis zu 32 TBs für Speicherung: <ul style="list-style-type: none"> ■ 130 MB pro Sekunde ■ 200 MB pro Sekunde für Leistung auf Unternehmensstufe ■ 32 bis 48 TB Speicherplatz: 200 MB pro Sekunde ■ 48 bis 64 TB Speicherplatz: 250 MB pro Sekunde <p>Die oben genannten Empfehlungen gelten für die Leistung einer einzelnen Operation. Sie benötigen möglicherweise mehr Leistung, je nachdem welches Ziel Sie für das Schreiben auf und das Lesen vom Datenträger haben.</p> <p>Hinweis: Beachten Sie jedoch, welche Auswirkungen die jeweiligen Festplattengeschwindigkeiten auf die Deduplizierungsleistung haben.</p> <p>Festplattengeschwindigkeiten können sich folgendermaßen auf die Deduplizierungsleistung auswirken:</p> <ul style="list-style-type: none"> ■ Computer mit einer Festplattengeschwindigkeit von mehr als 200 MB/s verfügen über optimale Lese- und Schreibleistung zur Deduplizierung. ■ Computer mit einer Festplattengeschwindigkeit zwischen

Element	Voraussetzungen und Empfehlungen
	<p>150–200 MB/s verfügen über ausreichende Lese- und Schreibleistung zur Deduplizierung.</p> <ul style="list-style-type: none"> ■ Bei Computern mit einer Festplattengeschwindigkeit zwischen 100-150 MB/s werden einige Vorgänge mit geringerer Leistung ausgeführt. ■ Computer mit einer Festplattengeschwindigkeit von unter 100 MB/s erfahren eine schlechte Leistung. Sie sollten die Lese- und Schreibleistung der Festplatte vor der Installation und Ausführung der Deduplizierung verbessern.
Deduplizierungsanforderung Deduplizierungsanforderung	<ul style="list-style-type: none"> ■ Storage Area Network (Fibre Channel oder iSCSI), direkt-angehängter Speicher (DAS) oder interne Datenträger werden unterstützt. Wechselplatten mit USB, eSATA- und FireWire-Geräte werden nicht unterstützt. ■ Der Backup Exec-Server sollte redundante Konnektivität zum Speicher haben. ■ Das Speichernetzwerk muss ein zugehöriges, außerordentlich schnelles Netzwerk mit maximal einer Zugriffsverzögerung von 1 Millisekunde pro Runde sein. ■ Das Speichernetz muss genügend Bandbreite haben, um Ihren Durchsatzzielen zu entsprechen. Die folgenden Speichernetzwerkbandbreiten werden unterstützt: <ul style="list-style-type: none"> ■ iSCSI ohne mit einer Bandbreite von mindestens 10 GBs pro Sekunde. ■ Fibre Channel SANs mit einer Bandbreite von mindestens 4 GBs pro Sekunde. ■ Eine minimale Bandbreite von 130 MB pro Sekunde für Lese- und Schreibvorgänge ist erforderlich. Eine Bandbreite, die kleiner ist als MB 130 pro Sekunde kann möglicherweise in den kleineren, weniger Ressource-intensiven Umgebungen verwendet werden. Jedoch während Verwendung sich erhöht, benötigt Deduplizierung mehr Bandbreite, ausreichenden Durchsatz für Deduplizierungsprozesse und Backup sicherzustellen. Andernfalls sind Leistung und Stabilität negativ betroffen.

Element	Voraussetzungen und Empfehlungen
Identifikationsdaten des Deduplizierungs-Speichergeräts	<p>Die folgenden Anforderungen gelten für die Anmeldedaten für ein Deduplizierungsspeichergerät:</p> <ul style="list-style-type: none">■ Das Kennwort kann nicht leer sein.■ Das Kennwort kann die folgenden Zeichen nicht enthalten: &, ", <, >, %, ^■ Das Kennwort kann nicht mit dem Bindestrich beginnen: -■ Das Kennwort darf nicht mit einem umgekehrten Schrägstrich (\) enden.
OpenStorage-Geräte	<p>Um ein Veritas PureDisk-Gerät oder ein Speichergerät eines anderen Herstellers als OpenStorage-Gerät zu verwenden, müssen Sie das Gerät und den passenden OpenStorage-Connector vom Gerätehändler erwerben.</p> <p>Sie können die Deduplication Feature mit OpenStorage-Geräten auf einem 64-Bit-Backup Exec-Server verwenden.</p> <p>Die Standardsystemanforderungen für Backup Exec gelten auch für Deduplication Feature, wenn Sie OpenStorage-Geräte nutzen.</p>
Client-seitige Deduplizierung für Windows	<p>Auf dem Server, auf dem Agent for Windows installiert ist, sind 1,5 GB Arbeitsspeicher erforderlich.</p> <p>32-Bit- und 64-Bit-Windows-Computer werden unterstützt.</p>
Client-seitige Deduplizierung für Linux	<p>Die kompatiblen Betriebssysteme für die clientseitige Deduplizierung unter Linux finden Sie in der Liste der mit Backup Exec kompatiblen Software.</p> <p>Ein 64-Bit-Linux-Computer ist erforderlich.</p> <p>Die folgenden Deduplizierungsgeräte können verwendet werden:</p> <ul style="list-style-type: none">■ Deduplizierungs-Plattenspeichergerät■ Veritas PureDisk OpenStorage ist der einzige OpenStorage-Gerätetyp, der die clientseitige Deduplizierung für Linux unterstützt. <p>Die folgenden Backup Exec-Funktionen sind erforderlich:</p> <ul style="list-style-type: none">■ Agent for Linux■ Deduplication Feature

Siehe "Installieren von Deduplication Feature" auf Seite 1056.

Installieren von Deduplication Feature

Bevor Sie eine Backup Exec-Edition mit Deduplication Feature installieren, müssen Sie sicherstellen, dass der Computer die Anforderungen erfüllt.

Siehe ["Anforderungen für Deduplication Feature"](#) auf Seite 1051.

Siehe ["Installieren zusätzlicher Agents und Funktionen auf dem lokalen Backup Exec-Server"](#) auf Seite 66.

Konvertieren einer älteren Version des Deduplizierungsspeichers in eine neuere Version

Backup Exec verbessert Geschwindigkeit und Deduplizierung beim Sichern auf Backup Exec-Deduplizierungsordner. Für die Konvertierung einer älteren Version des Deduplizierungsspeichers in eine neuere Version müssen Sie die vorhandenen Deduplizierungsdaten in ein neueres Format konvertieren. Die für die Konvertierung benötigte Zeit hängt von der Größe des Deduplizierungsspeichers und der Anzahl der Backup-Sätze ab.

So konvertieren Sie den Deduplizierungsspeicher von einer älteren Version in eine neuere Version

- 1 Es wird empfohlen, eine zweite Kopie der Deduplizierungsdaten zu erstellen, bevor Sie das Upgrade starten.
- 2 Stellen Sie sicher, dass Folgendes zutrifft:
 - Es ist mindestens 12 % freier Speicherplatz auf dem Datenträger mit dem Deduplizierungsspeicherordner vorhanden.
 - Die Deduplizierungsdienste werden ausgeführt.
 - Windows-Hotfix ist installiert.

Siehe ["Ausführen der Umgebungsprüfung vor Installation oder Upgrade von Backup Exec"](#) auf Seite 48.

- 3 Wenn Sie weiteren Speicherplatz auf dem Datenträger freizugeben müssen, können Sie dafür das Tool "pdde_gc.exe" verwenden. Wenn genügend freier Speicherplatz vorhanden ist, fahren Sie mit dem nächsten Schritt fort.

So führen Sie pdde_gc.exe aus

- Stellen Sie die ISO-Datei über die Backup Exec-Medien bereit oder aktualisieren Sie eine frühere Version von Backup Exec. Das Tool befindet sich auf dem Datenträger im Ordner

`<Bereitstellungspfad>\BE\WinNT\Install\PDDEMigration.`

Konvertieren einer älteren Version des Deduplizierungsspeichers in eine neuere Version

- Führen Sie in der Befehlszeile `pdde_gc.exe` ohne Parameter aus.

Wenn Sie mehr freien Speicherplatz benötigen, haben folgende Möglichkeiten:

- Verwenden Sie die Backup Exec-Konsole, um Backup-Sätze im Deduplizierungsspeicher ablaufen zu lassen.
- Führen Sie die CR-Warteschlangenverarbeitung zweimal aus.
- Führen Sie das Tool "pdde_gc.exe" erneut aus.

4 Aktualisieren Sie Backup Exec auf die neueste Version.

Siehe ["Installieren von Backup Exec mithilfe des Installationsassistenten"](#) auf Seite 55.

Nach der Aktualisierung von Backup Exec startet die Konvertierung der älteren Version des Deduplizierungsspeichers in eine neuere Version. Die vorhandenen Deduplizierungsdaten werden in ein neues Format konvertiert. Während des Konvertierungsvorgangs bleibt der Deduplizierungsspeicher offline. Alle laufenden Deduplizierungsaufträge schlagen fehl, und alle Aufträge, die einen anderen Speicher als Ziel haben, werden während der Konvertierung des Deduplizierungsspeichers weiterhin ausgeführt.

Die Backup Exec-Konsole zeigt die Meldung an, dass der Konvertierungsprozess begonnen hat. Abhängig vom Zeitaufwand für die Konvertierung wird innerhalb des Konvertierungsfortschritts alle 15 Minuten eine Meldung angezeigt. Es wird auch dann eine Meldung angezeigt, wenn die Konvertierung abgeschlossen wurde, fortgesetzt wird oder fehlgeschlagen ist.

5 Wenn die Konvertierung abgeschlossen wurde, werden Sie in der Backup Exec-Konsole aufgefordert, die Backup Exec-Dienste neu zu starten.

Wenn Sie auf "OK" klicken, wird das Dialogfeld "Backup Exec Services" angezeigt. Klicken Sie auf "Alle Dienste neu starten".

Klicken Sie in der Backup Exec-Administratorkonsole auf die Backup Exec-Schaltfläche, dann auf "Konfiguration und Einstellungen", "Backup Exec-Dienste" und schließlich auf "Alle Dienste neu starten".

Wenn die Konvertierung fehlschlägt, können Sie die Daten manuell in das neue Deduplizierungsformat konvertieren. Im folgenden Abschnitt finden Sie Informationen zum manuellen Konvertieren von Daten.

Wenn die Konvertierung aufgrund eines Server-Neustarts fehlschlägt, wird der Konvertierungsvorgang nach dem Abschluss des Neustarts fortgesetzt.

Erstellen oder Importieren eines älteren Deduplizierungsordners

Sie können in Backup Exec einen Deduplizierungsspeicherordner erstellen oder importieren. Es ist ein Deduplizierungsspeicherordner vorhanden, der erstellt wurde, als Sie noch die ältere Deduplizierungsversion verwendet haben, die nicht mehr von Backup Exec unterstützt wird. Wenn Sie versuchen, den Ordner zu importieren, wird eine Fehlermeldung angezeigt, und der Import schlägt fehl. Im folgenden Abschnitt wird beschrieben, wie Sie den älteren Deduplizierungsordner manuell in eine neuere von Backup Exec unterstützte Deduplizierungsversion konvertieren:

Nach dem Abschluss der Konvertierung können Sie den Ordner importieren. Es kann nur ein Deduplizierungsspeicher mit einem einzelnen Backup Exec-Medienserver konfiguriert sein.

Wiederherstellen eines älteren Deduplizierungsspeicher-Backups mithilfe von Backup Exec

Sie können einen vorhandenen Deduplizierungs-Backup-Satz mit Backup Exec wiederherstellen. Dieser Backup-Satz wurde mit einer älteren Deduplizierungsversion, die nicht mehr von Backup Exec unterstützt wird, erstellt und gesichert. Wenn Sie versuchen, den Backup-Satz wiederherzustellen, schlägt der Wiederherstellungsauftrag mit einer Ausnahmemeldung fehl, die sich auf die älteren Deduplizierungs-Backup-Sätze bezieht, die Daten werden jedoch wiederhergestellt. Im folgenden Abschnitt wird beschrieben, wie Sie den wiederhergestellten Deduplizierungsordner manuell in eine neuere unterstützte Deduplizierungsversion konvertieren:

Nach dem Abschluss der Konvertierung können Sie den wiederhergestellten Ordner importieren und diesen Ordner als Pfad für den Deduplizierungsspeicher für Backup Exec hinzufügen.

Konfigurieren eines OpenStorage-Geräts

OpenStorage ist eine Funktion von Veritas, die eine Integration intelligenter Datenträgergeräte in Backup Exec ermöglicht.

Die unterstützten Speichertypen finden Sie in der Liste der mit Backup Exec kompatiblen Hardware.

Einige intelligente Datenträgergeräte können mehrere logische Speichereinheiten umfassen. Jede logische Speichereinheit wird jedoch als einzelnes OpenStorage-Gerät hinzugefügt. Wenn Sie ein OpenStorage-Gerät hinzufügen, kann Backup Exec die logischen Speichereinheiten auf diesem Gerät automatisch ermitteln.

Hinweis: Wenn Sie die Daten auf einem OpenStorage-Gerät löschen, kann es möglicherweise bis zu 48 Stunden dauern, bis mehr Speicherplatz verfügbar wird. Backup Exec kann die Speicherplatzmenge, die verfügbar gemacht wird, nicht immer berechnen.

Wenn Sie Backup Exec Central Admin Server Feature verwenden, können Sie ein OpenStorage-Gerät zwischen mehreren Backup Exec-Servern freigeben. Sie können die gemeinsame Nutzung aktivieren, wenn Sie ein OpenStorage-Gerät hinzufügen. Sie können jederzeit neue Backup Exec-Server auswählen, die ein OpenStorage-Gerät gemeinsam verwenden, oder die Funktion für die gemeinsame Nutzung für Backup Exec-Server entfernen. Sie können einen anderen Backup Exec-Server angeben, auf dem Backup-Vorgänge ausgeführt werden sollen, wenn das OpenStorage-Gerät die Quelle eines Auftrags, wie zum Beispiel ein Duplizierungs- oder Verifizierungsauftrag ist.

Siehe ["Gemeinsames Nutzen eines Deduplizierungsgeräts durch mehrere Backup Exec-Server"](#) auf Seite 1077.

Bevor Sie ein OpenStorage-Gerät konfigurieren, benötigen Sie folgende Information:

- Den gewünschten Namen des OpenStorage-Geräts
- Den Namen des Anbieters für das OpenStorage-Gerät
- Der Name des Servers und das Login-Konto zum Zugreifen auf das OpenStorage-Gerät Sie können das System-Login-Konto nicht verwenden. Es wird empfohlen, dass Sie ein Login-Konto auswählen oder erstellen, das Sie ausschließlich für das Deduplizierungsspeichergerät verwenden. Sie sollten dieses Konto für keine anderen Vorgänge verwenden. Dieses Konto sollte keine Anmeldedaten enthalten, die abhängig von Kennwortaktualisierungsrichtlinien sind.
- Ob Sie Verschlüsselung aktivieren möchten, während Daten an das OpenStorage-Gerät gesendet werden und während die Daten darauf gespeichert werden.
- Die Anzahl der gleichzeitigen Vorgänge, die auf dem Gerät ausgeführt werden können. Diese Einstellung legt die Anzahl der Aufträge fest, die auf diesem Gerät gleichzeitig ausgeführt werden können. Die Anzahl von Aufträgen schwankt abhängig von Ihrer Hardware und Umgebung. Sie müssen diese Einstellung möglicherweise mehr als ein Mal anpassen. Es wird empfohlen, diesen Wert so niedrig einzustellen, dass das System nicht überlastet wird, aber hoch genug, dass Ihre Aufträge schnell ausgeführt werden können.

Um zu verhindern, dass ein Deduplizierungsauftrag an ein Nicht-Deduplizierungs-Gerät in einem Speicherpool gesendet wird, können Sie beliebigen Speicherpools ein OpenStorage-Gerät hinzufügen.

So konfigurieren Sie ein OpenStorage-Gerät

- 1** Klicken Sie auf der Registerkarte "Speicher" in der Gruppe "Konfigurieren" auf "Speicher konfigurieren".
- 2** Sie haben folgende Möglichkeiten:

Wenn Central Admin Server Feature nicht installiert ist	Klicken Sie auf "Netzwerkspeicher" und dann auf "Weiter".
Wenn Central Admin Server Feature installiert ist	Gehen Sie dazu in folgender Reihenfolge vor: <ul style="list-style-type: none">■ Wählen Sie einen Backup Exec-Server aus und klicken Sie auf "Weiter".■ Klicken Sie auf "Netzwerkspeicher" und dann auf "Weiter".
- 3** Klicken Sie auf "OpenStorage" und dann auf "Weiter".
- 4** Geben Sie einen Namen und eine Beschreibung für das OpenStorage-Gerät ein und klicken Sie dann auf "Weiter".
- 5** Sie haben folgende Möglichkeiten:

Wenn der Anbieter für das OpenStorage-Gerät aufgelistet ist	Wählen Sie den Anbieter aus und klicken Sie dann auf "Weiter".
Wenn der Anbieter für das OpenStorage-Gerät nicht aufgelistet ist	Gehen Sie dazu in folgender Reihenfolge vor: <ul style="list-style-type: none">■ Wählen Sie "Mein Anbieter steht nicht in der Liste" und klicken Sie auf "Weiter".■ Geben Sie den Anbieternamen ein und klicken Sie dann auf "Weiter".
- 6** Geben Sie den Namen des Servers und das Login-Konto zum Zugreifen auf das OpenStorage-Gerät ein und klicken Sie auf "Weiter".
- 7** Geben Sie die Anzahl der Vorgänge ein, die gleichzeitig auf dem OpenStorage-Gerät ausgeführt werden können, und klicken Sie dann auf "Weiter".
- 8** Lesen Sie die Übersicht und führen einen der folgenden Schritte aus:

So ändern Sie die Konfiguration

Gehen Sie dazu in folgender Reihenfolge vor:

- Klicken Sie auf die Überschrift, die die Elemente enthält, die Sie ändern möchten.
- Nehmen Sie alle Änderungen, vor und klicken Sie dann auf "Weiter", bis die Übersicht angezeigt wird.
- Klicken Sie auf "Fertigstellen".

So erstellen oder importieren Sie ein OpenStorage-Gerät

Klicken Sie auf "Fertigstellen".

Siehe ["Angeben eines Backup Exec-Servers mit Näherung zu einem gemeinsam genutzten OpenStorage-Gerät"](#) auf Seite 1063.

Bearbeiten von Eigenschaften eines OpenStorage-Geräts

Sie können alle Eigenschaften eines OpenStorage-Geräts anzeigen und einige der Eigenschaften ändern.

So bearbeiten Sie die Eigenschaften für ein OpenStorage-Gerät

- 1** Doppelklicken Sie auf der Registerkarte "Speicher" auf das OpenStorage-Gerät.
- 2** Wählen Sie im linken Teilfenster "Eigenschaften".

3 Ändern Sie die Eigenschaften nach Bedarf:

Name	Zeigt den benutzerdefinierten Namen für dieses OpenStorage-Gerät.
Beschreibung	Zeigt die benutzerdefinierte Beschreibung dieses OpenStorage-Geräts.
Backup Exec-Server mit Gerätenäherung	<p>Gibt den Server an, auf dem Backup-Vorgänge ausgeführt werden sollen, wenn das OpenStorage-Gerät von Servern in einer Central Admin Server Feature-Umgebung gemeinsam genutzt wird. Sie können einen Backup Exec-Server angeben, der sich physisch oder logisch in der Nähe des OpenStorage-Gerät befindet. Die Näherung des Backup Exec-Servers zum Gerät ist ein Vorteil, wenn das Gerät die Quelle eines Auftrags ist (zum Beispiel eines Duplizierungs- oder Überprüfungsauftrags) und Sie vermeiden möchten, den Auftrag über ein WAN auszuführen.</p> <p>Standardmäßig ist der Backup Exec-Server, auf dem Sie das OpenStorage-Gerät erstellen, der Server, der die Backup-Vorgänge für dieses Gerät ausführt.</p>
Login-Konto	Gibt den Namen des Login-Kontos an, das für den Zugriff auf das Gerät erforderlich ist.
Gleichzeitige Vorgänge	Gibt die maximale Zahl der Aufträge an, die Sie auf diesem Gerät gleichzeitig ausführen möchten.
Datenstrom teilen alle	Gibt die Größe an, bei der Backup Exec auf ein neues Image wechseln soll. Die Standardgröße ist 50 GB.
Datenstromgröße	Gibt die Größe eines einzelnen Schreibvorgangs an, der von Backup Exec gestartet wird. Die Standardgröße variiert basierend auf dem Typ des Geräts, das verwendet wird.

Angeben eines Backup Exec-Servers mit Näherung zu einem gemeinsam genutzten OpenStorage-Gerät

Strombehandlungsroutine

Gibt an, ob eine Datenstrom-Behandlungsroutine verwendet wird. Backup Exec legt diese Option automatisch fest, wenn Sie einen Servertyp auswählen. Für einige Typen von Geräten erscheint diese Option überhaupt nicht. Wenn Backup Exec diese Option nicht festlegt, fordern Sie die empfohlene Einstellung beim Hersteller des Geräts.

Clientseitige Deduplizierung

Zeigt, ob clientseitige Deduplizierung für dieses OpenStorage-Gerät aktiviert ist.

Clientseitige Deduplizierung aktiviert einen Remote-Computer, um Daten direkt an ein OpenStorage-Gerät zu schicken. Bei Einsatz der clientseitigen Deduplizierung wird der Backup Exec-Server umgangen, sodass der Backup Exec-Server andere Vorgänge ausführen kann.

Zu reservierender Speicherplatz für Vorgänge, die nicht zu Backup Exec gehören

Zeigt den Speicherplatz an, der für andere Anwendungen als Backup Exec zu reservieren ist. Der Standardwert ist 5 %.

- 4 Klicken Sie auf "Übernehmen", um die Änderungen zu speichern.

Angeben eines Backup Exec-Servers mit Näherung zu einem gemeinsam genutzten OpenStorage-Gerät

Sie können einen Backup Exec-Server mit physischer oder logischer Nähe zu einem OpenStorage-Gerät angeben, um Vorgänge für dieses Gerät auszuführen. Nähe des Backup Exec-Servers zum Gerät ist ein Vorteil, wenn das Gerät die Quelle eines Auftrags ist (zum Beispiel eines Duplizierungs- oder Überprüfungsauftrags) und Sie vermeiden möchten, den Auftrag über WAN auszuführen.

Standardmäßig ist der Backup Exec-Server, auf dem Sie das Gerät erstellen, der Server, auf dem die Backup-Vorgänge für das Gerät ausgeführt werden. Sie können einen Backup Exec-Server mit Näherung nur dann angeben, wenn das Gerät von Servern in einer Central Admin Server Option-Umgebung gemeinsam genutzt wird.

Wenn Sie den angegebenen Backup Exec-Server mit Gerätenäherung entfernen, werden Sie dazu aufgefordert, einen anderen Server anzugeben.

So geben Sie einen Backup Exec-Server mit Näherung zu einem freigegebenen OpenStorage-Gerät an

- 1 Doppelklicken Sie auf der Registerkarte "Speicher" auf den Namen des Geräts.
- 2 Wählen Sie im linken Teilfenster "Eigenschaften".
- 3 Wählen Sie im Feld "Backup Exec-Server mit Gerätenäherung" in der Dropdown-Liste den Server, auf dem Vorgänge für das Gerät ausgeführt werden sollen.
- 4 Klicken Sie auf "Übernehmen".

Erstellen oder Importieren des Deduplizierungsspeichers

Deduplizierungsdatenträgerspeicher bietet einen Backup-to-Disk-Ordner, den Sie als Ziel für Backup-Aufträge verwenden können. Wenn Sie Deduplizierungsdatenträgerspeicher verwenden, werden nur eindeutige Daten gespeichert.

Bevor Sie ein Deduplizierungsspeichergerät erstellen, überprüfen Sie die Anforderungen. Es wird empfohlen, einen dedizierten Datenträger und eine große Menge von RAM für Deduplizierungsspeicher.

Siehe ["Anforderungen für Deduplication Feature"](#) auf Seite 1051.

Sie können nur ein Deduplizierungsspeichergerät auf einem Backup Exec-Server erstellen. Sie können Deduplizierungsspeicher auf einer Speichergruppe erstellen. Jedoch wenn ein Deduplizierungsspeichergerät bereits auf einem Backup Exec-Server existiert, können Sie kein weiteres Gerät einer Speichergruppe hinzufügen, die mit diesem Backup Exec-Server verbunden ist.

Wenn Sie die Backup Exec-Option "Löschen" für ein Deduplizierungsspeichergerät verwenden, wird der Ordner aus der Backup Exec-Datenbank entfernt. Jedoch bleiben der Ordner und die Dateien darin auf dem Datenträger. Wenn Sie Backup-Sätze aus einem Deduplizierungs-Plattenspeichergerät löschen, kann es bis zu 48 Stunden dauern, bis mehr Speicherplatz verfügbar wird. Backup Exec kann die Speicherplatzmenge, die verfügbar gemacht wird, nicht immer berechnen.

Wenn Sie Backup Exec Central Admin Server Feature verwenden, können Sie ein Deduplizierungsspeichergerät auf mehreren Backup Exec-Servern gemeinsam nutzen. Sie können dies aktivieren, wenn Sie ein Deduplizierungsspeichergerät hinzufügen. Sie können neue Backup Exec-Server auswählen, um Deduplizierungsspeicher oder die Möglichkeit zur gemeinsamen Nutzung für Backup Exec-Server jederzeit zu entfernen.

Sie können einen neuen Deduplizierungsspeicher erstellen oder ein vorhandenes Deduplizierungsspeichergerät aus einem anderen Backup Exec-Server importieren.

Siehe ["Gemeinsames Nutzen eines Deduplizierungsgeräts durch mehrere Backup Exec-Server"](#) auf Seite 1077.

Bevor Sie ein Deduplizierungsspeichergerät erstellen oder importieren, halten Sie die folgenden Informationen bereit:

- Den gewünschten Namen des Deduplizierungsspeichergeräts
- Den Datenträger, auf dem das Deduplizierungsspeichergerät erstellt werden soll
 - Der Pfad des vorhandenen Deduplizierungsspeichergeräts, wenn Sie eines importieren.
 - Die Informationen für das Benutzerkonto, das verwendet wurde, als das vorhandene Deduplizierungsspeichergerät erstellt wurde.
- Das für den Zugriff auf das Deduplizierungsspeichergerät zu verwendende Login-Konto Sie können das System-Login-Konto nicht verwenden. Es wird empfohlen, dass Sie ein Login-Konto auswählen oder erstellen, das Sie ausschließlich für das Deduplizierungsspeichergerät verwenden. Sie sollten dieses Konto für keine anderen Vorgänge verwenden. Dieses Konto sollte keine Anmeldedaten enthalten, die abhängig von Kennwortaktualisierungsrichtlinien sind.

Die folgenden Anforderungen gelten für die Anmeldedaten für ein Deduplizierungsspeichergerät:

- Das Kennwort kann nicht leer sein.
- Das Kennwort kann die folgenden Zeichen nicht enthalten: &, ", <, >, %, ^
- Das Kennwort kann nicht mit dem Bindestrich beginnen: -
- Das Kennwort darf nicht mit einem umgekehrten Schrägstrich (\) enden.
- Ob die Verschlüsselung während der Übertragung der Daten an das Deduplizierungsspeichergerät und während die Daten dort gespeichert sind, aktiviert werden soll. Sie sollten die Backup Exec-Verschlüsselungsoptionen nicht für Backup-Aufträge verwenden, die Daten deduplizieren.
- Die Anzahl der gleichzeitigen Vorgänge, die auf dem Gerät ausgeführt werden können. Diese Einstellung legt die Anzahl von Aufträgen fest, die auf dieses Gerät gleichzeitig ausgeführt werden können. Die Anzahl von Aufträgen schwankt abhängig von Ihrer Hardware und Umgebung. Sie müssen diese Einstellung möglicherweise mehr als ein Mal anpassen. Es wird empfohlen, diesen Wert so niedrig einzustellen, dass das System nicht überlastet wird, aber hoch genug, dass Ihre Aufträge schnell ausgeführt werden können.

So erstellen oder importieren Sie einen Deduplizierungsspeicher

- 1 Klicken Sie auf der Registerkarte "Speicher" in der Gruppe "Konfigurieren" auf "Speicher konfigurieren".
- 2 Sie haben folgende Möglichkeiten:

Wenn Central Admin Server Feature nicht installiert ist	Wählen Sie "Plattenbasierter Speicher" und klicken Sie dann auf "Weiter".
Wenn Central Admin Server Feature installiert ist	<p>Gehen Sie dazu in folgender Reihenfolge vor:</p> <ul style="list-style-type: none"> ■ Wählen Sie den Backup Exec-Server aus, für den Sie den Deduplizierungsspeicher konfigurieren möchten und klicken Sie auf "Weiter". ■ Wählen Sie "Plattenbasierter Speicher" und klicken Sie dann auf "Weiter".
- 3 Klicken Sie auf "Deduplizierungsspeicher" und dann auf "Weiter".
- 4 Geben Sie einen Namen und eine Beschreibung für das Deduplizierungsspeichergerät ein und klicken Sie dann auf "Weiter".
- 5 Sie haben folgende Möglichkeiten:

So erstellen Sie ein neues Deduplizierungsspeichergerät	Klicken Sie auf "Weiter", um den Standardspeicherort im Feld zu akzeptieren.
So importieren Sie ein vorhandenes Deduplizierungsspeichergerät	Geben Sie den Pfad des vorhandenen Deduplizierungsspeichergeräts ein und klicken Sie dann auf "Weiter".
- 6 Klicken Sie auf den Pfeil und wählen Sie das gewünschte Login-Konto aus, um auf das Deduplizierungsspeichergerät zuzugreifen, oder klicken Sie auf "Hinzufügen/Bearbeiten", um ein Login-Konto zu erstellen, und klicken Sie dann auf "Weiter".
- 7 Geben Sie an, ob die Verschlüsselung während der Übertragung der Daten an das Deduplizierungsspeichergerät und während die Daten dort gespeichert sind, aktiviert werden soll, und klicken Sie auf "Weiter".

- 8 Geben Sie die Anzahl der Vorgänge ein, die gleichzeitig auf dem Deduplizierungsspeichergerät ausgeführt werden können, und klicken Sie dann auf "Weiter".
- 9 Überprüfen Sie die Speicherkonfigurationsübersicht und führen Sie einen der folgenden Schritte aus:

So ändern Sie eine Auswahl

Gehen Sie dazu in folgender Reihenfolge vor:

- Klicken Sie auf eine Überschrift und nehmen Sie die entsprechenden Änderungen vor.
- Klicken Sie im Assistenten wiederholt auf "Weiter", um die Übersicht erneut anzuzeigen.
- Klicken Sie auf "Fertigstellen".

So starten Sie die Konfiguration

Klicken Sie auf "Fertigstellen".

Bearbeiten der Eigenschaften eines Deduplizierungsspeichergeräts

Sie können einige Eigenschaften eines Deduplizierungsspeichergeräts bearbeiten.

So bearbeiten Sie die Eigenschaften eines Deduplizierungsspeichergeräts

- 1 Doppelklicken Sie auf der Registerkarte "Speicher" auf den Namen des Deduplizierungsspeichergeräts
- 2 Wählen Sie im linken Teilfenster "Eigenschaften".

3 Ändern Sie die Eigenschaften nach Bedarf:

Name	<p>Zeigt den Namen an, der beim Konfigurieren des Deduplizierungsspeichergeräts eingegeben wurde. Sie können den Namen jederzeit ändern.</p>
Beschreibung	<p>Zeigt die Beschreibung, die eingegeben wurde, als der Deduplizierungsdatenträgerspeicher konfiguriert wurde. Sie können die Beschreibung jederzeit ändern.</p>
Login-Konto	<p>Gibt das Login-Konto an, das verwendet wird, um auf das Gerät zuzugreifen.</p> <p>Wenn Sie das Login-Konto ändern, nachdem Sie das Gerät konfigurieren, werden zusätzliche Schritte erfordert, um Zugriff auf die Daten zu aktivieren, die bereits auf dem Gerät gespeichert sind.</p> <p>Siehe "Ändern des Kennworts für das Login-Konto für Deduplizierungsspeicher" auf Seite 1072.</p>
Verschlüsselung	<p>Aktiviert oder deaktiviert Verschlüsselung, während die Daten zum Gerät gesendet werden und während die Daten auf dem Gerät gespeichert werden.</p> <p>Sie sollten die Backup Exec-Verschlüsselungsoptionen nicht für Backup-Aufträge verwenden, die Daten deduplizieren.</p>
Gleichzeitige Vorgänge	<p>Gibt die maximale Zahl der Aufträge an, die Sie auf diesem Gerät gleichzeitig ausführen möchten.</p> <p>Die Anzahl von Aufträgen schwankt abhängig von Ihrer Hardware und Umgebung. Sie müssen diese Einstellung möglicherweise mehr als ein Mal anpassen. Es wird empfohlen, diesen Wert so niedrig einzustellen, dass das System nicht überlastet wird, aber hoch genug, dass Ihre Aufträge schnell ausgeführt werden können.</p>

Datenstromgröße	Gibt die Größe eines einzelnen Schreibvorgangs an, der von Backup Exec gestartet wird. Die Standardgröße variiert basierend auf dem Typ des Geräts, das verwendet wird.
Clientseitige Deduplizierung	<p>Zeigt, ob clientseitige Deduplizierung für dieses Gerät aktiviert ist.</p> <p>Clientseitige Deduplizierung aktiviert einen Remote-Computer, der konfiguriert wird, um Daten direkt zum Deduplizierungsdatenträgerspeicher zu schicken. Nachdem die Daten dedupliziert sind, werden nur eindeutige Daten direkt zum Deduplizierungsspeicher gesendet. Beim Verwenden dieser Option wird der Backup Exec-Server umgangen, wodurch der Backup Exec-Server andere Vorgänge durchführen kann.</p>
Prozentsatz des zu reservierenden Speicherplatzes für Vorgänge, die nicht zu Backup Exec gehören	Zeigt den Speicherplatz an, der für andere Anwendungen als Backup Exec zu reservieren ist;. Der Standardwert ist 5 %.
Protokolliergrad	Gibt den Typ der Informationen an, die Sie in die Diagnoseprotokolle für dieses Gerät einschließen möchten. Die Möglichkeiten reichen von nur den schweren Fehlern bis zu allen Meldungstypen.
Aufbewahrungsdauer für Protokolle	Gibt die Anzahl der Tage an, für die die Diagnoseprotokolle für dieses Gerät gespeichert werden.

Geringer Speicherplatz - Kritisch

Gibt den kritischen Schwellenwert für geringen Speicherplatz an, bei dem Backup Exec eine Warnmeldung senden soll. Backup Exec sendet Warnmeldungen, wenn die Menge des freien Speicherplatzes unter den Schwellenwert für geringen Speicherplatz fällt und erneut, wenn sie unter den Schwellenwert für Warnungen fällt. Die Menge des freien Speicherplatzes umfasst nicht den Speicherplatz, der für nicht mit Backup Exec zusammenhängende Vorgänge reserviert ist.

Sie können den Schwellenwert sowie die Größe des Speicherplatzes in Megabyte (MB) oder Gigabyte (GB) ändern. Dieser Schwellenwert muss kleiner als der Warnschwellenwert für geringen Speicherplatz sein.

Sie sollten den Schwellenwert etwas höher als den Mindestwert festlegen, der zum Ausführen von Aufträgen erforderlich ist. Somit kann das Speicherplatzproblem behoben werden, bevor die Aufträge fehlschlagen.

Die Standardeinstellung ist 5 %.

Diese Eigenschaft wird nur angezeigt, wenn der Deduplizierungsspeicher zu einer Speichergruppe gehört.

Geringer Speicherplatz – Warnung

Gibt den Schwellenwert für geringen Speicherplatz an, bei dem Backup Exec eine Warnmeldung senden soll. Wenn der freie Speicherplatz unter den Schwellenwert für Warnungen auf den kritischen Schwellenwert abfällt, wird eine weitere Warnmeldung gesendet. Die Menge des freien Speicherplatzes umfasst nicht den Speicherplatz, der für nicht mit Backup Exec zusammenhängende Vorgänge reserviert ist.

Sie können den Schwellenwert sowie die Größe des Speicherplatzes in Megabyte (MB) oder Gigabyte (GB) ändern. Dieser Schwellenwert muss kleiner als der Schwellenwert für geringen Speicherplatz sein.

Sie sollten den Schwellenwert etwas höher als den Mindestwert festlegen, der zum Ausführen von Aufträgen erforderlich ist. Somit kann das Speicherplatzproblem behoben werden, bevor die Aufträge fehlschlagen.

Die Standardeinstellung ist 15 %.

Diese Eigenschaft wird nur angezeigt, wenn der Deduplizierungsspeicher zu einer Speichergruppe gehört.

Geringer Speicherplatz

Gibt den Schwellenwert für geringen Speicherplatz an, bei dem Backup Exec eine Warnmeldung senden soll. Wenn der freie Speicherplatz unter den Schwellenwert für Warnungen auf den kritischen Schwellenwert abfällt, wird eine weitere Warnmeldung gesendet. Die Menge des freien Speicherplatzes umfasst nicht den Speicherplatz, der für nicht mit Backup Exec zusammenhängende Vorgänge reserviert ist.

Sie können den Schwellenwert sowie die Größe des Speicherplatzes in Megabyte (MB) oder Gigabyte (GB) ändern.

Sie sollten den Schwellenwert etwas höher als den Mindestwert festlegen, der zum Ausführen von Aufträgen erforderlich ist. Somit kann das Speicherplatzproblem behoben werden, bevor die Aufträge fehlschlagen.

Die Standardeinstellung ist 25 %.

Diese Eigenschaft wird nur angezeigt, wenn der Deduplizierungsspeicher zu einer Speichergruppe gehört.

- 4 Klicken Sie auf "Übernehmen", um die Änderungen zu speichern

Ändern des Kennworts für das Login-Konto für Deduplizierungsspeicher

Wenn Sie ein Backup Exec Exec-Login-Konto als Deduplizierungsspeichergerät angeben, wird ein zusätzliches Benutzerkonto für die Deduplizierungskomponenten mit demselben Benutzernamen und Kennwort erstellt. Wenn Sie allerdings die Identifikationsdaten für das Backup Exec-Login-Konto ändern, werden die Identifikationsdaten für das zusätzliche Benutzerkonto nicht automatisch geändert. Sie müssen das spausер.exe-Dienstprogramm verwenden, um das Kennwort für das zusätzliche Benutzerkonto zu aktualisieren. Dieses Konto wird "Benutzer 1"-Konto genannt, wenn Sie das spausер.exe-Dienstprogramm verwenden, um eine Liste von Benutzernamen anzuzeigen, die mit dem Deduplizierungsdatenträgerspeicher verknüpft sind.

So ändern Sie das Kennwort für das Login-Konto für Deduplizierungsdatenträgerspeicher

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- 2 Wählen Sie "Login-Konten" und dann "Login-Konten verwalten".
- 3 Wählen Sie das zu ändernde Backup Exec-Login-Konto aus und klicken Sie auf "Bearbeiten".
- 4 Geben Sie das aktuelle Kennwort für das Login-Konto ein und klicken Sie dann auf "OK".
- 5 Klicken Sie auf "Kennwort ändern".
- 6 Geben Sie das neue Kennwort im Feld "Kennwort" und im Feldand "Bestätigen" ein .
- 7 Klicken Sie auf "OK".
- 8 Wechseln Sie in der Eingabeaufforderung zum Installationsordner von Backup Exec und geben Sie folgenden Befehl ein:

```
spausers.exe -c -u <UserName>
```

Der Standardinstallationsordner von Backup Exec ist "C:<Backup Exec-Installationsordner>\Backup Exec".

Der Benutzername ist von Groß- und Kleinschreibung abhängig. Wenn Sie den Benutzernamen nicht kennen, geben Sie den folgenden Befehl ein, um den Benutzernamen zu finden, der mit "Benutzer 1" verknüpft ist:

```
spausers.exe -l
```

Sie werden aufgefordert, das ältere und ein neues Kennwort anzugeben. Stellen Sie sicher, dass das neue Kennwort dem Kennwort entspricht, das Sie in Schritt 6 verwendet haben.

Wählen von Speichergeräten für die gemeinsame Nutzung über Direktzugriff

Der Direktzugriff ermöglicht es einem Remote-Computer, Daten direkt an Speichergeräte zu schicken, die sich auf einem Backup Exec-Server befinden. Wenn die gemeinsame Nutzung über Direktzugriff aktiviert ist, wird der Backup Exec-Server umgangen.

Wenn Sie ein Deduplizierungs-Plattenspeichergerät oder ein OpenStorage-Gerät verwenden, das Client-seitige Deduplizierung unterstützt, und die gemeinsame Nutzung über Direktzugriff aktivieren, kann Backup Exec Client-seitige

Deduplizierungen durchführen. Beachten Sie, dass Client-seitige Deduplizierung CPU-intensiv ist.

Die gemeinsame Nutzung über Direktzugriff wird verfügbar, nachdem Sie einen Backup-Auftrag erstellt haben, in dem ein Deduplizierungsgerät ausgewählt und die folgende Option aktiviert ist: Dem Remote-Computer ermöglichen, direkt auf das Speichergerät zuzugreifen und eine Client-seitige Deduplizierung durchzuführen, falls diese unterstützt wird.

Nachdem der richtig konfigurierte Backup-Auftrag erstellt ist, wird die Option "Gemeinsame Nutzung über Direktzugriff" wie folgt angezeigt:

- Auf dem Detailbildschirm für einen Server auf der Registerkarte "Backup und Wiederherstellung".
- Auf dem Detailbildschirm für ein Speichergerät auf der Registerkarte "Speicher".

Darüber hinaus wird die Option "Direktzugriffseigenschaften" auf dem Detailbildschirm für einen Server auf der Registerkarte "Backup und Wiederherstellung" angezeigt.

So wählen Sie Speichergeräte für die gemeinsame Nutzung über Direktzugriff

- 1 Sie haben folgende Möglichkeiten:
 - Doppelklicken Sie auf der Registerkarte "Backup und Wiederherstellung" auf den Server, den Sie für die gemeinsame Nutzung der Geräte einrichten möchten.
 - Doppelklicken Sie auf der Registerkarte "Speicher" auf das Speichergerät, das Sie gemeinsam nutzen möchten.
- 2 Wählen Sie im linken Teilfenster "Gemeinsame Nutzung über Direktzugriff".
- 3 Wählen Sie die Kontrollkästchen für die Elemente aus, die Sie gemeinsam nutzen möchten.

Hinweis: Nach der Aktivierung der gemeinsamen Nutzung über Direktzugriff müssen Sie die Backup Exec-Dienste auf dem Backup Exec-Server neu starten, damit die Änderungen wirksam werden. Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Backup Exec-Dienste" aus. Klicken Sie dann auf "Alle Dienste neu starten".

Siehe ["Bearbeiten von Servereigenschaften für den Direktzugriff"](#) auf Seite 1074.

Bearbeiten von Servereigenschaften für den Direktzugriff

Für Server, für die der Direktzugriff aktiviert ist, können Sie folgende Schritte durchführen:

- Eine Beschreibung des Servers hinzufügen oder ändern
- ICMP-Pingvorgänge zur Erkennung des Servers aktivieren oder deaktivieren
- Ein Login-Konto für den Zugriff auf den Remote-Computer hinzufügen oder bearbeiten.

So bearbeiten Sie Servereigenschaften für den Direktzugriff

- 1 Auf der Registerkarte "Backup und Wiederherstellung" doppelklicken Sie auf den Server, für den der Direktzugriff aktiviert ist.
- 2 Wählen Sie im linken Teilfenster "Direktzugriffseigenschaften".
- 3 Bearbeiten Sie die folgenden Optionen wie benötigt:

Servername	Zeigt den Namen des Remote-Computers oder des verwalteten Backup Exec-Servers an.
Beschreibung	Hier können Sie eine Beschreibung des Servers eingeben.
Port	Zeigt den Port an, der für die Kommunikation zwischen dem Backup Exec-Server und dem Remote-Computer verwendet wird.
ICMP-Pingvorgänge zur Erkennung des Servers verwenden	Erlaubt die Verwendung von ICMP-Ping-Vorgängen auf dem Backup Exec-Server zum Erkennen des Remote-Computers.
Login-Konto	Gibt das Login-Konto an, das erforderlich ist, um auf den Remote-Computer zuzugreifen. Sie können ein neues Login-Konto hinzufügen oder ein vorhandenes Konto bearbeiten.

- 4 Um Änderungen zu speichern, klicken Sie auf "Übernehmen".

Ändern des Speicherorts für ein Deduplizierungsspeichergerät

Sie können den Speicherort eines vorhandenen Deduplizierungsspeichergeräts ändern. Sie können das Deduplizierungsspeichergerät auf einen anderen Datenträger auf dem gleichen Backup Exec-Server verschieben. Wenn Central

Admin Server Feature installiert ist, können Sie das Deduplizierungsspeichergerät auf einen anderen Backup Exec-Server verschieben. Nur ein Deduplizierungsspeichergerät wird pro Backup Exec-Server unterstützt.

Es wird empfohlen, dass Sie den gleichen Namen für das Deduplizierungsspeichergerät verwenden, wenn Sie den Speicherort ändern, aber dies ist nicht zwingend.

So ändern Sie den Speicherort eines Deduplizierungsspeichergeräts

- 1** Stellen Sie sicher, dass keine Aufträge aktiv sind, bis Sie das Ändern des Speicherorts für ein Deduplizierungsspeichergerät abgeschlossen haben.
- 2** Dokumentieren Sie den aktuellen Pfad des Deduplizierungsspeichergeräts, indem Sie die Eigenschaften des Geräts anzeigen.
- 3** Klicken Sie auf der Registerkarte "Speicher" mit der rechten Maustaste auf das Deduplizierungsspeichergerät und klicken Sie dann auf "Deduplizieren".
- 4** Klicken Sie erneut mit der rechten Maustaste auf das Deduplizierungsspeichergerät und klicken Sie dann auf "Löschen".
- 5** Wenn Sie gefragt werden, ob das Speichergerät gelöscht werden soll, klicken Sie auf "Ja".
- 6** Klicken Sie auf die Backup Exec-Schaltfläche, dann auf "Konfiguration und Einstellungen", auf "Backup Exec-Dienste" und schließlich auf "Alle Dienste anhalten".
- 7** Im Windows Explorer kopieren Sie das Deduplizierungsspeichergerät in den neuen Pfad bzw. auf den neuen Datenträger.

Hinweis: Dieser Schritt kann länger dauern, da alle Daten auf dem Gerät in den neuen Speicherort kopiert werden.

- 8** Klicken Sie in der Backup Exec-Administratorkonsole auf die Backup Exec-Schaltfläche, dann auf "Konfiguration und Einstellungen", "Backup Exec-Dienste" und schließlich auf "Alle Dienste neu starten".
- 9** Klicken Sie auf der Registerkarte "Speicher" auf "Speicher konfigurieren", auf "Plattenbasierter Speicher" und dann auf "Weiter".
- 10** Klicken Sie auf "Deduplizierungsspeicher" und dann auf "Weiter".
- 11** Geben Sie einen Namen und eine Beschreibung für das Deduplizierungsspeichergerät ein und klicken Sie dann auf "Weiter".

12 Sie haben folgende Möglichkeiten:

Wenn das Deduplizierungsspeichergerät in Backup Exec 2012 oder höher erstellt wurde	Klicken Sie auf "Neues Deduplizierungsspeichergerät erstellen".
Wenn das Deduplizierungsspeichergerät in einer Version vor Backup Exec 2012 erstellt wurde	Klicken Sie auf "Vorhandenes Deduplizierungsspeichergerät importieren" und geben Sie dann den Pfad ein, auf den Sie das Speichergerät verschoben haben.

13 Klicken Sie auf "Weiter".

14 Geben Sie das Login-Konto an, das für das ursprüngliche Deduplizierungsspeichergerät verwendet wurde, und klicken Sie dann auf "Weiter".

15 Geben Sie an, ob die Verschlüsselung aktiviert werden soll, und klicken Sie dann auf "Weiter".

16 Geben Sie die Anzahl von gleichzeitigen Vorgängen an, die auf dem Deduplizierungsspeichergerät ausgeführt werden können, und klicken Sie dann auf "Weiter".

17 Lesen Sie die Übersicht und klicken Sie auf "Fertigstellen".

18 Wenn das Deduplizierungsspeichergerät online ist, können Sie die ursprünglichen Dateien löschen.

Gemeinsames Nutzen eines Deduplizierungsgeräts durch mehrere Backup Exec-Server

Bei Verwendung von Backup Exec Central Admin Server Feature können Sie auswählen, welche Backup Exec-Server ein Deduplizierungsspeicher- oder OpenStorage-Gerät gemeinsam nutzen können. Wenn Sie ein Deduplizierungsspeicher- oder OpenStorage-Gerät hinzufügen, wird der Backup Exec-Server, mit dem Sie das Gerät hinzugefügt haben, automatisch zum gemeinsamen Nutzen ausgewählt.

Hinweis: Um ein Deduplizierungsspeichergerät gemeinsam zu nutzen, müssen Sie es als OpenStorage-Gerät auf allen Backup Exec-Servern, von denen Sie aus auf das Gerät zugreifen möchten, außer dem Backup Exec-Server, der zur Erstellung verwendet wurde, hinzufügen.

Diese Art des gemeinsamen Nutzens entspricht nicht dem gemeinsamen Nutzen des Direktzugriffs. Mit dem gemeinsamen Nutzen des Direktzugriffs umgeht ein Remote-Computer den Backup Exec-Server, um direkt auf Speichergeräte auf dem Backup Exec-Server zuzugreifen.

Siehe ["Freigeben von Speichergeräten"](#) auf Seite 544.

Siehe ["Wählen von Speichergeräten für die gemeinsame Nutzung über Direktzugriff"](#) auf Seite 1073.

Einsatz der clientseitigen Deduplizierung

Client-seitige Deduplizierung aktiviert einen Remote-Computer, um Daten direkt an ein OpenStorage-Gerät oder an ein Deduplizierungsdatenträgerspeichergerät zu senden. Bei Einsatz der clientseitigen Deduplizierung wird der Backup Exec-Server umgangen, sodass der Backup Exec-Server andere Vorgänge ausführen kann. Wenn Ihr Deduplizierungsgerät Client-seitige Deduplizierung unterstützt, dedupliziert ein Remote-Computer Daten und sendet nur die eindeutigen Daten direkt an ein Deduplizierungs-Plattenspeichergerät oder an ein OpenStorage-Gerät. Client-seitige Deduplizierung ist für Windows-Computer und Linux-Computer verfügbar.

Hinweis: Client-seitige Deduplizierung erhöht möglicherweise die CPU-Nutzung auf dem Remote-Computer, wenn Ihr Deduplizierungsgerät client-seitige Deduplizierung unterstützt.

Wenn Sie einen Backup-Auftrag mit Client-seitiger Deduplizierung erstellen, beachten Sie Folgendes:

- Der Backup-Auftrag darf Ressourcen von nur einem Remote-Computer enthalten.
- Agent for Windows ist auf dem Windows-Remote-Computer erforderlich, um eine Windows-Client-seitige Deduplizierung durchzuführen. Agent for Linux ist auf dem Linux-Computer erforderlich, um eine Linux-Client-seitige Deduplizierung durchzuführen.

Hinweis: Maximal werden mit der aktivierten clientseitigen Deduplizierung 64 Remote Agents pro Backup Exec-Server zugelassen.

- Der Remote-Computer muss per Ping erreichbar sein.
- Der Remote-Computer darf kein Backup Exec-Server sein.
- Für den Backup-Auftrag müssen ein Deduplizierungs-Plattenspeichergerät oder ein OpenStorage-Gerät verwendet werden.

- Die Option "Client-seitige Deduplizierung" muss in den Eigenschaften für das Speichergerät aktiviert sein.
- Die Option "Dem Remote-Computer ermöglichen, direkt auf das Speichergerät zuzugreifen und eine Client-seitige Deduplizierung durchzuführen, falls diese unterstützt wird" muss in den "Speicher" -Optionen für den Backup-Auftrag aktiviert sein. Diese Option ist standardmäßig aktiviert, wenn Sie ein Deduplizierungs-Plattenspeichergerät oder ein OpenStorage-Gerät als Ziel für einen Backup-Auftrag ausgewählt haben.

Wenn Sie den Remote-Computer nicht für die clientseitige Deduplizierung konfigurieren, werden die Daten zur Deduplizierung vom Remote-Computer an den Backup Exec-Server gesendet. Die deduplizierten Daten werden auf dem Deduplizierungsspeicher- bzw. OpenStorage-Gerät gesichert. Durch diesen Vorgang erhöht sich die CPU-Auslastung auf dem Backup Exec-Server. Es ist jedoch hilfreich, wenn Sie ältere Remote-Computer sichern.

Siehe ["Info zu Deduplication Feature"](#) auf Seite 1047.

Siehe ["So werden Backup-Aufträge für die Deduplizierung eingerichtet"](#) auf Seite 1079.

Siehe ["Bearbeiten von Eigenschaften eines OpenStorage-Geräts"](#) auf Seite 1061.

Siehe ["Bearbeiten der Eigenschaften eines Deduplizierungsspeichergeräts"](#) auf Seite 1067.

So werden Backup-Aufträge für die Deduplizierung eingerichtet

Wählen Sie zum Einrichten eines Backup-Auftrags zur Deduplizierung die Option "Auf Deduplizierungsspeicher sichern" aus. Wählen Sie in den Speicher Einstellungen entweder ein OpenStorage-Gerät oder ein Deduplizierungs-Plattenspeichergerät als Zielgerät aus und dann die zu verwendende Deduplizierungsmethode.

Die folgenden Deduplizierungsmethoden sind verfügbar:

- Zum Aktivieren der Client-seitigen Deduplizierung sollten Sie die Option "Dem Remote-Computer ermöglichen, direkt auf das Speichergerät zuzugreifen und eine Client-seitige Deduplizierung durchzuführen, falls diese unterstützt wird" auswählen. Dies ist die Standardoption. Wenn das Speichergerät, das Sie für den Auftrag auswählen, die clientseitige Deduplizierung nicht unterstützt, wird entweder die serverseitige Backup Exec-Deduplizierung oder die Appliance-Deduplizierung verwendet.
- Soll die serverseitige Backup Exec-Deduplizierung aktiviert werden, aktivieren Sie die Option "Dem Remote-Computer ermöglichen, über den Backup

Exec-Server auf das Speichergerät zuzugreifen und eine serverseitige Backup Exec-Deduplizierung durchzuführen, falls diese unterstützt wird". Wenn das Speichergerät, das Sie für den Auftrag auswählen, serverseitige Deduplizierung nicht unterstützt, wird Appliance-Deduplizierung verwendet.

Siehe ["Einsatz der clientseitigen Deduplizierung"](#) auf Seite 1078.

Verwenden der optimierten Duplizierung, um deduplizierte Daten zwischen OpenStorage-Geräten oder Deduplizierungsspeichergeräten zu kopieren

Backup Exec unterstützt die optimierte Duplizierung, mit der deduplizierte Daten direkt von einem OpenStorage-Gerät auf ein anderes OpenStorage-Gerät desselben Herstellers kopiert werden. Beide Geräte müssen am selben Backup Exec-Server angeschlossen sein. Beispielsweise können Sie Daten von einem Veritas PureDisk-Gerät auf ein anderes Veritas PureDisk-Gerät kopieren. Da die Daten dedupliziert werden, können nur eindeutige Daten zwischen den Geräten kopiert werden.

Um Daten zwischen OpenStorage-Geräten oder Deduplizierungs-Plattenspeichergeräten zu kopieren, müssen Sie einen Auftrag zum Kopieren von Backup-Sätzen erstellen. Das Zielgerät für den Duplizierungsauftrag muss der gleiche Gerätetyp vom selben Hersteller wie das Gerät sein, das im Quell-Backup-Auftrag verwendet wurde. Keine zusätzlichen Einstellungen sind erforderlich. Optimierte Duplizierung wird automatisch ausgeführt, wenn Sie einen Auftrag zum Duplizieren von Backup-Daten zwischen entsprechenden Geräten einrichten. Sie können Daten von jedem Gerät wiederherstellen.

Optimierte Duplizierung ist bei Backup-Sätzen möglich, die für Granular Recovery Technology aktiviert wurden (GRT). Jedoch unterstützen nur Plattenspeichergeräte für die Deduplizierung und PureDisk-Geräte optimierte Duplizierung für GRT-aktivierte Backup-Sätze.

Die unterstützten Speichergerättypen finden Sie in der Liste der mit Backup Exec kompatiblen Hardware.

Verwenden der optimierten Duplizierung, um deduplizierte Daten zwischen OpenStorage-Geräten oder Deduplizierungsspeichergeräten zu kopieren

Hinweis: Die OpenStorage-Geräte müssen vom gleichen Hersteller sein. Sie können optimierte Duplizierung zwischen OpenStorage-Geräten von den verschiedenen Händlern nicht durchführen. Wenn Sie versuchen, deduplizierte Daten zwischen OpenStorage-Geräten von den verschiedenen Händlern zu kopieren, wird normale Duplizierung anstelle der optimierten Duplizierung durchgeführt.

Verwenden der optimierten Duplizierung mit Central Admin Server Feature

Wenn Sie Central Admin Server Feature (CAS) verwenden, wird der Funktionsumfang der optimierten Duplizierung um folgende Vorgänge erweitert:

- Kopieren von Daten aus einem Deduplizierungsspeichergerät auf einem Backup Exec-Server auf einem Deduplizierungsspeichergerät auf einem anderen Backup Exec-Server.
- Kopieren von Daten aus einem OpenStorage-Gerät an einem Backup Exec-Server auf ein anderes OpenStorage-Gerät an einem anderen Backup Exec-Server.

Um die optimierte Duplizierung mit CAS zu verwenden, müssen folgende Anforderungen erfüllt sein:

- Sie benötigen eine Lizenz für Enterprise Server Feature. CAS wird im Rahmen von Enterprise Server Feature installiert.
- Alle Backup Exec-Server, die Sie mit CAS entweder als zentralen Administrationsserver oder als verwalteten Backup Exec-Server verwenden, müssen eine 64-Bit-Windows-Version verwenden.
- Die CAS-Umgebung muss einen zentralen Administrationsserver und mindestens einen verwalteten Backup Exec-Server enthalten.
- Für die clientseitige Deduplizierung und serverseitige Backup Exec-Deduplizierung müssen Sie einen Deduplizierungsspeicher auf dem Backup Exec-Server konfigurieren, aus dem Sie die deduplizierten Daten kopieren möchten. Sie müssen außerdem einen Deduplizierungsspeicher auf dem Backup Exec-Server konfigurieren, auf den Sie die deduplizierten Daten kopieren möchten.
- Bei der Anwendungsdeduplizierung muss der Backup Exec-Server, aus dem Sie die deduplizierten Daten kopieren möchten, das entsprechende Plugin für das OpenStorage-Gerät und ein richtig konfiguriertes OpenStorage-Gerät haben. Zusätzlich muss der Backup Exec-Server, auf den Sie die deduplizierten Daten kopieren möchten, ebenfalls das entsprechende Plugin für das OpenStorage-Gerät und ein richtig konfiguriertes OpenStorage-Gerät haben.

Verwenden der optimierten Duplizierung, um deduplizierte Daten zwischen OpenStorage-Geräten oder Deduplizierungsspeichergeräten zu kopieren

- Sie müssen Deduplizierungsgeräte zwischen Backup Exec-Servern gemeinsam nutzen.
- Sie müssen die Medien auf dem Zielsever inventarisieren und katalogisieren, bevor Sie alle Dateien vom kopierten Backup-Satz wiederherstellen. Sie müssen dies unabhängig von der Konfiguration der gemeinsamen Nutzung des Katalogs für CAS durchführen.

Verwenden der optimierten Duplizierung zum Übertragen von Backup-Daten an einen Remote-Standort

Sie können optimierte Duplizierung verwenden, um Backup-Daten über eine WAN-Verbindung an einen Remote-Standort zu übertragen. Sie sollten das Datenträgerspeichergerät der Zieldeduplizierung mit einem vollständigen Backup der Server vorauffüllen. Diese Aufgabe des Vorauffüllens ist auch unter der Bezeichnung "Seeding des Deduplizierungsspeichergeräts" bekannt. Seeding hilft, den zeitaufwendigen und Bandbreite-intensiven Prozess des Sendens von großen Mengen Backup-Daten über die WAN-Verbindung mit niedriger Bandbreite zu vermeiden.

Um für ein Gerät ein Seeding auszuführen, können Sie ein vollständiges Backup auf einem externen Speichergerät wie einem USB-Laufwerk speichern. Sie können dann das USB-Laufwerk an den Remote-Standort transportieren, wo sich der Backup Exec-Server und das Zieldeduplizierungsspeichergeräts befinden, und die Backup-Daten auf das Deduplizierungsspeichergerät kopieren.

Einrichten der optimierten Duplizierung

Sie richten einen duplizierten Backup-Auftrag ein, um eine optimierte Duplizierung durchzuführen.

Verwenden der optimierten Duplizierung, um deduplizierte Daten zwischen OpenStorage-Geräten oder Deduplizierungsspeichergeräten zu kopieren

Tabelle B-5 Einrichten der optimierten Duplizierung

Schritt	Weitere Informationen
<p>Wenn Sie CAS verwenden, führen Sie folgende Schritte durch:</p> <ul style="list-style-type: none"> ■ Gewährleisten Sie, dass ein zentraler Administrationsserver und mindestens ein verwalteter Backup Exec-Server verfügbar ist. ■ Gewährleisten Sie, dass der Backup Exec-Server, aus dem Sie die deduplizierten Daten kopieren möchten, ein Deduplizierungsspeichergerät (für client- oder serverseitige Backup Exec-Deduplizierung) bzw. ein OpenStorage-Gerät (für Anwendungsdeduplizierung) hat. Gewährleisten Sie außerdem, dass der Backup Exec-Server, auf den Sie die deduplizierten Daten kopieren möchten, ein Deduplizierungsspeichergerät (für client- oder serverseitige Backup Exec-Deduplizierung) bzw. ein OpenStorage-Gerät (für Anwendungsdeduplizierung) hat. ■ Gewährleisten Sie, dass die Backup Exec-Server für das gemeinsame Nutzen konfiguriert sind. <p>Hinweis: Diese Informationen gelten nur für CAS. Ist CAS nicht aktiviert, überspringen Sie diesen Schritt.</p>	<p>Siehe "Konfigurieren eines OpenStorage-Geräts" auf Seite 1058.</p> <p>Siehe "Erstellen oder Importieren des Deduplizierungsspeichers" auf Seite 1064.</p>
<p>Erstellen Sie einen Backup-Auftrag, der ein OpenStorage-Gerät oder ein Deduplizierungsdatenträgerspeichergerät als Ziel verwendet.</p>	<p>Siehe "Sichern von Daten" auf Seite 174.</p>

Schritt	Weitere Informationen
<p>Erstellen Sie einen Auftrag zum Duplizieren von Backup-Sätzen und wählen Sie das entsprechende OpenStorage-Gerät bzw. das Deduplizierungs-Plattenspeichergerät als Ziel aus.</p> <p>Hinweis: Das Zielgerät für den Duplizierungsauftrag muss der gleiche Gerätetyp vom selben Hersteller wie das Gerät sein, das im Quell-Backup-Auftrag verwendet wurde.</p>	<p>Siehe "Manuelles Duplizieren von Backup-Sätzen bzw. Auftragsverläufen" auf Seite 246.</p>

Siehe "[Gemeinsames Nutzen eines Deduplizierungsgeräts durch mehrere Backup Exec-Server](#)" auf Seite 1077.

Kopieren deduplizierter Daten auf Bänder

Mit Backup Exec können Sie deduplizierte Daten aus einem OpenStorage-Gerät auf Band kopieren und langfristig oder extern aufbewahren. Beim Kopieren der Daten auf Bänder werden diese wieder hydratisiert. Das heißt, die Dateien werden wieder in ihr ursprüngliches Format umgewandelt und sind somit nicht dedupliziert.

Um deduplizierte Daten auf Bänder zu kopieren, müssen Sie einen Backup-Auftrag zum Duplizieren erstellen, der die Backup-Sätze vom OpenStorage-Gerät auf ein Bandgerät kopiert.

Siehe "[Manuelles Duplizieren von Backup-Sätzen bzw. Auftragsverläufen](#)" auf Seite 246.

Verwendung der Deduplizierung mit Verschlüsselung

Sie sollten die Backup Exec-Verschlüsselungsoptionen nicht für Backup-Aufträge verwenden, die Daten deduplizieren. Daten können nicht dedupliziert werden, wenn die Backup Exec-Verschlüsselungsoptionen verwendet werden.

Wenn deduplizierte Daten auf einem Deduplizierungs-Plattenspeichergerät verschlüsselt werden sollen, können Sie die Verschlüsselungseigenschaft auf dem Deduplizierungs-Plattenspeichergerät aktivieren.

Siehe "[Verwaltung von Verschlüsselungscodes](#)" auf Seite 731.

Wiederherstellen eines Deduplizierungs-Plattenspeichergeräts oder von deduplizierten Daten

Sie können einen Deduplizierungsspeicher wiederherstellen, indem Sie den Wiederherstellungsassistenten ausführen. Wenn Sie ein Deduplizierungsdatenträgerspeichergerät wiederherstellen, wird der ursprüngliche Ordner gelöscht und wird dann durch den wiederhergestellten Ordner ersetzt.

Hinweis: Sie können die Wiederherstellung eines Deduplizierungsdatenträgerspeichergeräts nicht umleiten. Ein Deduplizierungs-Plattenspeichergerät muss an seinem ursprünglichen Speicherort wiederhergestellt werden.

Um deduplizierte Daten wiederherzustellen, können Sie einen regelmäßigen Wiederherstellungsauftrag erstellen. Es sind keine zusätzlichen Einstellungen erforderlich.

Siehe ["Wiederherstellen von Daten aus einem Server, einem Backup-Satz, einem Backup-Auftrag oder einem Speichergerät"](#) auf Seite 261.

So stellen Sie ein Deduplizierungs-Plattenspeichergerät wieder her

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" mit der rechten Maustaste auf den Computer, für den Sie das Deduplizierungs-Plattenspeichergerät wiederherstellen möchten, und klicken Sie dann auf "Wiederherstellen".
- 2 Wählen Sie "Shadow Copy-Komponenten" aus und klicken Sie auf "Weiter".
- 3 Folgen Sie den Anweisungen des Wiederherstellungsassistenten, um die Daten wiederherzustellen.

Siehe ["Notfallwiederherstellung des Deduplizierungsspeichergeräts"](#) auf Seite 1085.

Notfallwiederherstellung des Deduplizierungsspeichergeräts

Ein Deduplizierungsspeichergerät ist auf dem Backup Exec-Server verfügbar. Wenn es auf dem Backup Exec-Server einen Systemausfall gibt, gehen die Daten auf dem Deduplizierungsspeichergerät verloren. Deshalb sollten Sie Schritte unternehmen, um eine Wiederherstellung nach einem Systemausfall vorzubereiten. Damit Sie auf einen Systemausfall vorbereitet sind, können Sie mit Backup Exec

einen Snapshot eines Deduplizierungsspeichergeräts erstellen. Der Snapshot umfasst den Ordner und die Inhalte des Ordners. Sie können den Snapshot auf Band speichern, das Sie dann verwenden können, um den Deduplizierungsspeicher wiederherzustellen, nachdem Sie den Backup Exec-Server wiederhergestellt haben.

Wenn Sie Daten mithilfe des Snapshot wiederherstellen, treten die folgenden Prozesse auf:

- Backup Exec beendet die Deduplizierungsdienste, wenn diese ausgeführt werden. Die Deduplizierungsdienste sind von den Backup Exec-Diensten getrennt; die Backup Exec-Dienste sind somit nicht betroffen.
- Backup Exec löscht alle Dateien, die im Deduplizierungsspeicher vorhanden sind.
- Der Deduplizierungsdatenträgerspeicher wird an seinem ursprünglichen Ort, zusammen mit den Inhalten des Ordners, wiederhergestellt.
- Die Deduplizierungsdienste werden neu gestartet.

Hinweis: Wenn Sie Backup Exec Simplified Disaster Recovery (SDR) verwenden, um den Backup Exec-Server wiederherzustellen, stellt SDR den Deduplizierungsspeicher nicht während der Wiederherstellung des Backup Exec-Servers wieder her.

Vorbereitung für Notfallwiederherstellung eines Deduplizierungsspeichergeräts

Damit Sie auf einen Systemausfall vorbereitet sind, können Sie mit Backup Exec einen Snapshot eines Deduplizierungsspeichergeräts erstellen. Der Snapshot umfasst den Ordner und die Inhalte des Ordners. Sie können den Snapshot auf Band speichern, das Sie dann verwenden können, um Ihr Deduplizierungsdatenträgerspeichergerät nach einem Systemausfall wiederherzustellen.

So bereiten Sie sich auf die Notfallwiederherstellung eines Deduplizierungsdatenträgerspeichergeräts vor

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" mit der rechten Maustaste auf den Server in dem sich das Deduplizierungsdatenträgerspeichergerät befindet.
- 2 Wählen Sie "Backup" und dann "Auf Band sichern" aus.
- 3 Klicken Sie im Dialogfeld "Auswählen" auf "Bearbeiten".
- 4 Erweitern Sie "Shadow Copy-Komponenten" und "Benutzerdaten" und wählen Sie dann "Backup Exec-Deduplizierungsspeicher".

- 5 Klicken Sie auf "OK".
- 6 Legen Sie alle zusätzlichen Optionen fest, die Sie verwenden möchten.
Es wird empfohlen, dass dieser Auftrag kurz vor den
Deduplizierungswartungszeiten um 00:20 Uhr und 12:20 Uhr ausgeführt wird.
- 7 Klicken Sie auf "OK", um den Auftrag zu erstellen.

Siehe ["Wiederherstellen eines Deduplizierungs-Plattenspeichergeräts oder von deduplizierten Daten"](#) auf Seite 1085.

Notfallwiederherstellung von OpenStorage-Geräten

Bei OpenStorage-Geräten sind die folgenden Szenarien zur Notfallwiederherstellung möglich:

- Das Gerät fällt aus.
- Der Backup Exec-Server, der das Gerät nutzt, fällt aus.

Wenn das Gerät ausfällt, sollten Sie die Dokumentation vom Händler des Geräts zu Rate ziehen. Wenn der Backup Exec-Server ausfällt und Sie Backup Exec auf dem Backup Exec-Server neu installieren müssen, müssen Sie das Gerät erneut konfigurieren und die Medien inventarisieren und katalogisieren, nachdem der Backup Exec-Server wiederhergestellt wurde.

Backup Exec Agent for VMware

Dieser Anhang enthält folgende Themen:

- [Agent for VMware](#)
- [Anforderungen für die Verwendung des Agent for VMware](#)
- [Einsatz des Agent for VMware unter Windows Server 2016 und höher](#)
- [Installieren von Agent for VMware](#)
- [Hinzufügen eines VMware vCenter-Servers oder ESX-/ESXi-Host zur Serverliste auf der Registerkarte "Backup- und Wiederherstellung"](#)
- [Anzeigen von Details zu VMware-Ressourcen](#)
- [Installieren von Agent for Windows auf virtuellen VMware-Computern](#)
- [Push-Installation von Agent for Windows auf virtuellen VMware-Computern](#)
- [Info zum Einrichten einer vertrauenswürdigen Verbindung zu einem vCenter/ESX\(i\)-Server](#)
- [Empfehlungen dazu, wann virtuelle Backups und wann Backups mit Agent genutzt werden sollten.](#)
- [Sichern von virtuellen VMware-Computern](#)
- [Wiederherstellen virtueller VMware-Computer und VMDK-Dateien](#)
- [Info zur Sofortwiederherstellung eines virtuellen VMware-Computers](#)
- [Beheben von Fehlern mit dem Agent for VMware](#)

- [Informationen zur Funktion "Wiederherstellung bereit" für virtuelle VMware-Computer](#)

Agent for VMware

Mit Backup Exec Agent for VMware (Agent for VMware) können Sie virtuelle Computer sichern und wiederherstellen, die VMware ESX/ESXi/vSphere/vCenter nutzen.

Die unterstützten Betriebssysteme, Plattformen und Anwendungen finden Sie in der Liste der mit Backup Exec kompatiblen Hardware und Software.

Backup Exec führt ein Backup in einem Durchgang durch, um alle virtuellen Gastcomputer und VSS-fähigen Anwendungen, die auf den virtuellen Gastcomputern installiert sind, zu schützen. Backup Exec Granular Recovery Technology (GRT) ist standardmäßig für Dateien und Ordner aktiviert. Sie können ein GRT-fähiges Backup verwenden, um einzelne Dateien und Ordner aus einem virtuellen Windows-Gastcomputer wiederherzustellen, ohne den gesamten virtuellen Computer wiederherstellen zu müssen. Darüber hinaus können Sie einzelne Elemente aus Microsoft Exchange-, SQL, SharePoint und Active Directory wiederherstellen, die sich auf virtuellen Gastcomputern befinden, wenn Sie die Optionen für GRT auf Anwendungsebene im Backup-Auftrag auswählen. Beachten Sie, dass GRT auf Anwendungsebene nicht standardmäßig aktiviert ist. Sie müssen die gewünschten Optionen für GRT auf Anwendungsebene auswählen, wenn Sie einen Backup-Auftrag einrichten.

Informationen zu den Best Practices zum Einsatz des Backup Exec Agent for VMware finden Sie unter *Best Practices für Backup Exec*.

Die zusätzlichen Funktionen des Agent for VMware ermöglichen Folgendes:

- Umleiten der Wiederherstellung von Daten aus einem virtuellen Gastcomputer in einen anderen Ordner, Datenspeicher, Host oder ein anderes Netzwerk
- Sichern auf einem Festplatten- oder Bandgerät
- Ausführen inkrementeller und Differenzial-Backups Diese Funktion ist nur verfügbar, wenn die virtuellen Computer mit Hardwareversion 7 oder höher konfiguriert sind.

Siehe ["Anforderungen für die Verwendung des Agent for VMware"](#) auf Seite 1090.

Siehe ["Verwenden von Granular Recovery Technology \(GRT\) mit Agent for VMware"](#) auf Seite 1115.

Siehe ["Sichern von virtuellen VMware-Computern"](#) auf Seite 1100.

Siehe ["Wiederherstellen virtueller VMware-Computer und VMDK-Dateien"](#) auf Seite 1121.

Anforderungen für die Verwendung des Agent for VMware

Bevor Sie Agent for VMware verwenden, vergewissern Sie sich, dass die folgenden Anforderungen erfüllt sind:

- Installieren Sie die Lizenz für Agent for Hyper-V and VMware auf dem Backup Exec-Server. Der Backup Exec-Server führt Backup- und Wiederherstellungsaufträge aus.
- Legen Sie fest, ob Granular Recovery Technology (GRT) von Backup Exec zum Wiederherstellen einzelner Elemente von Microsoft-Anwendungen verwendet werden soll. Wenn Sie vorhaben, GRT zu verwenden, installieren Sie Agent for Windows auf den virtuellen Computern, auf denen Windows ausgeführt wird.

Hinweis: Wenn Sie GRT nutzen, stellen Sie sicher, dass Sie eindeutige Namen für virtuelle Computer verwenden. GRT-Vorgänge funktionieren möglicherweise nicht richtig, wenn doppelte Namen auftreten.

Siehe "[Verwenden von Granular Recovery Technology \(GRT\) mit Agent for VMware](#)" auf Seite 1115.

Siehe "[Installieren von Agent for Windows auf virtuellen VMware-Computern](#)" auf Seite 1094.

- Stellen Sie anhand der Hardwarekompatibilitätsliste und der Softwarekompatibilitätsliste sicher, dass Ihre Umgebung unterstützte Hardware und Software aufweist.
Die unterstützten Betriebssysteme, Plattformen und Anwendungen finden Sie in der Liste der mit Backup Exec kompatiblen Hardware und Software.
- Stellen Sie sicher, dass die Namen Ihrer virtuellen Computer keine Zeichen enthalten, die VMware nicht unterstützt. Nur die folgenden Zeichen dürfen in Namen von virtuellen Computern verwendet werden:
 - ASCII-Groß- und Kleinbuchstaben
 - Zahlen
 - Punkt (.)
 - Bindestrich (-)
 - Unterstrich (_)
 - Pluszeichen (+)
 - Linke und rechte Klammer ()

- Leerzeichen
Die Verwendung anderer als der oben aufgeführten Zeichen kann dazu führen, dass Backup-Aufträge fehlschlagen.
- Gewährleisten Sie, dass HTTPS-Port 443 auf dem vCenter-/ESXi-Server genutzt wird. Port 443 ist der Standard-HTTPS-Port. Backup Exec ist so konfiguriert, dass SSL-Port 443 zum Abrufen des SSL-Zertifikats vom vCenter-/ESXi-Server verwendet wird. Wenn der vCenter-Server nicht den Standard-HTTPS-Port 443 verwendet, müssen Sie den Server Backup Exec mit der Port-Nummer am Ende des Servernamens hinzufügen.
Beispiel: myvCenter60.Domäne: 482
- Wenn Sie VMware-vCenter Server 6 verwenden, gewährleisten Sie, dass keine Mischkonfiguration mit IPv4 und IPv6 vorliegt. VMware vCenter Server 6.0 unterstützt Mischkonfigurationen mit IPv4 und IPv6 nicht. Backup- und Wiederherstellungsaufträge schlagen möglicherweise in dieser Konfiguration fehl.

Einsatz des Agent for VMware unter Windows Server 2016 und höher

Die folgenden Informationen gelten für virtuelle Computer mit Windows Server 2016 oder höher:

- Wenn auf dem Backup Exec-Server ein Betriebssystem vor Server ausgeführt wird, kann die Granular Recovery Technology (Anwendungsebene und Datei/Ordner-Ebene) nicht für einen virtuellen Computer durchgeführt werden, der einen Datenträger mit dem Dateisystem "ReFS" hat. Ein Backup-Auftrag für einen virtuellen Computer, der mit Windows Server ReFS und GRT konfiguriert ist, wird mit dem Status "Erfolg mit Ausnahmen" abgeschlossen.

Hinweis: Backup Exec unterstützt GRT auf Datei-/Ordner-Ebene für das ReFS-Datenträger oder GRT auf Anwendungsebene für virtuelle Computer nur dann, wenn der Backup Exec-Server unter derselben oder einer höheren Betriebssystemversion als der virtuelle Computer ausgeführt wird.

Beispiel: Wenn der virtuelle Computer Windows Server 2016 und REFS-Datenträger nutzt, muss auf dem Backup Exec-Server ebenfalls Windows Server 2016 oder höher ausgeführt werden.

- Wenn der Backup Exec-Server ein Betriebssystem vor Windows Server ausführt, kann Granular Recovery Technology (Anwendungsebene und Datei/Ordner) nicht für den virtuellen Computer durchgeführt werden, der Volumes enthält,

auf denen die Windows Server 2016-Deduplizierung aktiviert ist. Ein Backup-Auftrag für einen virtuellen Computer, der mit einem Windows Server -Deduplizierungsdatenträger konfiguriert und auf dem GRT aktiviert ist, wird mit dem Status "Erfolg mit Ausnahmen" abgeschlossen.

Siehe ["Agent for VMware"](#) auf Seite 1089.

Installieren von Agent for VMware

Der Agent for VMware wird als Teil von Agent for Hyper-V and VMware installiert. Installieren Sie diese Lizenz auf dem Backup Exec-Server, um Agent for VMware zu aktivieren. Sie müssen den Agent nicht auf dem Hostserver installieren.

Siehe ["Installieren zusätzlicher Agents und Funktionen auf dem lokalen Backup Exec-Server"](#) auf Seite 66.

Hinzufügen eines VMware vCenter-Servers oder ESX-/ESXi-Host zur Serverliste auf der Registerkarte "Backup- und Wiederherstellung"

Sie können VMware vCenter-Server und ESX-/ESXi-Hosts der Liste von Servern auf der Registerkarte "Backup und Wiederherstellung" hinzufügen, damit Sie die virtuellen Computer sichern können, die darauf gehostet werden.

Wenn Sie diese Hosts hinzufügen, wird in Backup Exec die Meldung "Kein Vertrauen hergestellt" angezeigt, wenn zwischen den Hosts und dem Medienserver keine vertrauenswürdige Verbindung eingerichtet wurde. Das Backup bzw. die Wiederherstellung schlägt jedoch nicht fehl. In Backup Exec können Sie das Zertifikat verifizieren und die vertrauenswürdige Verbindung herstellen.

So fügen Sie einen VMware-vCenter Server oder ESX-/ESXi-Host der Liste von Servern auf der Registerkarte "Backup und Wiederherstellung" hinzu

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" unter "Server und virtuelle Hosts" auf "Hinzufügen".
- 2 Wählen Sie "VMWare vCenter-Server oder ESX-Host", und klicken Sie dann auf "Weiter".
- 3 Wählen Sie "Einen VMware vCenter- oder ESX-Server zur Serverliste hinzufügen" aus.
- 4 Geben Sie den Namen oder die IP-Adresse des hinzuzufügenden Hyper-V-Hosts und eine optionale Beschreibung ein.

- 5 Wenn Sie über Backup Exec den Agent for Windows auf allen virtuellen Gastcomputern des Host-Servers installieren möchten, stellen Sie sicher, dass die Option "Nach Hinzufügen des virtuellen Host Backup Exec Agent for Windows auf den virtuellen Gastcomputern installieren" aktiviert ist.

Um Granular Recovery Technology (GRT)-Backups der Microsoft-Anwendungen durchzuführen, die auf den virtuellen Computern installiert werden, muss der Agent for Windows auf den virtuellen Gastcomputern installiert sein. Wenn Sie Agent for Windows nicht auf den virtuellen Gastcomputern installieren möchten, deaktivieren Sie das Kontrollkästchen. Sie können den Agent for Windows später installieren, wenn Sie sich entscheiden, dass Sie GRT verwenden möchten.

- 6 Klicken Sie auf "Weiter".
- 7 Wählen Sie in der Dropdown-Liste das korrekte Login-Konto für den Server aus.

Beindet sich das korrekte Login-Konto nicht in der Liste, klicken Sie auf "Hinzufügen/Bearbeiten", um es der Liste hinzuzufügen.

- 8 Klicken Sie auf "Weiter".
- 9 Prüfen Sie die zusammenfassenden Informationen, und klicken Sie dann auf "Fertigstellen".

Siehe ["Serverliste auf der Registerkarte "Backup und Wiederherstellung"](#) auf Seite 166.

Siehe ["Installieren von Agent for Windows auf virtuellen VMware-Computern"](#) auf Seite 1094.

Siehe ["Erstellen eines Vertrauensverhältnisses zwischen dem Backup Exec-Server und einem Remote-Computer"](#) auf Seite 1031.

Anzeigen von Details zu VMware-Ressourcen

Auf der Registerkarte "Backup und Wiederherstellung" finden Sie ein Teilfenster "Details" im unteren Teil des Bildschirms. Das Teilfenster "Details" gibt zusätzliche Details für ausgewählte Servertypen aus der Serverliste im oberen Teil des Bildschirms an. Zusätzliche Details und Funktionalität erscheinen, wenn ein VMware-Host ausgewählt wird. Im Teilfenster "Details" für VMware-Ressourcen finden Sie Details über Backup-Aufträge der letzten 7 Tage, das Datum des letzten Backups und das Datum des nächsten geplanten Backups. Außerdem können Sie Daten sichern und wiederherstellen sowie die Liste virtueller Gastcomputer filtern.

Im Teilfenster "Details" für VMware-Ressourcen finden Sie Ressourcen, die nicht in der Serverliste angezeigt werden. Beispiele:

- Virtuelle Computer, auf denen der Agent for Windows nicht installiert ist.
- Virtuelle Computer ohne Windows (z. B. Linux).
- Virtuelle Computer, auf denen GRT-Backups nicht aktiviert sind.

Das Teilfenster "Details" für virtuelle VMWare-Computer enthält eine Kombination aus aktuellen und Verlaufsinformationen. Wenn Sie auf die Schaltfläche "Aktualisieren" klicken, kann Backup Exec alle Serverressourcen erkennen. Wurde jedoch ein virtueller Computer verschoben, gelöscht, oder wurden seine Identifikationsdaten geändert, tritt Folgendes auf:

- Wenn der virtuelle Computer nie gesichert wurde, löscht Backup Exec ihn aus dem Teilfenster "Details".
- Wenn der virtuelle Computer gesichert wurde, löscht Backup Exec ihn nicht aus dem Teilfenster "Details".

Wenn ein virtueller Computer umbenannt wurde, tritt im Teilfenster "Details" Folgendes auf:

- Wenn der virtuelle Computer gesichert wurde, schließt das Teilfenster "Details" einen Eintrag für den neuen Namen ein und behält den Eintrag für den alten Namen.
- Wenn der virtuelle Computer nie gesichert wurde, schließt das Teilfenster "Details" nur den neuen Namen des virtuellen Computers ein.

So zeigen Sie Details zu VMware-Ressourcen an

- ◆ Wählen Sie auf der Registerkarte "Backup und Wiederherstellung" einen VMWare-Host aus der Serverliste aus.

Die Ressourcen für den ausgewählten Host werden im Teilfenster "Details" angezeigt.

Installieren von Agent for Windows auf virtuellen VMware-Computern

Um Granular Recovery Technology (GRT) in Backup Exec für Microsoft-Anwendungsdaten zu verwenden, installieren Sie Agent for Windows auf allen virtuellen Computern, auf denen Windows ausgeführt wird. Dazu muss der vCenter- bzw. ESX/ESXi-Host bereits in der Serverliste auf der Registerkarte "Backup und Wiederherstellung" enthalten sein.

Hinweis: VMware Tools sollten installiert sein, bevor Sie den Agent for Windows auf einem virtuellen Gastcomputer installieren, wenn Sie den VSS-Anbieter von Backup Exec verwenden möchten.

Siehe ["Hinzufügen eines VMware vCenter-Servers oder ESX-/ESXi-Host zur Serverliste auf der Registerkarte "Backup- und Wiederherstellung" "](#) auf Seite 1092.

So installieren Sie den Agent for Windows auf virtuellen VMware-Computern

- 1** Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" unter "Server und virtuelle Hosts" auf "Hinzufügen".
- 2** Wählen Sie "VMWare vCenter-Server oder ESX-Host", und klicken Sie dann auf "Weiter".
- 3** Aktivieren Sie die Option "Backup Exec Agent for Windows auf den virtuellen Computern eines VMware-vCenter-Server oder ESX-Host installieren".
- 4** Wählen Sie den Server aus der Dropdown-Liste und klicken Sie dann auf "Weiter".
- 5** Aktivieren Sie die Option "Zulassen, dass Backup Exec ein Vertrauensverhältnis mit den Servern herstellt", und klicken Sie dann auf "Weiter".
- 6** Wählen Sie die virtuellen Gastcomputer aus, auf denen Agent for Windows installiert werden soll, und klicken Sie dann auf "Weiter".
- 7** Wählen Sie das Login-Konto für die virtuellen Gastcomputer aus, und klicken Sie dann auf "Weiter".

8 Wählen Sie die folgenden Optionen, und klicken Sie anschließend auf "Weiter".

Backup Exec Agent for Windows automatisch auf die aktuelle Version aktualisieren

Durch Auswählen dieser Option wird die neueste Version von Agent for Windows installiert, wenn eine ältere Version von Agent for Windows bereits auf den ausgewählten virtuellen Computern installiert ist.

Hinweis: Wenn Sie einfach das Vertrauen mit der vorhandenen Version des Agent for Windows wiederherstellen möchten, die bereits auf den ausgewählten virtuellen Computern installiert ist, sollten Sie dieses Kontrollkästchen deaktivieren.

Remote-Computer automatisch neu starten, nachdem der Backup Exec Agent for Windows installiert wurde und wenn ein Neustart erforderlich ist

Aktivieren Sie diese Option, damit Backup Exec den Remote-Computer automatisch neu starten kann, wenn dies erforderlich ist.

9 Prüfen Sie die Übersicht und klicken Sie dann auf "Installieren".

Push-Installation von Agent for Windows auf virtuellen VMware-Computern

Sie können den Assistenten Server hinzufügen verwenden, um den Agent for Windows über eine Push-Installation auf ausgewählten virtuellen VMware-Computern zu installieren. Sie können entscheiden, den Agent for Windows auf allen benötigten virtuellen Gastcomputern zu installieren oder nur auf bestimmten Computern. Beispiel: Wenn Sie wissen, dass einige der virtuellen Gastcomputer temporäre Computer sind und nicht gesichert werden müssen, können Sie jene aus der Installation ausschließen.

Hinweis: VMware Tools sollten installiert sein, bevor Sie den Agent for Windows auf einem virtuellen Gastcomputer installieren, wenn Sie den VSS-Anbieter von Backup Exec verwenden möchten.

So führen Sie eine Push-Installation von Agent for Windows auf virtuellen Computern aus

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" mit der rechten Maustaste auf den virtuellen Host und wählen Sie "Backup Exec Agent for Windows auf virtuellen Gastcomputern installieren".
- 2 Aktivieren Sie die Option "Zulassen, dass Backup Exec ein Vertrauensverhältnis mit den Servern herstellt" und klicken Sie dann auf "Weiter".
- 3 Aktivieren Sie die Option "Backup Exec Agent for Windows auf den virtuellen Gastcomputern eines VMware-vCenter oder ESX-Server installieren".
- 4 Wählen Sie im Feld "VMware vCenter oder ESX-Server" den VMware-Server aus, auf dem sich der virtuelle Computer befindet.
- 5 Klicken Sie auf "Weiter".
- 6 Wählen Sie die virtuellen Gastcomputer aus, auf denen Sie den Agent for Windows installieren möchten, und klicken Sie dann auf "Weiter".
- 7 Prüfen Sie, ob die ausgewählten virtuellen Computer online sind, wählen Sie das entsprechende Login-Konto für diese virtuellen Computer aus und klicken dann auf "Weiter".
- 8 Überprüfen Sie die Informationen im Fenster "Übersicht" und klicken Sie dann auf "Installieren".

Info zum Einrichten einer vertrauenswürdigen Verbindung zu einem vCenter/ESX(i)-Server

Wenn Sie die Hosts hinzufügen, stellt der Backup Exec-Medienserver eine Option zur Verfügung, um eine vertrauenswürdige Verbindung zum virtuellen Host-Server herzustellen. Beim Einrichten der vertrauenswürdigen Verbindung versucht Backup Exec, das vom Host vorgelegte SSL-Zertifikat zu validieren.

Gängige CA-Zertifikate anderer Anbieter werden automatisch validiert.

Wenn das Zertifikat selbstsigniert ist, wird es nicht erkannt. Sie müssen das Zertifikat validieren, damit die Vertrauensstellung eingerichtet werden kann. Backup Exec speichert die erforderlichen Informationen des SSL-Zertifikats des vCenter-Servers bzw. ESX(i)-Host in der Backup Exec-Datenbank. Wenn Sie später wieder eine Verbindung zum Server herstellen, müssen Sie das Zertifikat nicht erneut validieren.

Backup Exec versucht automatisch täglich zu einem geplanten Zeitpunkt, die Zertifikate für alle virtuelle Hosts zu validieren. Etwaige Änderungen am Serverzertifikat werden erkannt und der Server wird als nicht vertrauenswürdig gekennzeichnet. Ein Backup- bzw. Wiederherstellungsauftrag schlägt nicht fehl,

wenn der Auftrag für einen Server ausgeführt wird, der als nicht vertrauenswürdig gekennzeichnet ist. Wenn das Zertifikat abgelaufen ist, wird der Server als nicht vertrauenswürdig gekennzeichnet.

In Backup Exec-Konsole wird der Status "Kein Vertrauen hergestellt" für einen nicht vertrauenswürdigen Server angezeigt.

Einrichten einer vertrauenswürdigen Verbindung zu einem vCenter/ESX(i)-Server

Sie können eine vertrauenswürdige Verbindung zu einem vCenter/ESX(i)-Server auf der Registerkarte "Backup und Wiederherstellung" einrichten.

So richten Sie eine vertrauenswürdige Verbindung zu einem vCenter/ESX(i)-Server ein

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" mit der rechten Maustaste auf den Server, zu dem Sie eine vertrauenswürdige Verbindung hergestellt werden soll, und klicken Sie dann auf "Vertrauenswürdige Verbindung herstellen".
- 2 Wird das Zertifikat nicht automatisch erkannt, klicken Sie im Dialogfeld "Vertrauenswürdige Verbindung herstellen" auf "Zertifikat anzeigen", um die Identität des Host zu validieren.
- 3 Wenn das Zertifikat gültig ist, klicken Sie auf "Ja", um die vertrauenswürdige Verbindung herzustellen.

Wird die vertrauenswürdige Verbindung auf dem Central Administration Server (CAS) eingerichtet, wird der Status automatisch an alle Managed Media Server (MMS) gesendet.

Empfehlungen dazu, wann virtuelle Backups und wann Backups mit Agent genutzt werden sollten.

Backup Exec bietet zwei Backup-Methoden für virtuelle Computer an: virtuell und mit Agent.

Virtuelle Backups

Zum Ausführen virtueller Backups muss auf dem Backup Exec-Server Agent for VMware and Hyper-V installiert sein. Für Hyper-V-Umgebungen muss außerdem der Agent for VMware and Hyper-V auf dem Hyper-V-Host installiert sein. Darüber hinaus müssen der Host des virtuellen Computers oder der vCenter Server zu Backup Exec als Server hinzugefügt werden. Diese Backup-Methode verwendet

Empfehlungen dazu, wann virtuelle Backups und wann Backups mit Agent genutzt werden sollten.

VMware VADP-APIs oder Microsoft VSS-Snapshots, um virtuelle Computer zu schützen.

Virtuelle Backups werden für Folgendes empfohlen:

- Backups, die Granular Recovery Technology (GRT) auf Datei-/Ordnersebene erfordern

Hinweis: Der Agent for Windows muss auf dem virtuellen Computer installiert sein, damit GRT-Elemente auf Datei-/Ordnersebene im ursprünglichen Speicherort wiederhergestellt werden können.

- Einzel-Server-GRT auf Anwendungsebene für Active Directory, Exchange, SQL und SharePoint.

Hinweis: Der Agent for Windows muss auf dem virtuellen Computer installiert sein, damit GRT auf Anwendungsebene ausgeführt werden kann.

- Backups, die GRT nicht erfordern
- Virtuelle Computer (offline)
- Notfallwiederherstellung
- Vorlagen für virtuelle Computer

Virtuelle Backups werden nicht für Folgendes empfohlen:

- Backups von Oracle, Enterprise Vault, verteilten SharePoint-Farmen und Exchange DAG. Virtuelle Backups unterstützen GRT auf Anwendungsebene für diese Elemente nicht.

Backups mit Agent

Zum Ausführen von Backups mit Agent muss der Agent for Windows auf dem virtuellen Gastcomputer installiert sein. Diese Backup-Methode wird manchmal als "Legacy-Backup", "herkömmliches Backup" oder "Ingast-Backup" bezeichnet. Mit dieser Backup-Methode wird ein virtueller Computer als physischer Server behandelt.

Backups mit Agent werden für Folgendes empfohlen:

- Exchange DAG
- Oracle
- Enterprise Vault
- Verteilte SharePoint-Farm

- Eine Teilmenge der Dateien auf dem virtuellen Computer (kein Systemstatus)
- VMware-Fehlertolerante virtuelle Computer
- Virtuelle Computer mit Physical Raw Device Mapping (RDMS)

Backups mit Agent werden nicht für Folgendes empfohlen:

- Notfallwiederherstellung virtueller Computer
- Virtuelle Computer (offline)
- Vorlagen für virtuelle Computer

Sichern von virtuellen VMware-Computern

Wenn Sie einen Backup-Auftrag erstellen, können Sie einen gesamten vCenter-Server oder ESX-/ESXi-Host, Rechenzentren, Ordner oder einzelne virtuelle Computer auswählen. Außerdem kann die dynamische Einbeziehungsfunktion von Backup Exec neue virtuelle Computer und Ordner automatisch sichern, die gefunden werden, wenn ein Backup-Auftrag ausgeführt wird. Wenn Sie den vCenter-Server oder ESX/ESXi-Host für einen Backup-Auftrag auswählen, werden automatisch alle virtuellen Computer auf diesem Host gesichert. Sie können jedoch die Auswahl so bearbeiten, dass nur ausgewählte virtuelle Computer im Backup-Auftrag enthalten sind. In einem Backup eines vCenter-Servers oder ESX/ESXi-Host sind jedoch keine unabhängigen Datenträger oder Konfigurationsdateien für den vCenter-Server oder ESX/ESXi-Host enthalten.

Hinweise zum Sichern von virtuellen VMware-Computern

Sie sollten die folgenden Hinweise beachten, bevor Sie Backup-Aufträge für virtuelle VMware-Computer erstellen:

- Wenn Sie versuchen, einen virtueller Computer mit dem NetBIOS-Namen "LocalHost" zu sichern, wird die Fehlermeldung "e000976f - Der virtuelle Computer kann nicht auf dem Deduplizierungsgerät gesichert werden, das sich auf demselben virtuellen Computer befindet." ausgegeben.
- Backup-Aufträge schlagen für virtuelle Computer mit Physical Raw Disk Mapping-Geräten (RDM) fehl.
- RDM-Datenträger im Virtual Compatibility Mode werden automatisch in das Backup eines virtuellen Gastcomputers aufgenommen. Backup Exec kann jedoch die RDM-Datenträger mit Virtual Compatibility Mode oder die Dateidaten auf einem RDM-Datenträger nur über die umgeleitete Wiederherstellung wiederherstellen.
- Wenn Sie eine Exchange-Datenbankverfügbarkeitsgruppe (DAG) auf einem virtuellen Computer sichern möchten, verwenden Sie Backup Exec Agent for

Exchange. Der Agent for VMware unterstützt Backup von Exchange-DAGs nicht.

- Sie können Datenbanken nicht auf Geräten sichern, die an einem Computer angehängt werden, auf dem Remote Media Agent for Linux Servers installiert ist.
- Wenn Sie einen virtuellen Computer sichern, auf dem eine beliebige unterstützte Version von Microsoft SharePoint ausgeführt wird, kann die Verarbeitung über 30 Minuten dauern.

So sichern Sie virtuelle VMware-Computer

- 1** Auf der Registerkarte "Backup und Wiederherstellung" wählen Sie einen virtuellen Computer, einen ESXi-Host oder einen vCenter-Server aus der Serverliste.
- 2** Sie haben folgende Möglichkeiten:

Wenn Sie in Schritt 1 einen ESXi-Host oder einen vCenter Server ausgewählt haben

Klicken Sie oben auf der Seite in der Gruppe "Backups" auf "Backup" und wählen Sie dann die gewünschten Backup-Methode aus.

Sie können auch unten auf der Seite im Teilfenster "Details" auf "Backup" klicken und dann die gewünschte Backup-Methode auswählen.

Wenn Sie in Schritt 1 einen virtuellen Computer ausgewählt haben

Gehen Sie wie folgt vor:

- Klicken Sie oben auf der Seite in der Gruppe "Backups" auf "Backup" und wählen Sie dann die gewünschten Backup-Methode aus.
- Wählen Sie im Dialogfeld "Virtuellen Computer sichern" die gewünschte Backup-Methode für diesen virtuellen Computer ("Virtuelle Backups" oder "Backups mit Agent") und klicken Sie auf "Weiter".

Informationen dazu, welche Backup-Methode geeignet ist finden Sie im folgenden Thema:

Siehe "[Empfehlungen dazu, wann virtuelle Backups und wann Backups mit Agent genutzt werden sollten.](#)" auf Seite 1098.

Hinweis: Wenn Sie "Virtuelle Backups" ausgewählt haben und der Agent for VMware and Hyper-V nicht installiert ist, werden Sie aufgefordert, ihn zu installieren oder ein Backup mit Agent zu erstellen.

- Wenn Sie "Virtuelle Backups" ausgewählt haben, wählen Sie den Host des virtuellen Computers aus und klicken Sie dann auf "Weiter".
 Befindet sich der Host des virtuellen Computers nicht in der Liste der Server, klicken Sie auf "Hinzufügen" und schließen Sie den Assistenten ab, um den Host hinzuzufügen.

- 3 Klicken Sie im Dialogfeld "Eigenschaften der Backup-Definition" im Feld "Auswahl" auf "Bearbeiten", um Ressourcen der Backup-Auswahlliste hinzuzufügen oder daraus zu entfernen.
- 4 Aktivieren Sie im Dialogfeld "Backup-Auswahl" die Kontrollkästchen für die zu sichernden Ressourcen, und heben Sie die Markierung der Kontrollkästchen für die Quellen auf, nach denen nicht gefiltert werden soll.

- 5** Wählen Sie die Datenträger für den virtuellen Computer aus, der gesichert werden soll.

Sie können den gesamten virtuellen Computer (alle Festplatten) oder nur bestimmte Festplatten auswählen. Sie können Festplatten auch selektiv ausschließen.

- 6** Klicken Sie auf "OK".

Wenn Sie nur bestimmte Datenträger auswählen, wird das Popup "Teilweise ausgewählte Datenträger auf den virtuellen Computern" angezeigt.

Die Auftragsauswahl besteht aus einem oder mehreren virtuellen Computern, wobei nur einige der virtuellen Datenträger ausgewählt werden. Damit ein virtueller Computer auf Betriebssystem- und auf Anwendungsebene funktioniert, vergewissern Sie sich, dass alle erforderlichen Datenträger ausgewählt wurden.

Zum Durchführen der GRT Wiederherstellung für Ordner und Dateien sowie für Anwendungen, müssen Sie sicherstellen, dass das Systemlaufwerk ausgewählt wurde. Wählen Sie für GRT auf Anwendungsebene alle virtuellen Datenträger mit Anwendungsdaten aus.

- 7** Klicken Sie auf "OK".

- 8** Klicken Sie im Dialogfeld "Eigenschaften der Backup-Definition" im Feld "Backup" auf "Bearbeiten".

- 9** Wählen Sie im Dialogfeld "Backup-Optionen" im linken Teilfenster "Planen" und wählen Sie anschließend den Zeitplan für diesen Auftrag aus.

- 10** Wählen Sie im Dialogfeld "Backup-Optionen" im linken Teilfenster "Virtuelle Computer".

- 11** Legen Sie eine der folgenden Optionen für diesen Auftrag fest:

Element	Beschreibung
Vollständige Backup-Methode für virtuelle Computer verwenden, die inkrementelle oder Differenzial-Backups nicht unterstützen	Aktivieren Sie diese Option, falls Backup Exec ein vollständiges Backup durchführen soll, wenn kein inkrementelles oder differenzielles Backup durchgeführt werden kann. Wenn Sie diese Option nicht aktivieren und Backup Exec kein inkrementelles oder differenzielles Backup durchführen kann, schlägt der Auftrag fehl. Darüber hinaus muss ein vollständiges Backup durchgeführt werden, wenn Backup Exec eine Konfigurationsänderung erkennt. Wenn eine Konfigurationsänderung erkannt wird und Backup Exec kein vollständiges Backup durchführen kann, schlägt der Auftrag fehl, sofern diese Option nicht aktiviert wurde. Dieses Szenario trifft nur zu, wenn bereits ein vollständiges Backup und einige inkrementelle oder Differenzial-Backups durchgeführt wurden, und der nächste geplante Auftrag ein inkrementelles oder Differenzial-Backup ist.
Ausgeschaltete virtuelle Computer sichern	Aktivieren Sie diese Option, wenn Backup Exec sämtliche virtuelle Computer sichern soll, die ausgeschaltet sind.
Sofortwiederherstellung für alle virtuellen Computer aktivieren, auch für solche, die GRT nicht nutzen können	Aktivieren Sie diese Option, um die Sofortwiederherstellung aller virtuellen Computer zu aktivieren, auch für solche, die Granular Restore Technology nicht nutzen können.
Backup Exec Granular Recovery Technology (GRT) verwenden, um die Wiederherstellung einzelner Dateien und Ordner von virtuellen Computern zu aktivieren	<p>Durch Auswählen dieser Option können einzelne Dateien und Ordner aus dem Backup wiederhergestellt werden. Diese Option ist für virtuelle Computer, die nur das Windows-Betriebssystem verwenden.</p> <p>Die VMDK-Datei wird nicht gesichert, wenn die virtuelle Festplatte als unabhängiger Datenträger konfiguriert ist.</p> <p>Hinweis: GRT ist nicht für die Systemwiederherstellung (Recovery) ausgelegt, sondern nur für die Wiederherstellung einzelner Dateien und Ordner auf Windows-Computern.</p> <p>Siehe "Verwenden von Granular Recovery Technology (GRT) mit Agent for VMware" auf Seite 1115.</p>

Element	Beschreibung
GRT für Microsoft-Active Directory-Objekte auf virtuellen Computern aktivieren	Wenn Sie diese Option aktivieren, kann Backup Exec die Informationen erfassen, die erforderlich sind, um einzelne Active Directory-Objekte auf dem virtuellen Computer wiederherzustellen. Backup Exec nutzt die Identifikationsdaten, die für den virtuellen Computer verwendet wurden, auf dem Microsoft Active Directory installiert ist.
GRT für Microsoft Exchange-Datenbanken und Postfachelemente auf virtuellen Computern aktivieren	Aktivieren Sie diese Option, damit Backup Exec Informationen erfassen kann, die erforderlich sind, um einzelne Exchange-Datenbanken und Postfachelemente auf dem virtuellen Computer wiederherzustellen. Backup Exec nutzt die Identifikationsdaten, die für den virtuellen Computer verwendet wurden, auf dem Microsoft Exchange installiert ist.
GRT für Microsoft SQL (nur Datenbankstufe) auf virtuellen Computern aktivieren	Aktivieren Sie diese Option, damit Backup Exec die Informationen erfassen kann, die erforderlich sind, um einzelne SQL-Datenbankelemente auf dem virtuellen Computer wiederherzustellen. Backup Exec nutzt die Identifikationsdaten, die für den virtuellen Computer verwendet wurden, auf dem Microsoft SQL installiert ist.
Nach dem Sichern eines virtuellen Computers SQL Log-Backup ausführen	<p>Aktivieren Sie diese Option, damit Backup Exec die SQL-Protokolle für die Datenbanken, die Protokollierung verwenden, sichern kann. Nachdem die Protokolle gesichert wurden, werden die Daten aus den Protokollen in der Datenbank gespeichert und das Protokoll wird geleert.</p> <p>Wenn diese Option nicht aktiviert ist, wachsen die SQL-Protokolle, bis der Datenträger voll ist, oder Sie einen manuellen Auftrag zum Sichern der Protokolle ausführen.</p>
GRT für Microsoft SharePoint auf virtuellen Computern aktivieren	Aktivieren Sie diese Option, damit Backup Exec die Informationen erfassen kann, die für eine Wiederherstellung einzelner SharePoint-Elemente auf dem virtuellen Computer erforderlich sind. Backup Exec nutzt die Identifikationsdaten, die für den virtuellen Computer verwendet wurden, auf dem Microsoft SharePoint installiert ist.

Element	Beschreibung
Sichern mit Snapshot Provider Microsoft Volume Shadow Copy Service (VSS)	<p>Aktivieren Sie diese Option, damit Backup Exec einen stillgelegten Snapshot für den virtuellen Computer erstellen kann. Wenn der stillgelegte Snapshot nicht erstellt werden kann, erstellt Backup Exec einen absturzkonsistenten Snapshot.</p> <p>Hinweis: Backup Exec wählt diese Option automatisch, wenn Sie eine der Optionen für das Aktivieren von GRT für Microsoft-Anwendungen aktivieren.</p>
VSS Copy-Backup verwenden	<p>Aktivieren Sie diese Option, damit Backup Exec ein VSS-Copy-Backup anstelle eines vollständigen Backups durchführen kann. VSS Provider startet standardmäßig Snapshots über die Einstellung "Vollständiges Backup". Die Anwendung reagieren unterschiedlich auf diese Anfrage. Bei Microsoft Exchange werden die Datenbankprotokolle gekürzt. Wenn Sie diese Option nicht aktivieren, führt Backup Exec ein vollständiges VSS-Backup durch.</p>

Element	Beschreibung
Prioritätenliste für Transportmethode	

Element**Beschreibung**

Wählen Sie die Methode zum Übertragen der VMDK-Datei vom ESX/ESXi-Host aus. Sie müssen mindestens eine dieser Optionen auswählen. Wenn Sie mehr als eine Option auswählen, wird die Methode durch die Priorität und die verfügbaren Ressourcen bestimmt. Sie können die Optionen in der Liste nach oben oder nach unten verschieben, um die Priorität zu ändern.

Folgende Methoden sind verfügbar:

- **SAN** - Verwenden Sie SAN zum Verschieben virtueller Datenträgerdaten
Wenn Sie diese Option aktivieren, muss sich der virtuelle Computer in einem SAN befinden, auf das der Backup Exec-Server zugreifen kann. Bei dieser Transportmethode werden die Daten auf den Backup Exec-Server heruntergeladen, damit der ESX/ESXi-Server nicht beeinträchtigt wird.
- **NBD** - Den virtuellen Datenträger nicht für Übertragungen über das Netzwerk verschlüsseln
Verwenden Sie diese Option, wenn Sie kein SSL verwenden und eine der folgenden Bedingungen vorhanden ist:
 - Der virtuelle Computer befindet sich nicht auf dem SAN.
 - Der Backup Exec-Server hat keinen Zugriff auf das SAN.
- **NBDSSL** - Virtuelle Datenträgerdaten für Übertragungen im Netzwerk verschlüsseln
Verwenden Sie diese Option, wenn Sie SSL für die Sicherheit verwenden und eine der folgenden Bedingungen vorhanden ist:
 - Der virtuelle Computer befindet sich nicht auf dem SAN.
 - Der Backup Exec-Server hat keinen Zugriff auf das SAN.
- **Hotadd** - Verwenden Sie virtuelle Datenträgerdateien vom Backup Exec-Server auf dem virtuellen Computer
Verwenden Sie diese Option, wenn Sie die Funktion "Hotadd" für ESX/ESXi verwenden möchten.
Weitere Informationen zu Hotadd finden Sie in der VMware-Dokumentation.

Die VMDK-Datei wird nicht gesichert, wenn die virtuelle

Element	Beschreibung
	Festplatte als unabhängiger Datenträger konfiguriert ist.
Backup-Methode	<p>Wählen Sie die Backup-Methode aus, die Sie für die aufgelisteten Backup-Aufträge anwenden möchten. Sie können die Namen der Backup-Aufträge ändern oder unter den Eigenschaften in "Zeitplan" weitere Aufträge hinzufügen.</p> <p>Siehe "Konfigurieren von Backup-Methoden für Backup-Aufträge" auf Seite 215.</p>
12 Klicken Sie im Dialogfeld "Backup-Optionen" auf eine der für diesen Auftrag festzulegenden optionalen Einstellungen.	
13 Klicken Sie auf "OK".	
14 Klicken Sie im Dialogfeld "Eigenschaften der Backup-Definition" auf "OK".	
Wenn Sie die Methode "Virtuelle Backups" ausgewählt haben, wird der Backup-Auftrag in der Auftragsliste unter dem Namen des virtuellen Host oder der IP-Adresse angezeigt.	
Siehe "Automatisches Sichern neuer virtueller VMware-Computer mit Backup Exec während eines Backup-Auftrags" auf Seite 1115.	
Siehe "Verwenden von Granular Recovery Technology (GRT) mit Agent for VMware" auf Seite 1115.	

Festlegen von Backup-Standardoptionen für virtuelle Computer

Sie können die bei der Installation von Backup Exec für alle VMware-Backup-Aufträge festgelegten Standardeinstellungen verwenden oder eigene Standardeinstellungen wählen. Sie können die Standardeinstellungen übergehen, wenn Sie einzelne Aufträge erstellen.

So legen Sie Backup-Standardoptionen für virtuelle Computer fest

- 1** Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- 2** Wählen Sie "Auftragsstandardeinstellungen" und dann eine Backup-Option.

Beispiel: Wenn Sie die Standardoptionen für Backup-to-Disk von virtuellen Computer einrichten möchten, wählen Sie "Backup-to-Disk". Die Optionen, die angezeigt werden, hängen von den konfigurierten Speichergeräten ab. Verschiedene Standardoptionen können für Backup-Aufträge auf verschiedenen Speichertypen konfiguriert werden.

- 3 Im linken Teilfenster klicken Sie auf "Virtuelle Computer".
- 4 Wählen Sie die entsprechenden Optionen aus.

Element	Beschreibung
Vollständige Backup-Methode für virtuelle Computer verwenden, die inkrementelle oder Differenzial-Backups nicht unterstützen	Wählen Sie diese Option aus, um mit Backup Exec ein vollständiges Backup durchzuführen, wenn kein inkrementelles oder differenzielles Backup durchgeführt werden können. Wenn Sie diese Option nicht auswählen und Backup Exec kein inkrementelles oder differenzielles Backup durchführen kann, schlägt der Auftrag fehl. Darüber hinaus muss ein vollständiges Backup durchgeführt werden, wenn Backup Exec eine Konfigurationsänderung erkennt. Wenn eine Konfigurationsänderung erkannt wird und Backup Exec kein vollständiges Backup durchführen kann, schlägt der Auftrag fehl, sofern diese Option nicht aktiviert wurde. Dieses Szenario trifft nur zu, wenn bereits ein vollständiges Backup und einige inkrementelle oder Differenzial-Backups durchgeführt wurden, und der nächste geplante Auftrag ein inkrementelles oder Differenzial-Backup ist.
Ausgeschaltete virtuelle Computer sichern	Wählen Sie diese Option aus, um mit Backup Exec virtuelle Computer zu sichern, die ausgeschaltet sind.
Sofortwiederherstellung für alle virtuellen Computer aktivieren, auch für solche, die GRT nicht nutzen können.	Aktivieren Sie diese Option, um die Sofortwiederherstellung aller virtuellen Computer zu aktivieren, auch für solche, die Granular Restore Technology nicht nutzen können.
Backup Exec Granular Recovery Technology (GRT) verwenden, um die Wiederherstellung einzelner Dateien und Ordner von virtuellen Computern zu aktivieren	<p>Durch Auswählen dieser Option können einzelne Dateien und Ordner aus dem Backup wiederhergestellt werden. Diese Option ist für virtuelle Computer, die nur das Windows-Betriebssystem verwenden.</p> <p>Die VMDK-Datei wird nicht gesichert, wenn die virtuelle Festplatte als unabhängiger Datenträger konfiguriert ist.</p> <p>Hinweis: GRT ist nicht für die Systemwiederherstellung (Recovery) ausgelegt, sondern nur für die Wiederherstellung einzelner Dateien und Ordner auf Windows-Computern.</p>

Element	Beschreibung
GRT für Microsoft-Active Directory-Objekte auf virtuellen Computern aktivieren	Wenn Sie diese Option aktivieren, kann Backup Exec die Informationen erfassen, die erforderlich sind, um einzelne Active Directory-Objekte auf dem virtuellen Computer wiederherzustellen. Backup Exec nutzt die Identifikationsdaten, die für den virtuellen Computer verwendet wurden, auf dem Microsoft Active Directory installiert ist.
GRT für Microsoft Exchange-Datenbanken und Postfachelemente auf virtuellen Computern aktivieren	Aktivieren Sie diese Option, damit Backup Exec Informationen erfassen kann, die erforderlich sind, um einzelne Exchange-Datenbanken und Postfachelemente auf dem virtuellen Computer wiederherzustellen. Backup Exec nutzt die Identifikationsdaten, die für den virtuellen Computer verwendet wurden, auf dem Microsoft Exchange installiert ist.
GRT für Microsoft SQL (nur Datenbankstufe) auf virtuellen Computern aktivieren	Aktivieren Sie diese Option, damit Backup Exec die Informationen erfassen kann, die erforderlich sind, um einzelne SQL-Datenbankelemente auf dem virtuellen Computer wiederherzustellen. Backup Exec nutzt die Identifikationsdaten, die für den virtuellen Computer verwendet wurden, auf dem Microsoft SQL installiert ist.
Nach dem Sichern eines virtuellen Computers SQL Log-Backup ausführen	<p>Aktivieren Sie diese Option, damit Backup Exec die SQL-Protokolle für Datenbanken sichern kann, die die Protokollierung nutzen. Nachdem die Protokolle gesichert wurden, werden die Daten aus den Protokollen in der Datenbank gespeichert und das Protokoll wird geleert.</p> <p>Wenn diese Option nicht aktiviert ist, wachsen die SQL-Protokolle, bis der Datenträger voll ist, oder Sie einen manuellen Auftrag zum Sichern der Protokolle ausführen.</p>
GRT für Microsoft SharePoint auf virtuellen Computern aktivieren	Aktivieren Sie diese Option, damit Backup Exec die Informationen erfassen kann, die für eine Wiederherstellung einzelner SharePoint-Elemente auf dem virtuellen Computer erforderlich sind. Backup Exec nutzt die Identifikationsdaten, die für den virtuellen Computer verwendet wurden, auf dem Microsoft SharePoint installiert ist.

Element	Beschreibung
Virtuelle Computer, die sich für Backups in einem gespeicherten Zustand befinden müssen, ausschließen	<p>Wählen Sie diese Option aus, um alle virtuellen Offline-Computer, die keine Online-Backups unterstützen und beim Start des Backups laufen, vom Backup auszuschließen.</p> <p>Diese Option trifft nur auf den Agent for Hyper-V zu.</p>
Sichern mit Snapshot Provider Microsoft Volume Shadow Copy Service (VSS)	<p>Aktivieren Sie diese Option, damit Backup Exec einen stillgelegten Snapshot für den virtuellen Computer erstellen kann. Wenn der stillgelegte Snapshot nicht erstellt werden kann, erstellt Backup Exec einen absturzkonsistenten Snapshot.</p> <p>Hinweis: Backup Exec wählt diese Option automatisch, wenn Sie eine der Optionen für das Aktivieren von GRT für Microsoft-Anwendungen aktivieren.</p>
VSS Copy-Backup verwenden	<p>Aktivieren Sie diese Option, damit Backup Exec ein VSS-Copy-Backup anstelle eines vollständigen Backups durchführen kann. VSS Provider startet standardmäßig Snapshots über die Einstellung "Vollständiges Backup". Die Anwendung reagieren unterschiedlich auf diese Anfrage. Bei Microsoft Exchange werden die Datenbankprotokolle gekürzt. Wenn Sie diese Option nicht aktivieren, führt Backup Exec ein vollständiges VSS-Backup durch.</p>

Element	Beschreibung
Prioritätenliste für Transportmethode	

Element**Beschreibung**

Wählen Sie die Methode zum Übertragen der VMDK-Datei vom ESX/ESXi-Host aus. Sie müssen mindestens eine dieser Optionen auswählen. Wenn Sie mehr als eine Option auswählen, wird die Methode durch die Priorität und die verfügbaren Ressourcen bestimmt. Sie können die Optionen in der Liste nach oben oder nach unten verschieben, um die Priorität zu ändern.

Folgende Methoden sind verfügbar:

- **SAN** - Verwenden Sie SAN zum Verschieben virtueller Datenträgerdaten
Wenn Sie diese Option aktivieren, muss sich der virtuelle Computer in einem SAN befinden, auf das der Backup Exec-Server zugreifen kann. Bei dieser Transportmethode werden die Daten auf den Backup Exec-Server heruntergeladen, damit der ESX/ESXi-Server nicht beeinträchtigt wird.
- **NBD** - Den virtuellen Datenträger nicht für Übertragungen über das Netzwerk verschlüsseln
Verwenden Sie diese Option, wenn Sie kein SSL verwenden und eine der folgenden Bedingungen vorhanden ist:
 - Der virtuelle Computer befindet sich nicht auf dem SAN.
 - Der Backup Exec-Server hat keinen Zugriff auf das SAN.
- **NBDSSL** - Virtuelle Datenträgerdaten für Übertragungen im Netzwerk verschlüsseln
Verwenden Sie diese Option, wenn Sie SSL für die Sicherheit verwenden und eine der folgenden Bedingungen vorhanden ist:
 - Der virtuelle Computer befindet sich nicht auf dem SAN.
 - Der Backup Exec-Server hat keinen Zugriff auf das SAN.
- **Hotadd** - Verwenden Sie virtuelle Datenträgerdateien vom Backup Exec-Server auf dem virtuellen Computer
Verwenden Sie diese Option, wenn Sie die Funktion "Hotadd" für ESX/ESXi verwenden möchten.
Weitere Informationen zu Hotadd finden Sie in der VMware-Dokumentation.

Die VMDK-Datei wird nicht gesichert, wenn die virtuelle

Element	Beschreibung
Backup-Methode	<p>Festplatte als unabhängiger Datenträger konfiguriert ist.</p> <p>Wählen Sie die Backup-Methode aus, die Sie für die aufgelisteten Backup-Aufträge anwenden möchten. Sie können die Namen der Backup-Aufträge ändern oder unter den Eigenschaften in "Zeitplan" weitere Aufträge hinzufügen.</p> <p>Siehe "Konfigurieren von Backup-Methoden für Backup-Aufträge" auf Seite 215.</p>

5 Klicken Sie auf "OK".

Siehe ["Sichern von virtuellen VMware-Computern"](#) auf Seite 1100.

Automatisches Sichern neuer virtueller VMware-Computer mit Backup Exec während eines Backup-Auftrags

Die dynamische Einbeziehungsfunktion von Backup Exec schützt neue virtuelle Computer und Ordner, die erkannt werden, wenn ein Backup-Auftrag ausgeführt wird. Werden neue virtuelle Computer zwischen dem Erstellungs- und dem Ausführungszeitpunkt des Backup-Auftrags hinzugefügt, sichert Backup Exec diese automatisch. Da der Backup-Auftrag neue virtuelle Computer umfassen kann, kann das Ausführen des Auftrags mehr Speicherplatz und Zeit erfordern als erwartet. Der Auftragsverlauf zeigt die Anzahl virtueller Computer an, die gesichert wurden.

Wenn Sie einen VMware-Server auswählen, wird die dynamische Einbeziehung automatisch für alle untergeordneten Knoten aktiviert, die ein Ordner-Symbol haben. Wenn keine virtuellen Computer während eines Backup-Auftrags gefunden werden, schlägt dieser fehl.

Siehe ["Sichern von virtuellen VMware-Computern"](#) auf Seite 1100.

Verwenden von Granular Recovery Technology (GRT) mit Agent for VMware

Die Granular Recovery Technology (GRT) von Backup Exec ermöglicht die Wiederherstellung einzelner Laufwerke, Dateien und Ordner von einem Backup-Satz, ohne dass Sie den gesamten virtuellen Computer wiederherstellen müssen. Die Funktion ermöglicht außerdem die Wiederherstellung einzelner Elemente von den folgenden VSS-fähigen Anwendungen, die sich auf virtuellen Computern befinden:

Tabelle C-1 Datentypen, die Backup Exec für VSS-fähige Anwendungen auf virtuellen Computern sichert

Anwendung	Von Backup Exec gesicherte Datentypen
Microsoft Exchange	Postfächer, einzelne Meldungen, Kalenderelemente, Aufgaben, Journaleinträge und öffentliche Ordnerdaten (nur Datenträger-Backups)
Microsoft SQL	Datenbanken
Microsoft Active Directory	Einzelne Benutzerkonten, Druckerobjekte, Sites und Organisationseinheiten
Microsoft SharePoint	SharePoint-Daten

GRT funktioniert nur für die virtuellen Computer, die ein Windows-Betriebssystem verwenden. GRT funktioniert nicht für die Systemwiederherstellung.

GRT muss im VMware-Backup-Auftrag aktiviert werden. Wenn Sie einen Backup-Auftrag erstellen, sucht Backup Exec automatisch VSS-fähige Anwendungen auf virtuellen Computern. Während des Backup-Auftrags sichert Backup Exec die Daten der VSS-fähigen Anwendungen mithilfe von GRT. Backup Exec aktiviert standardmäßig GRT unter Verwendung derselben Identifikationsdaten, die verwendet wurden, um eine Verbindung zum virtuellen Computer herzustellen. Sie können GRT für beliebige VSS-fähige Anwendungstypen deaktivieren.

Hinweis: Backup Exec unterstützt die selektive Wiederherstellung einzelner Exchange- und SQL-Elemente nur in nicht geclusterten und nicht verteilten Konfigurationen.

Während des Backup-Auftrags erfasst Backup Exec Metadaten der Anwendungen. Wenn Backup Exec nicht in der Lage ist, Metadaten zu sammeln, können Sie einzelne Elemente für die Anwendungen nicht wiederherstellen. Jedoch kann der Backup-Auftrag andernfalls erfolgreich beendet werden.

Anforderungen für die Verwendung von GRT zum Sichern von Microsoft-Anwendungsdaten auf virtuellen Computern

Die folgenden Voraussetzung müssen erfüllt sein, damit Daten für Microsoft Exchange, SQL, SharePoint und Active Directory auf virtuellen Computern gesichert werden können:

- Der virtuelle Computer muss eingeschaltet sein.

- Sie müssen die passenden Identifikationsdaten für den virtuellen Computer eingeben. Stellen Sie sicher, dass die Identifikationsdaten für den virtuellen Computer Zugriff auf die VSS-fähigen Anwendungen ermöglichen.
- Der Backup Exec-Server muss in der Lage sein, eine Verbindung zum virtuellen Computer unter Verwendung des Netzwerknamens oder der IP-Adresse herzustellen.
- VMware-Tools sollten auf dem virtuellen Computer installiert sein.
- Backup Exec Agent for Windows muss auf dem virtuellen Computer installiert sein. Stellen Sie sicher, dass die VMware-Tools installiert sind, bevor Sie den Agent for Windows installieren.

Hinweis: Wenn Sie die VMware-Tools nach dem Agent for Windows installiert haben, sollten Sie die Datei `freeze.bat` aus Backup Exec RAWs-Installationspfad\VSS Provider in VMware Tools Installationspfad\backupscripts.d (beispielsweise \\Programme\VMware\VMware Tools\backupscripts.d) kopieren. Falls der Ordner "backupscripts.d" nicht existiert, müssen Sie ihn manuell erstellen. Alternativ dazu können Sie, anstatt die Datei "freeze.bat" zu verschieben, den Agent for Windows reparieren, wodurch automatisch alle fehlenden Dateien am entsprechenden Speicherort ablegt werden.

- Backup Exec Agent for Applications and Databases muss auf dem Backup Exec-Server installiert sein.
- Die richtige Anzahl Lizenzen muss für die Anwendungen, die Sie auf den virtuellen Computern schützen möchten, eingegeben werden.
- Das Betriebssystem auf dem virtuellen Computer muss VSS unterstützen.
- Die Optionen für GRT der Anwendungsebene müssen in den Backup-Aufträgen ausgewählt werden. Diese Optionen werden nicht standardmäßig ausgewählt.

Nicht unterstützte Konfigurationen für GRT

Bevor Sie einen GRT-aktivierten Backup-Auftrag für VMware-Ressourcen erstellen, überprüfen Sie die folgenden Informationen, um zu verstehen, welche Konfigurationen nicht für GRT unterstützt werden.

Tabelle C-2 Nicht unterstützte Konfigurationen für GRT

Nicht unterstützte Elemente	Details
Virtuelle Computer mit einer Kombination von unabhängigen und nicht unabhängigen Datenträgern	Backup Exec unterstützt GRT bei unabhängigen Datenträgern nicht.
Virtuelle Computer mit virtuellem RDM-Datenträger	Wenn Sie versuchen, ein Backup eines virtuellen Computers wiederherzustellen, der einen virtuellen RDM-Datenträger hat, kann die VMDK-Datei, die dem virtuellen RDM-Datenträger entspricht, nicht erstellt oder wiederhergestellt werden. Der Wiederherstellungsauftrag schlägt mit dem Fehler "Unable to open a disk of the virtual machine" (Fehler beim Öffnen eines Datenträgers auf dem virtuellen Computer) fehl. Nur nicht-virtuelle RDM-Datenträger können wiederhergestellt werden.
Virtuelle Computer mit RAID 5-Datenträgern	Backup Exec unterstützt Datei-/Ordner-GRT für RAID 5-Datenträger nicht. GRT auf Anwendungsebene für virtuelle Computer wird nicht unterstützt, wenn der virtuelle Computer mindestens einen RAID 5-Datenträger enthält.
Virtuelle Computer mit NTFS mit unbenannten Bereitstellungspunkten	Backup Exec unterstützt Datei-/Ordner-GRT für NTFS mit unbenannten Bereitstellungspunkten nicht. Der Wiederherstellungsauftrag schlägt fehl mit dem Fehler "Fehler beim Anhängen der Ressource. Vergewissern Sie sich, dass die ausgewählte Ressource vorhanden und online ist und wiederholen Sie den Vorgang." (Fehler beim Anhängen der Ressource. Vergewissern Sie sich, dass die ausgewählte Ressource vorhanden und online ist und wiederholen Sie den Vorgang.)

Nicht unterstützte Elemente	Details
Virtuelle Computer mit Hilfsprogramm-Partitionen	Datei-/Ordner-Wiederherstellungsaufträge schlagen fehl mit dem Fehler "Fehler beim Anhängen der Ressource. Vergewissern Sie sich, dass die ausgewählte Ressource vorhanden und online ist und wiederholen Sie den Vorgang." (Fehler beim Anhängen der Ressource. Vergewissern Sie sich, dass die ausgewählte Ressource vorhanden und online ist und wiederholen Sie den Vorgang.) Backup Exec unterstützt Backups von virtuellen Computern mit Hilfsprogramm-Partitionen nicht. Beachten Sie, dass das nicht dasselbe ist wie unbenannte Partitionen.
Wiederherstellungen aus vollständigen und inkrementellen Backups aus unterschiedlichen Speichergeräten	Backup Exec unterstützt Wiederherstellungen aus gemischten Medien nicht, wenn GRT im Backup-Auftrag aktiviert war. Beispiel: Wenn das vollständige Backup auf Band vorliegt und das inkrementelle Backup auf einem Plattenspeichergerät, schlägt der Wiederherstellungsauftrag fehl. Wiederherstellungen aus gemischten Medien werden unterstützt, wenn GRT nicht aktiviert ist.
Virtuelle Computer mit dynamischen Datenträgern (GPT-Partitionen)	Backup Exec unterstützt die granulare Wiederherstellung von Dateien, Ordnern und Anwendungen auf virtuellen Computern mit dynamischen Datenträgern (mit GPT- oder MBR-Partitionen) nicht.
Virtuelle Computer mit ReFS- und deduplizierten Datenträgern	Backup Exec unterstützt GRT auf Datei- bzw. Ordnebene nur für ReFS- und deduplizierten Datenträger bzw. GRT auf Anwendungsebene für virtuelle Computer, wenn auf dem Backup Exec-Server Windows Server 2012 oder höher ausgeführt wird.

Siehe ["Sichern von virtuellen VMware-Computern"](#) auf Seite 1100.

So funktioniert die Katalogisierung mit virtuellen Backups über VMware

Wenn Sie Granular Recovery Technology (GRT) für einen Backup-Auftrag eines virtuellen Computers aktivieren, können Sie den Katalogauftrag für GRT als Teil des Backup-Auftrags, als separaten Auftrag sofort nach Abschluss des Backup-Auftrags oder nach einem Zeitplan ausführen. Standardmäßig wird der Katalogvorgang sofort nach Abschluss des Backup-Auftrags ausgeführt.

Hinweis: Die Optionen für Instant GRT und Vollständige Katalogisierung werden für Backups auf Band nicht unterstützt.

Die Katalogisierung kann zeitaufwändig sein. Sie benötigt Zugriff auf das für das Backup genutzte Speichergerät. Sie sollten die Katalogisierung so planen, dass sie nicht während des Backups ausgeführt wird, damit kein Konflikt mit Backup-Aufträgen auftritt. Ist eine Katalogisierung geplant, wird sie nur für den neuesten Backup-Satz seit der letzten Katalogisierung ausgeführt. In dieser Situation kann nur der neueste Backup-Satz seit der letzten Katalogisierung für die granulare Wiederherstellung verwendet werden. Sie müssen die wiederherzustellenden Daten aus den Backup-Sätzen auswählen, bevor die vollständige Katalogisierung abgeschlossen ist. Der Suchassistent ist dafür nicht verfügbar.

Beispiel: Wenn Sie inkrementelle Backups einrichten, die alle 11 Stunden und der Katalogvorgang um Mitternacht ausgeführt werden, hätten Sie die folgenden Backup-Sätze:

- Vollständig (11:00 Uhr)
- Inkrementell 1 (22:00 Uhr)
- Katalog 1 (Mitternacht). Dieser Auftrag katalogisiert Inkrementell 1.
- Inkrementell 2 (09:00 Uhr)
- Inkrementell 3 (20:00 Uhr)
- Katalog 2 (Mitternacht). Dieser Auftrag katalogisiert Inkrementell 3. Inkrementell 2 ist nicht katalogisiert.
- Inkrementell 4 (07:00 Uhr)
- Inkrementell 5 (18:00 Uhr)
- Katalog 3 (Mitternacht). Dieser Auftrag katalogisiert Inkrementell 5. Inkrementell 4 ist nicht katalogisiert.
- Inkrementell 6 (05:00 Uhr) Dieses Backup ist nicht katalogisiert.

Im Beispiel wird die vollständige Katalogisierung nur für Inkrementell 5, Inkrementell 3 und Inkrementell 1 ausgeführt. Für solche Aufträge können Sie mit dem Suchassistenten die Daten durchsuchen oder nach einzelnen Elementen suchen, die wiederhergestellt werden sollen. Sie können zwar eine granulare Wiederherstellung auch mit Inkrementell 2, Inkrementell 4 und Inkrementell 6 ausführen, aber dies dauert länger, da sie nicht vollständig katalogisiert sind. Backup Exec zeigt die granularen Daten durch Bereitstellen des Backup-Satzes an.

So wird die Byteanzahl für Instant GRT und Vollständige Katalogisierung berechnet

In der "Auftragsüberwachung" und im "Auftragsverlauf" unterscheidet sich die Byteanzahl, die für einen Katalogvorgang angezeigt wird, möglicherweise von der Byteanzahl, die für den entsprechenden Backup-Auftrag angezeigt wird. Die Byteanzahl für einen Katalogauftrag ist möglicherweise höher als die Byteanzahl für einen Backup-Auftrag. Die Methode, mit der Backup Exec die Daten katalogisiert, hat Auswirkungen auf die Byteanzahl, die für den Katalogauftrag angezeigt wird.

- Wenn ein Katalogvorgang für ein vollständiges Backup durchgeführt wird, werden die Daten auf der Basis Datei-für-Datei gelesen und die Byteanzahl wird dementsprechend berechnet. Während des Auftrags des vollständigen Backups werden die Daten im Hinblick auf die Anzahl von Sektoren gelesen und die Byteanzahl wird basierend auf der Anzahl von Sektoren berechnet. Die Byteanzahl für einen Katalogauftrag ist möglicherweise höher als die Byteanzahl für einen Backup-Auftrag.
- Wenn der Katalogvorgang für ein inkrementelles Backup durchgeführt wird, sind alle Dateien auf dem virtuellen Datenträger anstelle der geänderten Dateien katalogisiert. Aus diesem Grund berücksichtigt die Byteanzahl für den Katalogauftrag das vollständige Backup und das inkrementelle Backup.

Siehe ["Konfigurieren der Optionen für Instant GRT und Vollständige Katalogisierung zum Verbessern der Backup-Leistung von GRT-Aufträgen"](#) auf Seite 656.

Wiederherstellen virtueller VMware-Computer und VMDK-Dateien

Sie können den Wiederherstellungsassistenten verwenden, um Folgendes wiederherzustellen:

- Ein vollständiger virtueller Computer.
- Die Virtual Machine Disk Format (VMDK)-Datei für einen virtuellen Computer.
- Einzelne Dateien und Ordner, die aus der VMDK-Datei und einzelnen Elementen von Microsoft SharePoint, Exchange, SQL oder Active Directory gesichert

wurden. Die Möglichkeit, einzelne Dateien und Ordner wiederherzustellen ist nur verfügbar, wenn Granular Recovery Technology (GRT) für den Backup-Auftrag aktiviert wurde.

Hinweis: GRT kann Systemzustandsdateien wie die aktive Registrierung nicht wiederherstellen.

Mit Backup Exec können Sie VMware-Daten entweder im Speicherort, aus dem sie gesichert wurden, oder einem anderen wiederherstellen. Das Wiederherstellen von Daten in einem anderen Speicherort wird als umgeleitete Wiederherstellung bezeichnet.

Eine umgeleitete Wiederherstellung ist für Notfallwiederherstellungssituationen nützlich. Wenn Sie eine umgeleitete Wiederherstellung durchführen, haben Sie die Option, den virtuellen Computer auf die neueste Hardwareversion wiederherzustellen, die die Zielumgebung unterstützt. Wenn Sie die Option nicht auswählen, den virtuellen Computer auf die neueste Hardwareversion wiederherzustellen, wird die ursprüngliche Hardwareversion des virtuellen Computers beibehalten, wenn er wiederhergestellt wird.

Hinweis: Die folgenden Schritte gelten für virtuelle Computer, die mit der virtuellen Backup-Methode gesichert wurden. Wenn Sie den virtuellen Computer mit dem Agent gesichert haben, folgen Sie den Anweisungen zum Wiederherstellen eines nicht virtuellen Backup.

Siehe ["Wiederherstellen von Daten aus einem Server, einem Backup-Satz, einem Backup-Auftrag oder einem Speichergerät"](#) auf Seite 261.

Siehe ["So stellen Sie virtuelle VMware-Computer bzw. VMDK-Dateien im Speicherort, aus dem sie gesichert wurden, wieder her"](#) auf Seite 1122.

Siehe ["So leiten Sie die Wiederherstellung eines virtuellen VMware-Computers oder von VMDK-Dateien auf einen anderen Host um"](#) auf Seite 1125.

Siehe ["So stellen Sie Daten in einem anderem Pfad wieder her"](#) auf Seite 1129.

So stellen Sie virtuelle VMware-Computer bzw. VMDK-Dateien im Speicherort, aus dem sie gesichert wurden, wieder her

- 1 Auf der Registerkarte "Backup und Wiederherstellung" haben Sie folgende Möglichkeiten:

So stellen Sie einzelne Dateien und Ordner aus einem GRT-Backup wieder her

Gehen Sie dazu wie folgt vor:

- Wählen Sie im Teilfenster "Details" am unteren Bildschirmrand den virtuellen Computer aus.
- Klicken Sie auf "Wiederherstellen" und wählen Sie dann "GRT-Daten wiederherstellen".
- Wählen Sie im Wiederherstellungsassistent "Dateien, Ordner oder Datenträger" aus und klicken Sie auf "Weiter".

So stellen Sie den gesamten virtuellen Computer bzw. virtuellen Datenträger wieder her

Gehen Sie dazu wie folgt vor:

- Wählen Sie im Teilfenster "Details" am unteren Bildschirmrand den virtuellen Computer aus.
- Klicken Sie auf "Wiederherstellen" und wählen Sie dann "Virtuellen Computer aus Host wiederherstellen".
- Wählen Sie im "Wiederherstellungsassistent" die Option "VMware-Daten" und klicken Sie auf "Weiter".

- 2 Erweitern Sie auf der Registerkarte "Ressourcenansicht" den Namen des virtuellen Hostservers, wählen Sie die Elemente aus, die Sie wiederherstellen möchten, und klicken Sie dann auf "Weiter".
- 3 Wenn das Fenster Von wo aus sollen die Daten wiederhergestellt werden? angezeigt wird, gewährleisten Sie, dass der korrekte Speicher angezeigt wird, aus dem wiederhergestellt werden soll, und klicken Sie auf "Weiter".
- 4 Wählen Sie "Am ursprünglichen Ort" und klicken Sie auf "Weiter".
- 5 Wählen Sie einen oder mehrere Modi zum Übertragen der VMDK-Datei auf den Host aus.

Sie müssen mindestens einen Modus auswählen. Wenn Sie mehr als eine Option auswählen, wird die Methode durch die Priorität und die verfügbaren Ressourcen bestimmt. Klicken Sie auf "Nach oben" bzw. "Nach unten", um die Priorität zu ändern.

NBD - Daten des virtuellen Datenträgers für Übertragungen innerhalb des Netzwerks nicht verschlüsseln	<p>Verwenden Sie diese Option, wenn Sie kein SSL verwenden und eine der folgenden Bedingungen gilt:</p> <ul style="list-style-type: none"> ■ Der virtuelle Computer befindet sich nicht auf dem SAN. ■ Der Backup Exec-Server hat keinen Zugriff auf das SAN.
NBDSSL - Daten des virtuellen Datenträgers für Übertragungen innerhalb des Netzwerks verschlüsseln	<p>Verwenden Sie diese Option, wenn Sie SSL für die Sicherheit verwenden und eine der folgenden Bedingungen gilt:</p> <ul style="list-style-type: none"> ■ Der virtuelle Computer befindet sich nicht auf dem SAN. ■ Der Backup Exec-Server hat keinen Zugriff auf das SAN.
Hotadd - Verwenden Sie virtuelle Datenträgerdateien vom Backup Exec-Server auf dem virtuellen Computer	<p>Verwenden Sie diese Option, wenn Sie die Funktion "Hotadd" für ESX/ESXi verwenden möchten. Mit der Funktion "Hotadd" können Sie einen virtuellen Computer als Proxyserver nutzen. Weitere Informationen zu Hotadd finden Sie in der VMware-Dokumentation.</p>
SAN – Zum Verschieben von virtuellen Datenträgerdaten SAN verwenden	<p>Wenn Sie diese Option auswählen, muss der virtuelle Computer SAN-Lese-Schreibzugriff auf dem VMware-Datenspeicher haben, der das Wiederherstellungsziel hostet. Bei dieser Transportmethode werden die Daten auf den Backup Exec-Server heruntergeladen, damit der ESX/ESXi-Server nicht beeinträchtigt wird.</p> <p>Hinweis: Der SAN-Transportmodus wird nicht zum Wiederherstellen von für schlanke Speicherzuweisung geeigneten Datenträgern empfohlen, da der NDB-Transportmodus bessere schneller ist.</p>

- 6 Füllen Sie eines der folgenden optionalen Felder aus, die für Ihre Umgebung gelten und klicken Sie dann auf "Weiter".

Vorhandene virtuelle Computer vor der Wiederherstellung löschen

Wählen Sie diese Option aus, wenn der virtuelle Computer, den Sie wiederherstellen, bereits auf dem Server existiert. Wenn Sie diese Option auswählen, werden die virtuellen Computer möglicherweise gelöscht, selbst wenn der Wiederherstellungsauftrag fehlschlägt. Sie können einen virtuellen Computer, der bereits auf dem virtuellen Server vorhanden ist, nur wiederherstellen, wenn Sie diese Option auswählen.

Virtuellen Computer nach der Wiederherstellung einschalten

Wählen Sie diese Option, wenn Backup Exec den wiederhergestellten virtuellen Computer einschalten soll, nachdem der Wiederherstellungsauftrag abgeschlossen ist.

- 7 Wenn Sie einen Befehl vor oder nach der Wiederherstellung ausführen oder Benachrichtigungen für diesen Wiederherstellungsauftrag aktivieren möchten, füllen Sie die Felder im Fenster Welche zusätzlichen Aufgaben möchten Sie vor und/oder nach einer Wiederherstellung ausführen? aus und klicken Sie dann auf "Weiter".
- 8 Geben Sie einen Namen für diesen Wiederherstellungsauftrag ein, wählen Sie den Zeitplan für den Auftrag aus und klicken Sie dann auf "Weiter".
- 9 Überprüfen Sie die Auftragsübersicht und klicken Sie dann auf "Fertigstellen".

So leiten Sie die Wiederherstellung eines virtuellen VMware-Computers oder von VMDK-Dateien auf einen anderen Host um

- 1 Auf der Registerkarte "Backup und Wiederherstellung" haben Sie folgende Möglichkeiten:

So stellen Sie einzelne Dateien und Ordner aus einem GRT-Backup wieder her

Gehen Sie dazu wie folgt vor:

- Wählen Sie im Teilfenster "Details" am unteren Bildschirmrand den virtuellen Computer aus.
- Klicken Sie auf "Wiederherstellen" und wählen Sie dann "GRT-Daten wiederherstellen".
- Wählen Sie im Wiederherstellungsassistent "Dateien, Ordner oder Datenträger" aus und klicken Sie auf "Weiter".

So stellen Sie den gesamten virtuellen Computer bzw. virtuellen Datenträger wieder her

Gehen Sie dazu wie folgt vor:

- Wählen Sie im Teilfenster "Details" am unteren Bildschirmrand den virtuellen Computer aus.
- Klicken Sie auf "Wiederherstellen" und wählen Sie dann "Virtuellen Computer aus Host wiederherstellen".
- Wählen Sie im "Wiederherstellungsassistent" die Option "VMware-Daten" und klicken Sie auf "Weiter".

- 2** Erweitern Sie auf der Registerkarte "Ressourcenansicht" den Namen des virtuellen Hostservers, wählen Sie die Elemente aus, die Sie wiederherstellen möchten, und klicken Sie dann auf "Weiter".
- 3** Wählen Sie "Auf einem anderen vCenter oder ESX-Server" und klicken Sie auf "Weiter".
- 4** Geben Sie den Namen des vCenter-Servers oder des ESX-/ESXi-Host ein, auf den Daten wiederhergestellt werden sollen, oder klicken Sie auf "Durchsuchen", um nach dem Server zu suchen.
- 5** Wählen Sie das richtige Login-Konto für den Server aus, auf dem Sie die Daten wiederherstellen möchten.
- 6** Klicken Sie auf "Durchsuchen" neben "Ordner des virtuellen Computers", um den Ordner auszuwählen, in den Sie Daten wiederherstellen möchten.
- 7** Klicken Sie auf "Durchsuchen" neben "Ressourcenpool", um den Ressourcenpool auszuwählen, in den Sie Daten wiederherstellen möchten.

- 8 Wenn Sie einen neuen Namen für den virtuellen Computer erstellen möchten, geben Sie ihn im Feld "Name des virtuellen Computers" ein. Sie sollten einen neuen Namen eingeben, wenn ein virtueller Computer mit dem gleichen Namen bereits auf dem Server existiert.
- 9 Wählen Sie das Netzwerk aus, das der neue virtuelle Computer verwenden soll, nachdem der Wiederherstellungsauftrag abgeschlossen ist.
- 10 Füllen Sie eines der folgenden optionalen Felder aus, die für Ihre Umgebung gelten und klicken Sie dann auf "Weiter".

Ursprüngliche Datenspeicherauswahl verwenden, wenn auf ausgewähltem Host verfügbar

Aktivieren Sie dieses Kontrollkästchen, um die ursprünglichen Datenspeicherauswahl auf dem virtueller Server zu verwenden. Wenn die ursprüngliche Datenspeicherauswahl nicht vorhanden ist, wird die aus den Backup-Daten verwendet.

Virtuellen Computer auf neueste Hardwareversion zurücksetzen, die die Zielumgebung unterstützt

Aktivieren Sie dieses Kontrollkästchen, um den virtuellen Computer unter Verwendung der neuesten VMware-Hardwareversion wiederherzustellen, die in Ihrer Umgebung verfügbar ist, anstatt die ursprüngliche Hardwareversion des virtuellen Computers zu verwenden.

Wenn Sie dieses Kontrollkästchen nicht aktivieren, wird die ursprüngliche Hardwareversion des virtuellen Computers beibehalten, wenn er wiederhergestellt wird.

Virtuelle Clients mit Thin Provisioning wiederherstellen

Aktivieren Sie dieses Kontrollkästchen, um den virtuellen Computer mit Thin Provisioning wiederherzustellen. Thin Provisioning unterstützt Sie bei der effizienteren Zuweisung der Speicherkapazität in Ihrer VMware ESX Server -Umgebung.

- 11 Wählen Sie einen oder mehrere Modi zum Übertragen der VMDK-Datei auf den Host aus.

Sie müssen mindestens einen Modus auswählen. Wenn Sie mehr als eine Option auswählen, wird die Methode durch die Priorität und die verfügbaren Ressourcen bestimmt. Klicken Sie auf "Nach oben" bzw. "Nach unten", um die Priorität zu ändern.

NBD - Daten des virtuellen Datenträgers für Übertragungen innerhalb des Netzwerks nicht verschlüsseln	<p>Verwenden Sie diese Option, wenn Sie kein SSL verwenden und eine der folgenden Bedingungen gilt:</p> <ul style="list-style-type: none"> ■ Der virtuelle Computer befindet sich nicht auf dem SAN. ■ Der Backup Exec-Server hat keinen Zugriff auf das SAN.
NBDSSL - Daten des virtuellen Datenträgers für Übertragungen innerhalb des Netzwerks verschlüsseln	<p>Verwenden Sie diese Option, wenn Sie SSL für die Sicherheit verwenden und eine der folgenden Bedingungen gilt:</p> <ul style="list-style-type: none"> ■ Der virtuelle Computer befindet sich nicht auf dem SAN. ■ Der Backup Exec-Server hat keinen Zugriff auf das SAN.
Hotadd - Verwenden Sie virtuelle Datenträgerdateien vom Backup Exec-Server auf dem virtuellen Computer	<p>Verwenden Sie diese Option, wenn Sie die Funktion "Hotadd" für ESX/ESXi verwenden möchten. Mit der Funktion "Hotadd" können Sie einen virtuellen Computer als Proxyserver nutzen. Weitere Informationen zu Hotadd finden Sie in der VMware-Dokumentation.</p>
SAN – Zum Verschieben von virtuellen Datenträgerdaten SAN verwenden	<p>Wenn Sie diese Option auswählen, muss der virtuelle Computer SAN-Lese-Schreibzugriff auf dem VMware-Datenspeicher haben, der das Wiederherstellungsziel hostet. Bei dieser Transportmethode werden die Daten auf den Backup Exec-Server heruntergeladen, damit der ESX/ESXi-Server nicht beeinträchtigt wird.</p> <p>Hinweis: Der SAN-Transportmodus wird nicht zum Wiederherstellen von für schlanke Speicherzuweisung geeigneten Datenträgern empfohlen, da der NDB-Transportmodus bessere schneller ist.</p>

- 12** Füllen Sie eines der folgenden optionalen Felder aus, die für Ihre Umgebung gelten und klicken Sie dann auf "Weiter".

Vorhandene virtuelle Computer vor der Wiederherstellung löschen

Wählen Sie diese Option aus, wenn der virtuelle Computer, den Sie wiederherstellen, bereits auf dem Server existiert. Wenn Sie diese Option auswählen, werden die virtuellen Computer möglicherweise gelöscht, selbst wenn der Wiederherstellungsauftrag fehlschlägt. Sie können einen virtuellen Computer, der bereits auf dem virtuellen Server vorhanden ist, nur wiederherstellen, wenn Sie diese Option auswählen.

Virtuellen Computer nach der Wiederherstellung einschalten

Wählen Sie diese Option, wenn Backup Exec den wiederhergestellten virtuellen Computer einschalten soll, nachdem der Wiederherstellungsauftrag abgeschlossen ist.

- 13** Wenn Sie einen Befehl vor oder nach der Wiederherstellung ausführen oder Benachrichtigungen für diesen Wiederherstellungsauftrag aktivieren möchten, füllen Sie die Felder im Fenster Welche zusätzlichen Aufgaben möchten Sie vor und/oder nach einer Wiederherstellung ausführen? aus und klicken Sie dann auf "Weiter".
- 14** Geben Sie einen Namen für diesen Wiederherstellungsauftrag ein, wählen Sie den Zeitplan für den Auftrag aus und klicken Sie dann auf "Weiter".
- 15** Überprüfen Sie die Auftragsübersicht und klicken Sie dann auf "Fertigstellen".

So stellen Sie Daten in einem anderem Pfad wieder her

- 1** Auf der Registerkarte "Backup und Wiederherstellung" haben Sie folgende Möglichkeiten:

So stellen Sie einzelne Dateien und Ordner aus einem GRT-Backup wieder her

Gehen Sie dazu wie folgt vor:

- Wählen Sie im Teilfenster "Details" am unteren Bildschirmrand den virtuellen Computer aus.
- Klicken Sie auf "Wiederherstellen" und wählen Sie dann "GRT-Daten wiederherstellen".
- Wählen Sie im Wiederherstellungsassistent "Dateien, Ordner oder Datenträger" aus und klicken Sie auf "Weiter".

So stellen Sie den gesamten virtuellen Computer bzw. virtuellen Datenträger wieder her

Gehen Sie dazu wie folgt vor:

- Wählen Sie im Teilfenster "Details" am unteren Bildschirmrand den virtuellen Computer aus.
- Klicken Sie auf "Wiederherstellen" und wählen Sie dann "Virtuellen Computer aus Host wiederherstellen".
- Wählen Sie im "Wiederherstellungsassistent" die Option "VMware-Daten" und klicken Sie auf "Weiter".

- 2 Erweitern Sie auf der Registerkarte "Ressourcenansicht" den Namen des virtuellen Hostservers, wählen Sie die Elemente aus, die Sie wiederherstellen möchten, und klicken Sie dann auf "Weiter".
- 3 Wählen Sie die Option "In anderem Pfad".
- 4 Geben Sie das Laufwerk und den Pfad ein, in den Sie Daten wiederherstellen möchten, und klicken Sie dann auf "Weiter".
- 5 Wenn Sie einen Befehl vor oder nach der Wiederherstellung ausführen oder Benachrichtigungen für diesen Wiederherstellungsauftrag aktivieren möchten, füllen Sie die Felder im Fenster Welche zusätzlichen Aufgaben möchten Sie vor und/oder nach einer Wiederherstellung ausführen? aus und klicken Sie dann auf "Weiter".
- 6 Geben Sie einen Namen für diesen Wiederherstellungsauftrag ein, wählen Sie den Zeitplan für den Auftrag aus und klicken Sie dann auf "Weiter".
- 7 Überprüfen Sie die Auftragsübersicht und klicken Sie dann auf "Fertigstellen".

Siehe ["Methoden für das Wiederherstellen von Daten in Backup Exec"](#) auf Seite 258.

Info zur Sofortwiederherstellung eines virtuellen VMware-Computers

Mit Backup Exec ist die Sofortwiederherstellung virtueller Computer möglich, ohne dass zunächst die darauf enthaltenen Daten aus einem Backup-Satz übertragen werden müssen. Backup Exec startet den sofort wiederhergestellten virtuellen Computer direkt über den Backup-Satz. Daraufhin kann auf dem vCenter- oder ESX/ESXi-Host darauf zugegriffen werden. Die Startzeit des Backup Exec-Servers hängt von der Netzwerk- und Speichergeschwindigkeit ab und nicht von der Größe des virtuellen Computers.

Zum vollständigen Wiederherstellen des virtuellen Computers verwenden Sie VMware Storage vMotion, um die Datendateien des virtuellen Computers aus dem Backup-Satz auf den vCenter- bzw. ESX/ESXi-Host zu migrieren. Nach dem Migrieren eines sofort wiederhergestellten virtuellen Computers können Sie diesen mit dem Agent for VMware sichern.

Auf sofort wiederhergestellten virtuellen Computern sind dieselben Aktionen möglich wie auf gewöhnlichen virtuellen Computern. Die Sofortwiederherstellung eines virtuellen Computers hat folgende Einsatzmöglichkeiten:

- Zugriff und Wiederherstellung einzelner Dateien und Ordner auf einem virtuellen Computer.
- Testen von Patches auf dem sofort wiederhergestellten virtuellen Computer, bevor sie auf Produktionssysteme angewendet werden.
- Fehlerbehebung auf einem virtuellen Computer oder Host, z. B. wenn der ESX-Host in der Produktionsumgebung nicht reagiert. Sie können den sofort wiederhergestellten virtuellen Computer nutzen, bis das Produktionssystem wieder online ist.
- Verifizieren des Backup-Satzes eines virtuellen Computers.
- Kopieren der VMDK-Datei und Entfernen des virtuellen Computers.
- Verifizieren einer Anwendung auf einem virtuellen Computer.
- Permanentes Wiederherstellen des virtuellen Computers mit Storage vMotion. Bei der Notfallwiederherstellung können Sie für den virtuellen Computer eine Sofortwiederherstellung durchführen und anschließend eine Migration planen, um ihn auf einen dauerhaften Speicher auf dem vCenter- oder ESX/ESXi-Host zu verschieben. Der wiederhergestellte virtuelle Computer bleibt während der Migration verfügbar, um Systemausfälle zu minimieren.

Sofort wiederhergestellte virtuelle Computer nutzen den Speicher des Backup Exec-Servers. Wenn Sie einen sofort wiederhergestellten virtuellen Computer entfernen, gehen alle Änderungen, die Sie an diesem vorgenommen haben, verloren.

Wenn Sie Änderungen am sofort wiederhergestellten virtuellen Computer vorgenommen haben, dann sollten Sie den virtuellen Computer aus dem Speicher des Backup Exec-Servers migrieren, um zu verhindern, dass Ihre Änderungen verloren gehen.

Da Backup Exec vor kurzem die Ausfallsicherheit der Sofortwiederherstellung verbessert hat, gehen die am virtuellen Computer vorgenommen Änderungen nun nicht mehr verloren, wenn Sie den Backup Exec-Server neu starten oder Probleme mit der Netzwerkverbindung auftreten. Der virtuelle Computer kann jedoch nicht verwendet werden, bis der Neustart des Servers abgeschlossen oder die Netzwerkverbindung wiederhergestellt ist.

Gewährleisten Sie, dass der virtuelle Computer aus dem Speicher des Backup Exec-Servers entfernt wird, wenn er nicht mehr benötigt wird oder entfernt wurde.

Die folgende Tabelle beschreibt die Sofortwiederherstellung eines virtuellen Computers.

Tabelle C-3 Sofortwiederherstellung eines virtuellen Computers

Schritt	Beschreibung
Schritt 1	Sie führen eine Sofortwiederherstellung aus dem Backup eines virtuellen VMware-Computers durch.
Schritt 2	Backup Exec virtualisiert den Backup-Satz.
Schritt 3	<p>Backup Exec erstellt auf dem Backup Exec-Server eine Freigabe in Form eines NFS-Datenspeichers.</p> <p>Der Datenspeicher ist für den Host verfügbar, auf dem der virtuelle Computer wiederhergestellt wird. Der Host hat nur Lesezugriff auf den NFS-Datenspeicher.</p> <p>Hinweis: Da der Windows Server keinen NFS-Schutz bietet, wird die von Backup Exec erstellte Freigabe im Netzwerk zur Verfügung gestellt.</p>
Schritt 4	Backup Exec erstellt einen virtuellen Computer auf dem Host und konfiguriert ihn mit Schreibzugriff auf den Datenspeicher.
Schritt 5	Backup Exec erstellt einen Snapshot des virtuellen Computers.
Schritt 6	Wenn Sie die Option zum Hochfahren des virtuellen Computers aktivieren, startet Backup Exec ihn automatisch.
Schritt 7	Sie können Storage vMotion zum Migrieren des virtuellen Computers aus dem Speicher des Backup ExecBackup Exec-Servers verwenden, wenn Sie am virtuellen Computer vorgenommene Änderungen speichern möchten.

Schritt	Beschreibung
Schritt 8	<p>Sie können einen der folgenden Aufträge ausführen:</p> <ul style="list-style-type: none"> Entfernen eines wiederhergestellten virtuellen Computers, der nicht mehr benötigt wird Entfernen des sofort wiederhergestellten virtuellen Computers aus dem Speicher des Backup Exec-Servers nach der Migration mit Storage vMotion <p>Warnung: Sie können Backup Exec erst aktualisieren, nachdem Sie alle wiederhergestellten virtuellen Computer entfernt haben.</p>

Unterschiede zwischen gewöhnlicher und Sofortwiederherstellung virtueller Computer

In der folgenden Tabelle sind die Unterschiede zwischen einer gewöhnlichen und Sofortwiederherstellung virtueller Computer aufgeführt.

Tabelle C-4 Unterschiede zwischen gewöhnlicher und Sofortwiederherstellung virtueller Computer

Element	Sofortwiederherstellung eines virtuellen Computers	Gewöhnliche Wiederherstellung eines virtuellen Computers
Datenübertragung	Bei der Sofortwiederherstellung werden keine Daten des virtuellen Computers übertragen.	Alle Daten des Backup-Satzes werden auf den Host übertragen.
Auftragsdauer	Die Sofortwiederherstellung nimmt weniger Zeit in Anspruch und die Auftragsdauer ist unabhängig von der Größe des virtuellen Computers.	Die Zeit für die gewöhnliche Wiederherstellung hängt von der Größe des virtuellen Computers und von der Netzwerk- und Speichergeschwindigkeit ab.
Lese- und Schreibvorgänge	Verwendet das Image des Backup-Satzes für alle Lesevorgänge. Verwendet einen Snapshot auf dem VMware-Host für alle Schreibvorgänge.	Daten werden auf den VMware-Host verschoben.
Datenspeicher	Verwendet bis zur Migration des sofort wiederhergestellten virtuellen Computers den Speicher des Backup Exec-Servers	Verwendet VMware-Host-Speicher.

Element	Sofortwiederherstellung eines virtuellen Computers	Gewöhnliche Wiederherstellung eines virtuellen Computers
Server-Neustart	<p>Durch die Verbesserung der Ausfallsicherheit der Sofortwiederherstellung bleibt beim Neustart des Backup Exec-Servers der Zugriff auf den sofort wiederhergestellten virtuellen Computer erhalten. Sobald der Neustart abgeschlossen bzw. die Netzwerkverbindung wiederhergestellt ist, wird der sofort wiederhergestellte virtuelle Computer automatisch wieder online geschaltet.</p> <p>Im Falle von Problemen mit der Netzwerkverbindung kann nach dem Wiederherstellen der Verbindung auf den wiederhergestellten virtuellen Computer zugegriffen werden.</p>	Der Backup Exec-Server und VMware-Host können neu gestartet werden.

Siehe ["Anforderungen an die Sofortwiederherstellung eines virtuellen VMware-Computers"](#) auf Seite 1134.

Siehe ["Hinweise zur Sofortwiederherstellung eines virtuellen VMware-Computers"](#) auf Seite 1135.

Siehe ["Erstellen eines Auftrags für die Sofortwiederherstellung eines virtuellen VMware-Computers"](#) auf Seite 1137.

Siehe ["Entfernen eines sofort wiederhergestellten virtuellen VMware-Computers"](#) auf Seite 1140.

Anforderungen an die Sofortwiederherstellung eines virtuellen VMware-Computers

Für die Sofortwiederherstellung eines virtuellen Computers gelten folgende Anforderungen:

- Installieren Sie die Rolle "Windows-Server für NFS" auf dem Backup Exec-Server. Weitere Informationen finden Sie in der Microsoft Windows-Dokumentation.
- Aktivieren Sie die Granular Recovery Technology von Backup Exec zum Wiederherstellen einzelner Elemente aus Microsoft-Anwendungen im

Backup-Auftrag von VMware. Wenn der virtuelle Computer nicht für GRT geeignet ist, können Sie die Option "Sofortwiederherstellung für alle virtuellen Computer aktivieren, auch für solche, die GRT nicht nutzen können." aktivieren. Beachten Sie, dass dann das Speicherformat des nächsten vollständigen Backups in eines geändert wird, das mit der Sofortwiederherstellung kompatibel ist.

Siehe ["Verwenden von Granular Recovery Technology \(GRT\) mit Agent for VMware"](#) auf Seite 1115.

- Sichern Sie virtuelle Computer mit der virtuellen Backup-Methode.
- Verwenden Sie Datenträgerspeicher für den Backup-Auftrag von VMware. Deduplizierungsspeicher, Cloud-Speicher und Plattenkassettengeräte wie RDX werden nicht unterstützt.
- Auf dem Host muss genug Speicherplatz zum Speichern etwaiger Änderungen am sofort wiederhergestellten virtuellen Computer vorhanden sein.
- Der Host muss vSphere 5.1 oder eine Nachfolgerversion verwenden.
- Stellen Sie anhand der Hardwarekompatibilitätsliste und der Softwarekompatibilitätsliste sicher, dass Ihre Umgebung unterstützte Hardware und Software aufweist.
Die unterstützten Betriebssysteme, Plattformen und Anwendungen finden Sie in der Liste der mit Backup Exec kompatiblen Hardware und Software.

Hinweise zur Sofortwiederherstellung eines virtuellen VMware-Computers

Vor der Sofortwiederherstellung eines virtuellen Computers sollten Sie folgende Hinweise beachten:

- Die Backup Exec-Befehlszeilenschnittstelle (BEMCLI) wird für die Sofortwiederherstellung nicht unterstützt.
- In gebündelten Backup Exec-Umgebungen wird die Sofortwiederherstellung eines virtuellen Computers nicht unterstützt.
- Für CAS-Umgebungen gilt Folgendes:
 - Der zentrale Administrationsserver oder der verwaltete Backup Exec-Server kann eine Sofortwiederherstellung eines virtuellen Computers durchführen, wenn dieser auf diesen Servern betrieben wird. Allerdings kann der verwaltete Backup Exec-Server die virtuellen Computer nur dann entfernen, wenn die Sofortwiederherstellung auf diesem Server durchgeführt wurde.

- Sie können eine Sofortwiederherstellung nach Delegieren des Auftrags an einen verwalteten Backup Exec-Server nicht von einem zentralen Administrationsserver verwalten.
- Entfernen oder migrieren Sie den sofort wiederhergestellten virtuellen Computer aus dem Speicher des Backup Exec-Servers, bevor Sie Backup Exec aktualisieren oder deinstallieren. Upgrades, Patch-Updates und Deinstallationen werden auf dem Backup Exec-Server und dem Host, auf dem Agent for VMware installiert ist, blockiert, wenn ein sofort wiederhergestellter virtueller Computer darauf ausgeführt wird.
- Werden sehr viele sofort wiederhergestellte virtuelle Computer gleichzeitig ausgeführt, wird die Leistung des Backup Exec-Servers beeinträchtigt. Sie sollten die in der Umgebung ausgeführten wiederhergestellten virtuellen Computer regelmäßig prüfen. Entfernen Sie nicht länger benötigte virtuelle Computer oder migrieren Sie diese auf den Host und entfernen Sie sie dann vom Backup Exec-Server.
- Bei der Migration wird Netzwerkbandbreite genutzt. Deshalb sollten Sie sie zu einem Zeitpunkt durchführen, zu dem andere Prozesse nur eine geringe Bandbreite benötigen.
- Beim Migrieren eines sofort wiederhergestellten virtuellen Computers sollten Sie auf dem VMware-Host einen Pfad verwenden, der sich vom ursprünglichen Speicherort des virtuellen Computers unterscheidet.
- Ein sofort wiederhergestellter virtueller Computer kann erst nach der Migration mit VMware Storage vMotion in einen Backup-Auftrag eingeschlossen werden.

Best Practices bei der Sofortwiederherstellung eines virtuellen VMware-Computers

Vor der Sofortwiederherstellung eines virtuellen Computers sollten Sie folgende Hinweise beachten:

- Zum Ausführen der Sofortwiederherstellung eines ESXi-Gastcomputers erstellt Backup Exec eine NFS-Freigabe mit den erforderlichen VMDK-Dateien und konfiguriert ESXi so, dass diese Freigabe genutzt wird. Die für die NFS-Freigabe festgelegten Berechtigungen sind so konfiguriert, dass der Zugriff auf Anforderungen begrenzt wird, die aus einer ESXi-IP-Adresse stammen. Wenn ein virtueller Gastcomputer NAT (Netzwerkadressenübersetzung) unter ESXi verwendet, kann er auf die NFS-Freigabe auf dem Backup Exec-Server zugreifen. Als Best Practice für Sicherheit wird empfohlen, Portgruppen mit bestimmten zugewiesenen NICs zu konfigurieren, sodass virtuelle Computer, die mit einer Portgruppe verbunden sind, von der anderen Portgruppe getrennt sind, über die ESXi Zugriff auf die NFS-Freigabe hat.

Erstellen eines Auftrags für die Sofortwiederherstellung eines virtuellen VMware-Computers

Sie können einen Auftrag für die Sofortwiederherstellung eines virtuellen VMware-Computers erstellen und diesen dann am ursprünglichen oder an einem anderen Speicherort wiederherstellen.

Wenn Sie den sofort wiederherzustellenden virtuellen Computer aus dem Speicher des Backup Exec-Servers in einen VMware-Speicher verschieben möchten, können Sie die Datendateien oder jeweiligen Datenträger des virtuellen Computers mittels Storage vMotion migrieren. Während der Migration werden die Datendateien des virtuellen Computers auf den VMware-Speicher übertragen, während der virtuelle Computer noch ausgeführt wird.

Hinweis: Für Anwendungen wie SharePoint und Exchange gilt: Stellen Sie alle virtuellen Computer wieder her, die die Anwendungen benötigen, um richtig zu funktionieren. Beispiel: In einer Microsoft Exchange-Umgebung müssen Sie die virtuellen Computer wiederherstellen, auf denen der Exchange-Client und das Active Directory ausgeführt werden, und dann eine Verbindung zwischen diesen beiden virtuellen Computern aufbauen.

Siehe ["Anforderungen an die Sofortwiederherstellung eines virtuellen VMware-Computers"](#) auf Seite 1134.

Führen Sie folgende Schritte zum Erstellen eines Auftrags für die Sofortwiederherstellung eines virtuellen VMware-Computers aus.

So erstellen Sie einen Auftrag für die Sofortwiederherstellung eines virtuellen VMware-Computers

- 1 Auf der Registerkarte "Backup und Wiederherstellung" wählen Sie den virtuellen Computer aus, der wiederhergestellt werden soll.
- 2 Klicken Sie in der Gruppe "Sofortwiederherstellung" auf "Sofortwiederherstellung eines virtuellen Computers".
- 3 Geben Sie im Dialogfeld "Sofortwiederherstellung eines virtuellen Computers" im Feld "Auftragsname" einen Namen für den Auftrag ein.
- 4 Geben Sie im Gruppenfeld "Backup-Satz-Auswahl" im Feld "Backup-Sätze anzeigen von" das Start- und Enddatum für die Backup-Sätze an, die in die Auswahl aufgenommen werden sollen.

Standardmäßig werden nur die Backup-Sätze für Aufträge angezeigt, die in den letzten 30 Tagen ausgeführt wurden.

- 5** Wählen Sie im Feld "Datenträgerbasierter Backup-Satz" den Backup-Satz aus, der für die Sofortwiederherstellung verwendet werden soll.

In der Liste werden nur Backup-Sätze angezeigt, die die Anforderungen für Sofortwiederherstellungen erfüllen.

- 6 Klicken Sie im linken Teilfenster auf "Ziel" und legen Sie folgende Optionen für den Auftrag fest:

Element	Beschreibung
Name des virtuellen Computers	Der Name des sofort wiederhergestellten virtuellen Computers.
Name des VMware vCenter-Servers oder ESX-Hosts	Der Name des vCenter-Servers oder ESX-Hosts.
Server-Login-Konto	Verwendet das Standard-Login-Konto, das erscheint. Sie können ein anderes Login-Konto für den vCenter-Server oder ESX-Host wählen.
Host	Der Name des ESX-Hosts, auf dem der sofort wiederhergestellte virtuelle Computer ausgeführt werden soll.
Ordner auf virtuellem Computer	Der Name des vorhandenen vSphere-Ordners, in dem der virtuelle Computer wiederhergestellt werden soll. Der Standardordner ist der Stamm des Datacenter.
Ressourcenpool	Der Name des Ressourcenpools, in dem der virtuelle Computer wiederhergestellt werden soll. Der Ressourcenpool ist optional.
VC-Netzwerk	Der Name des Netzwerks, das der wiederhergestellte virtuelle Computer verwenden soll. Wählen Sie ein anderes als das vom virtuellen Quellcomputer verwendete Netzwerk. Andernfalls kann es zu Netzwerkkonflikten zwischen dem virtuellen Quellcomputer und dem sofort wiederhergestellten virtuellen Computer kommen.
Datenspeicher oder Datenspeicher-Cluster zum Ablegen von mit virtuellen Computern eingegebenen Texten	Der Name des Datenspeichers, in dem vorübergehende Änderungen am wiederhergestellten virtuellen Computer gespeichert werden sollen.
Virtuellen Computer nach dem Wiederherstellen hochfahren	Ist diese Option aktiviert, kann Backup Exec den virtuellen Computer nach der Sofortwiederherstellung automatisch starten.

- 7 Wählen Sie im Dialogfeld "Sofortwiederherstellung eines virtuellen Computers" im linken Teilfenster "Planen" und wählen Sie anschließend den Zeitplan für diesen Auftrag aus.
- 8 (Optional) Wählen Sie im Dialogfeld "Sofortwiederherstellung eines virtuellen Computers" im linken Teilfenster "Benachrichtigung" und dann die Empfänger der Benachrichtigung beim Abschluss des Auftrags.
- 9 Klicken Sie auf "OK".

Entfernen eines sofort wiederhergestellten virtuellen VMware-Computers

Sofort wiederhergestellte virtuelle Computer müssen aus dem Speicher des Backup Exec-Servers entfernt werden, wenn sie migriert wurden oder nicht mehr benötigt werden. Beim Entfernen eines sofort wiederhergestellten virtuellen Computers entfernt Backup Exec alle Datenbankeinträge und alle zum Zeitpunkt des Auftrags erstellten Ordner.

Auch wenn Sie den virtuellen Computer aus dem VMware-Host mit dem VMware vSphere Client entfernen, müssen Sie den wiederhergestellten virtuellen Computer aus Backup Exec entfernen. Wenn Sie einen sofort wiederhergestellten virtuellen Computer aus dem VMware-Host entfernen, werden die Konfigurationsordner aus dem VMware-Speicher gelöscht. Außerdem wird die NFS-Freigabe entfernt, die für den wiederhergestellten Computer auf dem Backup Exec-Server erstellt wurde.

Hinweis: Data Lifecycle Management (DLM) für den Backup-Satz, mit dem der sofort wiederhergestellte virtuelle Computer erstellt wurde, wird erst dann ausgeführt, wenn der virtuelle Computer entfernt ist. Mit dem nächsten DLM-Zyklus läuft der Backup-Satz ab.

So entfernen Sie einen sofort wiederhergestellten virtuellen VMware-Computer

- 1 Wählen Sie auf der Registerkarte "Backup und Wiederherstellung" einen vSphere-Server oder einen ESX-Host aus, der den zu entfernenden wiederhergestellten Computer enthält.

Doppelklicken Sie auf einen vSphere-Server oder einen ESX-Host und klicken Sie dann links auf "Wiederhergestellte virtuelle Computer", um die sofort auf dem Server wiederhergestellten virtuellen Computer anzuzeigen.
- 2 Klicken Sie in der Gruppe "Sofortwiederherstellung" auf "Wiederhergestellten virtuellen Computer entfernen" und führen Sie einen der folgenden Schritte aus:

So entfernen Sie einen wiederhergestellten virtuellen Computer sofort Gehen Sie dazu in folgender Reihenfolge vor:

- Wählen Sie "Standardwerte verwenden und jetzt entfernen"
- Wählen Sie im Dialogfeld "Wiederhergestellte virtuelle Computer zum Entfernen auswählen" mindestens einen wiederhergestellten virtuellen Computer zum Entfernen aus.
- Klicken Sie auf "OK".

So passen Sie die Einstellungen an und entfernen einen wiederhergestellten virtuellen Computer

Gehen Sie dazu in folgender Reihenfolge vor:

- Wählen Sie "Einstellungen anpassen und entfernen".
- Wählen Sie im Dialogfeld "Wiederhergestellte virtuelle Computer zum Entfernen auswählen" mindestens einen wiederhergestellten virtuellen Computer zum Entfernen aus.
- Klicken Sie auf "OK".
- Geben Sie im Dialogfeld "Wiederhergestellten virtuellen Computer entfernen" im Feld "Auftragsname" einen Namen für den Auftrag ein.
- Fügen Sie im Feld "Server-Login-Konto" ein Login-Konto für den vCenter-Server oder ESX-Host ein oder bearbeiten Sie es.
- Aktivieren Sie die Option "Virtuellen Computer entfernen, obwohl sich im Speicher des Backup Exec-Servers und auf dem Host des virtuellen Computers Datenträger befinden", um einen sofort wiederhergestellten virtuellen Computer zu entfernen, der nicht vollständig migriert wurde oder Datenträger enthält, die sich nicht im Backup Exec-Speicher befinden.
- Wählen Sie im Dialogfeld "Wiederhergestellten virtuellen Computer entfernen" im linken Teilfenster "Planen" und wählen Sie anschließend den Zeitplan für diesen Auftrag aus.
- (Optional) Wählen Sie im Dialogfeld "Wiederhergestellten virtuellen Computer entfernen" im linken Teilfenster "Benachrichtigung" und dann die Empfänger der Benachrichtigung beim Abschluss des Auftrags.
- Klicken Sie auf "OK".

Beheben von Fehlern mit dem Agent for VMware

Falls Probleme mit VMware-Backup-Aufträgen auftreten, lesen Sie folgende Probleme und Behebungen.

Problem	Lösung
Ein VMware-Backup-Auftrag wurde angehalten und keine Daten wurden übertragen.	Wenn Sie versuchen, einen Auftrag in diesem Zustand abzubrechen, bleibt dieser im Zustand "Abbrechen ausstehend". Beenden Sie den Prozess "beremote.exe" und starten Sie dann alle Backup Exec-Dienste neu.
In einer vCenter 5.0-Umgebung kann das Sichern von duplizierten virtuellen Computern dazu führen, dass der Backup Exec Agent for Windows beendet wird.	Bearbeiten und sichern Sie die Konfiguration des duplizierten virtuellen Computers im VMware-vSphere Client, bevor Sie den Backup-Auftrag erstellen. Sie müssen dies nur einmal auf jedem duplizierten virtuellen Computer tun.

Informationen zur Funktion "Wiederherstellung bereit" für virtuelle VMware-Computer

Backup Exec verfügt seit der Version Backup Exec 16 Feature Pack 1 über die Funktion "Wiederherstellung bereit". Mit der Funktion "Wiederherstellung bereit" können Sie über den Vorgang "VM für Wiederherstellung validieren" die Wiederherstellbarkeit von virtuellen Computer validieren. Wenn Sie einen Auftrag zum Validieren eines virtuellen Computers für die Wiederherstellung erstellen und ausführen, werden erst einige Tests auf dem virtuellen Computer ausgeführt, nachdem dieser als zur Wiederherstellung bereit gekennzeichnet wurde.

Zur Wiederherstellung bereite virtuelle Computer können für die folgenden Aufgaben verwendet werden:

- Disaster Recovery-Bereitschaft: In einem Disaster Recovery-Szenario sind Administratoren sicher, dass die validierten virtuellen Computer wiederhergestellt werden.
- Backups in Cloud oder auf Band speichern: Validiert die Backup-Sätze, bevor sie in der Cloud und auf Band gespeichert werden.
- Prüfung und Compliance von Backups: Zum Erfüllen der Anforderungen auf Prüfung und die Einhaltung gesetzlicher Bestimmungen des Unternehmens können Sie Validierungsinformationen zu den Backups virtueller Computer angeben.

Während der Ausführung eines Auftrags zum Validieren eines virtuellen Computers für die Wiederherstellung wird der virtuelle Computer auf dem vCenter-Server oder ESX-Host mit dem Hostnamen im Format `validate_Name_des_virtuellen_Computers_GUID` registriert und dann eingeschaltet. Der virtuelle Computer wird nur für Validierungszwecke erstellt. Es ist eine temporärer Computer, der nach der Validierung entfernt wird. Nach dem Einschalten wird ein Heartbeat-Test ausgeführt, um zu prüfen, ob der Dienst "VMware Tools" ausgeführt wird.

Während der Validierung des virtuellen Computers erfolgt keine Datenübertragung.

Bei der Erstellung eines Auftrags zum Validieren eines virtuellen Computers für die Wiederherstellung können Sie die maximal zulässige Zeit für den Start des virtuellen Computers vor der Ausführung des Validierungsauftrags auswählen. Der Standardwert ist 10 Minuten. Sie können einen Wert zwischen 1 und 60 Minuten auswählen.

Siehe ["Konfigurieren der Standardeinstellungen für das Backup"](#) auf Seite 785.

Nach dem erfolgreichen Abschluss aller Prüfungsvorgänge wird der virtuelle Computer als zur Wiederherstellung bereit gekennzeichnet.

Alle während der Validierung erfassten Informationen sind Teil des Auftragsprotokolls. Nach der Validierung können Sie die Validierungsübersicht "Wiederherstellung bereit" erstellen, die die validierten virtuellen Computer enthält.

Siehe ["Validierungsübersicht "Wiederherstellung bereit""](#) auf Seite 843.

Doppelklicken Sie zum Anzeigen des Validierungsstatus auf der Registerkarte "Backup und Wiederherstellung" auf den Hostnamen bzw. auf der Registerkarte "Speicher" auf den Namen des Speichers. Klicken Sie im linken Teilfenster auf "Backup-Sätze". Für die ausgewählte Server- bzw. Speicheransicht wird der Validierungsstatus angezeigt.

Die folgende Tabelle beschreibt den Vorgang zur Validierung von virtuellen VMware-Computern für die Wiederherstellung.

Tabelle C-5 Validieren von virtuellen Computern für die Wiederherstellung

Schritt	Beschreibung
Schritt 1	Fügen Sie den vCenter-Server oder ESX-Host hinzu.
Schritt 2	Führen Sie ein plattenbasierten GRT-Backup des virtuellen Computers aus, der auf dem vCenter-Server oder ESX-Host gehostet wird. Die Funktion "Wiederherstellung bereit" unterstützt vollständige, inkrementelle und differenzielle Backup-Sätze.
Schritt 3	Führen Sie einen Auftrag zum Validieren eines virtuellen VMware-Computers für die Wiederherstellung aus.

Informationen zur Funktion "Wiederherstellung bereit" für virtuelle VMware-Computer

Schritt	Beschreibung
Schritt 4	Backup Exec virtualisiert den Backup-Satz.
Schritt 5	<p>Backup Exec erstellt auf dem Medienserver eine Freigabe in Form eines NFS-Datenspeichers. Der Datenspeicher wird auf dem Host, auf dem der virtuelle Computer für die Wiederherstellung validiert wird, verfügbar. Der Host hat nur Lesezugriff auf den NFS-Datenspeicher.</p> <p>Hinweis: Da Windows-Server für NFS nicht sicher ist, ist die von Backup Exec erstellte Freigabe auf dem Netzwerk verfügbar.</p>
Schritt 6	<p>Backup Exec führt die folgenden Tests in der angegebenen Reihenfolge auf dem zu validierenden virtuellen VMware-Computer aus.</p> <ul style="list-style-type: none"> ■ Registrieren des virtuellen Computers ■ Einschalten des virtuellen Computers ■ Heartbeat-Test auf dem virtuellen Computer
Schritt 7	Wenn alle Tests erfolgreich sind, kennzeichnet Backup Exec den VMware-Computer als validiert.

Tests, die auf dem zu validierenden virtuellen VMware-Computer ausgeführt werden

Auf dem zu validierenden virtuellen VMware-Computer werden die folgenden Tests ausgeführt.

Tabelle C-6 Auf einem virtuellen VMware-Computer ausgeführte Tests

Test	Beschreibung
Registrieren des virtuellen Computers	Beim ersten Test wird der virtuelle Computer auf dem vCenter-Server oder ESX-Host registriert.
Einschalten des virtuellen Computers	Im zweiten Test wird der registrierte virtuelle Computer eingeschaltet.
Taktsignal-Test	<p>Im dritten Test wird der Dienst "VMware Tools" überprüft. Wenn dieser Dienst erfolgreich auf dem eingeschalteten virtuellen Computer ausgeführt wird, war der Taktsignal-Test erfolgreich.</p> <p>Der Dienst "VMware Tools" muss auf dem virtuellen Computer, für den ein Backup erstellt wurde, installiert und aktiv sein, damit der Heartbeat-Test erfolgreich ausgeführt werden kann. Wenn "VMware Tools" nicht installiert ist, schlägt die Validierung fehl und für den entsprechenden Backup-Satz wird der Status "Validierung fehlgeschlagen" angezeigt.</p>

Alle Informationen zu den Testergebnissen sind auch im Auftragsprotokoll verfügbar.

Validierungsstatus für einen virtuellen VMware-Computer

Während der Validierung werden die folgenden Statuswerte für den Backup-Satz eines virtuellen VMware-Computers angezeigt:

- Validierung erfolgreich : Alle Tests für den Backup-Satz wurden erfolgreich abgeschlossen und der Backup-Satz ist nun für die Wiederherstellung bereit.
- Validierung fehlgeschlagen : Die Tests für den Backup-Satz konnten nicht erfolgreich abgeschlossen werden und der Backup-Satz ist nicht für die Wiederherstellung bereit.
- Validierung nicht möglich : Der virtuelle Computer konnte aufgrund von Problemen in der Umgebung nicht validiert werden. Daher können die Backup-Sätze nicht validiert werden.

Während der Validierung werden die folgenden Statuswerte für den Validierungsvorgang eines virtuellen VMware-Computers angezeigt:

- Erfolgreich : Alle Tests für die Validierung wurden abgeschlossen und der virtuelle Computer ist für die Wiederherstellung bereit.
- Erfolg mit Ausnahmen : Die Validierung war erfolgreich, aber beim Bereinigen der Ressourcen schlägt das Ausschalten fehl.
- Fehlgeschlagen : Die Validierung ist fehlgeschlagen oder wurde nicht ausgeführt.

Wenn die Validierung fehlschlägt oder Backup Exec den virtuellen Computer nicht für die Wiederherstellung validieren kann, werden weitere Informationen in das Validierungsauftragsprotokoll aufgenommen.

Im Folgenden finden Sie Details zu den Tests und zum Validierungsstatus.

Tabelle C-7 Validierungsstatus für einen virtuellen VMware-Computer

Validierungstest	Status des Backup-Satzes	Status des Validierungsauftrags	Ursache
Virtuellen Computer registrieren	Wenn die Registrierung erfolgreich abgeschlossen wurde, gehen Sie zum nächsten Prüfungsvorgang.		
	Validierung fehlgeschlagen	Fehlgeschlagen	Problem mit dem Backup-Satz
	Validierung nicht möglich	Fehlgeschlagen	Problem mit der Umgebung

Informationen zur Funktion "Wiederherstellung bereit" für virtuelle VMware-Computer

Validierungstest	Status des Backup-Satzes	Status des Validierungsauftrags	Ursache
Virtuellen Computer einschalten	Wurde der Computer eingeschaltet, gehen Sie zum nächsten Prüfungsvorgang.		
	Validierung nicht möglich	Fehlgeschlagen	Problem mit der Netzwerkverbindung oder Prüfungsvorgang wurde nicht versucht, weil die Registrierung fehlgeschlagen ist
Taktsignal-Test	Validierung nicht möglich	Fehlgeschlagen	Test nicht versucht
	Validierung fehlgeschlagen	Fehlgeschlagen	Problem beim Hochfahren oder Problem mit "VMware Tools"
	Validierung erfolgreich	Erfolgreich	Der virtuelle Computer ist validiert und für die Wiederherstellung bereit

Siehe ["Anforderungen zum Validieren eines virtuellen VMware-Computers für die Wiederherstellung"](#) auf Seite 1147.

Siehe ["Hinweise zur Validierung von virtuellen VMware-Computern für die Wiederherstellung"](#) auf Seite 1148.

Siehe ["Erstellen eines Auftrags zum Validieren eines virtuellen Computers für die Wiederherstellung"](#) auf Seite 1149.

Anforderungen zum Validieren eines virtuellen VMware-Computers für die Wiederherstellung

Machen Sie sich mit den folgenden Anforderungen vertraut, bevor Sie für einen virtuellen VMware-Computer einen Auftrag zum Validieren des virtuellen Computers für die Wiederherstellung konfigurieren:

- VMware Tools muss auf dem vCenter-Server oder ESX-Host installiert sein.
- Installieren Sie die Rolle "Windows-Server für NFS" auf dem Medienserver. Weitere Informationen finden Sie in der Microsoft Windows-Dokumentation.
- Aktivieren Sie die Granular Recovery Technology von Backup Exec zum Wiederherstellen einzelner Elemente während des VMware-Backup-Auftrags. Sichern Sie virtuelle Computer mit der virtuellen Backup-Methode. Wenn der virtuelle Computer nicht für GRT geeignet ist, können Sie die Option "Sofortwiederherstellung für alle virtuellen Computer aktivieren, auch für solche,

die GRT nicht nutzen können." aktivieren. Beachten Sie, dass dann das Speicherformat des nächsten vollständigen Backups in eines geändert wird, das mit der Sofortwiederherstellung kompatibel ist.

Siehe ["Verwenden von Granular Recovery Technology \(GRT\) mit Agent for VMware"](#) auf Seite 1115.

- Verwenden Sie Datenträgerspeicher für den Backup-Auftrag von VMware. Deduplizierungsspeicher, Cloud-Speicher und Plattenkassettengeräte wie RDX werden nicht unterstützt.
- Der Host muss vSphere 5.1 oder eine Nachfolgerversion verwenden.
- Stellen Sie anhand der Hardwarekompatibilitätsliste und der Softwarekompatibilitätsliste sicher, dass Ihre Umgebung unterstützte Hardware und Software aufweist. Die unterstützten Betriebssysteme, Plattformen und Anwendungen finden Sie in der Liste der mit Backup Exec kompatiblen Hardware und Software.

Hinweise zur Validierung von virtuellen VMware-Computern für die Wiederherstellung

Beachten Sie die folgenden Hinweise, bevor Sie für einen virtuellen VMware-Computer einen Auftrag zum Validieren eines virtuellen Computers für die Wiederherstellung konfigurieren:

- Die Backup Exec-Befehlszeilenschnittstelle (BEMCLI) wird für Aufträge zum Validieren von virtuellen Computern für die Wiederherstellung nicht unterstützt.
- Die Validierung von virtuellen VMware-Computern für die Wiederherstellung wird für geclusterte Backup Exec-Umgebungen nicht unterstützt.
- Für CAS-Umgebungen gilt Folgendes:
 - Wenn der zentrale Administrationsserver (CAS) über einen Backup-Satz verfügt, erstellen Sie den Auftrag zum Validieren eines virtuellen Computers für die Wiederherstellung nur auf dem CAS-Server. Wenn der verwaltete Backup Exec-Server ("Managed Backup Exec Server"/MBES) über einen Backup-Satz verfügt, erstellen Sie den Auftrag zum Validieren eines virtuellen Computers für die Wiederherstellung nur auf dem MBES-Server.
 - Sie können einen Auftrag zum Validieren eines virtuellen Computers für die Wiederherstellung nicht mehr von einem zentralen Administrationsserver aus ausführen, nachdem Sie den Auftrag an einen verwalteten Backup Exec-Server delegiert haben.

Best Practices zum Validieren eines virtuellen VMware-Computers für die Wiederherstellung

Beachten Sie die folgenden Best Practices, bevor Sie für einen virtuellen VMware-Computer einen Auftrag zum Validieren eines virtuellen Computers für die Wiederherstellung konfigurieren:

- Beim Validieren eines virtuellen Computers für die Wiederherstellung muss für VMware dieselbe Version des ESX-Host oder höher als Ziel angegeben werden.
- Es wird empfohlen, die neueste Version der VMware ISO Tools für den gesicherten virtuellen VMware-Computer zu installieren.
- Die maximale Anzahl Aufträge "Virtuellen Computer für die Wiederherstellung validieren", die parallel ausgeführt werden können, hängt von den verfügbaren NFS-Bereitstellungspunkten auf dem Ziel-ESX-Host ab.
NFS-Bereitstellungspunkte werden auch von sofort wiederhergestellten virtuellen Computern genutzt. Stellen Sie sicher, dass die erforderliche Anzahl von NFS-Bereitstellungspunkten zum Ausführen aller Aufträge verfügbar ist.
- Beim Validieren eines virtuellen Computers für die Wiederherstellung erstellt Backup Exec eine NFS-Freigabe mit den erforderlichen VMDK-Dateien und konfiguriert ESXi für die Verwendung der Freigabe. Die für die NFS-Freigabe festgelegten Berechtigungen sind so konfiguriert, dass der Zugriff auf Anforderungen begrenzt wird, die aus einer ESXi-IP-Adresse stammen. Wenn ein virtueller Gastcomputer NAT auf ESXi verwendet, kann er auf die NFS-Freigabe auf dem Backup Exec-Server zugreifen. Als Best Practice für Sicherheit wird empfohlen, Portgruppen mit bestimmten zugewiesenen NICs zu konfigurieren, sodass virtuelle Computer, die mit einer Portgruppe verbunden sind, von der anderen Portgruppe getrennt sind, über die ESXi Zugriff auf die NFS-Freigabe hat.

Erstellen eines Auftrags zum Validieren eines virtuellen Computers für die Wiederherstellung

Sie können einen Auftrag zum Validieren eines virtuellen Computers für einen VMware-Computer erstellen.

Siehe ["Anforderungen zum Validieren eines virtuellen VMware-Computers für die Wiederherstellung"](#) auf Seite 1147.

Gehen Sie dazu folgendermaßen vor:

So erstellen Sie einen Auftrag zum Validieren eines virtuellen Computers für die Wiederherstellung

- 1 Wählen Sie auf der Registerkarte "Backup und Wiederherstellung" den virtuellen Computer aus, der wiederhergestellt werden soll.
- 2 Klicken Sie in der Gruppe "Wiederherstellung bereit" auf "VM für Wiederherstellung validieren".
- 3 Geben Sie im Dialogfeld "Virtuellen Computer für die Wiederherstellung validieren" im Feld "Auftragsname" einen Namen für den Validierungsauftrag ein oder übernehmen Sie den Standardnamen.
- 4 Wählen Sie im Gruppenfeld "Backup-Satz-Auswahl" die gewünschten Backup-Sätze aus.

Element	Beschreibung
Verwenden Sie den neuesten datenträgerbasierten Backup-Satz, wenn der Auftrag ausgeführt wurde.	Gibt an, dass nur der neueste verfügbare datenträgerbasierte Backup-Satz verwendet wird, wenn der Auftrag zum Validieren des virtuellen VMware-Computers für die Wiederherstellung ausgeführt wird.
Datenträgerbasierten Backup-Satz auswählen	<p>Gibt an, dass ein verfügbarer datenträgerbasierter Backup-Satz für den Auftrag zum Validieren des virtuellen VMware-Computers für die Wiederherstellung verwendet werden soll.</p> <p>Backup-Sätze anzeigen von</p> <p>Das Start- und Enddatum für die Backup-Sätze, die in die Auswahl aufgenommen werden sollen.</p> <p>Standardmäßig werden nur die Backup-Sätze für Aufträge angezeigt, die in den letzten 30 Tagen ausgeführt wurden.</p>
Datenträgerbasierter Backup-Satz	<p>Der Backup-Satz, der für die Validierung verwendet werden soll.</p> <p>In der Liste werden nur Backup-Sätze angezeigt, die die Validierungsanforderungen erfüllen.</p>

- 5 Wählen Sie im Dialogfeld "Virtuellen Computer für die Wiederherstellung validieren" auf der linken Seite die Option "Ziel" und legen Sie dann die nachfolgenden Optionen für den Auftrag fest.

Element	Beschreibung
Name des VMware vCenter-Servers oder ESX-Hosts	<p>Der Name des vCenter-Servers oder ESX-Hosts.</p> <p>Hinweis: Sie können auch einen vCenter-Server oder -Host eingeben, der sich vom Quellserver bzw. -Host unterscheidet.</p>
Server-Login-Konto	Verwendet das Standard-Login-Konto, das erscheint. Sie können ein anderes Login-Konto für den vCenter-Server oder ESX-Host wählen.
Host	Der Name des ESX-Host, auf dem der validierte virtuelle Computer ausgeführt wird.
Ordner auf dem virtuellen Computer	<p>Der Name des vorhandenen vSphere-Ordners, für den der virtuelle Computer validiert werden soll.</p> <p>Der Standardordner ist der Stamm des Datacenter.</p>
Ressourcenpool	<p>Der Name des Ressourcenpools, für den der virtuelle Computer validiert werden soll.</p> <p>Der Ressourcenpool ist optional.</p>
Datenspeicher oder Datenspeicher-Cluster zum Speichern von virtuellen Computer-Schreibzugriffen	Wählen Sie den Namen des Datenspeichers aus, in dem alle am validierten virtuellen Computer vorgenommenen vorübergehenden Änderungen gespeichert werden sollen.

Informationen zur Funktion "Wiederherstellung bereit" für virtuelle VMware-Computer

- 6** Wählen Sie im Dialogfeld "Virtuellen Computer für die Wiederherstellung validieren" auf der linken Seite die Option "Plan" und legen Sie dann die Planung für diesen Vorgang fest.

Element	Beschreibung
Wiederkehrend	Wählen Sie diese Option, um einen wiederkehrenden Zeitplan für den Auftrag zu erstellen.
Jetzt ohne wiederkehrenden Zeitplan ausführen	Führt den Auftrag sofort ohne wiederkehrenden Zeitplan aus.
Ausführen am	Plant den Auftrag, der für ein bestimmtes Datum und eine bestimmte Uhrzeit auszuführen ist.
Ohne Zeitplan erstellen	Erstellt den Auftrag, ohne ihn zu planen. Bei dieser Option wird der Auftrag nicht zum Zeitpunkt der Erstellung ausgeführt. Der Auftrag bleibt ungeplant, bis Sie ihn ausführen.
Auftrag in Wartestellung senden	Hiermit können Sie den Auftrag senden, aber erst nach dem Ändern des entsprechenden Wartestatus ausführen.

- 7** (Optional) Wählen Sie im Dialogfeld "Virtuellen Computer für die Wiederherstellung validieren" auf der linken Seite die Option "Benachrichtigung" und legen Sie dann die Empfänger fest, die benachrichtigt werden sollen, wenn der Auftrag zum Validieren des virtuellen VMware-Computers für die Wiederherstellung abgeschlossen ist.

- 8** Klicken Sie auf "OK".

Der Auftrag zum Validieren des virtuellen Computers wird ausgeführt. Nach erfolgreichem Abschluss ist der virtuelle Computer für die Wiederherstellung bereit.

Doppelklicken Sie zum Anzeigen des Validierungsstatus auf der Registerkarte "Backup und Wiederherstellung" auf den vCenter-Server oder ESX-Host bzw. auf der Registerkarte "Speicher" auf den Namen des Speichers. Klicken Sie im linken Teilfenster auf "Backup-Sätze". Für die ausgewählte Server- bzw. Speicheransicht wird der Status in der Spalte "Validierungsstatus" angezeigt.

Backup Exec Agent for Microsoft Hyper-V

Dieser Anhang enthält folgende Themen:

- [Agent for Microsoft Hyper-V](#)
- [Anforderungen für die Verwendung des "Agent for Microsoft Hyper-V"](#)
- [Installieren des "Agent for Microsoft Hyper-V"](#)
- [Hinweise zum Einsatz des Agent for Hyper-V](#)
- [Speicherplatzoptimierung mit Agent for Hyper-V](#)
- [Hinzufügen eines Hyper-V-Hosts zur Serverliste auf der Registerkarte "Backup und Wiederherstellung"](#)
- [Anzeigen von Details zu Hyper-V-Ressourcen](#)
- [Installieren von Agent for Windows auf virtuellen Hyper-V-Computern](#)
- [Push-Installation von Agent for Windows auf virtuellen Hyper-V-Computern](#)
- [Sichern von virtuellen Computern mit Microsoft Hyper-V](#)
- [Wiederherstellen von virtuellen Microsoft Hyper-V-Computern](#)
- [Info zur Sofortwiederherstellung eines virtuellen Hyper-V-Computers](#)
- [Informationen zur Funktion "Wiederherstellung bereit" für virtuelle Hyper-V-Computer](#)
- [Fehlerbehebung bei Problemen mit Backup Exec Agent for Microsoft Hyper-V](#)

Agent for Microsoft Hyper-V

Mit Backup Exec Agent for Hyper-V ("Agent for Hyper-V") können Sie die folgenden Ressourcen sichern und wiederherstellen:

- Hyper-V-Hosts, die unter unterstützten Versionen von Microsoft Windows ausgeführt werden.
Die unterstützten Betriebssysteme, Plattformen und Anwendungen finden Sie in der Liste der mit Backup Exec kompatiblen Software.
- Alle virtuellen Computer, die sich lokal auf den Hyper-V-Hosts befinden.
- Geclusterte Hyper-V-Hosts, einschließlich virtuelle Computer, die sich auf gemeinsam genutzten Datenträgern (Clustered Shared Volumes, CSV) befinden.
- Virtuelle Computer, deren Datenträger sich auf dem Server Message Block (SMB) befinden.
- Virtuelle Computer, deren Datenträger sich auf dem Scale-out-Dateiserver befinden.

Der Hyper-V-Agent ermöglicht die Verwendung von drei Methoden für Backups:

- Die Methode Resilient Change Tracking (RCT): Diese Methode steht für virtuelle Computer zur Verfügung, die unter Microsoft Hyper-V Server 2016 oder höher gehostet werden und über die Konfigurationsversion 8.0 oder höher verfügen. RCT ist ein nativer Microsoft Hyper-V-Mechanismus für das Erfassen geänderter Daten auf den virtuellen Festplatten eines virtuellen Computers. Während des Backups wird Microsoft Hyper-V von Backup Exec aufgefordert, einen Kontrollpunkt für den ausgewählten virtuellen Computer zu erstellen. Das Backup wird für diesen Kontrollpunkt ausgeführt.

Nach dem Backup des virtuellen Computers und bevor der Kontrollpunkt mit dem virtuellen Basisdatenträger zusammengeführt wird, wird der Kontrollpunkt von Hyper-V zu einem Referenzpunkt konvertiert. Der Referenzpunkt stellt die Ansicht des Datenträgers des virtuellen Computers zu einem bestimmten Zeitpunkt dar.

Während des inkrementellen Backups desselben virtuellen Computers erstellt Backup Exec einen neuen Kontrollpunkt und nutzt diesen als Quelle für das Backup. Über Backup Exec wird eine Abfrage an Hyper-V gesendet, um die inkrementellen Änderungen zwischen dem während des vorherigen Backup-Auftrags erstellten Referenzpunkt und dem während des aktuellen Backup-Auftrags erstellten Kontrollpunkts zu erfassen. Nur die geänderten Daten am Kontrollpunkt werden gesichert.

Backup Exec unterstützt sowohl inkrementelle Backups als auch differenzielle Backups, wenn die RCT-Methode angewandt wird.

- Die Standardmethode: Diese Methode liest den gesamten virtuellen Datenträger und identifiziert die Änderungen, die gesichert werden müssen. Die erkannten geänderten Daten werden dann gesichert. Backup Exec unterstützt sowohl inkrementelle Backups als auch differenzielle Backups, wenn diese Methode angewandt wird.
- Die schnellere Methode: Diese Methode ist schneller als die Standardmethode, da alle Änderungen auf einen neuen Datenträger geschrieben werden und dann nur dieser Datenträger gesichert wird. Backup Exec unterstützt nur inkrementelle Backups, wenn diese Methode angewandt wird. Lesen Sie den Abschnitt "Konfigurieren der Standardeinstellungen für das Backup", um zu erfahren, wie die Einstellungen für inkrementelle und differenzielle Hyper-V-Backups konfiguriert werden.

Siehe ["Konfigurieren der Standardeinstellungen für das Backup"](#) auf Seite 785.

Bei einer neuen Installation

Bei einer neuen Installation von Backup Exec werden standardmäßig die RCT-Methode und die Standardmethode ausgewählt.

Bei der Installation einer Aktualisierung

Bei der Installation einer Aktualisierung bleiben die Einstellungen unverändert und die RCT-Methode wird nicht ausgewählt. Die zuvor ausgewählte Methode (Standardmethode oder schnellere Methode) wird nicht geändert. Wenn ein Backup für einen virtuellen Computer mit dem Hyper-V-Agent von Backup Exec durchgeführt wird, sollten Sie die folgenden Hinweise in Betracht ziehen, bevor Sie sich für eine Methode entscheiden.

Die Hyper-V-Version ist Microsoft Windows Server 2016 oder höher und der ausgewählte virtuelle Computer verfügt über die Konfigurationsversion 8.0 oder höher: Backup Exec versucht, die RCT-Methode anzuwenden, wenn die RCT-Methode in den Backup Exec-Einstellungen ausgewählt ist. Wenn die RCT-Methode nicht ausgewählt ist, wird von Backup Exec eine der ausgewählten Methoden (Standardmethode oder schnellere Methode) angewandt.

Wenn es sich bei der Hyper-V-Version um Windows Server 2012 R2 oder früher handelt, wird die RCT-Methode nicht unterstützt. Von Backup Exec wird eine der ausgewählten Methoden für standardmäßiges oder schnelleres Verarbeiten angewandt.

Online- und Offline-Backups

Backup Exec kann virtuelle Computer sichern, die online, offline oder gespeichert sind. Die virtuellen Computer, die Hyper-V-Integrationsdienste verwenden, können gesichert werden, während sie online sind. Sie können die virtuellen Online- und Offline-Computer in den gleichen Backup-Auftrag einschließen. Während des

Backups eines virtuellen Online-Computers führt Backup Exec ein Snapshot-Backup des Hyper-V-Hosts aus. Der Host führt wiederum einen Snapshot der virtuellen Computer auf dem Host aus. Backup Exec kann so virtuelle Server ohne Ausfallzeit sichern. Wenn ein Online-Backup nicht durchgeführt werden kann und die Option "Virtuelle Computer ausschließen, die zum Sichern gespeichert sein müssen" für den Backup-Auftrag ausgewählt wird, dann wird ein Offline-Backup durchgeführt. Mit einem Offline-Backup wird der virtuelle Computer kurz in einem gespeicherten Status angehalten. Der virtuelle Computer bleibt während des gesamten Backup-Auftrags nicht im gespeicherten Status.

Die Systemausfallzeiten für einen Backup-Auftrag im gespeicherten Modus richtet sich nach Folgendem:

- Der Größe des Arbeitsspeichers, der dem virtuellen Computer zugewiesen ist
- Die aktuelle Auslastung auf dem Host-Betriebssystem.

Informationen zu den Best Practices zum Einsatz des Backup Exec Agent for Microsoft Hyper-V finden Sie unter *Best Practices für Backup Exec*.

Siehe ["Anforderungen für die Verwendung des "Agent for Microsoft Hyper-V""](#) auf Seite 1156.

Siehe ["Sichern von virtuellen Computern mit Microsoft Hyper-V"](#) auf Seite 1167.

Siehe ["Wiederherstellen von virtuellen Microsoft Hyper-V-Computern"](#) auf Seite 1187.

Anforderungen für die Verwendung des "Agent for Microsoft Hyper-V"

Die unterstützten Betriebssysteme, Plattformen und Anwendungen finden Sie in der Liste der mit Backup Exec kompatiblen Hardware und Software.

Die folgenden Komponenten sind erforderlich:

Tabelle D-1 Anforderungen für den "Agent for Microsoft Hyper-V"

Software	Installiert auf
Eine unterstützte Version von Microsoft Hyper-V	Microsoft Hyper-V-Host

Software	Installiert auf
Backup Exec	<p>Backup Exec-Server</p> <p>Hinweis: Es wird empfohlen, dass der Backup Exec-Server eine Windows-Version ausführt, die mindestens der höchsten Windows-Version entspricht, die auf den virtuellen Computern in Ihrer Umgebung ausgeführt wird. Beispiel: Wenn Ihre virtuellen Computer Microsoft Windows Server 2012 ausführen, sollte auch der Backup Exec-Server Microsoft Windows Server 2012 ausführen.</p>
Agent for VMware and Hyper-V	<p>Microsoft Hyper-V-Host</p> <p>Hinweis: Wenn Sie Hyper-V in einer Clusterumgebung verwenden, müssen Sie den Agent for VMware und Hyper-V auf jedem Knotenpunkt im Cluster installieren. Wenn Sie die nicht tun, können Sie möglicherweise nicht alle Cluster-Backup-Quellen sehen, die für Backup verfügbar sind.</p>
VHDMount	<p>Backup Exec-Server (falls der Backup Exec-Server nicht der virtuelle Server ist).</p> <p>Hinweis: VHDMount ist nur dann erforderlich, wenn der Backup Exec-Server Microsoft Windows Server 2008 ausführt und die Hyper-V-Rolle nicht installiert ist. Sie können die VHDMount-Komponente von Microsoft Virtual Server 2005 R2 SP1 installieren. Zusätzlich dazu ist VHDMount für Granular Recovery Technology(GRT)-fähige Backups erforderlich. Wenn Sie nicht planen, GRT zu verwenden, ist VHDMount nicht erforderlich.</p>

Anforderungen für Online-Backups

Um ein Online-Backup ausführen zu können, müssen die folgenden Voraussetzungen erfüllt sein

- Prüfen Sie, ob auf der Microsoft-Website eine Version von Hyper-V Server und die unterstützten Windows Server-Gastversionen verfügbar sind.

- Hyper-V Integration Services with Backup (Volume Snapshot) ist installiert.

Hinweis: Die Verwendung einer falschen Version von Hyper-V Integration Services kann dazu führen, dass ein virtueller Computer offline statt online gesichert wird. Beispiel: Wenn Sie einen virtuellen Computer von einem Windows 2012 Hyper-V-Host auf eine Windows 2012 R2 Hyper-V-Host kopieren, wird Hyper-V-Integration Services nicht automatisch aktualisiert.

- Der virtuelle Server wird ausgeführt.

Wenn diese Bedingungen nicht erfüllt sind, wird der virtuelle Computer in einen gespeicherten Zustand versetzt, falls er ausgeführt wird. Wenn der virtuelle Computer ausgeschaltet wird, dann wird dieser virtuelle Computer nur dann gesichert, wenn Sie die Option "Ausgeschaltete virtuelle Computer sichern" im Dialogfeld "Virtuelle Computer" aktivieren.

Anforderungen für das Sammeln von Katalogdaten für Microsoft-Anwendungen

Damit Backup Exec Katalogdaten für Microsoft Exchange, SharePoint, Active Directory und SQL auf dem virtuellen Computer erfassen kann, sind auf dem virtuellen Computer die folgenden Elemente erforderlich:

- Eine lizenzierte Version des Backup Exec-Agent für die Anwendung.
- Der Agent for Windows.
Agent for Microsoft Hyper-V schließt eine Lizenz für "Agent for Windows" ein. Die Agents für Microsoft Exchange, Active Directory und SQL umfassen ebenfalls eine Lizenz für Agent for Windows. Es ist keine separate Lizenz für Agent for Windows erforderlich.
- Der virtuelle Computer muss online gesichert werden können.
- Die Identifikationsdaten, die Sie für den Zugriff auf den virtuellen Computer verwenden, müssen auch für den Zugriff auf die Anwendung gelten.

Anforderungen für virtuelle Computer

Elemente werden für virtuelle Computer benötigt:

- Virtuelle Computer müssen eindeutige Namen haben. Backup Exec unterstützt keine virtuellen Computer, die doppelte Namen haben.
- Sie müssen jedem NTFS-Datenträger, der auf einem virtuellen Computer existiert, Schattenspeicher zuweisen, wenn der virtuelle Computer das Windows 2008-Betriebssystem verwendet. Andernfalls schlagen die Backup-Aufträge für diese virtuellen Computer fehl.

- Agent for Windows muss auf dem virtuellen Computer installiert werden, damit einzelne Dateien und Ordner auf dem ursprünglichen virtuellen Computer wiederhergestellt werden können.
- Agent for Windows muss auf dem virtuellen Computer installiert sein, damit einzelne SQL-Datenbanken, Exchange-Elemente, SharePoint-Elemente und Active Directory-Objekte auf dem ursprünglichen virtuellen Computer wiederhergestellt werden können.
- Benutzen Sie Sonderzeichen, wie Prozentzeichen (%) oder Schrägstrich (/) nicht in den Hyper-V-Namen auf dem virtuellen Computer. Sonderzeichen könnten dazu führen, dass umgeleitete Wiederherstellungen fehlschlagen.

Siehe ["Agent for Microsoft Hyper-V"](#) auf Seite 1154.

Installieren des "Agent for Microsoft Hyper-V"

Backup Exec Agent for Microsoft Hyper-V wird als Teil des Agent for VMware and Hyper-V installiert. Agent for Microsoft Hyper-V wird auf dem Microsoft Hyper-V-Host installiert. Wenn der Backup Exec-Server zugleich der Microsoft Hyper-V-Host ist, können Sie Agent for Microsoft Hyper-V bei der Installation von Backup Exec installieren. Sie können die Installation auch erst dann durchführen, wenn Backup Exec bereits installiert ist.

Wenn Backup Exec nicht auf dem Microsoft Hyper-V-Host installiert ist, müssen Sie Agent for Windows über eine Push-Installation auf dem Microsoft Hyper-V-Host installieren. Agent for Microsoft Hyper-V muss nicht auf virtuellen Computern installiert werden. Auf dem Backup Exec-Server ist jedoch eine Lizenz für Agent for Microsoft Hyper-V erforderlich. Agent for Windows ist in Agent for Microsoft Hyper-V enthalten.

Siehe ["Installieren zusätzlicher Agents und Funktionen auf dem lokalen Backup Exec-Server"](#) auf Seite 66.

Siehe ["Installieren von Agent for Windows auf Remote-Computern über eine Push-Installation"](#) auf Seite 78.

Hinweise zum Einsatz des Agent for Hyper-V

Mit dem Backup Exec Agent for Hyper-V können Sie virtuelle Hyper-V-Computer, die auf Microsoft Windows Server 2012 und höher gehostet werden, sichern und wiederherstellen. Diese Version von Backup Exec unterstützt das VHDX-Dateiformat von Windows Server 2012 und höher sowie inkrementelle Microsoft-Backups.

- Virtuelle Computer nur mit VHD-Dateien

Sowohl GRT auf Datei-/Ordner Ebene als auch GRT auf Anwendungsebene wird vollständig unterstützt.

- Virtuelle Computer nur mit VHDX-Dateien
 - Backup Exec-Server mit Windows Server 2008 R2 oder niedriger
Wenn ein virtueller Computer nur VHDX-Dateien hat, wird GRT auf Datei-/Ordner- und Anwendungsebene unterstützt, sofern die VHDX-Dateien eine Kapazität von weniger als 2040 GB haben und die logische Sektorgröße im VHDX 512 Byte ist. Wenn die VHDX-Dateien eine Kapazität von mehr als 2040 GB haben, wird GRT auf Datei-/Ordner- und Anwendungsebene nicht unterstützt. Der Auftrag wird mit dem Status "Erfolg mit Ausnahmen" abgeschlossen, aber es steht keine GRT-Wiederherstellungsfunktion zur Verfügung. Eine vollständige Wiederherstellung des virtuellen Computers ist verfügbar.
 - Backup Exec-Server mit Windows Server 2012 oder höher
Sowohl GRT auf Datei-/Ordner Ebene als auch GRT auf Anwendungsebene wird vollständig unterstützt.
- Virtuelle Computer mit VHD- und VHDX-Dateien
 - Backup Exec-Server mit Windows Server 2008 R2 oder niedriger
Wenn ein virtueller Computer über eine Mischung von VHD- und VHDX-Dateien verfügt, aber alle VHDX-Dateien eine Kapazität von weniger als 2 TB haben und die logische Sektorgröße der VHDX-Dateien 512 Byte beträgt, wird sowohl GRT auf Datei-/Ordner Ebene als auch GRT auf Anwendungsebene vollständig unterstützt.
Wenn ein virtueller Computer über eine Mischung von VHD- und VHDX-Dateien verfügt, aber mindestens eine VHDX-Datei eine Kapazität von mehr als 2 TB hat, wird GRT auf Datei-/Ordner Ebene und GRT auf Anwendungsebene nicht unterstützt. Der Auftrag wird mit dem Status "Erfolg mit Ausnahmen" abgeschlossen, aber es steht keine GRT-Wiederherstellungsfunktion zur Verfügung. Eine vollständige Wiederherstellung des virtuellen Computers ist verfügbar.
 - Backup Exec-Server mit Windows Server 2012 oder höher
Sowohl GRT auf Datei-/Ordner Ebene als auch GRT auf Anwendungsebene wird vollständig unterstützt.
- Virtuelle Computer, die mit Fiber Channel HBAs konfiguriert sind, werden während der Backup-Aufträge übersprungen. Im Auftragsprotokoll ist eine Meldung aufgeführt, die besagt, dass der virtuelle Computer übersprungen wurde.
- Remote-VSS wird nicht unterstützt. Das heißt, virtuelle Computer mit .vhd- oder .vhdx-Dateien auf Freigaben werden nicht unterstützt.

- Das Backup einer VSS-Kopie eines virtuellen Computers wird nicht unterstützt.
- Backup Exec unterstützt keine Sofortwiederherstellung eines virtuellen Computers auf einen Hyper-V-Server, auf dem eine ältere Version ausgeführt wird als auf dem Hyper-V-Server, der zum Sichern des virtuellen Computers verwendet wurde. Beispiel: Ein virtueller Computer, für den über einen Hyper-V 2012-Host ein Backup durchgeführt wurde, kann nicht mit einer früheren Version von Hyper-V (zum Beispiel 2008 oder 2008 R2) auf einem virtuellen Computer wiederhergestellt werden.
- Virtuelle Computer, die über Speicherplätze verfügen, werden nicht unterstützt, weil Microsoft Hyper-V-VSS keine Snapshots von virtuellen Computern mit Speicherplätzen erstellen kann.
- Backups des virtuellen Computers mit Hyper-V-Replikation führen möglicherweise zu redundanten Backups des virtuellen Primärcomputers und des replizierten virtuellen Computers.
- Virtuelle Computer, die mit Remote-Speicher konfiguriert sind, werden während der Backup-Aufträge übersprungen. Das Auftragsprotokoll enthält eine Meldung über die virtuellen Computer, die übersprungen wurden.
- Wenn Sie einen Datenträger sichern, der sich auf einem vhdx-Datenträger befindet und bei deaktivierter Option "Schnellformatierung" formatiert wurde, entspricht die Größe des Backups der Größe des Datenträgers anstelle der Größe der gesicherten Daten.
- Virtuelle Computer, die VHDX-Dateien gemeinsam genutzt haben, werden aus einem Backup-Auftrag ausgeschlossen und der Auftrag schlägt fehl.
- Die Wiederherstellung eines virtuellen Gen2-Computers kann nur auf einen anderen Hyper-V-Host, der Windows Server 2012 R2 oder höher ausführt, umgeleitet werden.
- Wenn Sie GRT für einen virtuellen Hyper-V-Computer aktivieren möchten, auf dem Active Directory oder Active Directory Lightweight ausgeführt wird und diesen virtuellen Computer auf Band sichern möchten, muss auf dem Hyper-V-Host und dem Backup Exec-Server dieselbe Windows-Server-Version ausgeführt werden. Beispiel: Wenn Sie GRT für einen virtuellen Hyper-V-Computer aktivieren möchten, der Active Directory oder Active Directory Lightweight unter Windows Server 2012 R2 ausführt und diesen virtuellen Computer auf Band sicher möchten, müssen sowohl der Hyper-V-Host als auch der Backup Exec-Server Windows Server 2012 R2 ausführen.
- Benutzerdefinierte Kontrollpunkte werden von Backup Exec nicht wiederhergestellt, wenn ein virtueller Computer mit der RCT-Methode geschützt wird und im virtuellen Computer zum Zeitpunkt des Backups benutzerdefinierte Kontrollpunkte vorhanden waren. Alle Daten in den Datenträgern des virtuellen

Computers, einschließlich der Kontrollpunktdatenträger, werden wiederhergestellt, aber die Kontrollpunkte stehen im Hyper-V-Manager nicht zur Verfügung.

Wenn in einem virtuellen Computer benutzerdefinierte Kontrollpunkte vorhanden sind, werden diese Kontrollpunkte von Backup Exec nicht wiederhergestellt, falls der virtuelle Computer mit der RCT-Methode geschützt wird.

- Das Wiederherstellen eines auf einem freigegebenen SMB-/Scale-Out-Dateiserver gehosteten virtuellen Computers kann nur auf dem ursprünglichen Speicherort oder auf einem lokal gehosteten Datenträger auf dem Hyper-V-Host erfolgen. Die umgeleitete Wiederherstellung auf einen anderen freigegebenen SMB-/Scale-Out-Dateiserver wird nicht unterstützt. Nach der Wiederherstellung eines virtuellen Computers wird empfohlen, dass Sie ein vollständiges Backup des virtuellen Computers ausführen.

Siehe ["Anforderungen für die Verwendung des "Agent for Microsoft Hyper-V""](#) auf Seite 1156.

Speicherplatzoptimierung mit Agent for Hyper-V

Backup Exec versucht im Rahmen von Hyper-V-Backup-Aufträgen eine Speicherplatzoptimierung durchzuführen. Dies wird bei Möglichkeit immer durchgeführt.

Jedoch kann die Speicherplatzoptimierung in den folgenden Situationen nicht durchgeführt werden:

- Das Dateisystem ist nicht NTFS. Beispiel: Ist das Dateisystem FAT, ReFS oder Linux, wird der Vorgang nicht durchgeführt.
- Die Datenträger sind mit Windows-Speicherplätzen konfiguriert.
- Die Datenträger sind mit dynamischen Datenträgern (übergreifend, Stripeset, gespiegelt oder RAID 5) konfiguriert, entweder für MBR- oder GPT-Datenträger.
- Die VHD- bzw. VHDX-Datei ist zur Zeit des Backups nicht konsistent.

Eine Datei kann aus den folgenden Gründen nicht konsistent sein:

- Wenn ein Offline-Backup eines laufenden virtuellen Computers durchgeführt wird. Dies tritt möglicherweise auf, wenn die Hyper-V Integration Services nicht installiert sind, oder wenn die Version der Integration Services auf einem virtuellen Computer nicht mit der auf einem Hyper-V-Host identisch ist. Dies tritt möglicherweise auch auf, wenn auf dem virtuellen Computer ein nicht unterstütztes Betriebssystem ausgeführt wird.
- Die vom Benutzer erstellten Kontrollpunkte (Snapshots) erzeugen keine konsistenten Datenträger.

Hinzufügen eines Hyper-V-Hosts zur Serverliste auf der Registerkarte "Backup und Wiederherstellung"

Sie können einen Hyper-V-Host der Liste von Servern auf der Registerkarte "Backup und Wiederherstellung" hinzufügen, damit der Hostserver und der darauf gehostete virtuelle Computer für Backup-Aufträge ausgewählt werden können.

So fügen Sie einen Hyper-V-Hosts zur Serverliste auf der Registerkarte "Backup und Wiederherstellung" hinzu

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" unter "Server und virtuelle Hosts" auf "Hinzufügen".
- 2 Wählen Sie "Microsoft Hyper-V-Host", und klicken Sie dann auf "Weiter".
- 3 Aktivieren Sie die Option "Zulassen, dass Backup Exec ein Vertrauensverhältnis mit den Servern herstellt", und klicken Sie dann auf "Weiter".
- 4 Wählen Sie "Einen Microsoft Hyper-V-Server der Serverliste hinzufügen".
- 5 Geben Sie den Namen oder die IP-Adresse des hinzuzufügenden Hyper-V-Hosts und eine optionale Beschreibung ein.
- 6 Wenn Sie Agent for Windows auf allen virtuellen Computern des Hosts installieren möchten, stellen Sie sicher, dass die Option "Nach Hinzufügen des virtuellen Host Backup Exec Agent for Windows auf den virtuellen Computern installieren" ausgewählt ist.

Wenn Sie Agent for Windows nicht auf den virtuellen Gastcomputern installieren möchten, deaktivieren Sie das Kontrollkästchen.

- 7 Klicken Sie auf "Weiter".
- 8 Wählen Sie in der Dropdown-Liste das korrekte Login-Konto für den Server aus.

Befindet sich das korrekte Login-Konto nicht in der Liste, klicken Sie auf "Hinzufügen/Bearbeiten", um es der Liste hinzuzufügen.

- 9 Klicken Sie auf "Weiter".

- 10** Wählen Sie eine der folgenden Optionen, und klicken Sie anschließend auf "Weiter".

Backup Exec Agent for Windows automatisch auf die aktuelle Version aktualisieren

Ist diese Option aktiviert, kann Backup Exec die neueste Version von Agent for Windows installieren, wenn bereits eine ältere Version auf den ausgewählten virtuellen Computern installiert ist.

Remote-Computer automatisch neu starten, nachdem der Backup Exec Agent for Windows installiert wurde und wenn ein Neustart erforderlich ist

Aktivieren Sie diese Option, damit Backup Exec den Remote-Computer automatisch neu starten kann, wenn dies erforderlich ist.

- 11** Prüfen Sie die Übersicht und klicken Sie dann auf "Installieren".

Anzeigen von Details zu Hyper-V-Ressourcen

Auf der Registerkarte "Backup und Wiederherstellung" finden Sie ein Teilfenster "Details" im unteren Teil des Bildschirms. Das Teilfenster "Details" gibt zusätzliche Details für ausgewählte Servertypen aus der Serverliste im oberen Teil des Bildschirms an. Zusätzliche Details und Funktionalität erscheinen, wenn ein Hyper-V-Host ausgewählt wird. Das Teilfenster "Details" für Hyper-V-Ressourcen enthält Details über die Backup-Aufträge der letzten 7 Tage, das Datum des letzten Backups und das Datum des nächsten geplanten Backups. Außerdem können Sie Daten sichern und wiederherstellen sowie die Liste virtueller Gastcomputer filtern.

Das Teilfenster "Details" für Hyper-V virtuelle Computer schließt die Ressourcen, die möglicherweise nicht in der Serverliste erscheinen, ein, z.B.:

- Virtuelle Computer, auf denen der Agent for Windows nicht installiert ist.
- Virtuelle Computer ohne Windows (z. B. Linux).
- Virtuelle Computer, auf denen GRT-Backups nicht aktiviert sind.

Das Teilfenster "Details" für Hyper-V virtuelle Computer stellt eine Kombination von aktuellen Informationen und von historischen Informationen bereit. Wenn Sie auf die Schaltfläche "Aktualisieren" klicken, kann Backup Exec alle Serverressourcen erkennen. Wurde jedoch ein virtueller Computer verschoben, gelöscht, oder wurden seine Identifikationsdaten geändert, tritt Folgendes auf:

- Wenn der virtuelle Computer nie gesichert wurde, löscht Backup Exec ihn aus dem Teilfenster "Details".
- Wenn der virtuelle Computer gesichert wurde, löscht Backup Exec ihn nicht aus dem Teilfenster "Details".

Wenn ein virtueller Computer umbenannt wurde, tritt im Teilfenster "Details" Folgendes auf:

- Wenn der virtuelle Computer gesichert wurde, schließt das Teilfenster "Details" einen Eintrag für den neuen Namen ein und behält den Eintrag für den alten Namen.
- Wenn der virtuelle Computer nie gesichert wurde, schließt das Teilfenster "Details" nur den neuen Namen des virtuellen Computers ein.

Anzeigen der Details zu Hyper-V-Ressourcen

- ◆ Wählen Sie auf der Registerkarte "Backup und Wiederherstellung" einen Hyper-V-Host aus der Serverliste aus.

Die Ressourcen für den ausgewählten Host werden im Teilfenster "Details" angezeigt.

Installieren von Agent for Windows auf virtuellen Hyper-V-Computern

Um Granular Recovery Technology (GRT) in Backup Exec für Microsoft-Anwendungsdaten zu verwenden, installieren Sie Agent for Windows auf allen virtuellen Computern, auf denen Windows ausgeführt wird.

So installieren Sie Agent for Windows auf virtuellen Hyper-V-Computern

- 1** Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" unter "Server und virtuelle Hosts" auf "Hinzufügen".
- 2** Wählen Sie "Microsoft Hyper-V-Host", und klicken Sie dann auf "Weiter".
- 3** Aktivieren Sie die Option "Zulassen, dass Backup Exec ein Vertrauensverhältnis mit den Servern herstellt", und klicken Sie dann auf "Weiter".
- 4** Wählen Sie die Option "Backup Exec Agent for Windows auf den virtuellen Computern eines Microsoft Hyper-V-Host installieren".
- 5** Wählen Sie in der Dropdown-Liste den Hostserver aus, und klicken Sie dann auf "Weiter".
- 6** Wählen Sie die virtuellen Computer aus, auf denen Agent for Windows installiert werden soll, und klicken Sie dann auf "Weiter".
- 7** Wählen Sie das Login-Konto für die virtuellen Computer aus, und klicken Sie dann auf "Weiter".

- 8 Wählen Sie eine der folgenden Optionen, und klicken Sie anschließend auf "Weiter".

Backup Exec Agent for Windows automatisch auf die aktuelle Version aktualisieren

Ist diese Option aktiviert, kann Backup Exec die neueste Version von Agent for Windows installieren, wenn bereits eine ältere Version auf den ausgewählten virtuellen Computern installiert ist.

Remote-Computer automatisch neu starten, nachdem der Backup Exec Agent for Windows installiert wurde und wenn ein Neustart erforderlich ist

Aktivieren Sie diese Option, damit Backup Exec den Remote-Computer automatisch neu starten kann, wenn dies erforderlich ist.

- 9 Prüfen Sie die Übersicht und klicken Sie dann auf "Installieren".

Push-Installation von Agent for Windows auf virtuellen Hyper-V-Computern

Sie können den Assistenten Server hinzufügen verwenden, um eine Push-Installation des Agent for Windows auf ausgewählten virtuellen Hyper-V-Computern durchzuführen. Sie können wählen, ob der Agent for Windows auf allen benötigten virtuellen Gastcomputern, die ihn benötigen, oder nur auf bestimmten Computern installiert wird. Beispiel: Wenn Sie wissen, dass einige der virtuellen Gastcomputer temporäre Computer sind und nicht gesichert werden müssen, können Sie jene aus der Installation ausschließen.

So führen Sie eine Push-Installation von Agent for Windows auf virtuellen Hyper-V-Computern aus

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" mit der rechten Maustaste auf den virtuellen Host und wählen Sie "Agent for Windows auf virtuellen Gastcomputern installieren".
- 2 Aktivieren Sie die Option "Zulassen, dass Backup Exec ein Vertrauensverhältnis mit den Servern herstellt" und klicken Sie dann auf "Weiter".
- 3 Wählen Sie die Option "Backup Exec Agent for Windows auf den virtuellen Gastcomputern eines Microsoft Hyper-V-Servers installieren".
- 4 Wählen Sie im Feld "Microsoft Hyper-V-Server" den Hyper-V-Server aus, auf dem sich der virtuelle Computer befindet.
- 5 Klicken Sie auf "Weiter".

- 6 Wählen Sie die virtuellen Gastcomputer aus, auf denen Sie den Agent for Windows installieren möchten, und klicken Sie dann auf "Weiter".
- 7 Prüfen Sie, ob die ausgewählten virtuellen Computer online sind, wählen Sie das entsprechende Login-Konto für diese virtuellen Computer aus und klicken dann auf "Weiter".
- 8 Überprüfen Sie die Informationen o, Fenster "Übersicht" und klicken Sie dann auf "Installieren".

Sichern von virtuellen Computern mit Microsoft Hyper-V

Die folgenden Backup-Optionen sind für Microsoft Hyper-V verfügbar:

Tabelle D-2 Backup-Optionen für Microsoft Hyper-V

Containername	Ordner im Container	Was im Backup-Auftrag enthalten ist
Microsoft Hyper-V	Dieser Ordner enthält "Erster Speicher" und "Virtuelle Computer".	Wenn Sie den Container "Microsoft Hyper-V" für das Backup auswählen, enthält der Backup-Auftrag die Konfigurationseinstellungen für die Anwendung und alle virtuellen Computer.
Erster Speicher Hinweis: Dieser Container wird für Hyper-V 2012 und höher nicht angezeigt.	Dieser Ordner enthält die Sicherungskonfigurationen Sicherungskonfigurationen	Wenn Sie "Erster Speicher" zum Sichern auswählen, enthält der Backup-Auftrag eine einzelne XML-Datei, die die Hyper-V-Autorisierungskonfiguration enthält.
Hostkomponente Hinweis: Dieser Container wird nur für Hyper-V 2012 und höher angezeigt.	Dieser Ordner enthält die Sicherungskonfigurationen Sicherungskonfigurationen	Wenn Sie "Hostkomponente" zum Sichern auswählen, enthält der Backup-Auftrag mehrere Dateien, die die Hyper-V-Autorisierungskonfiguration enthalten.

Containername	Ordner im Container	Was im Backup-Auftrag enthalten ist
Virtuelle Computer	<p>Dieser Ordner enthält die virtuellen Computer, die sich auf dem virtuellen Server befinden.</p> <p>Hinweis: Es werden die übergeordneten Festplatten für die virtuellen Hyper-V-Computer angezeigt. Wenn sie eine übergeordnete Festplatte auswählen, sichert Backup Exec die ausgewählten übergeordneten und die dazugehörigen untergeordneten Datenträger des virtuellen Computers.</p>	

Containername	Ordner im Container	Was im Backup-Auftrag enthalten ist
		<p>Für einen einzelnen virtuellen Computer umfasst das Backup, basierend auf den ausgewählten Datenträgern oder der Auswahl des gesamten virtuellen Computers, die folgenden Elemente:</p> <ul style="list-style-type: none"> ■ VHD-Dateien für die ausgewählten Datenträger ■ AVHD-Dateien für die ausgewählten Datenträger ■ Speicher-Snapshot-Dateien ■ VSV-Dateien (in Hyper-V 2016 nicht enthalten) ■ BIN-Dateien (in Hyper-V 2016 nicht enthalten) ■ VHDX-Dateien (Hyper-V 2012 und höher) für die ausgewählten Datenträger ■ Avhdx-Dateien (Hyper-V 2012 und höher) für die ausgewählten Datenträger ■ VCMX-Dateien (Hyper-V 2016) ■ Die *XML-Konfigurationsdateien des virtuellen Computers ■ Hyper-V-verwaltete Snapshots <p>Hinweis: Wenn Sie versuchen, einen virtueller Computer mit dem NetBIOS-Namen "LocalHost" zu sichern, wird die Fehlermeldung "e000976f - Der virtuelle Computer kann nicht auf dem Deduplizierungsgerät gesichert werden, das sich auf demselben virtuellen Computer befindet." ausgegeben.</p> <p>Hinweis: Virtuelle Computer, auf denen sich Remote-VHD-Dateien befinden, werden vom Backup-Auftrag ausgeschlossen. Sie können Agent for Windows und den entsprechenden Backup Exec Agent verwenden, um virtuelle Computer zu schützen, auf denen sich Remote-VHD-Dateien</p>

Containername	Ordner im Container	Was im Backup-Auftrag enthalten ist
		<p>befinden.</p> <p>Warnung: Für virtuelle Computer mit Pass-Through-Datenträgern schlagen Backup-Aufträge fehl. Sie können Agent for Windows und den entsprechenden Backup Exec Agent auf virtuellen Computern mit Pass-Through-Datenträgern installieren und sie schützen, als ob sie physische Computer wären.</p> <p>Hinweis: Wenn Sie einen virtuellen Computer sichern, auf dem eine beliebige unterstützte Version von Microsoft SharePoint ausgeführt wird, kann die Verarbeitung über 30 Minuten dauern.</p>

Hinweis: Wenn Sie eine Exchange-Datenbankverfügbarkeitsgruppe (DAG) auf einem virtuellen Computer sichern möchten, verwenden Sie den Backup Exec Agent for Exchange. Der Agent for Hyper-V unterstützt Backup von Exchange-DAGs nicht.

So sichern Sie virtuelle Hyper-V-Computer

- 1 Auf der Registerkarte "Backup und Wiederherstellung" wählen Sie einen virtuellen Computer oder einen Hyper-V-Host aus der Serverliste.
- 2 Sie haben folgende Möglichkeiten:

Wenn Sie in Schritt 1 einen Hyper-V-Host ausgewählt haben:

Klicken Sie oben auf der Seite in der Gruppe "Backups" auf "Backup" und wählen Sie dann die gewünschten Backup-Methode aus.

Sie können auch unten auf der Seite im Teilfenster "Details" die zu sichernden Ressourcen auswählen und dann auf "Backup" klicken. Wählen Sie die gewünschte Backup-Methode aus.

Wenn Sie in Schritt 1 einen virtuellen Computer ausgewählt haben

Gehen Sie wie folgt vor:

- Klicken Sie oben auf der Seite in der Gruppe "Backups" auf "Backup" und wählen Sie dann die gewünschten Backup-Methode aus.
- Wählen Sie im Dialogfeld "Virtuellen Computer sichern" die gewünschte Backup-Methode für diesen virtuellen Computer ("Virtuelle Backups" oder "Backups mit Agent") und klicken Sie auf "Weiter".

Siehe ["Empfehlungen dazu, wann virtuelle Backups und wann Backups mit Agent genutzt werden sollten."](#) auf Seite 1098.

- Wenn Sie "Virtuelle Backups" ausgewählt haben, wählen Sie den Host des virtuellen Computers aus und klicken Sie dann auf "Weiter".

Befindet sich der Host des virtuellen Computers nicht in der Liste der Server, klicken Sie auf "Hinzufügen" und schließen Sie den Assistenten ab, um den Host hinzuzufügen.

- 3** Klicken Sie im Dialogfeld "Eigenschaften der Backup-Definition" im Feld "Auswahl" auf "Bearbeiten", um Ressourcen der Backup-Auswahlliste hinzuzufügen oder daraus zu entfernen.
- 4** Aktivieren Sie im Dialogfeld "Backup-Auswahl" die Kontrollkästchen für die zu sichernden Ressourcen, und heben Sie die Markierung der Kontrollkästchen für die Quellen auf, nach denen nicht gefiltert werden soll.
- 5** Wählen Sie die Datenträger für den virtuellen Computer aus, der gesichert werden soll.

Sie können den gesamten virtuellen Computer (alle Festplatten) oder nur bestimmte Festplatten auswählen. Sie können Festplatten auch selektiv ausschließen.

6 Klicken Sie auf "OK".

Wenn Sie nur bestimmte Datenträger auswählen, wird das Popup "Teilweise ausgewählte Datenträger auf den virtuellen Computern" angezeigt.

Die Auftragsauswahl besteht aus einem oder mehreren virtuellen Computern, wobei nur einige der virtuellen Datenträger ausgewählt werden. Damit ein virtueller Computer auf Betriebssystem- und auf Anwendungsebene funktioniert, vergewissern Sie sich, dass alle erforderlichen Datenträger ausgewählt wurden.

Zum Durchführen der GRT Wiederherstellung für Ordner und Dateien sowie für Anwendungen, müssen Sie sicherstellen, dass das Systemlaufwerk ausgewählt wurde. Wählen Sie für GRT auf Anwendungsebene alle virtuellen Datenträger mit Anwendungsdaten aus.

7 Klicken Sie auf "OK".

8 Klicken Sie im Dialogfeld "Backup-Eigenschaften" im Feld "Backup" auf "Bearbeiten".

9 Wählen Sie im Dialogfeld "Backup-Optionen" im linken Teilfenster "Planen" und wählen Sie anschließend den Zeitplan für diesen Auftrag aus.

10 Wählen Sie im Dialogfeld "Backup-Optionen" im linken Teilfenster "Virtuelle Computer".

11 Legen Sie eine der folgenden Optionen für diesen Auftrag fest.

Vollständige Backup-Methode für virtuelle Computer verwenden, die inkrementelle oder Differenzial-Backups nicht unterstützen	Durch Auswählen dieser Option wird festgelegt, dass Backup Exec einen vollständigen Backup-Auftrag ausführen kann, wenn kein inkrementelles oder differenzielles Backup des virtuellen Computers durchgeführt werden kann. Backup Exec kann aus verschiedenen Gründen nicht in der Lage sein, ein inkrementelles Backup oder differenzielles Backup durchzuführen. Dies ist z. B. der Fall, wenn die Snapshotkonfiguration oder die Konfiguration des Hostservers geändert wird. Ist diese Option nicht ausgewählt und kann kein inkrementelles bzw. differenzielles Backup ausgeführt werden, schlägt der Auftrag fehl.
Ausgeschaltete virtuelle Computer sichern	Wenn Sie diese Option aktivieren, kann Backup Exec virtuelle Computer sichern, auch wenn diese ausgeschaltet sind.
Sofortwiederherstellung für alle virtuellen Computer aktivieren, auch für solche, die GRT nicht nutzen können.	Aktivieren Sie diese Option, um die Sofortwiederherstellung aller virtuellen Computer zu aktivieren, auch für solche, die Granular Restore Technology nicht nutzen können.
Backup Exec Granular Recovery Technology (GRT) verwenden, um die Wiederherstellung einzelner Dateien und Ordner von virtuellen Computern zu aktivieren	Durch Auswählen dieser Option können einzelne Dateien und Ordner aus einem vollständigen Backup wiederhergestellt werden. Sie müssen Agent for Windows auf dem virtuellen Computer installieren, auf dem Sie Daten wiederherstellen möchten. Agent for Windows muss nicht auf dem virtuellen Computer installiert werden, um die Daten zu sichern.

GRT für Microsoft-Active Directory-Objekte auf virtuellen Computern aktivieren	Durch Auswählen dieser Option kann Backup Exec die Informationen sammeln, die erforderlich sind, um einzelne Active Directory-Objekte auf dem virtuellen Computer wiederherzustellen. Backup Exec nutzt die Identifikationsdaten, die für den virtuellen Computer verwendet wurden, auf dem Active Directory installiert ist.
GRT für Microsoft Exchange-Datenbanken und Postfachelemente auf virtuellen Computern aktivieren	Durch Auswählen dieser Option kann Backup Exec Informationen sammeln, die erforderlich sind, um einzelne Exchange-Datenbanken und Postfachelemente auf dem virtuellen Computer wiederherzustellen. Backup Exec verwendet die Identifikationsdaten, die für den virtuellen Computer verwendet wurden, auf dem Exchange installiert ist.
GRT für Microsoft SQL (nur Datenbankstufe) auf virtuellen Computern aktivieren	Durch Auswählen dieser Option kann Backup Exec die Informationen sammeln, die erforderlich sind, um einzelne SQL-Datenbankelemente auf dem virtuellen Computer wiederherzustellen. Backup Exec verwendet die Identifikationsdaten, die für den virtuellen Computer verwendet wurden, auf dem SQL installiert ist.
Nach dem Sichern eines virtuellen Computers SQL Log-Backup ausführen	Aktivieren Sie diese Option, damit Backup Exec das SQL-Protokoll sichern kann. Diese Option gilt für SQL-Datenbanken, die Dateien in einem Protokoll anstatt in der Datenbankdatei aktualisieren. Nachdem das SQL-Protokoll gesichert wurde, werden die Daten aus den Protokolldateien in der Datenbank abgelegt und die Protokolldateien werden geleert. Wenn Sie diese Option nicht aktivieren, wächst die Protokolldatei weiterhin, bis sie voll ist oder manuell gesichert wird.

GRT für Microsoft SharePoint auf virtuellen Computern aktivieren	Wenn Sie diese Option aktivieren, kann Backup Exec die für die Wiederherstellung von SharePoint-Daten auf dem virtuellen Computer erforderlichen Informationen erfassen. Backup Exec verwendet die Identifikationsdaten, die für den virtuellen Computer verwendet wurden, auf dem SharePoint installiert ist.
Virtuelle Computer ausschließen, die zum Backup in einem gespeicherten Status angehalten werden müssen	Durch Auswählen dieser Option werden alle im Offline-Modus befindlichen virtuellen Computer ausgeschlossen, die keine Online-Backups unterstützen und die zu Beginn des Backups ausgeführt werden.
Backup-Methode	Durch Auswählen dieser Option können Sie die Backup-Methode für die aufgeführten Backup-Aufträge ändern. Sie können die Namen der Backup-Aufträge ändern.

- 12** Klicken Sie im Dialogfeld "Backup-Optionen" auf eine der für diesen Auftrag festzulegenden optionalen Einstellungen.
- 13** Klicken Sie auf "OK".
- 14** Klicken Sie im Dialogfeld "Eigenschaften der Backup-Definition" auf "OK".

Wenn Sie die Methode "Virtuelle Backups" ausgewählt haben, wird der Backup-Auftrag in der Auftragsliste unter dem Namen des virtuellen Host oder der IP-Adresse angezeigt.

Festlegen der Standard- Backup-Optionen für Hyper-V

Sie können die bei der Installation von Backup Exec für alle Hyper-V-Backup-Aufträge festgelegten Standardeinstellungen verwenden oder eigene Standardeinstellungen wählen. Sie können die Standardeinstellungen übergehen, wenn Sie einzelne Aufträge erstellen.

So legen Sie die Standard- Backup-Optionen für Hyper-V fest

- 1** Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- 2** Wählen Sie "Auftragsstandardeinstellungen" und dann eine Backup-Option.
Beispiel: Wenn Sie die Standardoptionen für Backup-to-Disk von virtuellen Computer einrichten möchten, wählen Sie "Backup-to-Disk". Die Optionen, die angezeigt werden, hängen von den konfigurierten Speichergeräten ab. Verschiedene Standardoptionen können für Backup-Aufträge auf verschiedenen Speichertypen konfiguriert werden.
- 3** Im linken Teilfenster klicken Sie auf "Virtuelle Computer".

4 Wählen Sie die Standardoptionen aus, die Sie verwenden möchten.

Vollständige Backup-Methode für virtuelle Computer verwenden, die inkrementelle oder Differenzial-Backups nicht unterstützen	Durch Auswählen dieser Option wird festgelegt, dass Backup Exec einen vollständigen Backup-Auftrag ausführen kann, wenn kein inkrementelles oder differenzielles Backup des virtuellen Computers durchgeführt werden kann. Backup Exec kann aus verschiedenen Gründen nicht in der Lage sein, ein inkrementelles Backup oder differenzielles Backup durchzuführen. Dies ist z. B. der Fall, wenn die Snapshotkonfiguration oder die Konfiguration des Hostservers geändert wird. Ist diese Option nicht ausgewählt und kann kein inkrementelles bzw. differenzielles Backup ausgeführt werden, schlägt der Auftrag fehl.
Ausgeschaltete virtuelle Computer sichern	Wenn Sie diese Option aktivieren, kann Backup Exec virtuelle Computer sichern, auch wenn diese ausgeschaltet sind.
Sofortwiederherstellung für alle virtuellen Computer aktivieren, auch für solche, die GRT nicht nutzen können.	Aktivieren Sie diese Option, um die Sofortwiederherstellung aller virtuellen Computer zu aktivieren, auch für solche, die Granular Restore Technology nicht nutzen können.
Backup Exec Granular Recovery Technology (GRT) verwenden, um die Wiederherstellung einzelner Dateien und Ordner von virtuellen Computern zu aktivieren	Durch Auswählen dieser Option können einzelne Dateien und Ordner aus einem vollständigen Backup wiederhergestellt werden. Sie müssen Agent for Windows auf dem virtuellen Computer installieren, auf dem Sie Daten wiederherstellen möchten. Agent for Windows muss nicht auf dem virtuellen Computer installiert werden, um die Daten zu sichern.

GRT für Microsoft-Active Directory-Objekte auf virtuellen Computern aktivieren	Durch Auswählen dieser Option kann Backup Exec die Informationen erfassen, die erforderlich sind, um einzelne Active Directory-Objekte auf dem virtuellen Computer wiederherzustellen. Backup Exec nutzt die Identifikationsdaten, die für den virtuellen Computer verwendet wurden, auf dem Active Directory installiert ist.
GRT für Microsoft Exchange-Datenbanken und Postfachelemente auf virtuellen Computern aktivieren	Durch Auswählen dieser Option kann Backup Exec Informationen erfassen, die erforderlich sind, um einzelne Exchange-Datenbanken und Postfachelemente auf dem virtuellen Computer wiederherzustellen. Backup Exec verwendet die Identifikationsdaten, die für den virtuellen Computer verwendet wurden, auf dem Exchange installiert ist.
GRT für Microsoft SQL (nur Datenbankstufe) auf virtuellen Computern aktivieren	Durch Auswählen dieser Option kann Backup Exec die Informationen sammeln, die erforderlich sind, um einzelne SQL-Datenbankelemente auf dem virtuellen Computer wiederherzustellen. Backup Exec verwendet die Identifikationsdaten, die für den virtuellen Computer verwendet wurden, auf dem SQL installiert ist.
Nach dem Sichern eines virtuellen Computers SQL Log-Backup ausführen	Ermöglicht, dass Backup Exec das SQL-Protokoll sichert. Diese Option gilt für SQL-Datenbanken, die Dateien in einem Protokoll anstatt in der Datenbankdatei aktualisieren. Nachdem das SQL-Protokoll gesichert wurde, werden die Daten aus den Protokolldateien in der Datenbank abgelegt und die Protokolldateien werden geleert. Wenn Sie diese Option nicht aktivieren, wächst die Protokolldatei weiterhin, bis sie voll ist oder manuell gesichert wird.

GRT für Microsoft SharePoint auf virtuellen Computern aktivieren	Durch Auswählen dieser Option kann Backup Exec die für die Wiederherstellung von SharePoint-Daten auf dem virtuellen Computer erforderlichen Informationen erfassen. Backup Exec verwendet die Identifikationsdaten, die für den virtuellen Computer verwendet wurden, auf dem SharePoint installiert ist.
Virtuelle Computer ausschließen, die zum Backup in einem gespeicherten Status angehalten werden müssen	Schließt alle im Offline-Modus befindlichen virtuellen Computer aus, die keine Online-Backups unterstützen und die zu Beginn des Backups ausgeführt werden.
Backup-Methode	Hier können Sie die Backup-Methode für die aufgeführten Backup-Aufträge ändern. Sie können die Namen der Backup-Aufträge ändern.

5 Klicken Sie auf "OK".

So schützt Backup Exec automatisch neue virtuelle Computer während eines Backup-Auftrags

Die dynamische Einbeziehungsfunktion von Backup Exec schützt neue virtuelle Computer und Ordner, die gefunden werden, wenn ein Backup-Auftrag läuft. Wenn neue virtuelle Computer zwischen dem Zeitpunkt, zu dem der Backup-Auftrag erstellt wird, und dem Zeitpunkt, zu dem der Backup-Auftrag läuft, hinzugefügt werden, sichert Backup Exec automatisch die neuen virtuellen Computer. Da der Backup-Auftrag neue virtuelle Computer umfassen kann, kann das Ausführen des Auftrags mehr Speicherplatz und Zeit erfordern als erwartet. Der Auftragsverlauf zeigt die Anzahl virtueller Computer an, die gesichert wurden.

In der Backup-Auswahlliste wird die dynamische Einbeziehung für die folgenden Hyper-V-Knoten aktiviert:

- Microsoft Hyper-V
- Virtuelle Computer unter Microsoft Hyper-V
- Der Hyper-V-Host-Knoten
Wenn Sie den Host-Knoten auswählen, wird die dynamische Einbeziehung automatisch für den Microsoft Hyper-V-Knoten aktiviert.
- Virtuelle Computer von Microsoft Hyper-V HA
- Der Cluster-Namensknoten

Wenn Sie den Cluster-Namensknoten auswählen, wird die dynamische Einbeziehung automatisch für den Knoten der virtuellen Computer von Microsoft Hyper-V HA aktiviert.

Siehe ["Sichern von virtuellen Computern mit Microsoft Hyper-V"](#) auf Seite 1167.

Verwenden von Granular Recovery Technology (GRT) mit Agent for Hyper-V

Backup Exec Granular Recovery Technology (GRT) ermöglicht die Wiederherstellung einzelner Dateien und Ordner, ohne dass Sie den gesamten virtuellen Computer wiederherstellen müssen. Darüber hinaus können Sie einzelne Elemente aus den folgenden VSS-fähigen Anwendungen wiederherstellen, die auf virtuellen Computern installiert sind.

Backup Exec führt ein Backup in einem Durchgang durch, um die Hostkonfigurationsdaten, alle virtuellen Computer und VSS-fähigen Anwendungen, die auf den virtuellen Computern installiert sind, zu schützen. Die selektive Wiederherstellungstechnologie von Backup Exec (Granular Recovery Technology, GRT) auf Datei-/Ordnebene wird standardmäßig für Backup-Aufträge aktiviert. Sie können ein GRT-fähiges Backup verwenden, um einzelne Dateien und Ordner von einem virtuellen Windows-Computer wiederherzustellen, ohne den gesamten virtuellen Computer wiederherzustellen. Darüber hinaus können Sie einzelne Elemente von Microsoft Exchange-, SharePoint- und Active Directory-Anwendungen wiederherstellen, die sich auf virtuellen Computern befinden. Sie können einzelne Datenbanken von Microsoft SQL auch wiederherstellen, wenn es sich auf virtuellen Computern befindet.

Hinweis: Sie benötigen den passenden Backup Exec Agent for Microsoft Exchange, SQL, SharePoint oder Active Directory auf dem virtuellen Computer, um GRT durchzuführen.

Tabelle D-3 Datentypen, die Backup Exec für VSS-fähige Anwendungen auf virtuellen Computern schützt

Anwendung	Datentypen, die von Backup Exec geschützt werden
Microsoft Exchange	Postfächer, einzelne Meldungen, Kalenderelemente, Aufgaben, Journaleinträge und öffentliche Ordnerdaten (nur Datenträger-Backups)
Microsoft SQL	Datenbanken

Anwendung	Datentypen, die von Backup Exec geschützt werden
Microsoft Active Directory	Einzelne Benutzerkonten, Druckerobjekte, Sites und Organisationseinheiten
Microsoft SharePoint	SharePoint-Datenbanken

Hinweis: GRT wurde nicht für die Systemwiederherstellung entwickelt. Sie können jedoch eine vollständige Systemwiederherstellung durchführen, indem Sie den gesamten virtuellen Computer als Wiederherstellungsauswahl in einem Wiederherstellungsauftrag auswählen.

Wenn Sie einen Backup-Auftrag erstellen, sucht Backup Exec automatisch VSS-fähige Anwendungen auf virtuellen Computern. Während des Backup-Auftrags sichert Backup Exec die Daten der VSS-fähigen Anwendungen mithilfe von GRT. Backup Exec aktiviert standardmäßig GRT unter Verwendung derselben Identifikationsdaten, die verwendet wurden, um eine Verbindung zum virtuellen Computer herzustellen. Sie können GRT für beliebige VSS-fähige Anwendungstypen deaktivieren.

Um GRT zu verwenden, wählen Sie die wiederherzustellenden Dateien und Ordner aus der Liste aus, die nach dem Erweitern des NetBIOS-Namens oder Computernamens des virtuellen Computers angezeigt wird. Sie können keine einzelnen Ordner und Dateien von den virtuellen Computern auswählen, die beim Erweitern des Knotens "Virtuelle Computer" eingeblendet werden.

Hinweis: Backup Exec unterstützt die selektive Wiederherstellung einzelner Exchange- und SQL-Elemente nur in nicht geclusterten und nicht verteilten Konfigurationen.

Während des Backup-Auftrags erfasst Backup Exec Metadaten für die Anwendungen. Wenn Backup Exec nicht in der Lage ist, Metadaten zu sammeln, können Sie einzelne Elemente für die Anwendungen nicht wiederherstellen. Jedoch kann der Backup-Auftrag andernfalls erfolgreich beendet werden.

Backup Exec kann keine Metadaten in den folgenden Situationen erfassen:

- GRT ist für eine Anwendung deaktiviert.
- Backup Exec kann keine Verbindung mit dem virtuellen Computer herstellen.
- Für den virtuellen Computer wurden falsche Identifikationsdaten eingegeben.

Hinweis: Backup Exec verwendet den Microsoft Hyper-V Writer während der Backups der VSS-fähigen Anwendungen auf virtuellen Computern. Der Microsoft Hyper-V Writer schneidet Anwendungsprotokolle ab, bevor Daten auf das Speichergerät verschoben werden. Deshalb werden die Anwendungsprotokolle für die Anwendungen auf den virtuellen Computern abgeschnitten, wenn Sie Microsoft Hyper-V verwenden.

Anforderungen für die Verwendung von GRT zum Sichern von Microsoft-Anwendungsdaten auf virtuellen Computern

Die folgenden Elemente sind erforderlich, um Daten für Microsoft Exchange, SQL, Active Directory und SharePoint auf virtuellen Computern zu schützen:

- Der virtuelle Computer muss eingeschaltet sein.
- Sie müssen die passenden Identifikationsdaten für den virtuellen Computer eingeben. Stellen Sie sicher, dass die Identifikationsdaten für den virtuellen Computer Zugriff auf die VSS-fähigen Anwendungen ermöglichen.
- Der Backup Exec-Server muss in der Lage sein, eine Verbindung zum virtuellen Computer unter Verwendung des Netzwerknamens oder der IP-Adresse herzustellen.
- Backup Exec Agent for Windows muss auf dem virtuellen Computer installiert sein.
- Die richtige Anzahl Lizenzen muss für die Anwendungen, die Sie auf den virtuellen Computern schützen möchten, eingegeben werden.
- Das Betriebssystem auf dem virtuellen Computer muss VSS unterstützen.
- Die virtuelle Maschine kann keine dynamischen Datenträger, wie segmentierte, gespiegelte, gestreifte oder RAID 5 verwenden.

Nicht unterstützte Konfigurationen für GRT

Tabelle D-4 Nicht unterstützte Konfigurationen für GRT

Nicht unterstützte Elemente	Details
Wiederherstellungen aus vollständigen und inkrementellen Backups aus unterschiedlichen Speichergeräten	Backup Exec unterstützt Wiederherstellungen aus gemischten Medien nicht, wenn GRT im Backup-Auftrag aktiviert war. Beispiel: Wenn das vollständige Backup auf Band vorliegt und das inkrementelle Backup auf einem Plattenspeichergerät, schlägt der Wiederherstellungsauftrag fehl. Wiederherstellungen aus gemischten Medien werden unterstützt, wenn GRT nicht aktiviert ist.
Virtuelle Computer mit dynamischen Datenträgern (MBR- oder GPT-Partitionen)	Backup Exec unterstützt die granulare Wiederherstellung von Dateien, Ordnern und Anwendungen auf virtuellen Computern mit dynamischen Datenträgern (mit GPT- oder MBR-Partitionen) nicht.
Virtuelle Computer mit ReFS- und deduplizierten Datenträgern	Backup Exec unterstützt GRT auf Datei-/Ordner Ebene für ReFS- und deduplizierte Datenträger oder GRT auf Anwendungsebene für virtuelle Computer nur dann, wenn der Backup Exec-Server unter derselben oder einer höheren Betriebssystemversion als der virtuelle Computer ausgeführt wird. Für deduplizierte Datenträger muss auf dem Backup Exec-Server das Deduplication Feature installiert sein. Beispiel: Wenn der virtuelle Computer Windows Server 2016 und ReFS- bzw. deduplizierte Datenträger nutzt, muss auf dem Backup Exec-Server ebenfalls Windows Server 2016 oder höher ausgeführt werden. Für deduplizierte Datenträger muss auf dem Backup Exec-Server das Deduplication Feature installiert sein.

Nicht unterstützte Elemente	Details
Mit VHDX formatierte virtuelle Datenträger größer als 2 TB	GRT auf Datei-/Ordner- und Anwendungsebene -GRT für einen virtuellen Computer mit mindestens einer VHDX-Datei, die größer als 2 TB ist, wird nur unterstützt, wenn auf dem Backup Exec-Server Windows Server 2012 oder höher ausgeführt wird.

Sichern und Wiederherstellen virtueller Hyper-V-Computer mit hoher Verfügbarkeit

Wenn virtuelle Computer für Hochverfügbarkeit konfiguriert sind, werden sie in der Backup-Auswahlstruktur unter dem Knoten "Hyper-V-Computer mit hoher Verfügbarkeit" angezeigt. Virtuelle Computer, die nicht für Hochverfügbarkeit konfiguriert sind, verbleiben im Knoten "Microsoft Hyper-V". Wenn Sie eine Backup-Auswahl treffen, sucht Backup Exec nach virtuellen Computern mit hoher Verfügbarkeit. Wenn virtuelle Computer mit hoher Verfügbarkeit erkannt werden, erinnert Backup Exec Sie daran, diese virtuellen Computer für das Backup auszuwählen.

Die Auswahlmöglichkeiten für die Wiederherstellung sind denen für das Backup ähnlich. Sie können einen virtuellen Computer mit hoher Verfügbarkeit auf dieselbe Weise wie alle anderen virtuellen Computer wiederherstellen. Der virtuelle Computer behält seine hohe Verfügbarkeit bei. Wenn Sie jedoch die Wiederherstellung an einen anderen Hyper-V-Host umleiten, ist der virtuelle Computer nicht mehr in hohem Grade verfügbar, wenn der Wiederherstellungsauftrag abgeschlossen ist. Sie müssen den virtuellen Computer erneut konfigurieren, um in hohem Grade verfügbar zu sein.

Siehe ["Sichern von virtuellen Computern mit Microsoft Hyper-V"](#) auf Seite 1167.

Informationen zu Backups von auf SMB-/Scale-out-Dateiservern gehosteten virtuellen Computern

Backup Exec unterstützt Backups virtueller Computer, die auf SMB- und Scale-out-Dateiservern gehostet werden, wenn die virtuellen Computer unter Microsoft Hyper-V-Server 2016 oder höher gehostet werden und über die Konfigurationsversion 8.0 oder höher verfügen. Von Backup Exec wird zum Schutz solcher virtueller Computer die Methode Resilient Change Tracking (RCT) angewandt. Die Berechtigungen für diese virtuellen Computer müssen gemäß der Microsoft-Dokumentation konfiguriert werden

Das im Backup-Auftrag festgelegte Login-Konto muss über Administratorzugriff auf den Hyper-V-Host sowie über uneingeschränkten Zugriff auf den freigegebenen SMB-/Scale-out-Dateiserver verfügen.

Während des Backups oder der Wiederherstellung des virtuellen Computers werden von Backup Exec die Lese- und Schreibvorgänge des Hyper-V-Hosts des virtuellen Computers verarbeitet. Der Datenfluss vom freigegebenen Server verläuft zuerst zum Hyper-V-Host und anschließend zum Backup Exec-Server.

Siehe ["Agent for Microsoft Hyper-V"](#) auf Seite 1154.

So funktioniert die Katalogisierung mit virtuellen Backups über Hyper-V

Wenn Sie Granular Recovery Technology (GRT) für einen Backup-Auftrag eines virtuellen Computers aktivieren, können Sie den Katalogauftrag für GRT als Teil des Backup-Auftrags, als separaten Auftrag sofort nach Abschluss des Backup-Auftrags oder nach einem Zeitplan ausführen. Standardmäßig wird der Katalogvorgang sofort nach Abschluss des Backup-Auftrags ausgeführt.

Hinweis: Die Funktionen "Instant GRT" und "Vollständige Katalogisierung" werden für Backups auf Band nicht unterstützt.

Die Katalogisierung kann zeitaufwändig sein. Sie benötigt Zugriff auf das für das Backup genutzte Speichergerät. Sie sollten die Katalogisierung so planen, dass sie nicht während des Backups ausgeführt wird, damit kein Konflikt mit Backup-Aufträgen auftritt. Ist eine Katalogisierung geplant, wird sie nur für den neuesten Backup-Satz seit der letzten Katalogisierung ausgeführt. In diesem Fall kann nur der letzte Backup-Satz seit der letzten Katalogisierung für Granular Recovery auf virtuellen Hyper-V- und VMWare-Computern verwendet werden. Sie müssen die wiederherzustellenden Daten aus den Backup-Sätzen auswählen, bevor die vollständige Katalogisierung abgeschlossen ist. Der Suchassistent ist dafür nicht verfügbar.

Beispiel: Wenn Sie inkrementelle Backups einrichten, die alle 11 Stunden und der Katalogvorgang um Mitternacht ausgeführt werden, hätten Sie die folgenden Backup-Sätze:

- Vollständig (11:00 Uhr)
- Inkrementell 1 (22:00 Uhr)
- Katalog 1 (Mitternacht). Dieser Auftrag katalogisiert Inkrementell 1.
- Inkrementell 2 (09:00 Uhr)
- Inkrementell 3 (20:00 Uhr)

- Katalog 2 (Mitternacht). Dieser Auftrag katalogisiert Inkrementell 3. Inkrementell 2 ist nicht katalogisiert.
- Inkrementell 4 (07:00 Uhr)
- Inkrementell 5 (18:00 Uhr)
- Katalog 3 (Mitternacht). Dieser Auftrag katalogisiert Inkrementell 5. Inkrementell 4 ist nicht katalogisiert.
- Inkrementell 6 (05:00 Uhr) Dieses Backup ist nicht katalogisiert.

Im Beispiel wird die vollständige Katalogisierung nur für Inkrementell 5, Inkrementell 3 und Inkrementell 1 ausgeführt. Für solche Aufträge können Sie mit dem Suchassistenten die Daten durchsuchen oder nach einzelnen Elementen suchen, die wiederhergestellt werden sollen. Sie können zwar eine granulare Wiederherstellung auch mit Inkrementell 2, Inkrementell 4 und Inkrementell 6 ausführen, aber dies dauert länger, da sie nicht vollständig katalogisiert sind. Backup Exec zeigt die granularen Daten durch Bereitstellen des Backup-Satzes an.

So wird die Byteanzahl für Katalogisierungsvorgänge berechnet

In der "Auftragsüberwachung " und im "Auftragsverlauf" unterscheidet sich die Byteanzahl, die für einen Katalogvorgang angezeigt wird, möglicherweise von der Byteanzahl, die für den entsprechenden Backup-Auftrag angezeigt wird. Die Byteanzahl für einen Katalogauftrag ist möglicherweise höher als die Byteanzahl für einen Backup-Auftrag. Die Methode, mit der Backup Exec die Daten katalogisiert, hat Auswirkungen auf die Byteanzahl, die für den Katalogauftrag angezeigt wird.

- Wenn ein Katalogvorgang für ein vollständiges Backup durchgeführt wird, werden die Daten auf der Basis Datei-für-Datei gelesen und die Byteanzahl wird dementsprechend berechnet. Während des Auftrags des vollständigen Backups werden die Daten im Hinblick auf die Anzahl von Sektoren gelesen und die Byteanzahl wird basierend auf der Anzahl von Sektoren berechnet. Die Byteanzahl für einen Katalogauftrag ist möglicherweise höher als die Byteanzahl für einen Backup-Auftrag.
- Wenn der Katalogvorgang für ein inkrementelles Backup durchgeführt wird, sind alle Dateien auf dem virtuellen Datenträger anstelle der geänderten Dateien katalogisiert. Aus diesem Grund berücksichtigt die Byteanzahl für den Katalogauftrag das vollständige Backup und das inkrementelle Backup.

Siehe ["Konfigurieren der Optionen für Instant GRT und Vollständige Katalogisierung zum Verbessern der Backup-Leistung von GRT-Aufträgen"](#) auf Seite 656.

Wiederherstellen von virtuellen Microsoft Hyper-V-Computern

Sie können den Wiederherstellungsassistenten verwenden, um wie folgt Daten von den virtuellen Computern wiederherzustellen:

- Wiederherstellen eines vollständigen virtuellen Computers
- Wiederherstellen einzelner Dateien oder Ordner, die vom virtuellen Computer aus gesichert wurden (wenn Sie die GRT-Funktionen für den Backup-Auftrag ausgewählt haben).
- Wiederherstellen eines virtuellen Computers auf einem anderen Microsoft Hyper-V-Server.
- Umleiten von Flatfiles vom virtuellen Computer zu einem beliebigen Computer, auf dem Agent for Windows installiert ist.

Hinweise für die Wiederherstellung von Hyper-V virtuellen Computern

- Virtuelle Computer unter Linux müssen auf Ebene der VHD-Dateien vollständig wiederhergestellt werden.
- Die Wiederherstellung eines Microsoft Hyper-V virtuellen Computers, der innerhalb eines Bereitsstellungspunkts erstellt wird, schlägt fehl, wenn der Bereitsstellungspunkt zu der Zeit der Wiederherstellung nicht existiert. Um dieses Problem zu vermeiden, konfigurieren Sie den virtuellen Computer, um Pfade des GUID-Datenträgers ohne Bereitsstellungspunkte zu verwenden.
- Wiederherstellungen von virtuellen Computern mit Durchgangsdatenträgern, Fibre Channel-Adaptern und gemeinsam genutzten VHDX-Dateien schlagen möglicherweise fehl, wenn diese Elemente gelöscht worden sind oder zu der Zeit der Wiederherstellung nicht verfügbar sind. Der Wiederherstellungsauftrag ist erfolgreich, wenn Sie die Durchgangsdatenträger, Fibre Channel-Adapter oder gemeinsam genutzten VHDX-Dateien nicht gelöscht haben.
- Umadressierte Wiederherstellungen von teilweise ausgewählten virtuellen Computern können durchgeführt werden, aber der virtuelle Computer wird nicht registriert. Backup Exec versucht, virtuelle Computer nur dann zu registrieren, wenn sie vollständig wiederhergestellt werden.
- Wenn Sie einen virtuellen Computer wiederherstellen, der Datenträger umfasst, die ausgeschlossen wurden, entfernt Backup Exec die entsprechenden Datenträger von VM und löscht sie auf dem Host. Für solch ein Szenario gibt es die folgenden Möglichkeiten:

- Backup Exec hat den Datenträger erfolgreich von dem virtuellen Computer entfernt.
- Backup Exec hat den Datenträger erfolgreich von dem virtuellen Computer entfernt, es sind beim Löschen des Datenträgers vom Host jedoch Fehler aufgetreten. Sie können die Datenträger manuell vom Host löschen.
- Backup Exec kann den Datenträger nicht vom virtuellen Computer entfernen, da Fehler aufgetreten sind. Sie können die Datenträger manuell vom virtuellen Computer entfernen.

Hinweis: Die folgenden Schritte gelten für virtuelle Computer, die mit einem virtuellen Backup gesichert wurden. Wenn Sie den virtuellen Computer mit Agent gesichert haben, folgen Sie den Anweisungen zum Wiederherstellen eines nicht-virtuellen Backups.

Siehe ["Methoden für das Wiederherstellen von Daten in Backup Exec"](#) auf Seite 258.

So stellen Sie virtuelle Hyper-V-Computer wieder her

- 1 Auf der Registerkarte "Backup und Wiederherstellung" haben Sie folgende Möglichkeiten:

So stellen Sie einzelne Dateien und Ordner aus einem GRT-Backup wieder her Gehen Sie dazu wie folgt vor:

- Wählen Sie Teilfenster "Details" am unteren Bildschirmrand den virtuellen Computer aus.
- Klicken Sie auf "Wiederherstellen" und wählen Sie dann "GRT-Daten wiederherstellen".
- Wählen Sie im Wiederherstellungsassistent "Dateien, Ordner oder Datenträger" aus und klicken Sie auf "Weiter".

So stellen Sie den gesamten virtuellen Computer bzw. virtuellen Datenträger wieder her

Gehen Sie dazu wie folgt vor:

- Wählen Sie Teilfenster "Details" am unteren Bildschirmrand den virtuellen Computer aus.
- Klicken Sie auf "Wiederherstellen" und wählen Sie dann "Virtuellen Computer aus Host wiederherstellen".
- Wählen Sie im "Wiederherstellungsassistent" die Option "Hyper-V-Daten" und klicken Sie auf "Weiter".

- 2 Wählen Sie die Daten aus, die Sie wiederherstellen möchten, und klicken Sie dann auf "Weiter".

Hinweis: Für virtuelle Computer, die eine vom System reservierte Partition haben und mit Granular Recovery Technology gesichert werden, zeigt Backup Exec den virtuellen Computer unter einer Datenträger-GUID anstelle eines Laufwerksbuchstabens an. Um Daten von diesen virtuellen Computern wiederherzustellen, wählen Sie eine der Optionen zum Wiederherstellen in einem anderen Speicherort aus.

3 Wählen Sie den Speicherort, in dem Sie die Daten wiederherstellen möchten, aus und klicken Sie dann auf "Weiter".

Im ursprünglichen Speicherort

Wählen Sie diese Option aus, um den virtuellen Computer im gleichen Speicherort wieder herzustellen, aus dem er gesichert wurde.

In einem anderen Speicherort; Laufwerk und Pfad beibehalten

Wählen Sie diese Option aus, um den virtuellen Computer auf einem anderen Server, unter demselben Pfad wieder herzustellen. Sie müssen den Namen des Servers, auf den Sie die Wiederherstellung umleiten möchten, sowie das Login-Konto für diesen Server eingeben.

Beispiel: Der ursprüngliche virtuelle Computer befand sich unter "\\ServerA\D:\VMs\1.vhd" und soll unter "\\ServerB\D:\VMs\1.vhd" wiederhergestellt werden.

In einem anderen Speicherort; Laufwerk ändern, aber Pfad beibehalten

Wählen Sie diese Option aus, um den virtuellen Computer auf einem anderen Server wiederherzustellen und dabei zwar das Laufwerk, aber nicht den Pfadnamen zu ändern. Sie müssen den Namen des Servers und des Laufwerks eingeben, auf die Sie die Wiederherstellung umleiten möchten. Außerdem müssen Sie das Login-Konto für diesen Server eingeben.

Beispiel: Der ursprüngliche virtuelle Computer befand sich unter "\\ServerA\D:\VMs\1.vhd" und soll unter "\\ServerB\E:\VMs\1.vhd" wiederhergestellt werden.

In einem anderen Speicherort; das Laufwerk und den Pfad ändern, aber das ursprüngliche Laufwerk und den Pfadnamen im neuen Pfad einschließen

Wählen Sie diese Option aus, um den virtuellen Computer auf einem anderen Server wiederherzustellen, das Laufwerk zu ändern und das ursprüngliche Laufwerk und die Pfadnamen im neuen Pfad einzuschließen. Sie müssen den Namen des Servers, das Laufwerk und den Pfad eingeben, an den Sie die Wiederherstellung umleiten möchten. Außerdem müssen Sie das Login-Konto für diesen Server eingeben.

Beispiel: Die ursprünglichen virtuellen Computer befanden sich unter "\\ServerA\D:VMs\1.vhd" und "\\ServerA\E:VMs\2.vhd" und sollen unter "\\ServerB\Z:\ReplicatedVMs\D\VMs\1.vhd" und "\\ServerB\Z:\ReplicatedVMs\E\VMs\2.vhd" wiederhergestellt werden.

4 Wählen Sie die für diesen Wiederherstellungsauftrag gewünschten Optionen aus und klicken Sie dann auf "Weiter".

Eingeschaltete virtuelle Computer überschreiben

Wählen Sie diese Option aus, um eingeschaltete virtuelle Computer zu überschreiben und wiederherzustellen. Standardmäßig müssen virtuelle Computer vor der Wiederherstellung ausgeschaltet werden und der virtuelle Computer wird überschrieben. Wenn ein virtueller Computer während eines Wiederherstellungsauftrags aktiv ist, aber diese Option nicht aktiviert ist, schlägt der Auftrag fehl. Sie müssen den virtuellen Computer manuell ausschalten, bevor Sie den Wiederherstellungsauftrag erneut ausführen.

Eingeschaltete virtuelle Computer nicht überschreiben

Wählen Sie diese Option aus, um zu verhindern, dass eingeschaltete virtuelle Computer überschrieben und wiederhergestellt werden. Standardmäßig werden virtuelle Computer vor der Wiederherstellung ausgeschaltet und der virtuelle Computer wird überschrieben. Wenn ein virtueller Computer während eines Wiederherstellungsauftrags aktiv ist und diese Option aktiviert ist, schlägt der Auftrag fehl. Sie müssen den virtuellen Computer manuell ausschalten, bevor Sie den Wiederherstellungsauftrag erneut ausführen.

Virtuellen Computer nach dem Wiederherstellen einschalten und ab dem verfügbaren gespeicherten Zustand fortsetzen

Wählen Sie diese Option aus, um den virtuellen Computer automatisch einzuschalten, nachdem der Wiederherstellungsauftrag abgeschlossen ist. Der virtuelle Computer nimmt die Vorgänge ab dem gespeicherten Zustand seit dem Backup wieder auf.

Hinweis: Diese Option trifft nur auf virtuelle Computer zu, die unter Verwendung eines gespeicherten Zustandes gesichert werden. Virtuelle Computer, die online gesichert werden, haben keinen gespeicherten Zustand.

Virtuellen Computer nach dem Wiederherstellen einschalten und verfügbaren gespeicherten Zustand verwerfen

Wählen Sie diese Option aus, um den virtuellen Computer automatisch einzuschalten, nachdem der Wiederherstellungsauftrag abgeschlossen ist. Der virtuelle Computer verwirft den verfügbaren gespeicherten Status.

Hinweis: Diese Option trifft nur auf virtuelle Computer zu, die unter Verwendung eines gespeicherten Zustandes gesichert werden. Virtuelle Computer, die online gesichert werden, haben keinen gespeicherten Zustand.

- 5 Geben Sie einen Namen für diesen Wiederherstellungsauftrag ein, wählen Sie den Zeitplan für den Auftrag aus und klicken Sie dann auf "Weiter".
- 6 Überprüfen Sie die Auftragsübersicht und klicken Sie dann auf "Fertigstellen".

Info zur Sofortwiederherstellung eines virtuellen Hyper-V-Computers

Mit Backup Exec ist die Sofortwiederherstellung virtueller Computer aus einem Backup-Satz möglich, ohne dass zunächst die darauf enthaltenen Daten übertragen werden müssen. Backup Exec startet den sofort wiederhergestellten virtuellen Computer direkt über den Backup-Satz. Daraufhin kann auf dem Hyper-V-Host darauf zugegriffen werden. Die Startzeit des Computers hängt von der Netzwerk- und Speichergeschwindigkeit ab und nicht von der Größe des virtuellen Computers. Auf sofort wiederhergestellten virtuellen Computern sind dieselben Aktionen möglich wie auf gewöhnlichen virtuellen Computern.

Die Sofortwiederherstellung eines virtuellen Computers hat folgende Einsatzmöglichkeiten:

- Zugriff und Wiederherstellung einzelner Dateien und Ordner auf einem virtuellen Computer
- Testen von Patches auf dem sofort wiederhergestellten virtuellen Computer, bevor sie auf Produktionssysteme angewendet werden.
- Prüfen des Backup-Images des virtuellen Computers und der Anwendungen
- Prüfen einer Anwendung auf dem sofort wiederhergestellten virtuellen Computer
- Permanentes Wiederherstellen des sofort wiederhergestellten virtuellen Computers mithilfe der Hyper-V-Live- oder -Speichermigration. Bei der

Notfallwiederherstellung können Sie auf virtuellen Computern in wenigen Minuten eine Sofortwiederherstellung durchführen und anschließend eine Migration planen, um ihn auf einen dauerhaften Speicher auf einem Hyper-V-Host zu verschieben. Der wiederhergestellte virtuelle Computer bleibt auch während der Migration verfügbar, um Systemausfälle zu minimieren.

Hinweis: Das Sichern sofort wiederhergestellter virtueller Computer mit dem Agent for Hyper-V ist erst möglich, wenn Sie den virtuellen Computer aus dem Speicher des Backup Exec-Servers migriert und den virtuellen Computer auch aus dem Speicher des Backup Exec-Servers entfernt haben.

Wenn Sie einen sofort wiederhergestellten virtuellen Computer entfernen, dann gehen alle vorgenommenen Änderungen verloren. Migrieren Sie den virtuellen Computer aus dem Speicher des Backup Exec-Servers und entfernen Sie ihn aus Backup Exec, um die vorgenommenen Änderungen beizubehalten oder den sofort wiederhergestellten virtuellen Computer mit dem Agent for Hyper-V zu sichern.

Wenn Sie eine Sofortwiederherstellung ausführen, wird der ausgewählte Backup-Satz für den Hyper-V-Host über eine SMB-Freigabe auf dem Backup Exec-Server sichtbar. Die Festplatten des wiederhergestellten virtuellen Computers befinden sich zwar im Backup Exec-Speicher, nutzen aber die CPU des Hyper-V-Hosts zum Ausführen von Vorgängen. Alle Lesevorgänge werden auf den Backup Exec-Server umgeleitet und die Schreibvorgänge werden auf einem Datenträger an dem Speicherort gespeichert, der im Feld "Ziel für VC-Registrierung und Kontrollpunkt" beim Erstellen des Sofortwiederherstellungsauftrags angegeben wurde. Dieser Pfad befindet sich auf dem Hyper-V-Host, auf dem der virtuelle Computer wiederhergestellt werden soll.

Hinweis: Backup Exec meldet jede Woche, wie viele sofort wiederhergestellte virtuelle Computer auf dem Server ausgeführt werden. Standardmäßig wird die Benachrichtigung jeden Freitag um 14.00 Uhr ausgegeben.

Die folgende Tabelle beschreibt die Sofortwiederherstellung eines virtuellen Computers.

Tabelle D-5 Sofortwiederherstellung eines virtuellen Hyper-V-Computers

Schritt	Beschreibung
Schritt 1	Sie führen eine Sofortwiederherstellung aus dem Backup eines virtuellen Hyper-V-Computers durch.

Schritt	Beschreibung
Schritt 2	Der Backup Exec-Server virtualisiert den Backup-Satz.
Schritt 3	Backup Exec erstellt eine SMB-Freigabe.
Schritt 4	Backup Exec erstellt einen virtuellen Computer auf dem Hyper-V-Host.
Schritt 5	Backup Exec erstellt einen Snapshot des virtuellen Computers, sodass Schreibvorgänge auf dem lokalen Datenträger vorgenommen werden können.
Schritt 6	Wenn Sie die Option zum Hochfahren des virtuellen Computers nach dem Wiederherstellen aktivieren, startet Backup Exec ihn automatisch.
Schritt 7 (optional)	Sie können Live- oder Speichermigration zum Migrieren des virtuellen Computers aus dem Speicher des Backup Exec-Servers verwenden, wenn Sie am virtuellen Computer vorgenommene Änderungen speichern möchten.
Schritt 8	<p>Sie führen einen der folgenden Aufträge aus:</p> <ul style="list-style-type: none"> ■ Entfernen eines wiederhergestellten virtuellen Computers, der nicht mehr benötigt wird ■ Entfernen des sofort wiederhergestellten virtuellen Computers aus dem Speicher des Backup Exec-Servers nach der Migration des virtuellen Computers <p>Warnung: Sie können Backup Exec erst aktualisieren, nachdem Sie alle wiederhergestellten virtuellen Computer entfernt haben.</p>

Ausfallsicherheit der Sofortwiederherstellung

Da Backup Exec vor kurzem die Ausfallsicherheit sofort wiederhergestellter virtueller Computer verbessert hat, gehen die am virtuellen Computer vorgenommenen Änderungen nun nicht mehr verloren, wenn Sie den Backup Exec-Server oder den Hyper-V-Server neu starten, oder wenn Probleme mit der Netzwerkverbindung

auftreten. Nach dem Neustart einer dieser Server werden die Backup Exec-Dienste gestartet und der Virtualisierungsvorgang fortgesetzt.

Beim Ausführen des sofort wiederhergestellten virtuellen Computers auf dem Hyper-V-Host ergeben sich vier mögliche Ausfallsicherheitsszenarien:

- Der Backup Exec-Server wird neu gestartet und der Hyper-V-Server wird ausgeführt.
- Der Hyper-V-Server wird neu gestartet und der Backup Exec-Server wird ausgeführt.
- Der Backup Exec-Server und der Hyper-V-Server werden neu gestartet.
- Probleme mit der Netzwerkverbindung führen zur Unterbrechung der Verbindung zwischen dem Backup Exec-Server und dem Hyper-V-Host.

In jedem dieser Szenarien wird der virtuelle Computer automatisch neu gestartet, wenn der Neustart des Servers abgeschlossen oder die Netzwerkverbindung wiederhergestellt ist. Wenn der virtuelle Computer nicht automatisch gestartet wird, dann müssen Sie ihn möglicherweise auf dem Hyper-V-Host neu starten.

Hinweis: Der virtuelle Computer kann nicht verwendet werden, bis der Neustart des Servers abgeschlossen oder die Netzwerkverbindung wiederhergestellt ist.

Ausfallsicherheit der Sofortwiederherstellung für Hyper-V nutzt die Kommunikationsmethode CORBA. Eine Änderung der Konfiguration kann erforderlich sein, wenn der CORBA-Kommunikationsport auf dem Backup Exec-Server geändert werden muss. Der Backup Exec-Server und der Hyper-V-Server, auf dem sich der sofort wiederhergestellte virtuelle Computer befindet, müssen dieselbe Einstellungen des CORBA-Port haben.

So ändern Sie die Einstellung des CORBA-Port auf dem Backup Exec-Server

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Backup Exec-Einstellungen".
- 2 Wählen Sie im linken Teilfenster "Netzwerk und Sicherheit".
- 3 Aktivieren Sie unter "Benutzerdefinierte Port-Nummer (nur Oracle)" das Kontrollkästchen "Benutzerdefinierten Port für den Empfang von Vorgangsanforderungen vom Oracle-Server verwenden:" und geben Sie dieselbe Port-Nummer wie für den Hyper-V-Server ein.
- 4 Starten Sie alle Backup Exec Services neu und führen Sie das Backup erneut aus.

So ändern Sie die Einstellung des CORBA-Port auf dem Hyper-V-Host

- 1 Klicken Sie auf dem Computer mit dem Agent for Windows in der Taskleiste auf "Start > Alle Programme > Veritas Backup Exec > Backup Exec Agent Utility".
- 2 Klicken Sie auf die Registerkarte "Datenbankzugriff".
- 3 Aktivieren Sie das Kontrollkästchen "Benutzerdefinierten Port zur Verbindung mit dem Backup Exec-Server bei Oracle-Vorgängen verwenden".
- 4 Geben Sie eine Port-Nummer ein, die noch nicht genutzt wird und für Backup Exec verfügbar ist, und klicken Sie auf "OK".

Hinweis: Diese Port-Nummer muss mit der für den Backup Exec-Server konfigurierten identisch sein.

- 5 Starten Sie den Dienst "Backup Exec Remote Agent" auf dem Hyper-V-Server neu.

Unterschiede zwischen gewöhnlicher und Sofortwiederherstellung virtueller Computer

Die Sofortwiederherstellung eines virtuellen Computers unterscheidet sich in einigen Punkten von einer gewöhnlichen Wiederherstellung.

Tabelle D-6 Unterschiede zwischen gewöhnlicher und Sofortwiederherstellung virtueller Computer

Element	Sofortwiederherstellung eines virtuellen Computers	Gewöhnliche Wiederherstellung eines virtuellen Computers
Datenübertragung	Bei der Sofortwiederherstellung werden keine Daten des virtuellen Computers übertragen.	Alle Daten des Backup-Satzes werden auf den wiederhergestellten virtuellen Computer übertragen.
Auftragsdauer	Der Sofortwiederherstellungsauftrag wird sofort ausgeführt und es werden keine Backup-Daten übertragen. Die erforderliche Zeit hängt daher davon ab, wie lange das Freigeben des Backup-Satzes und das Registrieren des virtuellen Computers dauert.	Die Zeit für die gewöhnliche Wiederherstellung hängt von der Größe des virtuellen Computers und von der Netzwerk- und Speichergeschwindigkeit ab.

Element	Sofortwiederherstellung eines virtuellen Computers	Gewöhnliche Wiederherstellung eines virtuellen Computers
Lesevorgänge	Verwendet das Image des Backup-Satzes für alle Lesevorgänge. Verwendet einen Snapshot auf dem Hyper-V-Server für alle Schreibvorgänge.	Die Daten sind bereits auf den Hyper-V-Server verschoben. Daher besteht keine Abhängigkeit vom Backup Exec-Server.
Datenspeicher	Verwendet bis zur Migration des sofort wiederhergestellten virtuellen Computers den Speicher des Backup Exec-Servers.	Verwendet bereits den Speicher des Hyper-V-Servers.
Server-Neustart	Durch die Verbesserung der Ausfallsicherheit der Sofortwiederherstellung bleibt beim Neustart des Backup Exec-Servers oder des Hyper-V-Servers der Zugriff auf den sofort wiederhergestellten virtuellen Computer erhalten. Im Falle von Problemen mit der Netzwerkverbindung kann nach dem Wiederherstellen der Verbindung auf die wiederhergestellten virtuellen Computer zugegriffen werden. Wenn der virtuelle Computer nicht automatisch gestartet wird, dann müssen Sie ihn möglicherweise auf dem Hyper-V-Host neu starten.	Ein Neustart des Backup Exec- oder Hyper-V-Servers hat keine Auswirkungen auf den gewöhnlich wiederhergestellten virtuellen Computer.

Siehe ["Anforderungen für die Sofortwiederherstellung eines virtuellen Hyper-V-Computers"](#) auf Seite 1199.

Siehe ["Erstellen eines Auftrags für die Sofortwiederherstellung eines virtuellen Hyper-V-Computers"](#) auf Seite 1201.

Siehe ["Infos zum Entfernen eines sofort wiederhergestellten virtuellen Hyper-V-Computers"](#) auf Seite 1203.

Siehe ["Hinweise zur Sofortwiederherstellung eines virtuellen Hyper-V-Computers"](#) auf Seite 1200.

Anforderungen für die Sofortwiederherstellung eines virtuellen Hyper-V-Computers

Zum Konfigurieren einer Sofortwiederherstellung gelten folgende Anforderungen:

- Auf dem Hyper-V-Host muss genügend Speicherplatz zum Speichern aller Änderungen vorhanden sein, beispielsweise Schreibvorgänge auf virtuellen Datenträgern, die auf dem wiederhergestellten virtuellen Computer ausgeführt werden.
- Aktivieren Sie die Funktion "Granular Recovery Technology" von Backup Exec zum Wiederherstellen einzelner Elemente aus Microsoft-Anwendungen im Hyper-V-Backup-Auftrag. Wenn der virtuelle Computer nicht für GRT geeignet ist, können Sie die Option "Sofortwiederherstellung für alle virtuellen Computer aktivieren, auch für solche, die GRT nicht nutzen können." aktivieren. Beachten Sie, dass dann das Speicherformat des nächsten vollständigen Backups in eines geändert wird, das mit der Sofortwiederherstellung kompatibel ist. Siehe ["Verwenden von Granular Recovery Technology \(GRT\) mit Agent for Hyper-V"](#) auf Seite 1180.
- Beim Erstellen eines Sofortwiederherstellungsauftrags zeigt Backup Exec alle Backup-Sätze an, die für die Sofortwiederherstellung geeignet sind. Siehe ["Verwenden von Granular Recovery Technology \(GRT\) mit Agent for Hyper-V"](#) auf Seite 1180.
- Führen Sie die Sofortwiederherstellung virtueller Computer nur dann aus, wenn die auf einem virtuellen Agent basierenden GRT-fähigen Backup-Sätze auf einem Datenträgerspeichergerät gespeichert sind. Bandspeicher, Deduplizierungsspeicher, Cloud-Speicher und Plattenkassettengeräte wie RDX werden nicht unterstützt.
- In einer Umgebung, die nur über Netzwerkkarten verfügt, die mit IPv6 konfiguriert wurden, wird die Sofortwiederherstellung nur unterstützt, wenn der Hyper-V-Server entweder mit dem Namen "FQDN" oder "NetBIOS" auf den Backup Exec-Server zugreift.
- Stellen Sie anhand der Hardwarekompatibilitätsliste und der Softwarekompatibilitätsliste sicher, dass Ihre Umgebung unterstützte Hardware und Software aufweist. Die unterstützten Geräte, Betriebssysteme, Plattformen und Anwendungen finden Sie in der Liste der mit Backup Exec kompatiblen Hardware und Software.

Hinweise zur Sofortwiederherstellung eines virtuellen Hyper-V-Computers

Vor dem Konfigurieren einer Sofortwiederherstellung sollten Sie folgende Hinweise beachten:

- Die Backup Exec-Befehlszeilenschnittstelle (BEMCLI) wird für die Sofortwiederherstellung nicht unterstützt.
- In gebündelten Backup Exec-Umgebungen wird die Sofortwiederherstellung eines virtuellen Computers nicht unterstützt.
- Backup Exec unterstützt keine Sofortwiederherstellung eines virtuellen Computers auf einen Hyper-V-Server, auf dem eine ältere Version ausgeführt wird als auf dem Hyper-V-Server, der zum Sichern des virtuellen Computers verwendet wurde. Beispiel: Sie können keine Sofortwiederherstellung eines virtuellen Computers auf einen Hyper-V 2008-Server durchführen, wenn der virtuelle Computer auf einem Hyper-V 2012-Server gesichert wurde.
- Für CAS-Umgebungen gilt Folgendes:
 - Der zentrale Administrationsserver oder der verwaltete Backup Exec-Server kann eine Sofortwiederherstellung eines virtuellen Computers durchführen, wenn dieser auf diesen Servern betrieben wird. Allerdings kann der verwaltete Backup Exec-Server die virtuellen Computer nur dann entfernen, wenn die Sofortwiederherstellung auf diesem Server durchgeführt wurde.
 - Sie können eine Sofortwiederherstellung nach Delegieren des Auftrags an einen verwalteten Backup Exec-Server nicht von einem zentralen Administrationsserver verwalten.
- In den folgenden Fällen speichert Backup Exec Datenträger in einem anderen Format als beim ursprünglichen virtuellen Computer:
 - Wenn der Speicher des mit dem ursprünglichen virtuellen Computer verbundenen Datenträgers auf "Feste Größe" eingestellt ist, konvertiert Backup Exec die Einstellung während dem Backup auf "Dynamische Erweiterung". Beim Erstellen eines sofort wiederhergestellten virtuellen Computers wird dem Datenträgerspeicher die Eigenschaft "Dynamische Erweiterung" zugeordnet.
 - Gleichzeitig konvertiert Backup Exec während der Ausführung des Backup-Auftrags das Format der Datenträger des virtuellen Computers aus VHDX in VHD. Die Datenträger werden konvertiert, wenn der für den Backup-Auftrag ausgewählte virtuelle Computer auf einem Hyper-V-Server 2012 oder höher ausgeführt wird und der Backup Exec-Server auf einem Windows-Server 2008 R2 oder älter installiert ist.

Beim Erstellen eines sofort wiederhergestellten virtuellen Computers haben die Datenträger das Format "VHD". Zum Konvertieren der Datenträger in das Format "VHDX" migrieren Sie den virtuellen Computer aus dem Speicher des Backup Exec-Servers und führen Sie den Vorgang im Hyper-V Manager aus.

- Bei einer Sofortwiederherstellung eines virtuellen Computers wird der Speicherstand des zum Erstellen der Sofortwiederherstellung verwendeten Backup-Satzes nicht erhalten.
- Bei einer Sofortwiederherstellung eines virtuellen Computers werden die zum Erstellen der Sofortwiederherstellung vom Benutzer erstellten Snapshots im Backup-Satz nicht erhalten.
- Backup Exec unterstützt die Sofortwiederherstellung eines virtuellen Computers der zweiten Generation nur, wenn er auf einem Backup Exec-Server gesichert wurde, der unter Windows Server 2012 oder höher installiert ist.

Erstellen eines Auftrags für die Sofortwiederherstellung eines virtuellen Hyper-V-Computers

Sie können einen Auftrag für die Sofortwiederherstellung eines virtuellen Hyper-V-Computers erstellen und diesen dann am ursprünglichen oder an einem anderen Speicherort wiederherstellen.

Hinweis: Für Anwendungen wie SharePoint und Exchange gilt: Stellen Sie alle virtuellen Computer wieder her, die die Anwendungen benötigen, um richtig zu funktionieren. Beispiel: In einer Microsoft Exchange-Umgebung müssen Sie die virtuellen Computer wiederherstellen, auf denen der Exchange-Client und das Active Directory ausgeführt werden, und dann eine Verbindung zwischen diesen beiden virtuellen Computern aufbauen.

Siehe ["Anforderungen für die Sofortwiederherstellung eines virtuellen Hyper-V-Computers"](#) auf Seite 1199.

Führen Sie folgende Schritte zum Erstellen eines Auftrags für die Sofortwiederherstellung eines virtuellen Hyper-V-Computers aus:

So erstellen Sie einen Auftrag für die Sofortwiederherstellung eines virtuellen Hyper-V-Computers

- 1 Auf der Registerkarte "Backup und Wiederherstellung" wählen Sie den virtuellen Computer aus, der wiederhergestellt werden soll.
- 2 Klicken Sie in der Gruppe "Sofortwiederherstellung" auf "Sofortwiederherstellung eines virtuellen Computers".

- 3 Geben Sie im Dialogfeld "Sofortwiederherstellung eines virtuellen Computers" im Feld "Auftragsname" einen Namen für den Auftrag ein.
- 4 Geben Sie im Gruppenfeld "Backup-Satz-Auswahl" im Feld "Backup-Sätze anzeigen von" das Start- und Enddatum für die Backup-Sätze an, die in die Auswahl aufgenommen werden sollen.

Standardmäßig werden nur die Backup-Sätze der Aufträge angezeigt, die in den letzten 30 Tagen ausgeführt wurden.

- 5 Wählen Sie im Feld "Datenträgerbasierter Backup-Satz" den Backup-Satz für den wiederhergestellten virtuellen Computer aus.

In der Liste werden nur Backup-Sätze angezeigt, die die Anforderungen für Sofortwiederherstellungen erfüllen.

- 6 Klicken Sie im linken Teilfenster auf "Ziel" und legen Sie folgende Optionen für den Auftrag fest:

Element	Beschreibung
Name des virtuellen Computers	Geben Sie den Namen für den sofort wiederhergestellten virtuellen Computer ein, der in der Hyper-V-Manager-Konsole angezeigt werden soll.
Hyper-V-Servername	Wählen Sie den Namen des Hyper-V-Servers aus, auf dem der virtuelle Computer wiederhergestellt werden soll.
Server-Login-Konto	Wählen Sie den Namen des Login-Kontos, das für den Zugriff auf den Server erforderlich ist.
Ziel für VC-Registrierung und Kontrollpunkt	Wählen Sie den Pfad auf dem Hyper-V-Host, in dem die Konfigurationsdetails und die Kontrollpunktdatei (Datenträger) des wiederhergestellten virtuellen Computers gespeichert sind.
Virtuellen Computer nach dem Wiederherstellen hochfahren	Mit dieser Option wird der virtuelle Computer nach der Sofortwiederherstellung automatisch gestartet.

- 7 Wählen Sie im Dialogfeld "Sofortwiederherstellung eines virtuellen Computers" im linken Teilfenster "Planen" und wählen Sie anschließend den Zeitplan für diesen Auftrag aus.

8 (Optional) Wählen Sie im Dialogfeld "Sofortwiederherstellung eines virtuellen Computers" im linken Teilfenster "Benachrichtigung" und dann die Empfänger der Benachrichtigung beim Abschluss des Auftrags.

9 Klicken Sie auf "OK".

Siehe ["Aufgaben nach der Sofortwiederherstellung"](#) auf Seite 1203.

Aufgaben nach der Sofortwiederherstellung

Führen Sie diese Aufgaben nach der Sofortwiederherstellung vor Verwendung des sofort wiederhergestellten virtuellen Computers durch.

- Während der Sofortwiederherstellung deaktiviert Backup Exec die Netzwerkkarte auf dem virtuellen Computer. Um den Computer mit dem Netzwerk zu verbinden, müssen Sie die Netzwerkeinstellungen auf dem Computer konfigurieren.
- Wenn Sie den sofort wiederherzustellenden virtuellen Computer auf einen Hyper-V-Host verschieben möchten, können Sie die Datendateien oder jeweiligen Datenträger des virtuellen Computers mithilfe der Hyper-V-Live- oder -Speichermigration auf den Hyper-V-Host migrieren. Hinweis: Während der Migration werden die Datendateien des virtuellen Computers auf den Host-Computer übertragen, während der virtuelle Computer noch ausgeführt wird.

Die Migrationsschritte finden Sie auf der Website von Microsoft.

Infos zum Entfernen eines sofort wiederhergestellten virtuellen Hyper-V-Computers

Sofort wiederhergestellte virtuelle Computer müssen aus dem Speicher des Backup Exec-Servers entfernt werden, wenn sie migriert wurden oder nicht mehr benötigt werden. Durch Entfernen eines sofort wiederhergestellten virtuellen Computers werden alle Datenbankeinträge und alle zum Zeitpunkt des Auftrags erstellten Ordner bereinigt.

Auch wenn Sie den virtuellen Computer mit dem Hyper-V-Manager aus dem Hyper-V-Host entfernen, sollten Sie den wiederhergestellten virtuellen Computer aus Backup Exec entfernen. Wenn Sie einen sofort wiederhergestellten virtuellen Computer aus dem Hyper-V-Host entfernen, werden die Konfigurations- und Kontrollpunktordner aus dem Hyper-V-Speicher gelöscht. Auch die SMB-Freigabe, die auf dem Backup Exec-Server für den virtuellen Computer erstellt wurde, wird entfernt.

Wenn Sie den Auftrag "Wiederhergestellten virtuellen Computer entfernen" ausführen, prüft Backup Exec den Speicherstatus der Datenträger und hebt dann die Registrierung des virtuellen Computers auf dem Hyper-V-Host auf.

Folgende Status sind möglich:

- Werden alle Datenträger des sofort wiederhergestellten virtuellen Computers weiterhin auf dem Backup Exec-Speicher ausgeführt, hebt Backup Exec zuerst die Registrierung dieses virtuellen Computers auf dem Hyper-V-Host auf und entfernt ihn anschließend.
- Werden keine Datenträger des virtuellen Computers auf dem Backup Exec-Speicher ausgeführt, entfernt ihn Backup Exec sofort. Der virtuelle Computer ist auch nach dem Entfernen weiterhin verfügbar und Sie können ihn aus dem Hyper-V-Manager löschen.
- Werden noch Datenträger auf dem Backup Exec-Speicher ausgeführt und wurden andere in einen permanenten Speicher verschoben, schlägt der Auftrag "Wiederhergestellten virtuellen Computer entfernen" fehl. Sie können entweder alle Datenträger aus dem Backup Exec-Speicher verschieben und den Auftrag erneut ausführen, oder das Kontrollkästchen "Virtuellen Computer entfernen, obwohl sich im Speicher des Backup Exec-Servers und auf dem Host des virtuellen Computers Datenträger befinden" aktivieren, wenn die Änderungen nicht gespeichert werden sollen.
- Ist die Hyper-V-Replikation auf dem wiederhergestellten virtuellen Computer aktiviert, schlägt der Entfernungsauftrag fehl. Sie können die Replikation für diesen virtuellen Computer entfernen und den Auftrag erneut ausführen.
- Wenn der sofort wiederhergestellte virtuelle Computer gerade migriert wird, können Sie den Auftrag anschließend erneut ausführen.

Hinweis: Data Lifecycle Management (DLM) für den Backup-Satz, mit dem der sofort wiederhergestellte virtuelle Computer erstellt wurde, wird erst dann ausgeführt, wenn der virtuelle Computer entfernt ist. Mit dem nächsten DLM-Zyklus läuft der Backup-Satz ab.

Entfernen eines sofort wiederhergestellten virtuellen Hyper-V-Computers

Sofort wiederhergestellte virtuelle Computer müssen aus dem Speicher des Backup Exec-Servers entfernt werden, wenn sie migriert wurden oder nicht mehr benötigt werden.

So entfernen Sie einen sofort wiederhergestellten virtuellen Computer

- 1 Auf der Registerkarte "Backup und Wiederherstellung" wählen Sie den Hyper-V-Server aus, der den wiederhergestellten virtuellen Computer enthält, der entfernt werden soll.

Doppelklicken Sie auf einen Hyper-V-Server und klicken Sie dann im linken Teilfenster auf "Wiederhergestellte virtuelle Computer", um die sofort wiederhergestellten virtuellen Computer anzuzeigen.

- 2 Klicken Sie in der Gruppe "Sofortwiederherstellung" auf "Wiederhergestellten virtuellen Computer entfernen" und führen Sie einen der folgenden Schritte aus:

So entfernen Sie einen wiederhergestellten virtuellen Computer sofort Gehen Sie dazu in folgender Reihenfolge vor:

- Wählen Sie "Standardwerte verwenden und jetzt entfernen"
- Wählen Sie im Dialogfeld "Wiederhergestellte virtuelle Computer zum Entfernen auswählen" mindestens einen wiederhergestellten virtuellen Computer zum Entfernen aus.
- Klicken Sie auf "OK".

So passen Sie die Einstellungen an und entfernen einen wiederhergestellten virtuellen Computer

Gehen Sie nach folgender Reihenfolge vor:

- Wählen Sie "Einstellungen anpassen und entfernen".
- Wählen Sie im Dialogfeld "Wiederhergestellte virtuelle Computer zum Entfernen auswählen" mindestens einen wiederhergestellten virtuellen Computer zum Entfernen aus.
- Klicken Sie auf "OK".
- Geben Sie im Dialogfeld "Wiederhergestellten virtuellen Computer entfernen" im Feld "Auftragsname" einen Namen für den Auftrag ein.
- Fügen Sie im Feld "Server-Login-Konto" ein Login-Konto für den Hyper-V-Server hinzu oder bearbeiten Sie es.
- Aktivieren Sie die Option "Virtuellen Computer entfernen, obwohl sich im Speicher des Backup Exec-Servers und auf dem Host des virtuellen Computers Datenträger befinden", um die Datenträger zu entfernen, und fahren Sie dann mit dem Auftrag zum Entfernen des sofort wiederhergestellten virtuellen Computers fort. Wenn Sie diese Option nicht auswählen, können die Datenträger nicht entfernt werden und der Auftrag schlägt fehl.
- Wählen Sie im Dialogfeld "Wiederhergestellten virtuellen Computer entfernen" im linken Teilfenster "Planen" und wählen Sie anschließend den Zeitplan für diesen Auftrag aus.
- (Optional) Wählen Sie im Dialogfeld "Wiederhergestellten virtuellen Computer entfernen" im linken Teilfenster "Benachrichtigung" und dann die Empfänger der Benachrichtigung beim Abschluss des Auftrags.
- Klicken Sie auf "OK".

Best Practices bei der Sofortwiederherstellung eines virtuellen Hyper-V-Computers

Best Practices sind Tipps und Empfehlungen, die Ihnen helfen können, die Sofortwiederherstellungsfunktion für virtuelle Hyper-V-Computer effektiv zu verwenden.

- Entfernen oder migrieren Sie die sofort wiederhergestellten virtuellen Computer aus Backup Exec, bevor Sie den Backup Exec-Server aktualisieren oder deinstallieren. Upgrades und Patch-Upgrades werden nur dann blockiert, wenn auf dem Backup Exec-Server oder dem Hyper-V-Server eine Version ausgeführt wird, die älter ist als Backup Exec 16 Feature Pack 1, und ein sofort wiederhergestellter virtueller Computer auf diesen Servern ausgeführt wird. Deinstallationen werden auf den Backup Exec-Servern und dem Server, auf dem Agent for Hyper-V installiert ist, blockiert, wenn ein sofort wiederhergestellter virtueller Computer darauf ausgeführt wird.
- Werden sehr viele sofort wiederhergestellte virtuelle Computer gleichzeitig ausgeführt, wird möglicherweise die Leistung des Backup Exec-Servers beeinträchtigt. Sie sollten die in der Umgebung ausgeführten wiederhergestellten virtuellen Computer regelmäßig prüfen. Entfernen Sie nicht länger benötigte virtuelle Computer oder migrieren Sie diese auf den Host und entfernen Sie sie dann vom Backup Exec-Server.
Bei der Migration wird Netzwerkbandbreite genutzt. Deshalb sollten Sie sie zu einem Zeitpunkt durchführen, zu dem andere Prozesse nur eine geringe Bandbreite benötigen.
- Beim Migrieren eines sofort wiederhergestellten virtuellen Computers sollten Sie auf dem Hyper-V-Host einen Pfad verwenden, der sich vom ursprünglichen Speicherort des sofort wiederhergestellten virtuellen Computers unterscheidet.
- Für einen sofort wiederhergestellten virtuellen Computer, der auf einem Hyper-V-Host mit Backup Exec erstellt wurde, darf das Ziel nicht als ein Datenträger festgelegt sein, auf dem die Festplatten für den virtuellen Backup Exec-Computer gehostet werden.

Informationen zur Funktion "Wiederherstellung bereit" für virtuelle Hyper-V-Computer

Backup Exec verfügt seit der Version Backup Exec 16 Feature Pack 1 über die Funktion "Wiederherstellung bereit". Mit der Funktion "Wiederherstellung bereit" können Sie über den Vorgang "VM für Wiederherstellung validieren" die Wiederherstellbarkeit von virtuellen Computer validieren. Wenn Sie einen Auftrag zum Validieren eines virtuellen Computers für die Wiederherstellung erstellen und

ausführen, werden erst einige Tests auf dem virtuellen Computer ausgeführt, nachdem dieser als zur Wiederherstellung bereit gekennzeichnet wurde.

Zur Wiederherstellung bereite virtuelle Computer können für die folgenden Aufgaben verwendet werden:

- **Disaster Recovery-Bereitschaft:** In einem Disaster Recovery-Szenario sind Administratoren sicher, dass die validierten virtuellen Computer wiederhergestellt werden.
- **Backups in Cloud oder auf Band speichern:** Validiert die Backup-Sätze, bevor sie in der Cloud und auf Band gespeichert werden.
- **Prüfung und Compliance von Backups:** Zum Erfüllen der Anforderungen auf Prüfung und die Einhaltung gesetzlicher Bestimmungen des Unternehmens können Sie Validierungsinformationen zu den Backups virtueller Computer angeben.

Während der Ausführung eines Auftrags zum Validieren eines virtuellen Computers für die Wiederherstellung wird der virtuelle Computer auf dem Hyper-V-Server mit dem Hostnamen im Format *Validate_Name des virtuellen Computers_GUID* registriert und dann eingeschaltet. Nach dem Einschalten wird ein Heartbeat-Test ausgeführt, um zu prüfen, ob der Dienst "Hyper-V Heartbeat" ausgeführt wird.

Während der Validierung des virtuellen Computers erfolgt keine Datenübertragung.

Bei der Erstellung eines Auftrags zum Validieren eines virtuellen Computers für die Wiederherstellung können Sie die maximal zulässige Zeit für den Start des virtuellen Computers vor der Ausführung des Validierungsauftrags auswählen. Der Standardwert ist 10 Minuten. Sie können einen Wert zwischen 1 und 60 Minuten auswählen.

Siehe ["Konfigurieren der Standardeinstellungen für das Backup"](#) auf Seite 785.

Nach dem erfolgreichen Abschluss aller Prüfungsvorgänge wird der virtuelle Computer als zur Wiederherstellung bereit gekennzeichnet.

Alle während der Validierung erfassten Informationen sind Teil des Auftragsprotokolls. Nach der Validierung können Sie die Validierungsübersicht "Wiederherstellung bereit" erstellen, die die validierten virtuellen Computer enthält.

Siehe ["Validierungsübersicht "Wiederherstellung bereit" auf Seite 843.](#)

Doppelklicken Sie zum Anzeigen des Validierungsstatus auf der Registerkarte "Backup und Wiederherstellung" auf den Hostnamen bzw. auf der Registerkarte "Speicher" auf den Namen des Speichers. Klicken Sie im linken Teilfenster auf "Backup-Sätze". Für die ausgewählte Server- bzw. Speicheransicht wird der Validierungsstatus angezeigt.

Die folgende Tabelle beschreibt den Vorgang zur Validierung von virtuellen Hyper-V-Computern für die Wiederherstellung.

Tabelle D-7 Validieren von virtuellen Computern für die Wiederherstellung

Schritt	Beschreibung
Schritt 1	Fügen Sie den Hyper-V-Server hinzu.
Schritt 2	Führen Sie ein plattenbasierten GRT-Backup des virtuellen Computers aus, der auf dem Hyper-V-Server gehostet wird. Die Funktion "Wiederherstellung bereit" unterstützt vollständige, inkrementelle und differenzielle Backup-Sätze.
Schritt 3	Führen Sie den Auftrag zum Validieren eines virtuellen Hyper-V-Computers für die Wiederherstellung aus.
Schritt 4	Backup Exec virtualisiert den Backup-Satz.
Schritt 5	Backup Exec erstellt eine SMB-Freigabe.
Schritt 6	Backup Exec führt die folgenden Tests in der angegebenen Reihenfolge auf dem zu validierenden virtuellen Hyper-V-Computer aus. <ul style="list-style-type: none"> ■ Registrieren des virtuellen Computers ■ Einschalten des virtuellen Computers ■ Heartbeat-Test auf dem virtuellen Computer
Schritt 7	Wenn alle Tests erfolgreich sind, kennzeichnet Backup Exec den Hyper-V-Computer als validiert.

Tests, die auf dem zu validierenden virtuellen Hyper-V-Computer ausgeführt werden

Auf dem zu validierenden virtuellen Hyper-V-Computer werden die folgenden Tests ausgeführt.

Tabelle D-8 Tests, die auf dem virtuellen Hyper-V-Computer ausgeführt werden

Test	Beschreibung
Registrieren des virtuellen Computers	Beim ersten Test wird der virtuelle Computer auf dem Hyper-V-Server registriert.
Einschalten des virtuellen Computers	Im zweiten Test wird der registrierte virtuelle Computer eingeschaltet.

Test	Beschreibung
Taktsignal-Test	<p>Im dritten Test wird der Dienst "Heartbeat Integration Service" überprüft. Wenn dieser Dienst erfolgreich auf dem eingeschalteten virtuellen Computer ausgeführt wird, war der Taktsignal-Test erfolgreich.</p> <p>Integration Services müssen installiert und der Dienst "Hyper-V Heartbeat" muss aktiviert sein. Diese Dienste müssen aktiv sein, damit der Heartbeat-Test auf dem gesicherten virtuellen Computer ausgeführt werden kann. Wenn Integration Services nicht installiert sind, schlägt die Validierung fehl und für den entsprechenden Backup-Satz wird der Status "Validierung fehlgeschlagen" angezeigt.</p>

Alle Informationen zu den Testergebnissen sind auch im Auftragsprotokoll verfügbar.

Validierungsstatus für einen virtuellen Hyper-V-Computer

Während der Validierung werden die folgenden Statuswerte für den Backup-Satz eines virtuellen Hyper-V-Computers angezeigt:

- Validierung erfolgreich : Alle Tests für den Backup-Satz wurden erfolgreich abgeschlossen und der Backup-Satz ist nun für die Wiederherstellung bereit.
- Validierung fehlgeschlagen : Die Tests für den Backup-Satz konnten nicht erfolgreich abgeschlossen werden und der Backup-Satz ist nicht für die Wiederherstellung bereit.
- Validierung nicht möglich : Der virtuelle Computer konnte aufgrund von Problemen in der Umgebung nicht validiert werden. Daher können die Backup-Sätze nicht validiert werden.
Wenn der Dienst "Hyper-V Heartbeat" zur Zeit des Backup deaktiviert ist, schlägt die Validierung fehl und der Backup-Satz wird als "Validierung nicht möglich" gekennzeichnet.

Während der Validierung werden die folgenden Statuswerte für den Validierungsauftrag eines virtuellen Hyper-V-Computers angezeigt:

- Erfolgreich : Alle Tests für die Validierung wurden abgeschlossen und der virtuelle Computer ist für die Wiederherstellung bereit.
- Erfolg mit Ausnahmen : Die Validierung war erfolgreich, aber beim Bereinigen der Ressourcen schlägt das Ausschalten fehl.
- Fehlgeschlagen : Die Validierung ist fehlgeschlagen oder wurde nicht ausgeführt.

Wenn die Validierung fehlschlägt oder Backup Exec den virtuellen Computer nicht für die Wiederherstellung validieren kann, werden weitere Informationen in das Validierungsauftragsprotokoll aufgenommen.

Im Folgenden finden Sie Details zu den Tests und zum Validierungsstatus.

Tabelle D-9 Validierungsstatus für einen virtuellen Hyper-V-Computer

Validierungstest	Status des Backup-Satzes	Status des Validierungsauftrags	Weitere Schritte/Grund für Fehler
Virtuellen Computer registrieren	Wenn die Registrierung erfolgreich abgeschlossen wurde, gehen Sie zum nächsten Prüfungsvorgang.		
	Validierung fehlgeschlagen	Fehlgeschlagen	Problem mit dem Backup-Satz
	Validierung nicht möglich	Fehlgeschlagen	Problem mit der Umgebung
Virtuellen Computer einschalten	Wurde der Computer eingeschaltet, gehen Sie zum nächsten Prüfungsvorgang.		
	Validierung nicht möglich	Fehlgeschlagen	Problem mit der Netzwerkverbindung oder Prüfungsvorgang wurde nicht versucht, weil die Registrierung fehlgeschlagen ist
Taktsignal-Test	Validierung nicht möglich	Fehlgeschlagen	Test nicht versucht
	Validierung fehlgeschlagen	Fehlgeschlagen	Problem beim Hochfahren oder Problem mit "Heartbeat Integration Service"
	Validierung erfolgreich	Erfolgreich	Der virtuelle Computer ist validiert und für die Wiederherstellung bereit

Siehe ["Anforderungen zum Validieren eines virtuellen Hyper-V-Computers für die Wiederherstellung"](#) auf Seite 1212.

Siehe ["Hinweise zum Validieren eines virtuellen Hyper-V-Computers für die Wiederherstellung"](#) auf Seite 1212.

Siehe ["Erstellen eines Auftrags zum Validieren eines virtuellen Computers für die Wiederherstellung"](#) auf Seite 1214.

Anforderungen zum Validieren eines virtuellen Hyper-V-Computers für die Wiederherstellung

Machen Sie sich mit den folgenden Anforderungen vertraut, bevor Sie für einen virtuellen Hyper-V-Computer einen Auftrag zum Validieren des virtuellen Computers für die Wiederherstellung konfigurieren:

- Hyper-V Integration Services muss auf dem Hyper-V-Server installiert sein.
- Auf dem Hyper-V-Host muss genügend Speicherplatz zum Speichern aller Änderungen vorhanden sein, beispielsweise Schreibvorgänge auf virtuellen Datenträgern, die auf dem wiederhergestellten virtuellen Computer ausgeführt werden.
- Beim Erstellen des Auftrags zum Validieren des virtuellen Computers für die Wiederherstellung zeigt Backup Exec alle Backup-Sätze an, die für die Sofortwiederherstellung geeignet sind.
- Führen Sie den Auftrag zum Validieren des virtuellen Computers für die Wiederherstellung nur dann aus, wenn die Backup-Sätze mit virtuellem Agent auf einem Festplattenspeichergerät gespeichert sind. Bandspeicher, Deduplizierungsspeicher, Cloud-Speicher und Plattenkassettengeräte wie RDX werden nicht unterstützt.
Siehe ["Verwenden von Granular Recovery Technology \(GRT\) mit Agent for Hyper-V"](#) auf Seite 1180.
- In Netzwerkumgebungen, die nur über mit IPv6 konfigurierte Netzwerkkarten verfügen, wird der Vorgang zur Validierung eines virtuellen Computers für die Wiederherstellung nur dann unterstützt, wenn der Hyper-V-Server entweder mit dem "FQDN"- oder dem "NetBIOS"-Namen auf den Medienserver zugreift.
- Stellen Sie anhand der Hardwarekompatibilitätsliste und der Softwarekompatibilitätsliste sicher, dass Ihre Umgebung unterstützte Hardware und Software aufweist. Die unterstützten Betriebssysteme, Plattformen und Anwendungen finden Sie in der Liste der mit Backup Exec kompatiblen Hardware und Software.

Hinweise zum Validieren eines virtuellen Hyper-V-Computers für die Wiederherstellung

Machen Sie sich mit den folgenden Hinweisen vertraut, bevor Sie für einen virtuellen Hyper-V-Computer einen Auftrag zum Validieren des virtuellen Computers für die Wiederherstellung konfigurieren:

- Die Backup Exec-Befehlszeilenschnittstelle (BEMCLI) wird für Aufträge zum Validieren von virtuellen Computern für die Wiederherstellung nicht unterstützt.

- Die Validierung von virtuellen Computern für die Wiederherstellung wird für geclusterte Backup Exec-Umgebungen nicht unterstützt.
- Das Validieren von virtuellen Computern für die Wiederherstellung für einen Hyper-V-Server, auf dem eine ältere Version ausgeführt wird als auf dem zum Sichern des virtuellen Computers verwendeten Hyper-V-Server, wird von Backup Exec nicht unterstützt. Beispielsweise können Sie keinen Auftrag zum Validieren eines virtuellen Computers für die Wiederherstellung für einen Hyper-V 2008-Server durchführen, wenn der virtuelle Computer auf einem Hyper-V 2012-Server gesichert wurde.
- Backup Exec unterstützt das Validieren eines virtuellen Computers der zweiten Generation für die Wiederherstellung nur dann, wenn dieser unter einer Backup Exec-Version gesichert wurde, die unter Windows 2012 oder höher installiert ist.
- Für CAS-Umgebungen gilt Folgendes:
 - Wenn der zentrale Administrationsserver (CAS) über einen Backup-Satz verfügt, erstellen Sie den Auftrag zum Validieren eines virtuellen Computers für die Wiederherstellung nur auf dem CAS-Server. Wenn der verwaltete Backup Exec-Server ("Managed Backup Exec Server"/MBES) über einen Backup-Satz verfügt, erstellen Sie den Auftrag zum Validieren eines virtuellen Computers für die Wiederherstellung nur auf dem MBES-Server.
 - Sie können einen Auftrag zum Validieren eines virtuellen Computers für die Wiederherstellung nicht mehr von einem zentralen Administrationsserver aus ausführen, nachdem Sie den Auftrag an einen verwalteten Backup Exec-Server delegiert haben.

Best Practices beim Validieren eines virtuellen Hyper-V-Computers für die Wiederherstellung

Machen Sie sich mit den folgenden Best Practices vertraut, bevor Sie für einen virtuellen Hyper-V-Computer einen Auftrag zum Validieren des virtuellen Computers für die Wiederherstellung konfigurieren:

- Wählen Sie beim Validieren eines virtuellen Computers für die Wiederherstellung einen Zielordner auf einem Datenträger mit freiem Speicherplatz. Der temporäre virtuelle Computer erfordert mehr Speicherplatz als im für den virtuellen Computer konfigurierten Arbeitsspeicher verfügbar ist, der für die Wiederherstellung validiert wird.
- Es wird empfohlen, die neuesten Hyper-V-Integrationsdienste auf dem gesicherten virtuellen Hyper-V-Computer zu installieren.

- Beim Validieren eines virtuellen Computers für die Wiederherstellung wird empfohlen, dass die Version des Ziel-Hyper-V-Servers mit der des Hyper-V-Servers identisch ist, auf dem sich der virtuelle Computer befindet (als das Backup ausgeführt wurde).

Erstellen eines Auftrags zum Validieren eines virtuellen Computers für die Wiederherstellung

Sie können für einen virtuellen Hyper-V-Computer einen Auftrag zum Validieren des virtuellen Computers für die Wiederherstellung erstellen.

Siehe ["Anforderungen zum Validieren eines virtuellen Hyper-V-Computers für die Wiederherstellung"](#) auf Seite 1212.

Führen Sie folgende Schritte aus, um für einen virtuellen Hyper-V-Computer einen Auftrag zum Validieren eines virtuellen Computers für die Wiederherstellung zu erstellen.

So erstellen Sie einen Auftrag zum Validieren eines virtuellen Computers für die Wiederherstellung

- 1 Wählen Sie auf der Registerkarte "Backup und Wiederherstellung" den virtuellen Computer aus, der wiederhergestellt werden soll.
- 2 Klicken Sie in der Gruppe "Wiederherstellung bereit" auf "VM für Wiederherstellung validieren".
- 3 Geben Sie im Dialogfeld "Virtuellen Computer für die Wiederherstellung validieren" im Feld "Auftragsname" einen Namen für den Validierungsauftrag ein oder übernehmen Sie den Standardnamen.

- Wählen Sie im Gruppenfeld "Backup-Satz-Auswahl" die gewünschten Backup-Sätze aus.

Element	Beschreibung
Verwenden Sie den neuesten datenträgerbasierten Backup-Satz, wenn der Auftrag ausgeführt wurde.	Gibt an, dass nur der neueste verfügbare datenträgerbasierte Backup-Satz verwendet wird, wenn der Auftrag zum Validieren des virtuellen VMware-Computers für die Wiederherstellung ausgeführt wird.
Datenträgerbasierten Backup-Satz auswählen	<p>Gibt an, dass ein verfügbarer datenträgerbasierter Backup-Satz für den Auftrag zum Validieren des virtuellen Hyper-V-Computers für die Wiederherstellung verwendet werden soll.</p> <p>Backup-Sätze anzeigen von</p> <p>Das Start- und Enddatum für die Backup-Sätze, die in die Auswahl aufgenommen werden sollen.</p> <p>Standardmäßig werden nur die Backup-Sätze für Aufträge angezeigt, die in den letzten 30 Tagen ausgeführt wurden.</p>
Datenträgerbasierter Backup-Satz	<p>Der Backup-Satz, der für die Validierung verwendet werden soll.</p> <p>In der Liste werden nur Backup-Sätze angezeigt, die die Validierungsanforderungen erfüllen.</p>

- Wählen Sie im Dialogfeld "Virtuellen Computer für die Wiederherstellung validieren" auf der linken Seite die Option "Ziel" und legen Sie dann die nachfolgenden Optionen für den Auftrag fest.

Element	Beschreibung
Hyper-V-Servername	Gibt den Namen des Hyper-V-Servers an, auf dem der virtuelle Computer erstellt werden soll. Hinweis: Sie können auch einen anderen als den Hyper-V-Quellserver auswählen.
Server-Login-Konto	Der Name des Login-Kontos, das für den Zugriff auf den Hyper-V-Server erforderlich ist.
Ziel für VC-Registrierung und Kontrollpunkt	Wählen Sie den Pfad auf dem Hyper-V-Host, wo die Konfigurationsdetails und die Kontrollpunktdatei (Differenzierender Datenträger) des validierten virtuellen Computers gespeichert sind.

- Wählen Sie im Dialogfeld "Virtuellen Computer für die Wiederherstellung validieren" auf der linken Seite die Option "Plan" und legen Sie dann die Planung für diesen Vorgang fest.

Element	Beschreibung
Wiederkehrend	Wählen Sie diese Option, um einen wiederkehrenden Zeitplan für den Auftrag zu erstellen.
Jetzt ohne wiederkehrenden Zeitplan ausführen	Führt den Auftrag sofort ohne wiederkehrenden Zeitplan aus.
Ausführen am	Plant den Auftrag, der für ein bestimmtes Datum und eine bestimmte Uhrzeit auszuführen ist.
Ohne Zeitplan erstellen	Erstellt den Auftrag, ohne ihn zu planen. Bei dieser Option wird der Auftrag nicht zum Zeitpunkt der Erstellung ausgeführt. Der Auftrag bleibt ungeplant, bis Sie ihn ausführen.
Auftrag in Wartestellung senden	Hiermit können Sie den Auftrag senden, aber erst nach dem Ändern des entsprechenden Wartestatus ausführen.

- 7 (Optional) Wählen Sie im Dialogfeld "Virtuellen Computer für die Wiederherstellung validieren" auf der linken Seite die Option "Benachrichtigung" und legen Sie dann die Empfänger fest, die benachrichtigt werden sollen, wenn der Auftrag zum Validieren des virtuellen VMware-Computers für die Wiederherstellung abgeschlossen ist.
- 8 Klicken Sie auf "OK".

Der Auftrag zum Validieren des virtuellen Computers wird ausgeführt. Nach erfolgreichem Abschluss ist der virtuelle Computer für die Wiederherstellung bereit.

Doppelklicken Sie zum Anzeigen des Validierungsstatus auf der Registerkarte "Backup und Wiederherstellung" auf den Hostnamen bzw. auf der Registerkarte "Speicher" auf den Namen des Speichers. Klicken Sie im linken Teilfenster auf "Backup-Sätze". Für die ausgewählte Server- bzw. Speicheransicht wird der Validierungsstatus angezeigt.

Fehlerbehebung bei Problemen mit Backup Exec Agent for Microsoft Hyper-V

Dieser Abschnitt enthält Strategien zur Problemlösung, die als Hilfestellung bei der Behebung von Problemen mit Backup Exec Agent for Microsoft Hyper-V dienen.

- Während des Backups eines virtuellen Linux-Computers schlägt die Erstellung von Snapshots möglicherweise fehl, wenn die Integrationsdienste nicht innerhalb des virtuellen Computers ausgeführt werden. Beziehen Sie sich für weitere Informationen auf die Microsoft-Dokumentation und vergewissern Sie sich, dass innerhalb des virtuellen Computers die aktuellen Integrationsdienste bereitgestellt und ordnungsgemäß ausgeführt werden.
- Möglicherweise treten "Zugriff verweigert"-Fehlermeldungen auf, wenn Sie für einen auf einem freigegebenen SMB- oder Scale-out-Dateiserver gehosteten virtuellen Computer eine Backup-Suche oder ein Backup durchführen. Dies kann daran liegen, dass das in Backup Exec zur Verfügung gestellte Login-Konto nicht auf den freigegebenen Server zugreifen kann.

Backup Exec Agent for Microsoft SQL Server

Dieser Anhang enthält folgende Themen:

- [Info zum Agent for Microsoft SQL Server](#)
- [Voraussetzungen für die Verwendung des SQL Agent](#)
- [Info zum Installieren des SQL Agent](#)
- [Backup-Strategien für SQL](#)
- [Hinzufügen von SQL-Servern zur Serverliste auf der Registerkarte "Backup und Wiederherstellung"](#)
- [Konfigurieren von Backup Exec zum Ausführen einer Konsistenzprüfung vor jedem SQL-Backup](#)
- [Verwendung der Snapshot-Technologie mit dem SQL Agent](#)
- [Verwenden von Datenbank-Snapshots für SQL-Server](#)
- [Sichern von SQL-Datenbanken und Transaktionsprotokollen](#)
- [SQL-Datenbanken und Transaktionsprotokolle wiederherstellen](#)
- [Notfallwiederherstellung von SQL Server](#)

Info zum Agent for Microsoft SQL Server

Mit Agent for Microsoft SQL Server (SQL Agent) können Netzwerkadministratoren Backup- und Wiederherstellungsvorgänge in SQL-Installationen im Netzwerk durchführen. Die SQL-Datenbank-Backups können in die Netzwerk-Backups ohne separate Verwaltung oder eigene Hardware integriert werden.

Der SQL Agent bietet Unterstützung für Folgendes:

- Datenbank-, Transaktionsprotokoll- und Differenzial-Backups sowie Datenbankwiederherstellung und -austausch.
- Eine automatisierte Wiederherstellung der Systemdatenbanken.
- Simplified Disaster Recovery, das die Notfallwiederherstellung von SQL-Servern automatisiert.
- Wiederherstellungen von SQL-Datenbanken an anderen Speicherorten.
- Hot-Backup-Kopien von SQL-Datenbanken während der Backup-Vorgänge. Diese Funktion ermöglicht Ihnen, eine Kopie der durch eine SQL-Datenbank an Medien versandten eigentlichen Datenströme zur späteren Verwendung zu einem lokalen Verzeichnis zu leiten.
- Backups von mehreren Instanzen
- Standby-Datenbank. Wenn der primäre SQL-Server ausfällt oder für Wartungszwecke heruntergefahren wird, kann eine weitere Datenbank als Standby-Datenbank online geschaltet werden.
- Datenbank-Konsistenzprüfungen (DBCC - Database Consistency Checks) für jeden Backup- und Wiederherstellungsauftrag, einschließlich einer weniger aufwändigen Datenbank-Konsistenzprüfung, wobei nur die physische Konsistenz der Datenbank geprüft wird.
- Unterstützung für die Wiederherstellungsmodelle FULL, BULK_LOGGED und SIMPLE. Beim Wiederherstellungsmodell SIMPLE werden Kopien der Transaktionen nicht in der Protokolldatei gespeichert und das Ausführen von Protokoll-Backups verhindert. Datenbanken können daher nur in den Zustand vor dem letzten Backup wiederhergestellt werden. Ein Wiederherstellen der Datenbank in den Zustand vor dem Eintreten des Notfalls oder eine Point-in-Time-Wiederherstellung ist nicht möglich.
- Wiederherstellungen von Transaktionsprotokollen zu einem bestimmten Zeitpunkt oder zu einem genannten Vorgang in einem Protokoll, wenn Protokollzeichen eingesetzt werden.
- Datenbank-Snapshots.
- Beibehalten der Replikationseinstellungen während umgeleiteter Wiederherstellungsaufträge.
- Überprüfung nur von Wiederherstellungsaufträgen, die sowohl die Gültigkeit der auf dem Medium befindlichen SQL-Daten bestimmen, als auch die Möglichkeit der Ziel-SQL-Datenbank festzustellen, diese Daten zu akzeptieren, bevor die Datenbank während eines Wiederherstellungsauftrags gelöscht oder überschrieben wird.

- Sichern mit Prüfsummenerzeugung. Diese Option wird als Redundanzüberprüfung angewendet und arbeitet mit der Option "Nur Überprüfung von Wiederherstellungsauftrag".
- Fortsetzen von Wiederherstellungsaufträgen, wenn Fehler festgestellt werden. Diese Funktion ermöglicht Ihnen, von einem beschädigten Datenbank-Backup so viele Daten wie möglich wiederherzustellen.
- Einmalige Kopier-Backup-Aufträge, mit denen Sie eine Datenbank kopieren können, ohne die Wiederherstellungsabfolge (vollständig, differenzial, Protokoll) zu beeinträchtigen.
- In SQL Server 2008 oder höheren Versionen, die Komprimierung unterstützen, können Sie SQL-Softwarekomprimierung für Backup-Aufträge verwenden.

Informationen zu den Best Practices zum Einsatz des Backup Exec Agent for Microsoft SQL Server (SQL Agent) finden Sie unter *Best Practices für Backup Exec*.

Siehe ["Info zum Installieren des SQL Agent"](#) auf Seite 1221.

Voraussetzungen für die Verwendung des SQL Agent

Folgende Voraussetzungen müssen für den SQL Agent erfüllt sein:

- Backup Exec muss über die Zugriffsrechte zum Lesen der beiden folgenden SQL-Registrierungsschlüssel verfügen:
 - HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server
 - HKEY_LOCAL_MACHINE\Software\Microsoft\mssqlserverWenn Backup Exec nicht auf diese Registrierungsschlüssel zugreifen kann, schlägt die Wiederherstellung im Standardverzeichnis u. U. fehl, und die Option "Wiederherstellung der Systemdatenbank automatisieren" im SQL-Dialogfeld "Wiederherstellungsauftrag - Eigenschaften" funktioniert nicht.
Um sicherzustellen, dass Backup Exec über Zugriffsrechte verfügt, überprüfen Sie, ob das verwendete Login-Konto Administratorrechte für den Windows-Server hat, auf dem die SQL-Instanz installiert ist.
- Der Backup Exec-Server muss Zugriff auf die SQL-Installation haben.
- Den im Backup Exec-Login-Konto gespeicherten Login-Daten für das Backup und Wiederherstellung von SQL muss für die SQL-Instanz die Rolle des Systemadministrators zugewiesen sein.
Wenden Sie das Login bei der Überprüfung auf den Windows-Server an, auf dem SQL installiert ist, und nicht auf die tatsächliche SQL-Instanz.

Hinweis: SQL Server-Anmeldedaten werden nicht unterstützt.

- Agent for Windows muss auf allen SQL-Remote-Servern installiert sein, die Sie sichern möchten.
- Aufträge, die Standardinstanzen von SQL Server sichern bzw. wiederherstellen, schlagen eventuell fehl, es sei denn Sie aktualisieren auf Agent for Windows Version 2012 oder höher auf dem Computer, der die SQL-Serverinstanz enthält. Sie können auch die ausgewählten Backup-Aufträge bearbeiten und die SQL Server-Instanz aus der Registerkarte "Auswahldetails" löschen. Wählen Sie anschließend auf der Registerkarte "Durchsuchen" die SQL Server-Instanz aus.

Anforderungen an das jeweilige Betriebssystem und die für den SQL Agent unterstützten Service Packs finden Sie in der Liste der mit Backup Exec kompatiblen Software.

Siehe ["Testen von Login-Konten"](#) auf Seite 775.

Siehe ["Backup Exec-Login-Konten"](#) auf Seite 762.

Info zum Installieren des SQL Agent

Der SQL Agent wird als Teil des Agent for Applications and Databases installiert und kann lokale oder Remote-SQL Server-Datenbanken schützen.

Siehe ["Installieren zusätzlicher Agents und Funktionen auf dem lokalen Backup Exec-Server"](#) auf Seite 66.

Backup-Strategien für SQL

Backup Exec steht für versteckten Online-Datenbankschutz für SQL als Teil täglicher Backup-Routine, wodurch die Wiederherstellungschancen erhöht und Datenverluste minimiert werden, ohne die täglichen Datenbankaktivitäten zu stören. Die Verwendung von Datenbank-, Differenzial- und Protokoll-Backups bietet ein optimales Gleichgewicht zwischen den einzelnen Backup-Methoden und minimiert nach einem Notfall die zum Wiederherstellen einer Datenbank benötigte Zeit.

Berücksichtigen Sie die folgenden Aspekte bei der Entscheidung über die Backup-Methode für den besten Datenschutz in typischen Umgebungen:

- Führen Sie in Kleinbüros jeden Abend ein vollständiges Datenbank-Backup und täglich Transaktionsprotokoll-Backups aus.
- Führen Sie in mittelgroßen Umgebungen wöchentlich ein vollständiges Datenbank-Backup und täglich Transaktionsprotokoll-Backups sowie außer an

dem Tag, an dem das vollständige Backup ausgeführt wird, tägliche Differenzial-Backups aus.

- In größeren Umgebungen sollten Differenzial-Backups von Datenbanken täglich, vollständige Backups wöchentlich und Transaktionsprotokoll-Backups nach Bedarf ausgeführt werden. Viele Firmen führen einmal wöchentlich vollständige Backups durch, wobei während der Woche Differenzial-Backups vorgezogen werden, um die Dauer des Backups auf ein Minimum zu beschränken.

Dem Zeitgewinn durch weniger vollständige Backups und mehr Differenzial-Backups steht die längere Wiederherstellungszeit gegenüber, wenn Daten unter Verwendung eines vollständigen Datenbank-Backups, des letzten Differenzial-Datenbank-Backup sowie allen nach dem letzten Differenzial-Datenbank-Backup erstellten Protokoll-Backups wiederhergestellt werden müssen.

Die für Sie beste Lösung hängt von der Größe der jeweiligen Umgebung, der Anzahl der pro Tag verarbeiteten Transaktionen und von den Anforderungen Ihrer Benutzer im Fall einer Wiederherstellung ab.

Berücksichtigen Sie beim Entwickeln einer SQL-Backup-Strategie folgende Aspekte:

Tabelle E-1 Empfehlungen für das Backup von SQL

SQL-Backup-Strategien	Beschreibung
Schützen Sie den gesamten SQL-Server.	Um sicherzustellen, dass SQL vollständig geschützt wird, sichern Sie regelmäßig die folgenden Elemente: <ul style="list-style-type: none">■ Das Systemlaufwerk, auf dem SQL installiert ist.■ Die Windows-Registrierung sowie den Systemstatus.■ Transaktionsprotokolle.
Führen Sie beim Aktualisieren neue vollständige Datenbank-Backups aus.	Führen Sie beim Aktualisieren von SQL neue vollständige Datenbank-Backups aus. Sie können u. U. Backups von einer Version oder einer SQL-Service Pack-Version zu anderen Versionen nicht wiederherstellen.
Führen Sie Konsistenzprüfungen vor Backups aus.	Es wird empfohlen, vor einem Backup Konsistenzprüfungen auszuführen. Wenn Datenbanken oder Transaktionsprotokolle zum Zeitpunkt des Backups Fehler enthalten, werden diese auch bei der Wiederherstellung übernommen, sofern eine Wiederherstellung überhaupt möglich ist. Siehe "Konfigurieren von Backup Exec zum Ausführen einer Konsistenzprüfung vor jedem SQL-Backup" auf Seite 1224.

Hinzufügen von SQL-Servern zur Serverliste auf der Registerkarte "Backup und Wiederherstellung"

SQL Server Backup-Strategien	Beschreibung
Sichern Sie Ihre Systemdatenbanken regelmäßig.	<p>Sichern Sie die Master-Datenbank und die installierten Service Packs nach allen Vorgängen, bei denen Informationen in der Datenbank geändert werden, besonders nach folgenden Vorgängen:</p> <ul style="list-style-type: none"> ■ Erstellen neuer Datenbanken ■ Hinzufügen von Dateien zu einer bereits vorhandenen Datenbank ■ Hinzufügen oder Ändern von Benutzernamen oder Kennwörtern <p>Wenn Änderungen nicht gesichert werden, bevor die Master-Datenbank wiederhergestellt werden muss, gehen die Änderungen verloren.</p>
Führen Sie jeweils nur ein Backup aus.	Planen Sie nicht die gleichzeitige Ausführung mehrerer Backups einer Datenbank oder ihres Transaktionsprotokolls.
Sichern Sie Transaktionsprotokolle von Datenbanken, die für die vollständige Wiederherstellung konfiguriert sind.	Sichern Sie Transaktionsprotokolle von Datenbanken, da die Transaktionsprotokolle immer größer werden, wenn Sie sie nicht sichern.

Hinzufügen von SQL-Servern zur Serverliste auf der Registerkarte "Backup und Wiederherstellung"

Auf der Registerkarte "Backup und Wiederherstellung" können Sie SQL-Server zur Serverliste hinzufügen, um die SQL-Datenbanken für ein Backup auszuwählen.

Hinzufügen von SQL-Servern zur Serverliste auf der Registerkarte "Backup und Wiederherstellung"

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" unter "Server und virtuelle Hosts" auf "Hinzufügen".
- 2 Wählen Sie "Microsoft Windows-Computer und -Server", und klicken Sie dann auf "Weiter".
- 3 Mit Hilfe des Assistenten "Server hinzufügen" fügen Sie den SQL-Server der Serverliste in der Registerkarte "Backup und Wiederherstellung" hinzu.

Siehe ["Serverliste auf der Registerkarte "Backup und Wiederherstellung"](#) auf Seite 166.

Konfigurieren von Backup Exec zum Ausführen einer Konsistenzprüfung vor jedem SQL-Backup

Wenn Sie Datenbanken oder Transaktionsprotokolle mit Fehlern sichern, bestehen diese Fehler nach der Wiederherstellung des Backups weiter. In einigen Fällen kann dies eine erfolgreiche Wiederherstellung verhindern. Backup Exec ermöglicht es Ihnen, die logische und physische Konsistenz der Daten vor und nach einem Backup zu prüfen. Fehler bei der Konsistenzprüfung werden von SQL im Backup Exec-Auftragsprotokoll aufgezeichnet. Es wird dringend empfohlen, vor jedem Backup eine Konsistenzprüfung durchzuführen.

Standardmäßig ist die Backup-Auftrag-Standardoption "Konsistenzprüfung vor dem Backup" für "" aktiviert.

Bei der Konsistenzprüfung von Backup Exec werden die folgenden SQL Server-Dienstprogramme für die Konsistenzprüfung eingesetzt:

- CHECKDB
- CHECKCATALOG
- PHYSICAL_ONLY

CHECKDB, CHECKCATALOG, NEWALLOC und PHYSICAL_ONLY werden für Datenbanken betreffende Vorgänge eingesetzt.

Weitere Informationen zu diesen Dienstprogrammen finden Sie in der Microsoft SQL-Dokumentation.

So führen Sie eine Konsistenzprüfung vor einem SQL-Backup aus

- 1 Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und dann "Auftragsstandardeinstellungen".
- 2 Wählen Sie einen Backup-Auftragstyp aus.

Beispiel: Wenn Sie die Standardoptionen für SQL Server einrichten möchten, wählen Sie "Backup-to-Disk". Die verfügbaren Optionen hängen vom Typ der konfigurierten Speichergeräte ab. Sie können verschiedene Standardoptionen für die Backup-Aufträge konfigurieren, die Sie an verschiedene Speichergerätetypen senden.
- 3 Klicken Sie im Dialogfeld "Standardeinstellungen für Backup-Auftrag" im linken Teilfenster auf "Microsoft SQL".
- 4 Im Feld "Konsistenzprüfung vor dem Backup" muss eine Konsistenzprüfung aktiviert sein.
- 5 Klicken Sie auf "OK".

Siehe ["Sichern von SQL-Datenbanken und Transaktionsprotokollen"](#) auf Seite 1228.

Verwendung der Snapshot-Technologie mit dem SQL Agent

Backup Exec nutzt standardmäßig die Snapshot-Technologie für SQL-Server-Backups. Der SQL Agent unterstützt vollständige Snapshot-Backups unter Verwendung des Volumenschattenkopie-Diensts (VSS) von Microsoft. Dieser Snapshot-Provider-Dienst ist nur für Windows 2008 oder höher verfügbar. Die Nutzung der Snapshot-Technologie kann die Wiederherstellungszeit und die Backup-Leistung auf dem Server reduzieren.

Wenn ein Backup-Auftrag gesendet wird, der die Snapshot-Technologie verwendet, wird von jedem Datenträger ein Snapshot erstellt. Damit wird eine Aufzeichnung der Daten zu einem bestimmten Zeitpunkt bereitgestellt. Backup Exec verwendet die Snapshots, um vorübergehend die Schreibaktivität auf einem Datenträger zu unterbrechen, um den Snapshot zu erstellen. Die Daten werden von den Snapshots gesichert, und danach werden die Snapshots gelöscht.

Hinweis: Verwenden Sie die Snapshot-Technologie mit Aufträgen, die Deduplizierungsgeräte verwenden.

Vor der Verwendung der Snapshot-Technologie mit dem SQL Agent beachten Sie folgende Informationen:

- Bei der Snapshot-Technologie wird eine Momentaufnahme der SQL-Datenbank als sogenannter "Snapshot" erstellt und anschließend gesichert. Die eigentliche SQL-Datenbank bleibt geöffnet und für Benutzer verfügbar.
- SQL-Backups, die die Snapshot-Technologie verwenden, sind deutlich größer als normale SQL-Backups (auch bekannt als Streaming-Backups).
- Es wird dringend empfohlen, vor dem Backup eine Konsistenzprüfung durchzuführen.
Siehe ["Konfigurieren von Backup Exec zum Ausführen einer Konsistenzprüfung vor jedem SQL-Backup"](#) auf Seite 1224.
- Der SQL Agent unterstützt nur vollständige Snapshot-Backups. Transaktionsprotokoll- und Differenzial-Snapshots werden nicht unterstützt.
- Mit dem SQL Agent sind Snapshots und Streaming-Backups beim Wiederherstellen von SQL-Daten zueinander kompatibel.
- Die Durchführung von Datenbankkonsistenzprüfungen vor und nach Backups hat Auswirkungen auf die Dauer der Backup-Aufträge.

Die folgenden SQL-Backup-Optionen sind nicht mit Snapshot-Backups unterstützt:

- Prüfsummen auf Backups anwenden (SQL 2005 oder höher)

Diese Option wird als Redundanzprüfung verwendet und funktioniert mit der Wiederherstellungsoption Nur überprüfen, Daten nicht wiederherstellen.

- SQL Server 2008 Enterprise Edition-Softwarekomprimierung
- Von SQL-Backups Datenträgerkopien erstellen und auf dem SQL-Server ablegen, auf dem sich die Datenbank befindet

Hinweis: Microsoft Virtual Shadow Copy Service-Snapshots (VSS) sind nicht das gleiche wie SQL-Datenbank-Snapshots. VSS-Snapshots ermöglichen das Erstellen von Point-in-Time-Snapshots von Datenträgern und Freigaben, wohingegen Datenbank-Snapshots das Erstellen von Point-in-Time-Kopien von SQL-Datenbanken ermöglichen.

Siehe "[Verwenden von Datenbank-Snapshots für SQL-Server](#)" auf Seite 1226.

Verwenden von Datenbank-Snapshots für SQL-Server

Mit SQL-Datenbank-Snapshots können Sie eine Datenbank schnell in den Zustand zurückversetzen, in dem sie sich zum Zeitpunkt der Snapshot-Erstellung befand. Wenn Sie einen Datenbank-Snapshot verwenden, ist keine vollständige Wiederherstellung der Host-Datenbank erforderlich, um die Datenbank zurückzusetzen. Beachten Sie jedoch, dass Änderungen, die zwischen der Erstellung des Datenbank-Snapshots und dem Zeitpunkt der Zurücksetzung vorgenommen werden, nicht berücksichtigt werden.

Backup Exec SQL Agent verwendet die SQL-Datenbank zum Erstellen von Datenbank-Snapshots, d. h. schreibgeschützte Zeitpunktkopien einer vorhandenen Host-Datenbank. Führt Backup Exec einen SQL-Backup-Auftrag unter Verwendung der Backup-Methode Datenbank-Snapshot aus, wird an die Host-Datenbank eine Anfrage mit der Aufforderung zur Erstellung eines Datenbank-Snapshot gesendet.

Hinweis: Die Snapshot-Backup-Methode für SQL-Datenbanken wird nur von SQL Server Enterprise Edition unterstützt.

Datenbank-Snapshots können nicht auf Speichermedien gesichert werden. Sie werden stattdessen in eine SQL-Snapshot-Datei auf dem Datenträger geschrieben. Nach Abschluss des Datenbank-Snapshot-Auftrags erstellt Backup Exec Verlaufs- und Auftragsprotokollinformationen, die den Status des Auftrags angeben.

Da Datenbank-Snapshots nicht gesichert werden können, gehen alle Datenbank-Snapshots verloren, wenn der Datenträger, auf dem sich die

Host-Datenbank befindet, ausfällt. Ihre Datenbankschutzstrategie sollte daher nicht nur aus Datenbank-Snapshots bestehen. Vielmehr sollten diese Teil einer umfassenden Backup Exec-Datenbankschutzstrategie sein, die vollständige, differenzielle und Transaktionsprotokoll-Backups der SQL-Datenbank umfasst.

Informationen dazu finden Sie in der Microsoft SQL-Dokumentation.

Hinweis: SQL-Datenbank-Snapshots sind nicht das Gleiche wie Microsoft Virtual Shadow Copy Service-Snapshots (VSS). VSS-Snapshots ermöglichen das Erstellen von Point-in-Time-Snapshots von Datenträgern und Freigaben, wohingegen Datenbank-Snapshots das Erstellen von Point-in-Time-Kopien von SQL-Datenbanken ermöglichen.

Hinweis: Informationen zu gelöschten SQL-Datenbank-Snapshots wird regelmäßig aus den Katalogen entfernt. Bei erneuter Katalogisierung eines Backup-Mediums werden die Kataloginformationen zu Datenbank-Snapshots ebenfalls regelmäßig entfernt.

Datenbank-Snapshots für SQL Server, die mit Backup Exec erstellt wurden, ermöglichen ein Zurücksetzen einer SQL-Datenbank auf den Zustand zu einem früheren Zeitpunkt, ohne dass ein vollständiger Datenbankwiederherstellungs-Auftrag ausgeführt werden muss.

Wenn Sie SQL-Datenbank-Snapshots in der Ressourcenansicht des Wiederherstellungsassistenten anzeigen, werden sie als Backup-Sätze und in chronologischer Reihenfolge (neuester Snapshot zuerst) dargestellt.

Beim Zurücksetzen von Datenbanken ist Folgendes zu beachten:

- Sie können eine SQL-Datenbank, die zurückgesetzt wurde, nicht rückgängig machen.
- Vor dem Zurücksetzen der Datenbank löscht Backup Exec alle vorhandenen Datenbank-Snapshots, mit Ausnahme des für die Zurücksetzung verwendeten Snapshot. Nach dem Löschen können die Datenbank-Snapshots nicht wiederhergestellt werden.
- Datenbank-Snapshot-Wiederherstellungsaufträge können nicht umgeleitet werden.

Sichern von SQL-Datenbanken und Transaktionsprotokollen

Backup Exec schließt drei Methoden für das Unterstützen von Datenbanken ein: Vollständig, Differenziell und Nur vollständige Kopie. Bei vollständigen Backups wird die gesamte Datenbank samt Systemtabellen gesichert. Beim Differenzial-Backup werden nur die seit dem letzten vollständigen Backup an der Datenbank vorgenommenen Änderungen gesichert. Das Kopier-Backup funktioniert wie das vollständige Backup, nur dass es sich nicht auf zukünftige Differenzial- oder Protokoll-Backups auswirkt.

Differenzial-Backups sind weniger umfangreich und damit schneller als vollständige Backups und können aus diesem Grunde häufiger durchgeführt werden. Da Differenzial-Backups nur eine Wiederherstellung des zum Zeitpunkt des Differenzial-Backups vorliegenden Systemzustands ermöglichen, sollten Sie nach der Erstellung eines Differenzial-Backups zusätzlich mehrere Protokoll-Backups erstellen. Mit Transaktionsprotokoll-Backups können Sie die Datenbank bis genau zum Eintreten des Fehlers wiederherstellen.

Verwenden Sie Differenzial-Backups bei nur relativ wenigen Datenänderungen zwischen vollständigen Backups oder bei häufigen Änderungen derselben Daten. Differenzial-Backups arbeiten u. U. auch einwandfrei in Ihrer Umgebung, wenn Sie das Wiederherstellungsmodell SIMPLE verwenden und Backups häufiger benötigen, Sie jedoch nicht über die notwendige Zeit für regelmäßige vollständige Backups verfügen. Wenn Sie die Wiederherstellungsmodelle FULL oder BULK_LOGGED verwenden, können Sie mithilfe von Differenzial-Backups die Zeitdauer verringern, die zum Implementieren von Protokoll-Backups beim Wiederherstellen einer Datenbank erforderlich ist.

Wenn Sie nur Datenbank-Backups anstelle einer Mischung aus Datenbank- und Protokoll-Backups ausführen möchten, verwenden Sie das einfache Wiederherstellungsmodell für die Datenbank, damit das Transaktionsprotokoll automatisch abgeschnitten wird, wenn ein Kontrollpunkt in der Datenbank auftritt. Dadurch wird ein Überfüllen der Transaktionsprotokolle verhindert, da mit anderen Wiederherstellungsmodellen die Protokolle nach einem Datenbank-Backup nicht gelöscht werden.

Beim Wiederherstellungsmodell SIMPLE werden Kopien der Transaktionen nicht in der Protokolldatei gespeichert und das Ausführen von Protokoll-Backups verhindert.

Wenn Sie keine Transaktionsprotokoll-Backups ausführen möchten, können die Datenbanken nur in den Zustand vor dem letzten Backup wiederhergestellt werden. Ein Wiederherstellen der Datenbank in den Zustand vor dem Eintreten des Fehlers oder zu einem anderen bestimmten Zeitpunkt ist nicht möglich.

Systemdatenbanken können nur mithilfe des vollständigen Backups gesichert werden; die Protokoll- bzw. Differenzialverfahren können nicht für das Master-Datenbank-Backup verwendet werden.

Hinweis: Sie können Datenbanken nicht auf Speicher sichern, die an einem Computer angehängt sind, auf dem Remote Media Agent for Linux Server installiert ist.

Der SQL Agent unterstützt eine gespiegelte SQL-Datenbankkonfiguration, obgleich Microsoft die folgenden Beschränkungen auf die Spiegelung der SQL-Datenbanken anwendet:

- Sie können eine gespiegelte SQL-Datenbank nicht sichern oder wiederherstellen. Wenn Sie versuchen, eine gespiegelte Datenbank zu sichern oder wiederherzustellen, schlägt der Backup-Auftrag oder der Wiederherstellungsauftrag fehl.
- Sie können die primäre SQL-Datenbank nicht wiederherstellen, während sie in einer gespiegelten Konfiguration konfiguriert ist. Um die primäre SQL-Datenbank wiederherzustellen, müssen Sie die Datenbank-Spiegelung der primären Datenbank beenden.
- Sie können eine primäre SQL-Datenbank und deren Transaktionsprotokolle nur sichern, wenn der Backup-Auftrag die Datenbank nicht in einem nicht-wiederhergestellten Zustand lässt.

Sie können Standardoptionen für Backup-Aufträge für alle SQL-Backup-Aufträge festlegen. Bei der Erstellung jedes Backup-Auftrags verwendet dieser die Standardoptionen, sofern Sie die Optionen für diesen bestimmten Auftrag nicht ändern.

Automatischer Ausschluss von SQL-Daten bei Backups auf Datenträgerebene

Wenn Sie einen Datenträger auswählen, der SQL-Daten zum Sichern enthält, wird vom SQL Agent festgelegt, welche SQL-Daten bei einem Backup auf Datenträgerebene nicht berücksichtigt werden sollen. So sollten beispielsweise MDF- und LDF-Dateien nicht Teil des Backups sein, da das SQL-System diese exklusiv geöffnet hat. Diese Dateien werden automatisch von der Funktion "Ausschließen aktiver Dateien" vom Backup ausgeschlossen. Wenn der Ausschluss nicht während eines Backup ohne Snapshots erfolgte, werden die Dateien als "Wird gerade benutzt – übersprungen" angezeigt. Wenn der Ausschluss nicht während eines Snapshot-Backups erfolgte, kann dies zu einem inkonsistenten Sichern der Daten und zu Wiederherstellungsproblemen führen.

Wenn Sie einem Backup auf Datenträgerebene dennoch SQL-Daten hinzufügen möchten, müssen Sie die zu sichernde Datenbank zunächst entladen. Führen Sie anschließend den Backup-Auftrag aus.

Sichern von SQL-Clustern

Sie müssen möglicherweise Ressourcencontainer für SQL-Cluster manuell hinzufügen, bevor Sie die Datenbanken sichern können:

Zum Hinzufügen von Ressourcencontainern installieren Sie Agent for Windows auf den physischen Cluster-Knoten. Wird der Ressourcencontainer für den virtuellen SQL-Server nicht automatisch erkannt, verwenden Sie den Assistenten "Server hinzufügen", um den virtuellen Ressourcencontainer für den virtuellen SQL-Clusterknoten hinzuzufügen. Wenn Sie den Assistenten "Server hinzufügen" ausführen, deaktivieren Sie die Option "Agent for Windows aktualisieren", da dieser bereits installiert ist. Treffen Sie dann eine Backup-Auswahl aus dem hinzugefügten virtuellen Ressourcencontainer.

Sichern von SQL-Transaktionsprotokollen

Beim Ausführen von Backups von Protokollen sollten Sie Backup Exec ausschließlich für das Backup von Transaktionsprotokollen verwenden.

Backup Exec enthält zwei Methoden für das Backup von Transaktionsprotokollen: "Protokoll" und "Protokoll nicht kürzen".

Wenden Sie die Methode "Protokoll nicht kürzen" nur dann an, wenn die Datenbank beschädigt ist oder Datenbankdateien fehlen. Mit dieser Methode werden Transaktionen gesichert, auf die Sie u. U. sonst nicht zugreifen können, wenn sich die Datenbank in diesem Zustand befindet. Verwenden Sie bei einer Datenbankwiederherstellung dieses Transaktionsprotokoll-Backup gemeinsam mit einem Datenbank-Backup oder einer anderen vorher genannten Backup-Methode für Transaktionsprotokolle, bis Sie zu dem Punkt gelangen, an dem diese fehlgeschlagen sind. Nicht reservierte Transaktionen werden jedoch automatisch zurückgesetzt. Reservierte Transaktionen werden beim Verwenden der Methode "Protokoll nicht kürzen" nach dem Protokoll-Backup nicht gelöscht.

Um "Protokoll nicht kürzen" zur Wiederherstellung einer Datenbank zu verwenden, sollten Sie über ein Datenbank-Backup verfügen, die vor dem Backup mit "Protokoll nicht kürzen" erstellt wurde. Im Transaktionsprotokoll befinden sich nur die bei der Wiederherstellung verwendeten Protokolldateien, die zur vollständigen Wiederherstellung einer Datenbank nicht ausreichen. Sie benötigen mindestens ein Datenbank-Backup und ein Protokoll-Backup der Datenbank, um die Datenbank wiederherzustellen.

Vorsicht: Verwenden Sie für ein Backup von Protokolldateien keine dieser Methoden, wenn die SQL-Datenbank ein einfaches Wiederherstellungsmodell nutzt. Mit dem Wiederherstellungsmodell SIMPLE können Sie Daten nur bis zum letzten vollständigen bzw. Differenzial-Backup wiederherstellen. Wenn Sie ein Protokoll-Backup einer Datenbank mit dem einfachen Wiederherstellungsabschlussstatus verwenden, wird das Backup mit Ausnahmen abgeschlossen.

Um die Datenbankeigenschaften zu prüfen, klicken Sie unterhalb der Datenbankverwaltungstools auf dem SQL-Server mit der rechten Maustaste auf die Datenbank. Klicken Sie dann auf "Eigenschaften" und auf die Registerkarte "Optionen", und zeigen Sie die Konfigurationseinstellungen an.

Sichern von SQL-Datenbanken und Transaktionsprotokollen

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" mit der rechten Maustaste auf einen SQL-Server und klicken Sie dann mit der rechten Maustaste auf die Auswahl.

Um mehrere Server auszuwählen, klicken Sie bei gedrückter Umschalttaste oder Strg-Taste auf die Servernamen und klicken Sie dann mit der rechten Maustaste auf einen der ausgewählten Server.

- 2 Wählen Sie "Backup" und anschließend den Typ des durchzuführenden Backups aus.
- 3 Klicken Sie im Dialogfeld "Eigenschaften der Backup-Definition" im Feld "Auswahl" auf "Bearbeiten".
- 4 Aktivieren Sie im Dialogfeld "Backup-Auswahl" die Kontrollkästchen für die zu sichernden Ressourcen, und heben Sie die Markierung der Kontrollkästchen für die Quellen auf, nach denen nicht gefiltert werden soll.

Hinweis: Sie können die zu sichernden SQL-Datenbanken auf der Registerkarte "Durchsuchen" auswählen. Im rechten Teilfenster des Dialogfeldes "Backup-Auswahl", können Sie Name, Größe, Typ, Änderungszeit und Attribute für die Auswahl anzeigen. Die Attribute liefern den Status der Datenbank. Wenn es also Probleme gibt, können Sie diese lösen, bevor Sie den Backup-Auftrag ausführen. Sie können auch über die Registerkarte "Auswahldetails" bestimmte Dateien oder Dateitypen einschließen bzw. ausschließen.

- 5 Klicken Sie auf "OK".
- 6 Klicken Sie im Dialogfeld "Eigenschaften der Backup-Definition" im Feld "Backup" auf "Bearbeiten".

- 7 Wählen Sie im Dialogfeld "Backup-Optionen" einen Zeitplan für diesen Auftrag.
- 8 Wählen Sie im Dialogfeld "Backup-Optionen" ein Speichergerät für diesen Auftrag.
- 9 Wählen Sie im Dialogfeld "Backup-Optionen" im linken Teilfenster "Microsoft SQL".
- 10 Legen Sie eine der folgenden Optionen für diesen Auftrag fest:

Backup-Methode

Wählen Sie eine der folgenden Backup-Methoden aus, die Sie für diesen Auftrag anwenden möchten:

- Vollständig - Datenbanken sichern
Diese Option sichert die gesamte Datenbank. Dies ist die Standardeinstellung.
- Vollständige Kopie - Datenbanken (Kopie) sichern
Diese Option sichert die gesamte Datenbank, ohne Auswirkung auf zukünftige Differenzial- oder Protokoll-Backups.
Anders als bei vollständigen Backups wird bei der Methode "Vollständig kopieren" der Basis-Backup-Satz für Differenzial-Backups nicht zurückgesetzt. Dieser gibt die seit dem letzten vollständigen Backup geänderten Datenblöcke an.
Nach einem vollständigen Backup können Sie mit der Backup-Methode "Vollständig kopieren" eine Kopie der SQL-Datenbank erstellen, ohne dass sich dies auf den für zukünftige Differenzial-Backups erforderlichen Basis-Backup-Satz auswirkt.

Backup-Methode

Wählen Sie eine der folgenden SQL-spezifischen Backup-Methoden aus, die Sie für diesen Auftrag anwenden möchten:

- **Vollständig - Datenbanken sichern**
 Diese Option sichert die gesamte Datenbank. Dies ist die Standardeinstellung.
- **Vollständige Kopie - Datenbanken (Kopie) sichern**
 Diese Option sichert die gesamte Datenbank, ohne Auswirkung auf zukünftige Differenzial- oder Protokoll-Backups.
 Anders als bei vollständigen Backups wird bei der Methode "Vollständig kopieren" der Basis-Backup-Satz für Differenzial-Backups nicht zurückgesetzt. Dieser gibt die seit dem letzten vollständigen Backup geänderten Datenblöcke an.
 Nach einem vollständigen Backup können Sie mit der Backup-Methode "Vollständig kopieren" eine Kopie der SQL-Datenbank erstellen, ohne dass sich dies auf den für zukünftige Differenzial-Backups erforderlichen Basis-Backup-Satz auswirkt.
- **Automatisch: Transaktionsprotokoll sichern, wenn aktiviert und dann Datenbankänderungen seit dem letzten vollständigen oder inkrementellen Backup sichern**
 Mit dieser Option können Sie die gesamte SQL-Instanz sichern, auch wenn einige Datenbanken keine Protokoll-Backups unterstützen. Alle Datenbanken werden unter Verwendung des inkrementellen Backups (Blockebene) gesichert. Darüber hinaus werden die Datenbanken, die Protokoll-Backups unterstützen, mit dem Protokoll-Backup gesichert.
Hinweis: Wenn Snapshot nicht aktiviert wird, kann kein inkrementelles Backup (Blockebene) durchgeführt werden. Stattdessen wird das Differenzial-Backup verwendet.
- **Protokoll - Transaktionsprotokoll sichern und kürzen**
 Diese Option sichert nur die Daten, die im Transaktionsprotokoll enthalten sind. Sie sichert keine Datenbankdaten. Nach dem Sichern des Transaktionsprotokolls werden reservierte Transaktionen entfernt (abgeschnitten).
 Wenn die Datenbanken für das einfache SQL Server-Wiederherstellungsmodell konfiguriert sind, werden Backups von Protokolldateien nicht unterstützt.

Um das Wiederherstellungsmodell zu ändern, verwenden Sie die SQL-Administrationstools, um das Wiederherstellungsmodell auf "Vollständig" festzulegen. Sie sollten ein neues vollständiges Backup ausführen, wenn Sie den Wiederherstellungsmodus ändern, bevor ein Backup von Protokolldateien ausgeführt wird.

Alternativ können Sie nur vollständige Backups ausführen oder vollständige und Differenzial-Backups der SQL-Datenbanken ausführen.

Siehe ["Konfigurieren von Backup Exec zum Ausführen einer Konsistenzprüfung vor jedem SQL-Backup"](#) auf Seite 1224.

- **Protokoll nicht kürzen - Sichern ohne Kürzen des Transaktionsprotokolls**
 Diese Option sichert die Datenbank, wenn sie beschädigt ist oder Datenbankdateien fehlen. Da bei dem Verfahren "Protokoll nicht kürzen" nicht auf die Datenbank zugegriffen wird, können Sie weiterhin Transaktionen sichern, auf die Sie sonst eventuell keinen Zugriff hätten. Verwenden Sie bei einer Datenbankwiederherstellung dieses Transaktionsprotokoll-Backup gemeinsam mit einem Datenbank-Backup oder einer anderen vorher genannten Backup-Methode für Transaktionsprotokolle, bis Sie zu dem Punkt gelangen, an dem diese fehlgeschlagen sind. Nicht durchgeführte Transaktionen werden jedoch automatisch zurückgesetzt. Durchgeführte Transaktionen werden beim Verwenden der Methode "Protokoll nicht kürzen" nach dem Protokoll-Backup nicht gelöscht.
- **Differenziell – Datenbankänderungen seit dem letzten vollständigen Backup sichern**
 Diese Option sichert nur die Änderungen, die an der Datenbank oder Dateigruppe seit dem letzten vollständigen Backup vorgenommen wurden. Da Differenzial-Backups nur eine Wiederherstellung des zum Zeitpunkt des Differenzial-Backups vorliegenden Systemzustands ermöglichen, sollten Sie nach der Erstellung eines Differenzial-Backups zusätzlich mehrere Protokoll-Backups erstellen.

- Differenziell (Blockebene) - Änderungen an der Datenbank seit dem letzten vollständigen Backup sichern - zusammen mit Auftrag zum Konvertieren in virtuellen Computer
 Diese Option sichert alle Datenblöcke und Protokolle, die seit dem letzten vollständigen Backup erstellt oder geändert wurden.
- Inkrementell (Blockebene): Änderungen an der Datenbank seit dem letzten vollständigen oder inkrementellen Backup sichern - zusammen mit Auftrag zum Konvertieren in virtuellen Computer
 Diese Option sichert alle Datenblöcke und Protokolle, die seit dem letzten vollständigen oder inkrementellen Backup erstellt oder geändert wurden.
- Datenbank-Snapshot - schreibgeschützte Zeitpunktkopie von Datenbanken
 Diese Option erstellt eine schreibgeschützte Kopie einer anderen Datenbank zu einem bestimmten Zeitpunkt.
 Siehe ["Verwenden von Datenbank-Snapshots für SQL-Server"](#) auf Seite 1226.

Hinweis: Differenzielle oder inkrementelle SQL-Backups werden nur für die Konvertierung in virtuelle Computer unterstützt, wenn Sie die Backup-Methoden "Automatisch", "Differenzial (Blockebene)" oder "Inkrementell (Blockebene)" verwenden.

Zusätzlich führt Backup Exec ein vollständiges Backup aus, wenn Sie die Backup-Methoden "Automatisch" oder "Protokoll" auswählen, wenn vorher auf die Datenbank kein vollständiges Backup ausgeführt wurde. Ein vollständiges Backup wird auch unter folgenden Bedingungen ausgeführt:

- Eine neue Datenbank wird hinzugefügt oder wiederhergestellt.
- Backup Exec führte das letzte vollständige Backup nicht aus.
- Anstelle eines vollständigen Backups wurden nur eine vollständige Kopie und ein inkrementelles Backup auf der Datenbank ausgeführt.

Siehe ["Konfigurieren von Backup-Methoden für Backup-Aufträge"](#) auf Seite 215.

Konsistenzprüfung vor dem Backup Wählen Sie eine der folgenden Konsistenzprüfungen vor Durchführung eines Backups aus:

- Keine
Diese Option führt keine Konsistenzprüfung vor einem Backup aus. Es wird empfohlen, entweder vor oder nach dem Backup eine Konsistenzprüfung durchzuführen.
- Vollständige Prüfung ohne Indexe
Diese Option schließt Indizes von der Konsistenzprüfung aus. Dadurch wird die Konsistenzprüfung erheblich beschleunigt, ist jedoch nicht so gründlich.
- Vollständiger Scan mit Indexen
Diese Option schließt Indizes in die Konsistenzprüfung ein. Fehler werden protokolliert.
- Nur physische Überprüfung
Diese Option führt eine weniger aufwändige Prüfung der physischen Konsistenz der Datenbank durch. Diese Option prüft nur die Integrität der physischen Struktur der Seite. Dies ist die Standardeinstellung.

Siehe ["Konfigurieren von Backup Exec zum Ausführen einer Konsistenzprüfung vor jedem SQL-Backup"](#) auf Seite 1224.

Mit Backup fortfahren, wenn Konsistenzprüfung fehlschlägt Wählen Sie dies aus, wenn Sie mit dem Backup-Vorgang fortfahren möchten, selbst wenn die Konsistenzprüfung fehlschlägt. Führen Sie ggf. das Backup beim Fehlschlagen der Konsistenzprüfung fort, wenn Ihrer Meinung nach ein Backup der Datenbank im aktuellen Zustand besser ist als überhaupt kein Backup, oder wenn Sie eine sehr große Datenbank mit nur einem geringfügigen Problem in einer Tabelle sichern.

Konsistenzprüfung nach dem Backup

Wählen Sie die Konsistenzprüfung aus, die nach einem Backup ausgeführt werden soll. Da Datenbanktransaktionen während oder nach der Konsistenzprüfung, aber auch vor den Backup-Prozessen auftreten können, sollte die Konsistenzprüfung nach dem Backup erfolgen, um sicherzustellen, dass die Daten zum Zeitpunkt des Backups konsistent waren.

Folgende Optionen sind verfügbar:

- Keine
Diese Option führt keine Konsistenzprüfung nach einem Backup aus. Es wird empfohlen, nach jedem Backup eine Konsistenzprüfung durchzuführen. Dies ist die Standardeinstellung.
- Vollständige Prüfung ohne Indexe
Diese Option schließt Indizes von der Konsistenzprüfung aus. Dadurch wird die Konsistenzprüfung erheblich beschleunigt, ist jedoch nicht so gründlich.
- Vollständiger Scan mit Indexen
Diese Option schließt Indizes in die Konsistenzprüfung ein. Fehler werden protokolliert.
- Nur physische Überprüfung
Diese Option führt eine weniger aufwändige Prüfung der physischen Konsistenz der Datenbank durch. Diese Option prüft nur die Integrität der physischen Struktur der Seite. Dies ist die Standardeinstellung.

Prüfsummen auf Backups anwenden (SQL 2005 oder höher)

Fügen Sie den durch Backup Exec gesicherten SQL-Datenbankdaten Prüfsummen hinzu. Das Hinzufügen von Prüfsummen zu den gesicherten Daten ist erforderlich, wenn Sie die Option "Nur überprüfen, Daten nicht wiederherstellen" verwenden möchten. Die Verwendung dieser Option und der Option "Nur überprüfen, Daten nicht wiederherstellen" stellt sicher, dass bei der Wiederherstellung der SQL-Datenbank ein überprüftes SQL-Backup verwendet wird.

Von SQL-Backups Datenträgerkopien erstellen und auf dem SQL-Server ablegen, auf dem sich die Datenbank befindet	<p>Erstellen Sie eine Datenträgerkopie der SQL-Datenbank, die gesichert werden soll. Mit dieser Option können Sie gleichzeitig eine SQL-Datenbank in einem Speichermedium sichern und eine Kopie der Datenbank in ein Festplattenverzeichnis schreiben, das Sie mithilfe der Option "In Pfad speichern" festlegen können.</p> <p>Diese Option gibt IT-Administratoren die Möglichkeit, SQL-Datenbanken zu sichern und zugleich Datenbankadministratoren Kopien der Datenbank auf Festplatte bereitzustellen, welche u. a. für Tests oder Wiederherstellungen verwendet werden können.</p> <p>Hinweis: Diese Option unterstützt Snapshot-Technologie nicht.</p>
In Pfad speichern	<p>Geben Sie einen Pfad an, in dem die Datenträgerkopien von SQL-Backups gespeichert werden sollen.</p>

SQL Server 2008 Enterprise Edition-Softwarekomprimierung Wählen Sie eine Komprimierungseinstellung aus, die Sie für diesen Backup-Auftrag verwenden möchten:

- Keine
Es wird keine Komprimierung verwendet.
- Komprimierung
Verwenden Sie SQL Server 2008 oder höher, sofern von der installierten SQL Server-Instanz unterstützt.

SQL komprimiert die Daten auf dem Computer, auf dem SQL Server 2008 Enterprise Edition oder höher installiert ist. Folglich sollten schnellere Backups von SQL 2008 oder höher möglich sein, wenn Sie die SQL-Komprimierung verwenden.

Die unterstützten Betriebssysteme, Plattformen, Anwendungen und Service Packs finden Sie in der Liste der mit Backup Exec kompatiblen Software.

Es wird empfohlen, dass Sie die Softwarekomprimierung aus SQL 2008 oder höher nicht für Backup-Aufträge verwenden, die auch die von Backup Exec gestartete Softwarekomprimierung verwenden. Die Komprimierung schafft nur minimale Vorteile, wenn Sie die Backup Exec-Komprimierung aktivieren. In Aufträgen, in denen beide Komprimierungsarten eingesetzt werden, können sich die Backup-Zeiten sogar erhöhen.

Die Softwarekomprimierung bei SQL 2008 oder höher wird nicht verwendet, wenn ein Backup-Auftrag mit Daten aus SQL 2008 oder höher die Advanced Open File-Option verwendet.

Hinweis: Sie können diese Option nicht für Backup-Aufträge verwenden, die Daten deduplizieren.

Einmaliges Backup

Gibt eine der folgenden Methoden für einmalige Backups an:

- **Vollständig - Datenbanken sichern**
 Diese Option sichert die gesamte Datenbank. Dies ist die Standardeinstellung.
 Siehe ["Sichern von SQL-Datenbanken und Transaktionsprotokollen"](#) auf Seite 1228.
- **Vollständige Kopie - Datenbanken (Kopie) sichern**
 Diese Option sichert die gesamte Datenbank, ohne Auswirkung auf zukünftige Differenzial- oder Protokoll-Backups.
 Anders als bei vollständigen Backups wird bei der Methode "Vollständig kopieren" der Basis-Backup-Satz für Differenzial-Backups nicht zurückgesetzt. Dieser gibt die seit dem letzten vollständigen Backup geänderten Datenblöcke an.
 Nach einem vollständigen Backup können Sie mit der Backup-Methode "Vollständig kopieren" eine Kopie der SQL-Datenbank erstellen, ohne dass sich dies auf den für zukünftige Differenzial-Backups erforderlichen Basis-Backup-Satz auswirkt.
- **Datenbank-Snapshot - Schreibgeschützte**
 Point-in-Time-Kopie einer anderen Datenbank
 Diese Option erstellt eine schreibgeschützte Kopie einer anderen Datenbank zu einem bestimmten Zeitpunkt.
 Siehe ["Verwenden von Datenbank-Snapshots für SQL-Server"](#) auf Seite 1226.
- **Protokoll nicht kürzen - Sichern ohne Kürzen des Transaktionsprotokolls**
 Diese Option sichert die Datenbank, wenn sie beschädigt ist oder Datenbankdateien fehlen. Da bei dem Verfahren "Protokoll nicht kürzen" nicht auf die Datenbank zugegriffen wird, können Sie weiterhin Transaktionen sichern, auf die Sie sonst eventuell keinen Zugriff hätten. Verwenden Sie bei einer Datenbankwiederherstellung dieses Transaktionsprotokoll-Backup gemeinsam mit einem Datenbank-Backup oder einer anderen vorher genannten Backup-Methode für Transaktionsprotokolle, bis Sie zu dem Punkt gelangen, an dem diese fehlgeschlagen sind. Nicht durchgeführte Transaktionen werden jedoch automatisch zurückgesetzt. Durchgeführte Transaktionen werden beim Verwenden der Methode

"Protokoll nicht kürzen" nach dem Protokoll-Backup nicht gelöscht.

- Protokoll - Transaktionsprotokoll sichern und kürzen
 Diese Option sichert nur die Daten, die im Transaktionsprotokoll enthalten sind. Sie sichert keine Datenbankdaten. Nach dem Sichern des Transaktionsprotokolls werden reservierte Transaktionen entfernt (abgeschnitten).

Wenn die Datenbanken für das einfache SQL Server-Wiederherstellungsmodell konfiguriert sind, werden Backups von Protokolldateien nicht unterstützt. Um das Wiederherstellungsmodell zu ändern, verwenden Sie die SQL-Administrationstools, um das Wiederherstellungsmodell auf "Vollständig" festzulegen. Sie sollten ein neues vollständiges Backup ausführen, wenn Sie den Wiederherstellungsmodus ändern, bevor ein Backup von Protokolldateien ausgeführt wird.

Alternativ können Sie nur vollständige Backups ausführen oder vollständige und Differenzial-Backups der SQL-Datenbanken ausführen.

Warnung: Data Lifecycle Management (DLM) löscht alle abgelaufenen Backup-Sätze, die von einem einmaligen Backup-Auftrag erstellt wurden. DLM bewahrt den letzten Backup-Satz nicht mehr auf, nachdem der Aufbewahrungszeitraum abgelaufen ist, wenn der Backup-Satz aus einem einmaligen Backup stammt. Um zu verhindern, dass die Backup-Sätze automatisch gelöscht werden, können Sie spezifische Backup-Sätze manuell aufbewahren oder das Ablaufdatum ändern.

Siehe ["Löschen abgelaufener Backup-Sätze auf plattenbasiertem Speicher durch Data Lifecycle Management \(DLM\)"](#) auf Seite 393.

Siehe ["Konfigurieren von Backup Exec zum Ausführen einer Konsistenzprüfung vor jedem SQL-Backup"](#) auf Seite 1224.

- 11** Klicken Sie im Dialogfeld "Backup-Optionen" auf eine der für diesen Auftrag festzulegenden optionalen Einstellungen.
- 12** Klicken Sie auf "OK".
- 13** Klicken Sie im Dialogfeld "Eigenschaften der Backup-Definition" auf "OK".

Siehe ["Hinzufügen einer Stufe zu einer Backup-Definition"](#) auf Seite 244.

Siehe ["Bearbeiten von Backup-Definitionen"](#) auf Seite 226.

Siehe ["Ändern der Standardeinstellungen für Backup-Aufträge"](#) auf Seite 630.

Festlegen der Standard-Backup-Optionen für SQL Server

Sie können die bei der Installation von Backup Exec für alle SQL Server-Aufträge festgelegten Standardeinstellungen verwenden oder eigene Standardeinstellungen wählen. Sie können die Standardeinstellungen übergehen, wenn Sie einzelne Aufträge erstellen.

So legen Sie Standard-Backup-Optionen für SQL Server fest

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- 2 Wählen Sie "Auftragsstandardeinstellungen" und dann eine Backup-Option.
Beispiel: Wenn Sie die Standardoptionen für SQL Server einrichten möchten, wählen Sie "Backup-to-Disk". Die Optionen, die angezeigt werden, hängen von den konfigurierten Speichergerätetypen ab. Sie können verschiedene Standardoptionen für die Backup-Aufträge konfigurieren, die Sie an verschiedene Speichergerätetypen senden.
- 3 Klicken Sie im linken Teilfenster auf "Microsoft SQL".
- 4 Wählen Sie die entsprechenden Optionen aus.

Backup-Methode

Wählen Sie eine der folgenden Backup-Methoden aus, die Sie für diesen Auftrag anwenden möchten:

- **Vollständig - Datenbanken sichern**

Diese Option sichert die gesamte Datenbank. Dies ist die Standardeinstellung.

- **Vollständige Kopie - Datenbanken (Kopie) sichern**

Diese Option sichert die gesamte Datenbank, ohne Auswirkung auf zukünftige Differenzial- oder Protokoll-Backups.

Anders als bei vollständigen Backups wird bei der Methode "Vollständig kopieren" der Basis-Backup-Satz für Differenzial-Backups nicht zurückgesetzt. Dieser gibt die seit dem letzten vollständigen Backup geänderten Datenblöcke an.

Nach einem vollständigen Backup können Sie mit der Backup-Methode "Vollständig kopieren" eine Kopie der SQL-Datenbank erstellen, ohne dass sich dies auf den für zukünftige Differenzial-Backups erforderlichen Basis-Backup-Satz auswirkt.

Backup-Methode

Wählen Sie eine der folgenden SQL-spezifischen Backup-Methoden aus, die Sie für diesen Auftrag anwenden möchten:

- **Vollständig - Datenbanken sichern**
 Diese Option sichert die gesamte Datenbank. Dies ist die Standardeinstellung.
- **Vollständige Kopie - Datenbanken (Kopie) sichern**
 Diese Option sichert die gesamte Datenbank, ohne Auswirkung auf zukünftige Differenzial- oder Protokoll-Backups.
 Anders als bei vollständigen Backups wird bei der Methode "Vollständig kopieren" der Basis-Backup-Satz für Differenzial-Backups nicht zurückgesetzt. Dieser gibt die seit dem letzten vollständigen Backup geänderten Datenblöcke an.
 Nach einem vollständigen Backup können Sie mit der Backup-Methode "Vollständig kopieren" eine Kopie der SQL-Datenbank erstellen, ohne dass sich dies auf den für zukünftige Differenzial-Backups erforderlichen Basis-Backup-Satz auswirkt.
- **Automatisch: Transaktionsprotokoll sichern, wenn aktiviert und dann Datenbankänderungen seit dem letzten vollständigen oder inkrementellen Backup sichern**
 Mit dieser Option können Sie die gesamte SQL-Instanz sichern, auch wenn einige Datenbanken keine Protokoll-Backups unterstützen. Alle Datenbanken werden unter Verwendung des inkrementellen Backups (Blockebene) gesichert. Darüber hinaus werden die Datenbanken, die Protokoll-Backups unterstützen, mit dem Protokoll-Backup gesichert.
Hinweis: Wenn Snapshot nicht aktiviert wird, kann kein inkrementelles Backup (Blockebene) durchgeführt werden. Stattdessen wird das Differenzial-Backup verwendet.
- **Protokoll - Transaktionsprotokoll sichern und kürzen**
 Diese Option sichert nur die Daten, die im Transaktionsprotokoll enthalten sind. Sie sichert keine Datenbankdaten. Nach dem Sichern des Transaktionsprotokolls werden reservierte Transaktionen entfernt (abgeschnitten).
 Wenn die Datenbanken für das einfache SQL Server-Wiederherstellungsmodell konfiguriert sind, werden Backups von Protokolldateien nicht unterstützt.

Um das Wiederherstellungsmodell zu ändern, verwenden Sie die SQL-Administrationstools, um das Wiederherstellungsmodell auf "Vollständig" festzulegen. Sie sollten ein neues vollständiges Backup ausführen, wenn Sie den Wiederherstellungsmodus ändern, bevor ein Backup von Protokolldateien ausgeführt wird.

Alternativ können Sie nur vollständige Backups ausführen oder vollständige und Differenzial-Backups der SQL-Datenbanken ausführen.

Siehe ["Konfigurieren von Backup Exec zum Ausführen einer Konsistenzprüfung vor jedem SQL-Backup"](#) auf Seite 1224.

- **Protokoll nicht kürzen - Sichern ohne Kürzen des Transaktionsprotokolls**
 Diese Option sichert die Datenbank, wenn sie beschädigt ist oder Datenbankdateien fehlen. Da bei dem Verfahren "Protokoll nicht kürzen" nicht auf die Datenbank zugegriffen wird, können Sie weiterhin Transaktionen sichern, auf die Sie sonst eventuell keinen Zugriff hätten. Verwenden Sie bei einer Datenbankwiederherstellung dieses Transaktionsprotokoll-Backup gemeinsam mit einem Datenbank-Backup oder einer anderen vorher genannten Backup-Methode für Transaktionsprotokolle, bis Sie zu dem Punkt gelangen, an dem diese fehlgeschlagen sind. Nicht durchgeführte Transaktionen werden jedoch automatisch zurückgesetzt. Durchgeführte Transaktionen werden beim Verwenden der Methode "Protokoll nicht kürzen" nach dem Protokoll-Backup nicht gelöscht.
- **Differenziell – Datenbankänderungen seit dem letzten vollständigen Backup sichern**
 Diese Option sichert nur die Änderungen, die an der Datenbank oder Dateigruppe seit dem letzten vollständigen Backup vorgenommen wurden. Da Differenzial-Backups nur eine Wiederherstellung des zum Zeitpunkt des Differenzial-Backups vorliegenden Systemzustands ermöglichen, sollten Sie nach der Erstellung eines Differenzial-Backups zusätzlich mehrere Protokoll-Backups erstellen.

- Differenziell (Blockebene) - Änderungen an der Datenbank seit dem letzten vollständigen Backup sichern - zusammen mit Auftrag zum Konvertieren in virtuellen Computer
 Diese Option sichert alle Datenblöcke und Protokolle, die seit dem letzten vollständigen Backup erstellt oder geändert wurden.
- Inkrementell (Blockebene): Änderungen an der Datenbank seit dem letzten vollständigen oder inkrementellen Backup sichern - zusammen mit Auftrag zum Konvertieren in virtuellen Computer
 Diese Option sichert alle Datenblöcke und Protokolle, die seit dem letzten vollständigen oder inkrementellen Backup erstellt oder geändert wurden.
- Datenbank-Snapshot - schreibgeschützte Zeitpunktkopie von Datenbanken
 Diese Option erstellt eine schreibgeschützte Kopie einer anderen Datenbank zu einem bestimmten Zeitpunkt.
 Siehe ["Verwenden von Datenbank-Snapshots für SQL-Server"](#) auf Seite 1226.

Hinweis: Differenzielle oder inkrementelle SQL-Backups werden nur für die Konvertierung in virtuelle Computer unterstützt, wenn Sie die Backup-Methoden "Automatisch", "Differenzial (Blockebene)" oder "Inkrementell (Blockebene)" verwenden.

Zusätzlich führt Backup Exec ein vollständiges Backup aus, wenn Sie die Backup-Methoden "Automatisch" oder "Protokoll" auswählen, wenn vorher auf die Datenbank kein vollständiges Backup ausgeführt wurde. Ein vollständiges Backup wird auch unter folgenden Bedingungen ausgeführt:

- Eine neue Datenbank wird hinzugefügt oder wiederhergestellt.
- Backup Exec führte das letzte vollständige Backup nicht aus.
- Anstelle eines vollständigen Backups wurden nur eine vollständige Kopie und ein inkrementelles Backup auf der Datenbank ausgeführt.

Siehe ["Konfigurieren von Backup-Methoden für Backup-Aufträge"](#) auf Seite 215.

Konsistenzprüfung vor dem Backup Wählen Sie eine der folgenden Konsistenzprüfungen vor Durchführung eines Backups aus:

- Keine
Diese Option führt keine Konsistenzprüfung vor einem Backup aus. Es wird empfohlen, entweder vor oder nach dem Backup eine Konsistenzprüfung durchzuführen.
- Vollständige Prüfung ohne Indexe
Diese Option schließt Indizes von der Konsistenzprüfung aus. Dadurch wird die Konsistenzprüfung erheblich beschleunigt, ist jedoch nicht so gründlich.
- Vollständiger Scan mit Indexen
Diese Option schließt Indizes in die Konsistenzprüfung ein. Fehler werden protokolliert.
- Nur physische Überprüfung
Diese Option führt eine weniger aufwändige Prüfung der physischen Konsistenz der Datenbank durch. Diese Option prüft nur die Integrität der physischen Struktur der Seite. Dies ist die Standardeinstellung.

Siehe ["Konfigurieren von Backup Exec zum Ausführen einer Konsistenzprüfung vor jedem SQL-Backup"](#) auf Seite 1224.

Mit Backup fortfahren, wenn Konsistenzprüfung fehlschlägt Wählen Sie dies aus, wenn Sie mit dem Backup-Vorgang fortfahren möchten, selbst wenn die Konsistenzprüfung fehlschlägt. Führen Sie ggf. das Backup beim Fehlschlagen der Konsistenzprüfung fort, wenn Ihrer Meinung nach ein Backup der Datenbank im aktuellen Zustand besser ist als überhaupt kein Backup, oder wenn Sie eine sehr große Datenbank mit nur einem geringfügigen Problem in einer Tabelle sichern.

Konsistenzprüfung nach dem Backup

Wählen Sie die Konsistenzprüfung aus, die nach einem Backup ausgeführt werden soll. Da Datenbanktransaktionen während oder nach der Konsistenzprüfung, aber auch vor den Backup-Prozessen auftreten können, sollte die Konsistenzprüfung nach dem Backup erfolgen, um sicherzustellen, dass die Daten zum Zeitpunkt des Backups konsistent waren.

Folgende Optionen sind verfügbar:

- Keine
Diese Option führt keine Konsistenzprüfung nach einem Backup aus. Es wird empfohlen, nach jedem Backup eine Konsistenzprüfung durchzuführen. Dies ist die Standardeinstellung.
- Vollständige Prüfung ohne Indexe
Diese Option schließt Indizes von der Konsistenzprüfung aus. Dadurch wird die Konsistenzprüfung erheblich beschleunigt, ist jedoch nicht so gründlich.
- Vollständiger Scan mit Indexen
Diese Option schließt Indizes in die Konsistenzprüfung ein. Fehler werden protokolliert.
- Nur physische Überprüfung
Diese Option führt eine weniger aufwändige Prüfung der physischen Konsistenz der Datenbank durch. Diese Option prüft nur die Integrität der physischen Struktur der Seite. Dies ist die Standardeinstellung.

Prüfsummen auf Backups anwenden (SQL 2005 oder höher)

Fügen Sie den durch Backup Exec gesicherten SQL-Datenbankdaten Prüfsummen hinzu. Das Hinzufügen von Prüfsummen zu den gesicherten Daten ist erforderlich, wenn Sie die Option "Nur überprüfen, Daten nicht wiederherstellen" verwenden möchten. Die Verwendung dieser Option und der Option "Nur überprüfen, Daten nicht wiederherstellen" stellt sicher, dass bei der Wiederherstellung der SQL-Datenbank ein überprüftes SQL-Backup verwendet wird.

Von SQL-Backups Datenträgerkopien erstellen und auf dem SQL-Server ablegen, auf dem sich die Datenbank befindet	<p>Erstellen Sie eine Datenträgerkopie der SQL-Datenbank, die gesichert werden soll. Mit dieser Option können Sie gleichzeitig eine SQL-Datenbank in einem Speichermedium sichern und eine Kopie der Datenbank in ein Festplattenverzeichnis schreiben, das Sie mithilfe der Option "In Pfad speichern" festlegen können.</p> <p>Diese Option gibt IT-Administratoren die Möglichkeit, SQL-Datenbanken zu sichern und zugleich Datenbankadministratoren Kopien der Datenbank auf Festplatte bereitzustellen, welche u. a. für Tests oder Wiederherstellungen verwendet werden können.</p> <p>Hinweis: Diese Option unterstützt Snapshot-Technologie nicht.</p>
In Pfad speichern	<p>Geben Sie einen Pfad an, in dem die Datenträgerkopien von SQL-Backups gespeichert werden sollen.</p>

SQL Server 2008 Enterprise Edition-Softwarekomprimierung Wählen Sie eine Komprimierungseinstellung aus, die Sie für diesen Backup-Auftrag verwenden möchten:

- Keine
Es wird keine Komprimierung verwendet.
- Komprimierung
Verwenden Sie SQL Server 2008 oder höher, sofern von der installierten SQL Server-Instanz unterstützt.

SQL komprimiert die Daten auf dem Computer, auf dem SQL Server 2008 Enterprise Edition oder höher installiert ist. Folglich sollten schnellere Backups von SQL 2008 oder höher möglich sein, wenn Sie die SQL-Komprimierung verwenden.

Die unterstützten Betriebssysteme, Plattformen und Anwendungen finden Sie in der Liste der mit Backup Exec kompatiblen Software.

Es wird empfohlen, dass Sie die Softwarekomprimierung aus SQL 2008 oder höher nicht für Backup-Aufträge verwenden, die auch die von Backup Exec gestartete Softwarekomprimierung verwenden. Die Komprimierung schafft nur minimale Vorteile, wenn Sie die Backup Exec-Komprimierung aktivieren. In Aufträgen, in denen beide Komprimierungsarten eingesetzt werden, können sich die Backup-Zeiten sogar erhöhen.

Die Softwarekomprimierung bei SQL 2008 oder höher wird nicht verwendet, wenn ein Backup-Auftrag mit Daten aus SQL 2008 oder höher die Advanced Open File-Option verwendet.

Hinweis: Sie können diese Option nicht für Backup-Aufträge verwenden, die Daten deduplizieren.

Einmaliges Backup

Gibt eine der folgenden Methoden für einmalige Backups an:

- **Vollständig - Datenbanken sichern**
 Diese Option sichert die gesamte Datenbank. Dies ist die Standardeinstellung.
 Siehe ["Sichern von SQL-Datenbanken und Transaktionsprotokollen"](#) auf Seite 1228.
- **Vollständige Kopie - Datenbanken (Kopie) sichern**
 Diese Option sichert die gesamte Datenbank, ohne Auswirkung auf zukünftige Differenzial- oder Protokoll-Backups.
 Anders als bei vollständigen Backups wird bei der Methode "Vollständig kopieren" der Basis-Backup-Satz für Differenzial-Backups nicht zurückgesetzt. Dieser gibt die seit dem letzten vollständigen Backup geänderten Datenblöcke an.
 Nach einem vollständigen Backup können Sie mit der Backup-Methode "Vollständig kopieren" eine Kopie der SQL-Datenbank erstellen, ohne dass sich dies auf den für zukünftige Differenzial-Backups erforderlichen Basis-Backup-Satz auswirkt.
- **Datenbank-Snapshot - Schreibgeschützte**
 Point-in-Time-Kopie einer anderen Datenbank
 Diese Option erstellt eine schreibgeschützte Kopie einer anderen Datenbank zu einem bestimmten Zeitpunkt.
 Siehe ["Verwenden von Datenbank-Snapshots für SQL-Server"](#) auf Seite 1226.
- **Protokoll nicht kürzen - Sichern ohne Kürzen des Transaktionsprotokolls**
 Diese Option sichert die Datenbank, wenn sie beschädigt ist oder Datenbankdateien fehlen. Da bei dem Verfahren "Protokoll nicht kürzen" nicht auf die Datenbank zugegriffen wird, können Sie weiterhin Transaktionen sichern, auf die Sie sonst eventuell keinen Zugriff hätten. Verwenden Sie bei einer Datenbankwiederherstellung dieses Transaktionsprotokoll-Backup gemeinsam mit einem Datenbank-Backup oder einer anderen vorher genannten Backup-Methode für Transaktionsprotokolle, bis Sie zu dem Punkt gelangen, an dem diese fehlgeschlagen sind. Nicht durchgeführte Transaktionen werden jedoch automatisch zurückgesetzt. Durchgeführte Transaktionen werden beim Verwenden der Methode

"Protokoll nicht kürzen" nach dem Protokoll-Backup nicht gelöscht.

- Protokoll - Transaktionsprotokoll sichern und kürzen
Diese Option sichert nur die Daten, die im Transaktionsprotokoll enthalten sind. Sie sichert keine Datenbankdaten. Nach dem Sichern des Transaktionsprotokolls werden reservierte Transaktionen entfernt (abgeschnitten).

Wenn die Datenbanken für das einfache SQL Server-Wiederherstellungsmodell konfiguriert sind, werden Backups von Protokolldateien nicht unterstützt. Um das Wiederherstellungsmodell zu ändern, verwenden Sie die SQL-Administrationstools, um das Wiederherstellungsmodell auf "Vollständig" festzulegen. Sie sollten ein neues vollständiges Backup ausführen, wenn Sie den Wiederherstellungsmodus ändern, bevor ein Backup von Protokolldateien ausgeführt wird.

Alternativ können Sie nur vollständige Backups ausführen oder vollständige und Differenzial-Backups der SQL-Datenbanken ausführen.

Siehe ["Konfigurieren von Backup Exec zum Ausführen einer Konsistenzprüfung vor jedem SQL-Backup"](#) auf Seite 1224.

5 Klicken Sie auf "OK".

Siehe ["Sichern von SQL-Datenbanken und Transaktionsprotokollen"](#) auf Seite 1228.

SQL-Datenbanken und Transaktionsprotokolle wiederherstellen

Mit SQL Agent können Sie SQL Server-Datenbanken wiederherstellen. Sie können die Datenbanken an ihrem ursprünglichen Speicherort wiederherstellen oder die Wiederherstellung an einen neuen Speicherort umleiten. Die Anzahl von Aufträgen, über die Sie entscheiden, hängt von den Typen von Backup-Aufträgen ab, die die Datenbank schützen. Wenn Sie einen Auftrag zur Wiederherstellung einer Datenbank verwenden, wählen Sie alle Backup-Sätze aus, die angewendet werden sollen. Berücksichtigen Sie dabei das vollständige Backup, eventuelle Differenzial- und Protokoll-Backups.

Bei sehr großen Datenbanken kann dieser Vorgang einige Stunden dauern. Währenddessen meldet Backup Exec, dass keine Daten übertragen werden, und in der Ansicht "Auftragsüberwachung" wird das Feld "Byte (Anzahl)" nicht aktualisiert.

Wenn SQL das Füllen der Dateien mit Nullen abgeschlossen hat, wird der Wiederherstellungsauftrag fortgesetzt. Dieser Vorgang gilt für alle Datenbankwiederherstellungen, ist jedoch nur bei den sehr großen Datenbanken bemerkbar.

Verschlüsselte SQL-Datenbanken wiederherstellen

SQL 2008 unterstützt Transparent Database Encryption (TDE), die die Verschlüsselung von SQL-2008-Datenbanken auf der Backup-Satz-Ebene ermöglicht.

Wenn Sie eine Datenbank sichern, die TDE verwendet, empfiehlt Microsoft, dass Sie die Zertifikat-Schlüssel und -Verschlüsselungen mit der Datenbank sichern. Wenn Sie die Zertifikat-Schlüssel und -Verschlüsselungen nicht einschließen, müssen Sie alle Backup- und Wiederherstellungs-Vorgänge innerhalb der ausgewählten SQL-Instanz ausführen.

Hinweis: Backup Exec kann die Wiederherstellung der Datenbank-Daten, die TDE verwendeten, nur umleiten, wenn die Zertifikatsschlüssel und Verschlüsselungscodes auf die Ziel-Instanz angewendet werden. Wenn die Zertifikat-Schlüssel und -Verschlüsselungen nicht auf die Ziel-Instanz angewendet werden, erscheint eine Fehlermeldung, dass das Zertifikat thumbprint nicht gefunden werden kann. Konsultieren Sie Ihre Microsoft SQL-Dokumentation 2008.

Wiederherstellen von Daten aus SQL-Transaktionsprotokollen bis zu einem bestimmten Zeitpunkt

Sie können Transaktionen von einem Transaktionsprotokoll bis einschließlich einem Zeitpunkt im Transaktionsprotokoll wiederherstellen. Wenn dieser Zeitpunkt erreicht ist, wird die Wiederherstellung anhand des Transaktionsprotokolls beendet. In der Ereignisanzeige Ihrer Clientanwendung finden Sie die Daten und Uhrzeiten der Transaktionen.

Falls der angegebene Zeitpunkt hinter der Zeitspanne liegt, die das jüngste wiederherzustellende Transaktionsprotokoll umfasst, ist die Wiederherstellung erfolgreich. Es wird jedoch eine Warnung ausgegeben und die Datenbank verbleibt in einem vorläufigen Zustand. Falls der angegebene Zeitpunkt vor der Zeitspanne liegt, die das wiederherzustellende Transaktionsprotokoll umfasst, werden keine Transaktionen wiederhergestellt.

So führen Sie eine Wiederherstellung von einem SQL-Transaktionsprotokoll bis zu einem genannten Vorgang aus

Sie können Vorgänge aus einem Transaktionsprotokoll bis zu einem genannten Vorgang oder Markierung (einschließlich) wiederherstellen. Wenn der genannte Vorgang erreicht ist, wird die Wiederherstellung anhand des Transaktionsprotokolls beendet.

Da diese genannten Vorgänge nicht unbedingt eindeutige Namen haben, können Sie auch ein Datum und eine Uhrzeit festlegen. Bei der Wiederherstellung wird ab diesem Zeitpunkt nach dem genannten Vorgang gesucht. Wenn Sie beispielsweise eine Wiederherstellung von einem Protokoll bis zum genannten Vorgang "Mittagspause", gefunden nach dem 2.6.2000 und 11.30 Uhr, festlegen, wird bei der Wiederherstellung erst nach diesem Zeitpunkt nach "Mittagspause" gesucht. In der Ereignisanzeige Ihrer Clientanwendung finden Sie die Daten und Uhrzeiten der Transaktionen.

Falls der genannte Vorgang nicht gefunden wird, ist die Wiederherstellung erfolgreich. Es wird jedoch eine Warnung ausgegeben, und die Datenbank verbleibt in einem vorläufigen Zustand.

Hinweis: Bei den Transaktionsnamen muss die Groß-/Kleinschreibung beachtet werden. Vergewissern Sie sich, dass Sie bei der Angabe eines benannten Vorgangs die richtigen Groß- und Kleinbuchstaben eingeben.

Wiederherstellungen von SQL umleiten

Sie können folgende Umleitungen vornehmen:

- Ein Datenbank-Backup zu einem anderen Server oder zu einer anderen Datenbank oder Instanz.
- Differenzial- und Protokoll-Backups zum Zielverzeichnis der zugehörigen, wiederherzustellenden Datenbank.
- Datenbank aus einer 32- oder 64-Bit-Plattform auf eine andere Plattform.

Wiederherstellungen, die aus einem Einzelauftrag oder mehreren Aufträgen bestehen, können in umgeleiteten Wiederherstellungsvorgängen verwendet werden.

SQL-Datenbanken und Transaktionsprotokolle wiederherstellen

- 1** Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" mit der rechten Maustaste auf den Server, aus dem Sie Daten wiederherstellen möchten, und klicken Sie dann auf "Wiederherstellen".
- 2** Wählen Sie "Microsoft SQL Server-Datenbanken" aus und klicken Sie dann "Weiter".
- 3** Befolgen Sie die Anweisungen des "Assistenten für Wiederherstellungsaufträge", um die Daten wiederherzustellen.

Siehe ["Wiederherstellen der SQL-Master-Datenbank"](#) auf Seite 1259.

Wiederherstellen der SQL-Master-Datenbank

Folgende Symptome können auf eine Beschädigung der Master-Datenbank hinweisen:

- SQL kann nicht gestartet werden.
- Segmente sind fehlerhaft bzw. es treten Eingabe-/Ausgabefehler auf.
- Ein vom SQL Server-Dienstprogramm Database Consistency Checker (DBCC) erstellter Bericht.

Wenn die Master-Datenbank schwer beschädigt ist und SQL nicht gestartet werden kann, bietet sich für den Start von SQL folgende Möglichkeit an: Anstatt das Rebuild Master-Dienstprogramm auszuführen oder SQL neu zu installieren, können Sie die beschädigten oder fehlenden Datenbanken durch die Kopien der Master- und Modelldatenbanken ersetzen, die von Backup Exec automatisch erstellt und aktualisiert werden, wenn Backups an diesen Datenbanken ausgeführt werden. Nachdem SQL erneut ausgeführt wird, können Sie nach Bedarf alle anderen Datenbanken wiederherstellen.

Wenn keine Kopien der Master- und Modelldatenbanken erstellt wurden, müssen Sie das Dienstprogramm REBUILDM.EXE von Microsoft verwenden, um die Master-Datenbank neu zu erstellen und SQL zu starten.

Da alle seit dem letzten Backup an der Master-Datenbank vorgenommenen Änderungen bei der Wiederherstellung des Backup verloren gehen, müssen diese Änderungen erneut angewendet werden. Wurden nach dem Backup der Master-Datenbank Benutzerdatenbanken erstellt, kann auf diese Datenbanken erst dann zugegriffen werden, wenn sie von dem Backup wiederhergestellt oder SQL erneut hinzugefügt werden.

Hinweis: Es wird empfohlen, zuerst die Master-Datenbank in einem separaten Auftrag wiederherzustellen. Der SQL-Server wird während der Wiederherstellung der Master-Datenbank neu gestartet. Wenn andere Datenbank-Wiederherstellungen im gleichen Auftrag eingeschlossen sind, schlagen diese fehl.

Wiederherstellen der SQL-Master-Datenbank

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" in der Ansicht "Serverliste" mit der rechten Maustaste auf den Server, aus dem Sie die SQL-Master-Datenbank wiederherstellen möchten, und klicken Sie dann auf "Wiederherstellen".
- 2 Wählen Sie "Microsoft SQL Server-Datenbanken" aus und klicken Sie dann "Weiter".
- 3 Wählen Sie den Backup-Satz aus der das letzte Master-Datenbank-Backup enthält, und klicken Sie dann "Weiter".
- 4 Verwenden Sie die Standardeinstellungen oder wählen Sie die entsprechenden Optionen aus, und folgen Sie den Schritten in den weiteren Teilfenstern des Assistenten.
- 5 Wenn Sie aufgefordert werden, eine Konsistenzprüfung auszuführen, stellen Sie sicher, dass nach der Wiederherstellung eine Prüfung ausgeführt wird.

Nach der Wiederherstellung wird SQL im Mehrbenutzermodus neu gestartet.
- 6 Stellen Sie die restlichen SQL-Datenbanken wieder her.

Siehe ["Neustarten von SQL unter Verwendung von Datenbankkopien"](#) auf Seite 1260.

Neustarten von SQL unter Verwendung von Datenbankkopien

Sie können SQL mit Kopien der Datenbank von vorherigen Backups manuell neu starten und die Master-Datenbank dann wiederherstellen.

Siehe ["Wiederherstellen der SQL-Master-Datenbank"](#) auf Seite 1259.

Tabelle E-2 Neustarten von SQL unter Verwendung von Datenbankkopien

Schritt	Aktion
Schritt 1	<p>Stellen Sie sicher, dass die SQL-Dienste nicht ausgeführt werden.</p> <p>Detaillierte Informationen finden Sie in der SQL Server-Dokumentation.</p>

Schritt	Aktion
Schritt 2	<p>Überprüfen Sie, ob die Datenbankkopien vorhanden sind.</p> <p>Stellen Sie ggf. die Master- und Modelldatenbankkopien aus einem Backup-Satz auf dasselbe Verzeichnis wieder her, das die ursprünglichen Master- und Modelldatenbanken enthält.</p>
Schritt 3	<p>Wechseln Sie im Windows Explorer in das Standarddatenverzeichnis und löschen Sie die folgenden Dateien:</p> <ul style="list-style-type: none"> ■ master.mdf ■ mastlog.ldf ■ model.mdf ■ modellog.ldf.
Schritt 4	<p>Ändern Sie die Namen der Kopien auf ihre ursprünglichen Namen zurück.</p> <p>Verwenden Sie keine schreibgeschützten Dateien, da die SQL-Dienste sonst nicht starten werden.</p>
Schritt 5	Verwenden Sie SQL Service Control Manager, um SQL Server zu starten.
Schritt 6	Stellen Sie die neuesten Änderungen an der Master-Datenbank wieder her.

Die Datenbankkopien tragen die Bezeichnungen MASTER\$4IDR, MASTLOG\$4IDR, MODEL\$4IDR und MODELLOG\$4IDR.

Tabelle E-3 Speicherorte für SQL-Datenbankkopien

SQL-Datenbankkopie	Speicherort
Eine Erstinstallation von SQL 2005 oder höher	C:\Programme\Microsoft SQL Server\MSSQL.1\MSSQL\Data*.*
Eine zweite installierte Instanz von SQL 2005 oder höher	C:\Programme\Microsoft SQL Server\MSSQL.2\MSSQL\Data*.*

SQL-Datenbankkopie	Speicherort
SQL 2008-Standardinstallation	C:\Programme\Microsoft SQL Server\MSSQL10.<Instanzname>\MSSQL\Data

In der folgenden Tabelle sind die Namen der kopierten Datenbanken und der ursprüngliche Datenbankname aufgeführt.

Tabelle E-4 SQL-Datenbanknamen

Name der Datenbankkopie	Ursprünglicher Datenbankname
master\$4idr	master.mdf
mastlog\$4idr	mastlog.ldf
model\$4idr	model.mdf
modellog\$4idr	modellog.ldf

Notfallwiederherstellung von SQL Server

Beim Neustart von SQL ist der Einsatz von Backup Exec zum Wiederherstellen von SQL schneller als das Ausführen des Rebuild Master-Dienstprogramms oder ein erneutes Installieren von SQL. Mit Backup Exec können Sie die beschädigten oder fehlenden Datenbanken durch Kopien der Master- und Modelldatenbanken ersetzen, die Backup Exec automatisch erstellt und beim Ausführen von Backups dieser Datenbanken stets aktualisiert.

Falls Sie Simplified Disaster Recovery (SDR) verwenden, ersetzt SDR während einer SDR-Wiederherstellung von C die beschädigten Datenbanken automatisch durch Kopien der Master- und Modell-Datenbanken. Sie können dann SQL neu starten und das letzte Master-Datenbank-Backup und ggf. andere Datenbanken wiederherstellen.

In diesem Abschnitt sind folgenden Themen enthalten:

- Siehe „[Vorbereiten der Notfallwiederherstellung von SQL](#)“ auf Seite 1262.
- Siehe „[Voraussetzungen für die SQL-Notfallwiederherstellung](#)“ auf Seite 1263.
- Siehe „[Notfallwiederherstellung für einen gesamten SQL Server oder für SQL-Datenbanken](#)“ auf Seite 1264.

Vorbereiten der Notfallwiederherstellung von SQL

Führen Sie Folgendes zum Vorbereiten der Notfallwiederherstellung von SQL aus:

- Sichern Sie regelmäßig System- und Benutzerdatenbanken sowie Transaktionsprotokolle.
Kopien der Master- und Modelldatenbanken werden bei Backup Exec automatisch erstellt, wenn die Master- und Modelldatenbanken gesichert werden. Backup Exec platziert diese Kopien in demselben Verzeichnis, in dem sich die Datenbanken befinden. Dort müssen sie für die Aktualisierung aufbewahrt werden.
Die folgende Tabelle gibt die Speicherorte von MS SQL-Datenbanken an:
Die Kopien der Master- und Modelldatenbanken heißen folgendermaßen:
 - Master\$4idr
 - Mastlog\$4idr
 - Model\$4idr
 - Modellog\$4idr
- Sichern Sie die Systemlaufwerke, auf denen die SQL-Instanzen installiert sind. Beim Sichern des Systemlaufwerks, auf dem eine SQL-Instanz installiert ist, werden Kopien der Master- und Modelldatenbanken gesichert. Durch das Sichern des Systemlaufwerks, auf dem sich SQL befindet, werden auch alle Ausführungsdateien und Registrierungseinstellungen gesichert, die für die Ausführung von SQL erforderlich sind.
- Führen Sie nach allen an SQL vorgenommenen Änderungen ein Backup der Master-Datenbank durch.
- Führen Sie Aufzeichnungen über alle installierten Service Packs.
- Stellen Sie sicher, dass Sie auf eine Wiederherstellung des gesamten Servers, und nicht nur von SQL, vorbereitet sind.

Voraussetzungen für die SQL-Notfallwiederherstellung

Zum Ausführen der Wiederherstellung benötigen Sie folgende Elemente

- Das letzte Backup des SQL-Verzeichnisses (\Programme\Microsoft SQL Server\MSSQL) sowie der Windows-Registrierung bzw. des Systemstatus.
- Die SQL-Datenbank-Backups und Differenzial- und Protokoll-Backups.
- Ein Administrator-Login-Konto (oder gleichwertiges Konto) während der Wiederherstellung.

Notfallwiederherstellung für einen gesamten SQL Server oder für SQL-Datenbanken

Sie können entweder den gesamten Server einschließlich der SQL-Datenbanken aus vollständigen System-Backups wiederherstellen oder nur die SQL-Datenbanken auf einem neu installierten oder anderen verfügbaren SQL Server wiederherstellen.

Die Wiederherstellung des gesamten Servers einschließlich der SQL-Datenbanken hat den zusätzlichen Vorteil, dass andere Anwendungen und Daten, die zum Zeitpunkt des Fehlers auf dem Server gespeichert waren, wiederhergestellt werden. Der gesamte Server kann mit einem der folgenden beiden Verfahren wiederhergestellt werden:

- Manuelle Wiederherstellung des Windows-Servers und anschließende manuelle Wiederherstellung der SQL-Datenbanken. Bei dieser Methode wird zuerst der Windows-Server von Gesamtsystem-Backups und anschließend werden die SQL-Datenbanken wiederhergestellt.
- Simplified Disaster Recovery. Mit dieser Option wird eine automatisierte Methode zur Wiederherstellung des Windows-Servers sowie der SQL-Datenbanken von vollständigen System-Backups gewährleistet.

Siehe ["Hinweise zum Einsatz von Simplified Disaster Recovery mit Exchange, SQL, SharePoint, CAS, Hyper-V-Hosts und Deduplication Feature"](#) auf Seite 999.

Beachten Sie beim Wiederherstellen der SQL-Datenbanken Folgendes:

- Um nur die SQL-Datenbanken auf einem neu installierten oder anderen verfügbaren Server wiederherzustellen, muss der Server auf derselben Hardware-Plattform (plattformübergreifende Wiederherstellungen werden nicht unterstützt) sowie unter derselben Version von SQL mit derselben Service Pack-Version wie der ursprüngliche Server ausgeführt werden.
- Informationen zum Wiederherstellen von SQL-Datenbanken unter einer bereits vorhandenen SQL-Installation mit weiteren aktiven Datenbanken finden Sie unter:

Siehe ["Manuelle Wiederherstellung eines SQL Server "](#) auf Seite 1264.

Manuelle Wiederherstellung eines SQL Server

Wenn Sie SQL manuell wiederherstellen, müssen Sie zuerst den Windows-Server von den vollständigen Systems-Backups wiederherstellen. Wenn die Wiederherstellung des Windows-Computers abgeschlossen ist oder wenn eine neue Server-Installation zur Verfügung steht, kann mit der Wiederherstellung der SQL-Datenbanken begonnen werden.

Weitere Informationen zum Ausführen einer manuellen Notfallwiederherstellung finden Sie in den folgenden Abschnitten:

Siehe ["Durchführen einer manuellen Notfallwiederherstellung eines lokalen Backup Exec-Servers auf einem Windows-Computer"](#) auf Seite 1006.

Siehe ["Manuelles Ausführen der Notfallwiederherstellung eines Remote-Backup Exec-Servers oder Remote-Agent auf einem Windows-Computer"](#) auf Seite 1011.

Um SQL-Datenbanken wiederherstellen zu können, muss SQL ausgeführt werden. SQL kann jedoch nur gestartet werden, wenn die Master- und Modelldatenbanken vorhanden sind.

Sie können die Master- und Modelldatenbanken wiederherstellen und SQL starten, indem Sie eine der folgenden Methoden anwenden:

- Benennen Sie die von Backup Exec erstellten Dateien um, die die Master- und Modelldatenbanken ersetzen. Nachdem die Master- und Modelldatenbanken auf SQL vorhanden sind, müssen Sie SQL starten und anschließend alle weiteren Datenbanken wiederherstellen.

Siehe ["Neustarten von SQL unter Verwendung von Datenbankkopien"](#) auf Seite 1260.

- Installieren Sie SQL neu.

Hier wird nur das Neustarten von SQL mithilfe der von Backup Exec erstellten Master- und Modelldatenbanken beschrieben. Weitere Informationen zum Rebuild Master-Dienstprogramm oder zur Neuinstallation von SQL finden Sie in der Dokumentation zu Microsoft SQL.

Wenn Sie auf eine neue SQL-Installation wiederherstellen, beginnen Sie mit der Master-Datenbank.

Siehe ["Wiederherstellen der SQL-Master-Datenbank"](#) auf Seite 1259.

Backup Exec Agent for Microsoft Exchange Server

Dieser Anhang enthält folgende Themen:

- Informationen zum Backup Exec Exchange Agent
- Voraussetzungen für die Verwendung des Exchange Agents
- Bewilligen von Berechtigungen auf dem Exchange Server, um Datenbank-Backups und -wiederherstellungen sowie Granular Recovery Technology-Vorgänge zu ermöglichen
- Info zur Installation des Exchange Agent
- Hinzufügen von Exchange-Servern und Datenbankverfügbarkeitsgruppe zur Serverliste auf der Registerkarte "Backup und Wiederherstellung"
- So erstellen Sie bevorzugte Server-Konfigurationen für Microsoft Exchange Database Availability Groups (DAG).
- Für Exchange empfohlene Konfigurationen
- Voraussetzungen für den Zugriff auf Exchange-Postfächer
- Backup-Strategien für Exchange
- Wie Granular Recovery Technology mit dem Exchange-Informationsspeicher funktioniert
- Snapshot-Backups und Backups auf einem anderen Host mit dem Exchange Agent

- [Sichern von Exchange-Daten](#)
- [Wiederherstellen von Exchange-Daten](#)
- [Notfallwiederherstellung für Exchange-Server](#)

Informationen zum Backup Exec Exchange Agent

Backup Exec Agent for Microsoft Exchange Server (Exchange Agent) ermöglicht es Backups von Microsoft Exchange Server-Datenbanken mit Netzwerk-Backups ohne separate Verwaltung oder zugehörige Hardware zu integrieren.

Der Exchange Agent stellt folgende Funktionen bereit:

- Wiederherstellen einzelner Elemente aus den Backups, für die Sie Granular Recovery Technology aktivieren
- Wiederherstellen auf eine PST-Datei
- Wiederherstellen öffentlicher Ordner
- Wiederherstellen einer Datenbank in einem bestimmten Laufwerk bzw. Pfad
- Neuerstellen eines Postfachkontos
- Suchen nach einer bestimmten Meldung, die wiederhergestellt werden soll
- Wiederherstellen einzelner Datenbanken aus Snapshot-Backups mit der Funktion "Wiederherstellungsdatenbank" in Exchange Server 2010 und höher.
- Seeding einer Kopie der Datenbank aus Exchange Server 2010 und höher Das Seeding fügt eine Datenbank-Kopie an einem Speicherort auf einem anderen Postfachserver in einer Datenbankverfügbarkeitsgruppe hinzu.
- Offhost-Backup mit Granular Recovery Technology (GRT) für Exchange Server.

Informationen zu den Best Practices zum Einsatz des Backup Exec Agent for Microsoft Exchange Server finden Sie unter *Best Practices für Backup Exec*.

Siehe ["Info zur Installation des Exchange Agent"](#) auf Seite 1277.

Siehe ["Backup-Strategien für Exchange"](#) auf Seite 1284.

Siehe ["Für Exchange empfohlene Konfigurationen "](#) auf Seite 1281.

Siehe ["Granular Recovery Technology"](#) auf Seite 737.

Voraussetzungen für die Verwendung des Exchange Agents

Der Backup Exec-Server muss folgende Voraussetzungen erfüllen:

Tabelle F-1 Backup Exec-Server-Anforderungen für Backup Exec Exchange Agent

Backup Exec-Server-Anforderungen	Beschreibung
Unterstützung des Exchange Agents	<ul style="list-style-type: none"> ■ Eine Lizenz für Backup Exec for Microsoft Exchange Server (Exchange Agent) muss auf dem Backup Exec-Server eingegeben werden. ■ Der Backup Exec Agent for Windows muss auf jedem Remote-Exchange Server, den Sie sichern möchten, installiert werden. ■ Der Backup Exec-Server muss Zugriff auf den Exchange-Server haben. Die unterstützten Betriebssysteme, Plattformen, Anwendungen und Service Packs finden Sie in der Liste der mit Backup Exec kompatiblen Software. ■ Es wird die Verwendung eines Backup Exec-Dienstkontos mit Administratorenrechten (Domäne und lokal) für den Exchange-Server empfohlen. Bei Exchange 2010 und höher können Sie volle Exchange-Berechtigungen oder minimale Berechtigungen haben, die das Sichern und Wiederherstellen von Datenbanken sowie das Ausführen von Granular Recovery Technology-Vorgängen ermöglichen. Siehe "Bewilligen von Berechtigungen auf dem Exchange Server, um Datenbank-Backups und -wiederherstellungen sowie Granular Recovery Technology-Vorgänge zu ermöglichen" auf Seite 1272.

Backup Exec-Server-Anforderungen	Beschreibung
Unterstützung der Granular Recovery Technology (GRT) für die Wiederherstellung einzelner Elemente aus Informationsspeicher-Backups	<ul style="list-style-type: none"> ■ Ein Version von Microsoft Windows, die Minifilter-Treiber unterstützt, muss für Microsoft Exchange installiert werden. Die unterstützten Betriebssysteme, Plattformen, Anwendungen und Service Packs finden Sie in der Liste der mit Backup Exec kompatiblen Software. ■ Speicher, den Sie für Backups mit aktivierter GRT-Option verwenden, können zusätzliche Anforderungen haben. ■ Wenn Exchange-Protokolldateien auf einem erweiterten Formatdatenträger oder 512e-Datenträger sind, muss der Backup Exec-Server auch einen ähnlichen lokalen Datenträger haben, der zur Durchführung von GRT-Vorgängen verfügbar ist. <p>Siehe "Granular Recovery Technology" auf Seite 737.</p>

Folgende Voraussetzungen gelten für den Exchange-Server zusammen mit Backup Exec Exchange Agent:

Tabelle F-2 Exchange-Server-Voraussetzungen

Exchange-Server-Voraussetzungen	Beschreibung
Für Vorgänge auf allen Exchange-Servern	<p>Das Benutzerkonto muss ein Mitglied der folgenden Gruppen sein:</p> <ul style="list-style-type: none"> ■ Die Administrator-Gruppe ■ Die Domänenadministratoren <p>Zur Unterstützung der Funktion "Granular Recovery Technology" müssen Sie das entsprechende Exchange Server-Verwaltungsprogramm verwenden, um dem Benutzer die erforderlichen Berechtigungen zuzuweisen. In Exchange 2010 oder höher ist dies beispielsweise die Rolle "Organization Management".</p> <p>Es wird empfohlen, dass das Benutzerkonto volle Exchange-Berechtigungen auf dem Exchange Server hat. Wenn das Benutzerkonto keine vollen Exchange-Berechtigungen für Exchange 2010 und höher hat, können Sie minimale Berechtigungen erteilen, die das Sichern und Wiederherstellen von Datenbanken sowie das Ausführen von Granular Recovery Technology-Vorgängen ermöglichen.</p> <p>Siehe "Bewilligen von Berechtigungen auf dem Exchange Server, um Datenbank-Backups und -wiederherstellungen sowie Granular Recovery Technology-Vorgänge zu ermöglichen" auf Seite 1272.</p>

Exchange-Server-Voraussetzungen	Beschreibung
<p>So sichern Sie Exchange Server 2010 und höher und stellen ihn wieder her</p>	<p>Folgende Anforderungen gelten zum Sichern und Wiederherstellen von Exchange Server 2010 und höher:</p> <ul style="list-style-type: none"> ■ Sie müssen den Agent for Windows auf allen Postfachserverknoten im DAG installieren, um die Datenbanken auf einer Datenbankverfügbarkeitsgruppe zu sichern (DAG). ■ Sie benötigen lokale Administratorrechte auf jedem Knoten einer Datenbankverfügbarkeitsgruppe und auf dem Microsoft Exchange-Postfachserver, um Microsoft Exchange-Datenbankdateien zu sichern und wiederherzustellen. ■ Sie können minimale Berechtigungen konfigurieren, damit ein Benutzerkonto Datenbank-Backups und Wiederherstellung durchführt und Granular Recovery auf Exchange-Servern unterstützt, wenn Sie volle Berechtigungen nicht haben können. ■ Für Microsoft Exchange Server 2013, müssen Sie Microsoft Exchange Server 2013 mit dem kumulativen Update 1 oder höher haben installiert. <p>Siehe "Bewilligen von Berechtigungen auf dem Exchange Server, um Datenbank-Backups und -wiederherstellungen sowie Granular Recovery Technology-Vorgänge zu ermöglichen" auf Seite 1272.</p> <p>Siehe "Infos zum Agent for Windows" auf Seite 1028.</p>

Anforderungen an das jeweilige Betriebssystem für den Exchange Agent finden Sie in der Liste der mit Backup Exec kompatiblen Software.

Siehe ["Konfigurieren von Backup Exec, um Daten für Backup zu suchen"](#) auf Seite 708.

Bewilligen von Berechtigungen auf dem Exchange Server, um Datenbank-Backups und -wiederherstellungen sowie Granular Recovery Technology-Vorgänge zu ermöglichen

Ein Benutzerkonto muss auf Postfächer auf dem Exchange Server zugreifen, um Backup Exec-Vorgänge durchzuführen. Um auf Exchange Server zuzugreifen, müssen Sie Berechtigungen mit vollem Zugriff auf Exchange Server haben. Wenn Sie den Zugriff auf Exchange Server einschränken möchten, können Sie minimale Berechtigungen bewilligen, anhand derer Benutzer Datenbank-Backups und -wiederherstellungen sowie Granular Recovery Technology (GRT)-Vorgänge durchführen können.

Stellen Sie sicher, dass das Benutzerkonto die Rechte des lokalen Administrators auf Exchange Server hat und verwenden Sie dann eine der folgenden Methoden, um die Berechtigungen zu bewilligen:

- Vollständige Zugriffsberechtigung auf Unternehmensadministrator- und Unternehmensmanagementebene zulassen. Es wird empfohlen, dass das Benutzerkonto volle Exchange-Berechtigungen auf Exchange Server hat, um Backup Exec-Vorgänge durchzuführen.
Berechtigungen werden dann automatisch auf alle neuen Exchange-Server übertragen, die Sie auf der Ebene hinzufügen, der die Berechtigungen erteilt wurden.

Hinweis: Sie benötigen Administratorberechtigungen in Exchange, um anderen Konten Berechtigungen zu erteilen.

- Wenn das Benutzerkonto keine vollständigen Exchange-Berechtigungen für Backup Exec-Vorgänge haben kann, können Sie minimale Berechtigungen bewilligen. Aufgrund minimaler Berechtigungen können Benutzer Datenbank-Backups und -wiederherstellungen sowie Granular Recovery Technology-Vorgänge explizit auf dem jeweiligen Exchange Server durchführen. Wenn Sie Berechtigungen explizit erteilen und dann einen weiteren Exchange Server hinzufügen, müssen Sie auch dem hinzugefügten Server explizit Berechtigungen zuweisen.

[Erteilen von minimalen Berechtigungen für ein Benutzerkonto zur Durchführung von Datenbank-Backups und -wiederherstellungen von Exchange-Servern](#)

[Erteilen von minimalen Berechtigungen für ein Benutzerkonto zur Unterstützung von Granular Recovery Technology auf Exchange-Servern](#)

Erteilen von minimalen Berechtigungen für ein Benutzerkonto zur Durchführung von Datenbank-Backups und -wiederherstellungen von Exchange-Servern

Sie können minimale Berechtigungen für ein Benutzerkonto erteilen, mit denen Datenbank-Backups und -Wiederherstellungen auf einem Exchange-Server durchgeführt werden können.

Um volle Berechtigungen für Microsoft Exchange 2010 und höher zu erteilen, verwenden Sie ein Konto mit der Rolle "Organisationsverwaltung".

So erteilen Sie minimale Berechtigungen für ein Benutzerkonto zur Durchführung von Datenbank-Backups und -wiederherstellungen von einem Exchange-Server

- ◆ Sie haben folgende Möglichkeiten:

Erteilen von Berechtigungen für ein Benutzerkonto mit der Exchange-Verwaltungskonsolle in Microsoft Exchange 2010 oder Exchange Admin Center in Microsoft Exchange 2013 und höher

Fügen Sie das Benutzerkonto den folgenden Rollen hinzu:

- Öffentliche Ordnerverwaltung
- Empfängerverwaltung
- Serververwaltung

So erteilen Sie minimale Berechtigungen für ein Benutzerkonto unter Verwendung der Exchange-Verwaltungsshell

Gehen Sie dazu in folgender Reihenfolge vor:

- Geben Sie folgenden Befehl ein:

```
new-RoleGroup -Name  
<Rollengruppenname> -Roles  
@("Datenbankkopien",  
"Datenbanken",  
"Exchange-Server",  
"Überwachung", "Erstellung  
von E-Mail-Empfängern",  
"E-Mail-Empfänger",  
"Empfängerrichtlinien"  
"E-Mail-aktivierte  
Öffentliche Ordner",  
"Öffentliche Ordner")
```

Beispiel:

```
new-RoleGroup -Name  
BackupExecRoles -Roles  
@("Datenbankkopien",  
"Datenbanken",  
"Exchange-Server",  
"Überwachung", "Erstellung  
von E-Mail-Empfängern",  
"E-Mail-Empfänger",  
"Empfängerrichtlinien"  
"E-Mail-aktivierte  
Öffentliche Ordner",  
"Öffentliche Ordner")
```

- Geben Sie folgenden Befehl ein:

```
Add-RoleGroupMember -Identity  
<Rollengruppenname> -Member  
<Name des Benutzerkontos>
```

Beispiel:

```
Add-RoleGroupMember -Identity  
BackupExecRoles -Member  
BackupExecUser
```

Erteilen von minimalen Berechtigungen für ein Benutzerkonto zur Unterstützung von Granular Recovery Technology auf Exchange-Servern

Sie können minimale Berechtigungen für ein Benutzerkonto erteilen, mit dem nur Granular Recovery Technology (GRT) auf einem Exchange-Server unterstützt werden kann.

Weitere Informationen zum Empfängerbereich finden Sie in der Microsoft Exchange-Dokumentation.

So erteilen Sie minimale Berechtigungen für ein Benutzerkonto zur ausschließlichen Unterstützung von Granular Recovery Technology auf einem Exchange-Server unter Verwendung der Exchange-Verwaltungsshell

1 Geben Sie folgenden Befehl ein:

```
New-ManagementRole -Name "<Name der Verwaltungsrolle>" -Parent  
ApplicationImpersonation
```

Beispiel:

```
New-ManagementRole -Name "EWSImpersonationRole" -Parent  
ApplicationImpersonation
```

2 Geben Sie folgenden Befehl ein:

```
New-ManagementRoleAssignment -Role "<Name der  
Verwaltungsrollenzuweisung>" -User <Benutzername> -Name  
"<Zuweisungsname>"
```

Beispiel:

```
New-ManagementRoleAssignment -Role "EWSImpersonationRole" -User  
BackupExecUser -Name "BackupExecUser-EWSImpersonation"
```

3 Sie haben folgende Möglichkeiten:

Für Exchange 2010 Geben Sie folgenden Befehl ein:

```
New-ThrottlingPolicy -Name "<Name der  
Drosselungsrichtlinie>" - EWSMaxConcurrency  
$null -PowerShellMaxConcurrency $null  
-EWSMaxSubscriptions $null
```

Beispiel:

```
New-ThrottlingPolicy -Name  
"EWSRestoreThrottlingPolicy" - EWSMaxConcurrency  
$null -PowerShellMaxConcurrency $null  
-EWSPercentTimeInCAS $null -EWSPercentTimeInAD  
$null -EWSPercentTimeInMailboxRPC $null
```

Exchange 2013 und höher Geben Sie folgenden Befehl ein:

```
New-ThrottlingPolicy -Name "<Name der  
Drosselungsrichtlinie>" -EwsCutoffBalance  
Unlimited -EwsMaxBurst Unlimited  
-EwsMaxConcurrency Unlimited -ExchangeMaxCmdlets  
Unlimited -MessageRateLimit Unlimited  
-PowershellCutoffbalance Unlimited  
-PowershellMaxBurst Unlimited  
-PowershellMaxCmdlets Unlimited  
-PowershellMaxConcurrency Unlimited  
-PowershellMaxOperations Unlimited  
-RecipientRateLimit Unlimited  
-ThrottlingPolicyScope Regular
```

Beispiel:

```
New-ThrottlingPolicy -Name  
"EWSRestoreThrottlingPolicy" -EwsCutoffBalance  
Unlimited -EwsMaxBurst Unlimited  
-EwsMaxConcurrency Unlimited -ExchangeMaxCmdlets  
Unlimited -MessageRateLimit Unlimited  
-PowershellCutoffbalance Unlimited  
-PowershellMaxBurst Unlimited  
-PowershellMaxCmdlets Unlimited  
-PowershellMaxConcurrency Unlimited  
-PowershellMaxOperations Unlimited  
-RecipientRateLimit Unlimited  
-ThrottlingPolicyScope Regular
```


4 Geben Sie folgenden Befehl ein:

```
Set-Mailbox -Identity <Benutzername> -ThrottlingPolicy "Name der Drosselungsrichtlinie"
```

Beispiel:

```
Set-Mailbox -Identity BackupExecUser -ThrottlingPolicy "EWSRestoreThrottlingPolicy"
```

5 Geben Sie folgenden Befehl ein:

```
Set-ThrottlingPolicyAssociation -Identity <Benutzername> -ThrottlingPolicy "Name der Drosselungsrichtlinie"
```

Beispiel:

```
Set-ThrottlingPolicyAssociation -Identity BackupExecUser -ThrottlingPolicy "EWSRestoreThrottlingPolicy"
```

Info zur Installation des Exchange Agent

Der Exchange Agent wird als Teil des Agent for Applications and Databases installiert und kann lokale oder Remote-Exchange Server-Datenbanken schützen.

Damit Exchange Agent unterstützt werden kann, muss der Backup Exec-Server Zugriff auf den Exchange Server haben.

Die unterstützten Betriebssysteme, Plattformen, Anwendungen und Service Packs finden Sie in der Liste der mit Backup Exec kompatiblen Software.

Hinweis: Wenn Sie Microsoft Exchange Tools und Backup Exec gemeinsam auf einem Server installieren, muss Exchange Tools zuerst installiert werden. Wenn Sie Backup Exec vor Exchange Tools installieren, müssen Sie den Backup Exec-Server nach Abschluss der Exchange Tools-Installation erneut starten.

Siehe ["Installieren zusätzlicher Agents und Funktionen auf dem lokalen Backup Exec-Server"](#) auf Seite 66.

Hinzufügen von Exchange-Servern und Datenbankverfügbarkeitsgruppe zur Serverliste auf der Registerkarte "Backup und Wiederherstellung"

Sie können der Liste von Servern auf der Registerkarte "Backup und Wiederherstellung" einen Exchange-Server und eine Datenbankverfügbarkeitsgruppe (Database Availability Group, DAG) hinzufügen, damit diese Server für Backup-Aufträge ausgewählt werden können. Wenn Sie in der Gruppe "Server und virtuelle Hosts" auf der Registerkarte "Backup und Wiederherstellung" auf "Hinzufügen" klicken, können Sie Microsoft Windows-Computer und -Server hinzufügen.

Hinweis: Wenn Sie eine Microsoft Exchange-Datenbankverfügbarkeitsgruppe hinzufügen, sollten Sie nach dem Installieren des Agent for Windows jeden Exchange Server manuell neu starten. Wenn Sie auswählen, dass nach der Installation ein automatischer Neustart erfolgen soll, werden möglicherweise alle Exchange-Server in der DAG gleichzeitig neu gestartet.

So fügen Sie einen Exchange-Servers oder DAG zur Serverliste auf der Registerkarte "Backup und Wiederherstellung" hinzu

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" unter "Server und virtuelle Hosts" auf "Hinzufügen".
- 2 Sie haben folgende Möglichkeiten:

So fügen Sie einen Exchange-Server hinzu	Klicken Sie auf "Microsoft Windows-Computer und -Server".
So fügen Sie einen DAG hinzu	Klicken Sie auf "Microsoft Exchange-Datenbankverfügbarkeitsgruppen".
- 3 Klicken Sie auf "Weiter".
- 4 Mit Hilfe des Assistenten "Server hinzufügen" fügen Sie die Exchange-Server oder DAG der Serverliste in der Registerkarte "Backup und Wiederherstellung" hinzu.

Siehe ["Sichern von Exchange-Daten"](#) auf Seite 1290.

So erstellen Sie bevorzugte Server-Konfigurationen für Microsoft Exchange Database Availability Groups (DAG).

Bevorzugte Server-Konfigurationen sind Auflistungen einer oder mehrerer Server und Sites, die Sie als bevorzugte Backup-Quellen auswählen. Bevorzugte Server-Konfigurationen haben als Backup-Quellen Vorrang, wenn Datenbankkopien zwischen mehreren Servern repliziert werden. Sie können bevorzugte Server-Konfigurationen für Microsoft Exchange Database Availability Groups (DAG) erstellen.

Sie müssen keine bevorzugte Server-Konfiguration erstellen, um replizierte Datenbankkopien zu sichern. Sie können Backup Exec den besten Server auswählen lassen, von dem aus die replizierten Datenbankkopien gesichert werden sollen. Die Kennzeichnung einer bevorzugten Server-Konfiguration gibt Ihnen mehr Kontrolle über Ihre Backup-Aufträge. Beispielsweise können Sie eine lokale bevorzugte Server-Konfiguration auswählen, um zu vermeiden, dass replizierte Daten über Ihrem WAN gesichert werden müssen.

Backup Exec bezieht automatisch alle untergeordneten Elemente der Site oder DAG ein, die Sie als Teil der bevorzugten Server-Konfiguration auswählen. Wenn Sie sicherstellen möchten, dass ein Backup lokal durchgeführt wird, können Sie den lokalen Standort als die bevorzugte Server-Konfiguration auswählen. Backup Exec wählt einen beliebigen lokalen Server aus, der während des Backup-Auftrags der Site zugeordnet ist. Wenn Sie sicherstellen möchten, dass ein bestimmter Server für das Backup verwendet wird, wählen Sie nur diesen Server als die bevorzugte Server-Konfiguration aus.

Sie können bevorzugte Server-Konfigurationen für Microsoft Exchange Database Availability Groups (DAG) erstellen. Bevorzugte Server-Konfigurationen geben Ihnen mehr Kontrolle über Ihre Backup-Aufträge, da Sie einen bevorzugten Server angeben können, von dem Backup Exec replizierte Daten sichert.

Dieses Thema enthält Informationen über die folgenden Themen:

- [Erstellen von bevorzugten Server-Konfigurationen](#)
- [Löschen bevorzugter Serverkonfigurationen](#)
- [Festlegen einer bevorzugten Serverkonfiguration als Standard](#)
- [Entfernen des Standardstatus für eine bevorzugte Serverkonfiguration](#)

So erstellen Sie bevorzugte Server-Konfigurationen für Microsoft Exchange Database Availability Groups (DAG).

Erstellen von bevorzugten Server-Konfigurationen

So erstellen Sie bevorzugte Server-Konfigurationen

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Bevorzugte Server".
- 2 Klicken Sie auf "Neu".
- 3 Wählen Sie eine Active Directory-Gesamtstruktur aus, die die Exchange DAG-Mitglieder enthält, die als zum Sichern bevorzugte Server angegeben werden sollen
- 4 Geben Sie einen Namen für die Gruppe bevorzugter Server ein
Sie müssen einen Namen eingeben, bevor die bevorzugte Server-Konfiguration erstellt werden kann.
- 5 Klicken Sie auf "Neu", um die Listen der verfügbaren und ausgewählten Server zu aktivieren, aus denen Sie den bevorzugten Server auswählen.
- 6 Wählen Sie in der Liste "Verfügbare Server" die Server und Sites aus, die Sie in der bevorzugten Serverkonfiguration verwenden möchten.
- 7 Klicken Sie im Dialogfeld "Bevorzugte Server" auf "OK".
- 8 Im Dialogfeld "Bevorzugte Server verwalten" klicken Sie auf "OK".

Löschen bevorzugter Serverkonfigurationen

So löschen Sie bevorzugte Server-Konfigurationen

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Bevorzugte Server".
- 2 Wählen Sie die bevorzugte Server-Konfiguration aus, die Sie löschen möchten.
- 3 Klicken Sie auf "Löschen".
- 4 Klicken Sie auf "OK".

Festlegen einer bevorzugten Serverkonfiguration als Standard

Sie können eine bevorzugte Server-Konfiguration als Standard für alle Backup-Aufträge festlegen, die geeignete Replikationsdaten enthalten. Wenn Sie Daten von einer Microsoft Exchange Database Availability Group sichern, können Sie Backup Exec so einrichten, dass es standardmäßig Ihre bevorzugte Server-Konfiguration verwendet. Sie können die ausgewählte Konfiguration für bevorzugte Server für bestimmte Aufträge in den Backup-Auftragseinstellungen ändern.

Wenn Sie eine Standardkonfiguration für bevorzugte Server festlegen, wird diese nicht auf vorhandene Backup-Aufträge angewendet. Die Konfiguration wird für alle folgenden Backup-Aufträge verwendet, die Sie erstellen.

So legen Sie einen Standard für eine bevorzugte Server-Konfiguration fest

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Bevorzugte Server".
- 2 Wählen Sie die bevorzugte Server-Konfiguration aus, die Sie als Standard festlegen möchten.
- 3 Klicken Sie auf "Als Standard einrichten".
- 4 Klicken Sie auf "OK".

Entfernen des Standardstatus für eine bevorzugte Serverkonfiguration

Wenn die bevorzugte Server-Konfiguration nicht mehr als Standard verwendet werden soll, können Sie den Standardstatus entfernen.

So entfernen Sie den Standard-Status für eine bevorzugte Server-Konfiguration

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie zuerst "Konfiguration und Einstellungen" und dann "Bevorzugte Server".
- 2 Wählen Sie die bevorzugte Server-Konfiguration aus, von der Sie den Standard-Status entfernen möchten.
- 3 Klicken Sie auf "Als Standard entfernen".
- 4 Klicken Sie auf "OK".

Für Exchange empfohlene Konfigurationen

Lesen Sie vor dem Ausführen von Exchange-Backups die folgenden Empfehlungen zur Konfiguration von Exchange, um die Wiederherstellung aus Backups zu vereinfachen:

Tabelle F-3 Für Exchange empfohlene Konfigurationen

Empfehlung	Beschreibung
Speichern Sie Transaktionsprotokolldateien auf einem von der Datenbank physisch getrennten Datenträger.	Diese Konfigurationseinstellung hat die größten Auswirkungen auf die Leistung von Exchange. Die Einstellung ist zudem für die Wiederherstellung wichtig, da Transaktionsprotokolle eine zusätzliche Ressource für die Wiederherstellung darstellen.

Empfehlung	Beschreibung
Deaktivieren Sie auf dem SCSI-Controller die Option "Schreibcache".	Im Windows-Betriebssystem werden keine Puffer verwendet. Wenn daher Exchange von Windows über den Abschluss des Schreibvorgangs benachrichtigt wird, ist der Schreibvorgang auf den Datenträger beendet. Wenn die Option "Schreibcache" aktiviert ist, behandelt Windows den Vorgang so, als sei der Schreibvorgang auf den Datenträger beendet, und diese inkorrekte Information wird an Exchange (oder andere Anwendungen) weitergeleitet. Dadurch kann es zur Beschädigung von Daten kommen, wenn das System nicht mehr reagiert, bevor der Vorgang tatsächlich auf den Datenträger geschrieben wurde.
Deaktivieren Sie nach Möglichkeit die Umlaufprotokollierung.	Die Umlaufprotokollierung minimiert das Risiko, dass die Festplatte mit Transaktionsauftragsprotokollen gefüllt wird. Wenn jedoch eine angemessene Backup-Strategie ausgewählt wurde, werden Transaktionsauftragsprotokolle während des Backups gelöscht, um Speicherplatz freizugeben. Wenn die Umlaufprotokollierung aktiviert ist, werden Transaktionsprotokolle überschrieben und inkrementelle und differenzielle Backups von Speichergruppen und Datenbanken deaktiviert. Die Wiederherstellung kann in diesem Fall nur aus dem letzten vollständigen Backup erfolgen.
Der Exchange-Server sollte nicht als Domänencontroller eingesetzt werden.	Im Falle einer Notfallwiederherstellung ist es sehr viel einfacher, Exchange wiederherzustellen, wenn nicht zuerst Active Directory wiederhergestellt werden muss.
Installieren Sie Exchange in einer Domäne, die über mindestens zwei Domänencontroller verfügt.	Die Replikation von Active Directory ist nur mit mehreren Domänencontrollern in einer Domäne möglich. Falls der Domänencontroller ausfällt und Active Directory beschädigt wird, können einige Transaktionen möglicherweise nicht wiederhergestellt werden, wenn sie nicht im letzten Backup enthalten waren. Mit mindestens zwei Domänencontrollern in einer Domäne können Datenbanken auf dem ausgefallenen Domänencontroller mittels Replikation aktualisiert werden, um nach der Wiederherstellung der Datenbank-Backups fehlende Transaktionen einzufügen.

Siehe ["Voraussetzungen für den Zugriff auf Exchange-Postfächer"](#) auf Seite 1283.

Voraussetzungen für den Zugriff auf Exchange-Postfächer

Für Informationsspeichervorgänge muss Backup Exec Zugriff auf ein eindeutig benanntes Postfach innerhalb der Exchange-Organisation haben, abhängig davon, wie die Backup- und Wiederherstellungsaufträge konfiguriert sind.

Der Zugriff auf ein eindeutig benanntes Postfach ist für folgende Vorgänge erforderlich:

- Konfigurieren eines Backup-Auftrags mit allen der folgenden Einstellungen:
 - Das Zielgerät ist ein anderes Speichergerät als ein Backup-to-Disk-Ordner.
 - Die Funktion "Granular Recovery Technology" ist aktiviert.
 - Es wird eine andere Backup-Methode als eine Snapshot-Methode angewendet.
- Die Wiederherstellung bezieht sich auf Postfächer und öffentliche Ordner.

Wenn Sie Postfächer oder öffentliche Ordner zum Sichern auswählen, müssen Sie ein Backup Exec-Login-Konto für die Verbindung zum Exchange-Server verwenden. Backup Exec sucht nach einem Postfach mit dem gleichen Namen wie dem Benutzernamen, der im Backup Exec-Login-Konto gespeichert ist.

Wenn Sie ein Backup Exec-Login-Konto verwenden, in dem ein eindeutiger Benutzername gespeichert ist und zu dem ein entsprechendes Postfach mit dem gleichen Namen gehört, werden Sie nicht zur Eingabe eines zusätzlichen Login-Kontos aufgefordert. Andernfalls müssen Sie ein Backup Exec-Login-Konto mit dem Namen eines eindeutig benannten Postfachs innerhalb der Exchange-Organisation auswählen oder erstellen.

Ein Name ist eindeutig, wenn seine ersten fünf Zeichen in keinem anderen Postfachnamen verwendet werden. Wenn Sie z. B. EXCH1 als Postfachnamen eingeben und ein anderer Postfachname EXCH1BACKUP vorhanden ist, kann Backup Exec den Namen nicht akzeptieren. Sie werden aufgefordert, einen anderen Postfachnamen auszuwählen.

Sie können ein Login-Konto auswählen oder erstellen, das eine der folgenden Voraussetzungen erfüllt:

- Ein Login-Konto, bei dem der Benutzername einem eindeutigen Postfachnamen entspricht.
- Ein Login-Konto, das ein eindeutiges Alias für ein Postfach verwendet. Das Benutzerkonto, das die Verbindung mit dem Exchange-Server herstellt, muss ebenfalls Zugriff auf dieses Postfach haben.

- Ein Login-Konto, das den vollständigen Computernamen für ein Postfach verwendet. Das Benutzerkonto, das die Verbindung mit dem Exchange-Server herstellt, muss ebenfalls Zugriff auf dieses Postfach haben.

Ein Beispiel für einen vollständigen Computernamen lautet:

/O=Exchange_Organization/OU=Administrative_Group/CN=Recipients/CN=mailbox_name

Siehe ["Granular Recovery Technology"](#) auf Seite 737.

Siehe ["Backup Exec-Login-Konten"](#) auf Seite 762.

Backup-Strategien für Exchange

Backup Exec gewährleistet ständigen Online-Schutz von Exchange-Datenbanken als Teil der täglichen Backup-Routine. Dadurch wird die Leistung von Datenwiederherstellungen erhöht und Datenverluste werden minimiert, ohne dass der tägliche Arbeitsablauf gestört wird. Backup Exec schützt Exchange-Daten bis hin zu einzelnen Datenbanken, Postfächer und öffentlichen Ordnern mit vollständigen, Kopier-, inkrementelle und differenzielle Backups.

Bei der Entscheidung für eine Backup-Methode sind folgende Gesichtspunkte zu berücksichtigen:

- In kleinen Büroumgebungen mit relativ wenigen über das System gesendeten Nachrichten gewährleistet ein tägliches vollständiges Backup einen zuverlässigen Schutz der Daten und die schnellste Wiederherstellung. Bei einem starken Zuwachs von Protokolldateien können beispielsweise mittags inkrementelle Online-Backups ausgeführt werden, um einen zusätzlichen Wiederherstellungspunkt bereitzustellen und den Zuwachs der Protokolldateien automatisch zu verwalten.
- In größeren Umgebungen sollten inkrementelle Backups verwendet werden, um täglich mehrere Wiederherstellungspunkte bereitzustellen und den Zuwachs von Protokolldateien zu verwalten. Viele Unternehmen führen wöchentliche vollständige Backups durch und erstellen während der Woche lediglich inkrementelle Backups, um die Laufzeit der Backups auf ein Minimum zu beschränken. Dem Zeitgewinn durch dieses Verfahren steht die längere Wiederherstellungszeit gegenüber, wenn Daten unter Verwendung eines vollständigen Backups sowie aller inkrementellen Backups wiederhergestellt werden müssen.

Berücksichtigen Sie bei der Auswahl der für Sie am besten geeigneten Lösung die Größe der Umgebung, die Anzahl der täglich verarbeiteten Transaktionen und die Anforderungen Ihrer Benutzer an eine Wiederherstellung.

Entscheiden Sie sich für eine der folgenden Backup-Strategien:

- Führen Sie vollständige Backups mit Aktivierung der Option zum Wiederherstellen einzelner ausgewählter Elemente aus. So können Sie einzelne E-Mail-Nachrichten und -Ordner wiederherstellen, ohne die gesamte Datenbank wiederherstellen zu müssen.

Abhängig von Ihrer Umgebung sollten Sie vollständige Backups wie folgt durchführen:

- So oft wie möglich, jedoch mindestens einmal täglich.
 - Täglich mit regelmäßigen Differenzial-Backups im Tagesverlauf.
 - Im Abstand von mehreren Tagen (mindestens einmal pro Woche) mit häufigen inkrementellen Backups zwischen den einzelnen vollständigen Backups.
- Führen Sie Exchange-Backups getrennt von anderen Backup-Aufträgen aus.

Zusätzlich zum Sichern der Exchange-Datenbanken sollten Sie auch die folgenden Daten regelmäßig sichern:

Tabelle F-4 Backup-Auswahlen für Exchange-Konfigurationsdaten

Empfohlene Backup-Auswahlen für Konfigurationsdaten	Beschreibung
Dateisystem	<p>Sichern Sie Ordner und Laufwerke mit Dateien für Windows und Exchange. Diese befinden sich normalerweise im Stammlaufwerk C:\, je nach Umgebung jedoch möglicherweise auch an einem anderen Speicherort.</p> <p>Hinweis: Sichern Sie das C:\-Laufwerk, jedoch nicht das von Exchange erstellte virtuelle Laufwerk, wenn dieses virtuelle Laufwerk in Ihrer Umgebung vorhanden ist. Es soll lediglich der Zugriff mit Windows Explorer auf Exchange-Daten ermöglicht werden, möglicherweise werden nicht alle Dateisystemfunktionen repliziert. Backup- und Wiederherstellungsvorgänge werden weder empfohlen noch unterstützt.</p>
Windows-Registrierung	<p>Sichern Sie die Registrierung durch ein vollständiges Backup.</p>

Empfohlene Backup-Auswahlen für Konfigurationsdaten	Beschreibung
Systemstatus und/oder Shadow Copy-Komponenten	<p>Wählen Sie Systemstatus und erstellen Sie ein vollständiges Backup, um folgende Komponenten zu sichern:</p> <ul style="list-style-type: none"> ■ Die IIS-Metabasis (Internetinformationsdienste) ■ Windows-Registrierung <p>Siehe "Info zum Auswählen von zu sichernden Daten" auf Seite 186.</p> <p>Wenn der gesamte Server wiederhergestellt werden muss, müssen Sie den Systemstatus und Shadow Copy-Komponenten wiederherstellen.</p>
Active Directory	<p>Wählen Sie zum Sichern von Active Directory auf den Domänencontrollern die Option "Systemstatus", und führen Sie dann ein vollständiges Backup durch.</p> <p>Wenn in der Exchange Server-Datenbank die Konfiguration geändert wurde (beispielsweise durch Hinzufügen, Ändern oder Löschen von Objekten), sichern Sie Active Directory auf den Domänencontrollern.</p> <p>Hinweis: Zur effizienten Replikation von Active Directory sollten Sie mehrere Domänencontroller so in den Domänen verteilen, dass beim Ausfall eines Domänencontrollers weiterhin für Redundanz gesorgt ist.</p>

Hinweis: Konfigurieren Sie ein Informationsspeicher-Backup mit aktivierter Granular Recovery Technology-Funktion (GRT), um einzelne Postfächer, E-Mail-Nachrichten und öffentliche Ordner wiederherzustellen.

Siehe ["Granular Recovery Technology"](#) auf Seite 737.

Siehe ["Notfallwiederherstellung für Exchange-Server"](#) auf Seite 1316.

Wie Granular Recovery Technology mit dem Exchange-Informationsspeicher funktioniert

Backup Exec Granular Recovery Technology (GRT) lässt Sie einzelne Objekte von einem Informationsspeicher-Backup wiederherstellen, ohne das ganze Backup wiederherstellen zu müssen. Sie sollten die Anforderungen für ein Backup mit aktivierter GRT-Option überprüfen, bevor Sie es konfigurieren.

Siehe ["Granular Recovery Technology"](#) auf Seite 737.

Wenn Sie Elemente auswählen, um von GRT-aktivierten Backups wiederherzustellen, können Sie die oberste Ebene des Informationsspeichers nicht auswählen. Um diese Elemente wiederherzustellen, müssen Sie das gesamte Postfach wiederherstellen.

Hinweis: Wenn Sie eine granulare Wiederherstellung eines verbundenen, gemeinsam genutzten oder Websitepostfachs ausführen, wählen Sie die Option "Benutzerkonten und E-Mail-Postfächer neu erstellen, wenn sie nicht bereits auf dem Zielsystem existieren" nicht. Solche Postfächer müssen manuell erstellt werden, bevor Sie die Wiederherstellung durchführen. Jedoch können Sie Benutzerkonten für verbundene Postfächer wiederherstellen, wenn Sie eine granulare Wiederherstellung des Active Directory aus einem Backup des Domänencontrollers durchführen. Weitere Informationen zum Erstellen solcher Postfächer finden Sie in der Dokumentation zu Microsoft Exchange.

GRT kann auch bei der Erstellung eines Offhost-Backup für den Informationsspeicher aktiviert werden. Mithilfe des Offhost-Backup kann Backup Exec den Backup-Vorgang vom Hostcomputer auf den Backup Exec-Server verschieben. Beim Hostcomputer handelt es sich um den Remote-Computer, auf dem die für das Backup ausgewählten Datenträger vorliegen. Für das Ausführen des Offhost-Backup mit aktivierter GRT-Funktion müssen Sie zunächst die Backup Exec Advanced Disk-based Feature auf dem Backup Exec-Server installieren.

GRT und Microsoft Exchange Web Services

Backup Exec verwendet Microsoft Exchange-Web-Dienste (EWS), um das Granular Recovery Technology-Feature zu unterstützen. EWS bietet Unterstützung für das Wiederherstellen von einzelnen Postfächern, E-Mails und öffentlichen Ordnern aus einem Backup einer Datenbank von Exchange Server 2010 oder höher.

Hinweis: Sie brauchen das MAPI Client- und Collaboration Data Objects-Paket nicht zu installieren, wenn Sie EWS verwenden, aber .NET 4.0 muss installiert werden.

Um EWS zu verwenden, um einzelne Elemente wiederherzustellen, deaktiviert Backup Exec die Client-Drosselungsrichtlinie für die Ressourcen-Identifikationsdaten, die Sie für den Wiederherstellungsauftrag angeben. Die Client-Drosselungsrichtlinie setzt Begrenzungen der Verbindungsbandbreite auf dem Client Access-Server durch.

Backup Exec erstellt auch eine Identitätswechselrolle und eine Rollenzuweisung für Exchange-Identitätswechsel. Die Zuweisung der Exchange-Personifizierungsrolle verbindet die Personifizierungsrolle mit den Backup Exec-Ressourcen-Identifikationsdaten, die Sie für den Wiederherstellungsauftrag angeben.

Backup Exec erstellt die folgenden Rollen und weist sie zu:

- EWSImpersonationRole
- EWSImpersonationRoleAssignment

Siehe ["Granular Recovery Technology"](#) auf Seite 737.

Siehe ["Konfigurieren der Optionen für Instant GRT und Vollständige Katalogisierung zum Verbessern der Backup-Leistung von GRT-Aufträgen"](#) auf Seite 656.

Siehe ["Info zum Einsatz von Advanced Disk-based Backup Feature"](#) auf Seite 1519.

Snapshot-Backups und Backups auf einem anderen Host mit dem Exchange Agent

Exchange Agent unterstützt nun auch Volumeschattenkopie-Dienst (VSS) von Microsoft. Hierbei handelt es sich um einen Snapshot-Provider-Dienst, der nur unter Windows Server 2008 und höher verfügbar ist. Mit VSS wird eine Momentaufnahme (Zeitpunktansicht) der Exchange-Datenbank als sog. Snapshot erstellt und anschließend gesichert. Die eigentliche Exchange-Datenbank bleibt geöffnet und für Benutzer verfügbar.

Mit dem Offhost-Backup kann der Backup-Vorgang auf einem Backup Exec-Server anstatt auf dem Exchange-Server verarbeitet werden. Die Ausführung des Backup auf einem Backup Exec-Server statt auf dem Exchange-Server ermöglicht eine höhere Backup-Leistung und verringert die Last des Remote-Computers.

Wenn ADBO (Advanced Disk-based Backup Feature) auf dem Backup Exec-Server installiert ist, können Sie das Backup Exec GRT Feature beim Erstellen eines Offhost-Backup des Informationsspeichers einsetzen.

Siehe ["Festlegen von Standardoptionen für Granular Recovery Technology festlegen \(GRT\)"](#) auf Seite 744.

Dieser Abschnitt enthält Informationen zu folgenden Themen:

- [Snapshot-Backup für Exchange-Daten konfigurieren](#)
- [Fehlerbehebung für Exchange Agent-Snapshot-Aufträge und Aufträge auf einem anderen Host](#)

Folgende Funktionen werden von Exchange Agent-Snapshots nicht unterstützt:

- NAS-Konfigurationen
- Mischen von Snapshot-Backups und Backups ohne Snapshots
Aufgrund einer Einschränkung in Microsoft Exchange dürfen keine Snapshot-Backups ausgeführt werden, wenn Nicht-Snapshot-Backups als Teil einer Backup-Methode ausgeführt werden. Ebenso sollten keine herkömmlichen Backups verwendet werden, wenn Snapshot-Backups erstellt werden.

Die unterstützten Speichertypen finden Sie in der Liste der mit Backup Exec kompatiblen Hardware.

Die Art der verfügbaren Backup-Methode bei Verwendung von VSS mit Exchange Agent hängt von der Exchange Server-Version ab:

Tabelle F-5 Verfügbare Backup-Methoden für Exchange-Snapshot-Versionen

Exchange-Version	Verfügbare Backup-Methoden
Exchange Server 2010 und höher	<p>Die folgenden Backup-Methoden sind verfügbar:</p> <ul style="list-style-type: none"> ■ Vollständiges Backup ■ Kopier-Backup ■ Differenzielles Backup ■ Inkrementelles Snapshot-Backup ■ Wiederherstellung einzelner Datenbanken

Snapshot-Backup für Exchange-Daten konfigurieren

Sie können ein Snapshot-Backup für Exchange-Daten ausführen.

Tabelle F-6 Snapshot-Backup für Exchange-Daten konfigurieren

Schritt	Aktion
Schritt 1	<p>Es wird empfohlen, vor einem Snapshot-Backup Konsistenzprüfungen auszuführen.</p> <p>Siehe "Sichern von Exchange-Daten" auf Seite 1290.</p>

Schritt	Aktion
Schritt 2	Erstellen Sie einen Exchange-Backup-Auftrag. Siehe "Sichern von Exchange-Daten" auf Seite 1290.
Schritt 3	Wenn Daten, die für Snapshot-Backups nicht unterstützt werden, in der Backup-Auswahl enthalten sind, aktivieren Sie die Option "Logische Datenträger für das Backup nacheinander verarbeiten", damit der Auftrag mit Fehlern fertig gestellt werden kann. Diese Option ist unter "Advanced Disk-based Backup Option" im Dialogfeld "Standardeinstellungen für Backup-Auftrag" und im Dialogfeld "Optionen" für einen Backup-Auftrag enthalten.
Schritt 4	Planen oder starten Sie den Backup-Auftrag. Siehe "Sichern von Daten" auf Seite 174.

Fehlerbehebung für Exchange Agent-Snapshot-Aufträge und Aufträge auf einem anderen Host

Unter folgenden Umständen schlägt ein Exchange Agent-Snapshot-Auftrag fehl:

- Der Exchange Agent-Snapshot schlägt fehl.
- Umlaufprotokollierung ist aktiviert und das inkrementelle oder Differenzial-Backup wurde gewählt.
- Eine nicht unterstützte Version von Exchange wurde installiert. Die unterstützten Versionen von Exchange finden Sie in der Liste der mit Backup Exec kompatiblen Software.

Sichern von Exchange-Daten

Zum Sichern von Exchange-Daten können folgende Objekte ausgewählt werden:

- Einzelne Datenbanken (nur Exchange 2010 und höher)
- Datenbankverfügbarkeitsgruppen (DAG)
Sie müssen einen Exchange Agent-Lizenzschlüssel auf dem Backup Exec-Server für jeden Exchange-Server in der DAG eingeben, den Sie sichern möchten. Sie müssen dann Agent for Windows auf allen Servern in der DAG installieren.

Jede Datenbank innerhalb der DAG muss durch den DAG-Behälter gesichert werden, der in der Serverliste auf der Registerkarte "Backup und Wiederherstellung" angezeigt wird. Der DAG-Container zeigt ein Exchange-Logo auf dem Server an.

Hinweis: Wenn Sie Exchange-Datenbanken hinzufügen, nachdem Sie einen Backup-Auftrag erstellt haben, müssen Sie den Backup-Auftrag bearbeiten, um die neue Auswahl einzuschließen.

Sie können Standardoptionen für Backup-Aufträge für alle Exchange-Backup-Aufträge festlegen. Bei der Erstellung jedes Backup-Auftrags verwendet dieser die Standardoptionen, sofern Sie die Optionen für diesen bestimmten Auftrag nicht ändern.

Automatischer Ausschluss von Exchange-Daten bei Backups auf Datenträgerebene

Wenn Sie einen Datenträger auswählen, der Exchange-Daten zum Sichern enthält, verwendet der Exchange Agent die Funktion "Aktiver Dateiausschluss", um Exchange-Daten, die nicht enthalten sein sollten, automatisch aus einem Backup auf Datenträgerebene auszuschließen. Beispielsweise sollten EDB- und STM-Dateien sowie Transaktionsprotokolldateien nicht in ein Backup auf Datenträgerebene aufgenommen werden, da sie zur exklusiven Verwendung von Exchange geöffnet werden.

Wenn der Ausschluss während eines Backup ohne Snapshots nicht erfolgte, werden die Dateien als "gerade benutzt - übersprungen" angezeigt. Während eines Snapshot-Backup werden diese Dateien möglicherweise inkonsistent gesichert, was zu Wiederherstellungsproblemen führen kann.

Obwohl es nicht empfohlen wird, können Sie Exchange-Daten in ein Backup auf Datenträgerebene einschließen. Dazu müssen die zu sichernden Speichergruppen zuerst entladen werden, bevor Sie den Backup-Auftrag ausführen.

So sichern Sie Exchange-Daten

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" mit der rechten Maustaste auf den Server mit den Exchange-Daten, die gesichert werden sollen.

Um mehrere Server zu sichern, klicken Sie bei gedrückter Umschalttaste oder Strg-Taste auf die Servernamen und klicken Sie dann mit der rechten Maustaste auf einen der ausgewählten Server.

- 2 Wählen Sie "Backup" und anschließend den Typ des durchzuführenden Backups aus.

- 3** Klicken Sie im Dialogfeld "Eigenschaften der Backup-Definition" im Feld "Auswahl" auf "Bearbeiten".
- 4** Aktivieren Sie im Dialogfeld "Backup-Auswahl" die zu sichernden Ressourcen, und deaktivieren Sie die Ressourcen, die nicht gesichert werden sollen.
- 5** Klicken Sie auf "OK".
- 6** Klicken Sie im Dialogfeld "Eigenschaften der Backup-Definition" im Feld "Backup" auf "Bearbeiten".
- 7** Klicken Sie im Dialogfeld "Backup-Optionen" im linken Teilfenster auf "Planen" und wählen Sie anschließend den Zeitplan für diesen Auftrag aus.
- 8** Klicken Sie im Dialogfeld "Backup-Optionen" im linken Teilfenster auf "Speicher" und wählen Sie anschließend ein Speichergerät für diesen Auftrag aus.
- 9** Wählen Sie im Dialogfeld "Backup-Optionen" im linken Teilfenster "Microsoft Exchange".
- 10** Legen Sie eine der folgenden Optionen für diesen Auftrag fest:

Beim Verwenden des Snapshot-Providers Microsoft Volumeschattenkopie-Dienst (VSS) vor dem Backup eine Konsistenzprüfung durchführen

Wählen Sie diese Option aus, um eine Konsistenzprüfung durchzuführen, wenn die Option "Microsoft Volumeschattenkopie-Dienst" ausgewählt ist. Die Option "Microsoft Volumeschattenkopie-Dienst" wird automatisch verwendet, wenn in den Eigenschaften von Advanced Disk-based Backup Option ein Software-Backup ausgewählt ist. Sie können auch den "Microsoft Volumeschattenkopie-Dienst" in den Backup-Eigenschaften von Advanced Open File Option auswählen.

Bei der Konsistenzprüfung des Snapshot wird festgestellt, ob beschädigte Daten vorliegen.

Wenn diese Option aktiviert ist und die davon abhängige Option "Mit Backup fortfahren, wenn Konsistenzprüfung fehlschlägt" nicht ausgewählt wurde, werden die Daten bestimmter, als beschädigt erkannter Exchange-Objekte nicht gesichert. Alle unbeschädigten Exchange-Objekte werden gesichert.

Beispiel: Wenn eine bestimmte Exchange-Datenbankdatei beschädigt ist, wird nur diese aus dem Backup ausgeschlossen. Alle anderen Datenbank- und Transaktionsprotokolldateien werden gesichert.

Wenn die Option "Mit Backup fortfahren, wenn Konsistenzprüfung fehlschlägt" aktiviert wurde, werden alle Exchange-Daten gesichert, egal ob beschädigte Dateien vorhanden sind oder nicht.

Siehe ["Snapshot-Backups und Backups auf einem anderen Host mit dem Exchange Agent"](#) auf Seite 1288.

Mit Backup fortfahren, wenn Konsistenzprüfung fehlschlägt

Wählen Sie diese Option aus, um den Backup-Auftrag fortzusetzen, selbst wenn die Konsistenzprüfung fehlschlägt. Unter Umständen empfiehlt es sich, den Auftrag fortzusetzen, wenn ein Backup der Datenbank im aktuellen Zustand besser ist als überhaupt kein Backup oder wenn Sie eine sehr große Datenbank mit nur einem geringfügigen Problem sichern.

Exchange in einer
Datenbankverfügbarkeitsgruppe

Geben Sie eine der folgenden Backup-Quellen für Exchange an:

- Sichern Sie von der passiven Kopie und wenn diese nicht verfügbar ist, versuchen Sie es mit der aktiven Kopie (empfohlen)
Sichert standardmäßig eine passive Kopie der Datenbank. Bei Exchange 2010 und höher wählt Backup Exec die passive Kopie basierend auf Ihren Einstellungen unter "Bevorzugter Server" aus. Steht jedoch die passive Kopie nicht zur Verfügung, sichert Backup Exec die aktive Kopie der Datenbank. Während des Backups kann die Leistung der Datenbank abnehmen, wenn diese über ein WAN gesichert wird.
- Nur von passiver Kopie sichern (wenn nicht verfügbar, schlägt der Auftrag fehl)
Sichert die passive Kopie der Datenbank. Wenn Backup Exec nicht auf die passive Kopie zugreifen kann, schlägt der Auftrag fehl. In diesem Fall wird weder die aktive noch die passive Datenbank gesichert. Wählen Sie diese Option aus, wenn Sie nicht wünschen, dass die Leistung der aktiven Kopie der Datenbank beeinträchtigt wird.
Bei Exchange Server 2010 und höher wählt Backup Exec die passive Kopie basierend auf Ihren Einstellungen unter "Bevorzugter Server" aus.
Hinweis: Sie müssen die Einstellungen "Bevorzugter Server" konfiguriert haben, um diese Option zu verwenden.
- Nur von aktiver Kopie sichern (wenn nicht verfügbar, schlägt der Auftrag fehl)
Sichert die aktive Kopie der Datenbank. Wenn Backup Exec nicht auf die aktive Kopie zugreifen kann, schlägt der Auftrag fehl. Daher wird weder die aktive noch die passive Kopie gesichert.
Die aktive Kopie enthält neuere Informationen als die passive Kopie. Wenn Sie also die aktive Kopie sichern, verfügen Sie über ein Backup der neuesten Datenbankdaten.
- Nur aus der bevorzugten Serverkonfiguration sichern (Zuerst mit der passiven Kopie und falls

diese nicht verfügbar ist, mit der aktiven Kopie. Der Auftrag schlägt fehl, wenn die Kopien nicht in der bevorzugten Serverkonfiguration verfügbar sind.)

Das Backup kann aus der bevorzugten Serverkonfiguration ausgeführt werden, die Sie als bevorzugte Backup-Quelle angeben. Backup Exec wählt die passive Kopie der Datenbank als erste Backup-Quelle aus. Steht jedoch die passive Kopie der Datenbank nicht zur Verfügung, wählt Backup Exec die aktive Kopie als Backup-Quelle. Sind keine Kopien der Datenbank zum Sichern auf den konfigurierten bevorzugten Servern verfügbar, schlägt der Auftrag fehl.

Siehe ["So erstellen Sie bevorzugte Server-Konfigurationen für Microsoft Exchange Database Availability Groups \(DAG\)."](#) auf Seite 1279.

Bevorzugte Serverkonfiguration

Geben Sie die bevorzugte Serverkonfiguration an, die für die Option "High Availability Server" genutzt werden soll.

Klicken Sie auf "Ändern", um eine neue bevorzugte Serverkonfiguration zu erstellen oder eine vorhandene zu bearbeiten.

Siehe ["So erstellen Sie bevorzugte Server-Konfigurationen für Microsoft Exchange Database Availability Groups \(DAG\)."](#) auf Seite 1279.

Backup-Methode

Geben Sie eine der folgenden Backup-Methoden an, die Sie für diesen Auftrag verwenden möchten:

- **Vollständig – Backup-Datenbanken und Protokolle (Protokolle abschneiden)**
Diese Option sichert die Datenbanken sowie die mit ihnen verknüpften Transaktionsprotokolldateien. Nach dem Sichern der Datenbanken und Transaktionsprotokolle werden die Transaktionsprotokolldateien gelöscht, wenn Transaktionen vollständig in der Datenbank reserviert wurden.
- **Vollständige Kopie – Backup-Datenbanken und Protokolle**
Diese Option sichert die Datenbanken sowie die mit ihnen verknüpften Transaktionsprotokolldateien. Die Transaktionsprotokolle werden nach dem Backup jedoch nicht gelöscht.
Verwenden Sie diese Option, um ein vollständiges Backup einer Datenbank vorzunehmen, ohne den Zustand von derzeit ausgeführten inkrementellen oder differenziellen Backups zu beeinflussen.

Backup Exec Granular Recovery Technology (GRT) zum Aktivieren der Wiederherstellung einzelner Postfächer, E-Mails und öffentlicher Ordner von Informationsspeicher-Backups verwenden

Wählen Sie diese Option aus, um die Wiederherstellung einzelner Elemente von Backups des Informationsspeichers zu aktivieren. Stellen Sie sicher, dass die Backups die Anforderungen für Granular Recovery Technology erfüllen.

Hinweis: Es wird empfohlen, dass Sie GRT-fähige, inkrementelle Exchange-Backups nicht an Deduplizierungsspeichergeräte senden. Die Transaktionsprotokolle enthalten hauptsächlich eindeutige Daten, die sich nicht gut deduplizieren lassen. Optimale Ergebnisse erhalten Sie, wenn Sie eine Backup-Definition, die ein vollständiges Backup von Exchange auf ein Deduplizierungsspeichergerät und dann ein inkrementelles Backup auf ein Festplattenspeichergerät ausführt, erstellen.

Siehe ["Granular Recovery Technology"](#) auf Seite 737.

Siehe ["Konfigurieren der Optionen für Instant GRT und Vollständige Katalogisierung zum Verbessern der Backup-Leistung von GRT-Aufträgen"](#) auf Seite 656.

Backup-Methode

Geben Sie eine der folgenden Exchange-spezifischen Backup-Methoden für diesen Auftrag an:

- **Vollständig – Backup-Datenbanken und Protokolle (Protokolle abschneiden)**
Diese Option sichert die Datenbanken sowie die mit ihnen verknüpften Transaktionsprotokolldateien. Nach dem Sichern der Datenbanken und Transaktionsprotokolle werden die Transaktionsprotokolldateien gelöscht, wenn Transaktionen vollständig in der Datenbank reserviert wurden.
- **Vollständige Kopie – Backup-Datenbanken und Protokolle**
Diese Option sichert die Datenbanken sowie die mit ihnen verknüpften Transaktionsprotokolldateien. Die Transaktionsprotokolle werden nach dem Backup jedoch nicht gelöscht.
Verwenden Sie diese Option, um ein vollständiges Backup einer Datenbank vorzunehmen, ohne den Zustand von derzeit ausgeführten inkrementellen oder differenziellen Backups zu beeinflussen.
- **Differenziell - Protokolle sichern**
Diese Option sichert alle Transaktionsprotokolle, die seit dem letzten vollständigen Backup erstellt oder geändert wurden. Die Transaktionsprotokolle werden nach dem Backup jedoch nicht gelöscht.
Zum Wiederherstellen aus Differenzial-Backups sind das letzte differenzielle und das letzte vollständige Backup erforderlich.
Wenn die Umlaufprotokollierung aktiviert ist, können keine Differenzial-Backups durchgeführt werden.
- **Inkrementell – Protokolle sichern (Protokolle kürzen)**
Diese Option sichert alle Transaktionsprotokolle, die seit dem letzten vollständigen oder inkrementellen Backup erstellt oder geändert wurden. Die Transaktionsprotokolle für bereits in der Datenbank reservierte Transaktionen werden anschließend gelöscht.

Um aus inkrementellen Backups wiederherzustellen, sind das letzte vollständige Backup und alle seitdem ausgeführten inkrementellen Backups erforderlich.
 Siehe "[Snapshot-Backups und Backups auf einem anderen Host mit dem Exchange Agent](#)" auf Seite 1288.

Backup Exec Granular Recovery Technology (GRT) zum Aktivieren der Wiederherstellung einzelner Postfächer, E-Mails und öffentlicher Ordner von Informationsspeicher-Backups verwenden

Wählen Sie diese Option aus, um die Wiederherstellung einzelner Elemente von Backups des Informationsspeichers zu aktivieren. Stellen Sie sicher, dass die Backups die Anforderungen für Granular Recovery Technology erfüllen.

Hinweis: Es wird empfohlen, dass Sie GRT-fähige, inkrementelle Exchange-Backups nicht an Deduplizierungsspeichergeräte senden. Die Transaktionsprotokolle enthalten hauptsächlich eindeutige Daten, die sich nicht gut deduplizieren lassen. Optimale Ergebnisse erhalten Sie, wenn Sie eine Backup-Definition, die ein vollständiges Backup von Exchange auf ein Deduplizierungsspeichergerät und dann ein inkrementelles Backup auf ein Festplattenspeichergerät ausführt, erstellen.

Siehe "[Granular Recovery Technology](#)" auf Seite 737.

Siehe "[Konfigurieren der Optionen für Instant GRT und Vollständige Katalogisierung zum Verbessern der Backup-Leistung von GRT-Aufträgen](#)" auf Seite 656.

11 Legen Sie alle zusätzlichen Optionen für diesen Auftrag fest.

Siehe "[Sichern von Daten](#)" auf Seite 174.

12 Klicken Sie auf "OK".

Siehe "[Hinzufügen von Exchange-Servern und Datenbankverfügbarkeitsgruppe zur Serverliste auf der Registerkarte "Backup und Wiederherstellung"](#)" auf Seite 1278.

Siehe "[Ändern der Standardeinstellungen für Backup-Aufträge](#)" auf Seite 630.

Siehe "[Bearbeiten von Backup-Definitionen](#)" auf Seite 226.

Siehe "[Bearbeiten von Stufen](#)" auf Seite 245.

Festlegen von Standard-Backup-Optionen für Exchange Server

Sie können die bei der Installation von Backup Exec für alle Exchange-Server-Aufträge festgelegten Standardeinstellungen verwenden oder eigene Standardeinstellungen wählen. Sie können die Standardeinstellungen übergehen, wenn Sie einzelne Aufträge erstellen.

So legen Sie die Standard-Backup-Optionen für Exchange Server fest

- 1** Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- 2** Wählen Sie "Auftragsstandardeinstellungen" und dann eine Backup-Option.
Beispiel: Wenn Sie die Standardoptionen für Exchange Server-Backups einrichten möchten, wählen Sie "Backup-to-Disk". Die Optionen, die angezeigt werden, hängen von den konfigurierten Speichergerätetypen ab. Sie können verschiedene Standardoptionen für die Backup-Aufträge konfigurieren, die Sie an verschiedene Speichergerätetypen senden.
- 3** Klicken Sie im linken Teilfenster auf "Microsoft Exchange".
- 4** Wählen Sie die entsprechenden Optionen aus.

Beim Verwenden des Snapshot-Providers Microsoft Volumeschattenkopie-Dienst (VSS) vor dem Backup eine Konsistenzprüfung durchführen

Wählen Sie diese Option aus, um eine Konsistenzprüfung durchzuführen, wenn die Option für Volume Shadow Copy Service ausgewählt ist. Die Option "Microsoft Volumeschattenkopie-Dienst" wird automatisch verwendet, wenn in den Eigenschaften von Advanced Disk-based Backup Option ein Software-Backup ausgewählt ist. Sie können auch den "Microsoft Volumeschattenkopie-Dienst" in den Backup-Eigenschaften von Advanced Open File Option auswählen.

Bei der Konsistenzprüfung des Snapshot wird festgestellt, ob beschädigte Daten vorliegen.

Wenn diese Option aktiviert ist und die davon abhängige Option "Mit Backup fortfahren, wenn Konsistenzprüfung fehlschlägt" nicht ausgewählt wurde, werden die Daten bestimmter, als beschädigt erkannter Exchange-Objekte nicht gesichert. Alle unbeschädigten Exchange-Objekte werden gesichert.

Beispiel: Wenn eine bestimmte Exchange-Datenbankdatei beschädigt ist, wird nur diese aus dem Backup ausgeschlossen. Alle anderen Datenbank- und Transaktionsprotokolldateien werden gesichert.

Wenn die Option "Mit Backup fortfahren, wenn Konsistenzprüfung fehlschlägt" aktiviert wurde, werden alle Exchange-Daten gesichert, egal ob beschädigte Dateien vorhanden sind oder nicht.

Siehe ["Snapshot-Backups und Backups auf einem anderen Host mit dem Exchange Agent"](#) auf Seite 1288.

Mit Backup fortfahren, wenn Konsistenzprüfung fehlschlägt

Wählen Sie diese Option aus, um den Backup-Auftrag fortzusetzen, selbst wenn die Konsistenzprüfung fehlschlägt. Unter Umständen empfiehlt es sich, den Auftrag fortzusetzen, wenn ein Backup der Datenbank im aktuellen Zustand besser ist als überhaupt kein Backup oder wenn Sie eine sehr große Datenbank mit einem nur geringfügigen Problem sichern.

Exchange in einer
Datenbankverfügbarkeitsgruppe

Geben Sie eine der folgenden Backup-Quellen für Exchange an:

- Sichern Sie von der passiven Kopie und wenn diese nicht verfügbar ist, versuchen Sie es mit der aktiven Kopie (empfohlen)

Sichert standardmäßig eine passive Kopie der Datenbank. Bei Exchange 2010 und höher wählt Backup Exec die passive Kopie basierend auf Ihren Einstellungen unter "Bevorzugter Server" aus. Steht jedoch die passive Kopie nicht zur Verfügung, sichert Backup Exec die aktive Kopie der Datenbank. Während des Backups kann die Leistung der Datenbank abnehmen, wenn diese über ein WAN gesichert wird.

- Nur von passiver Kopie sichern (wenn nicht verfügbar, schlägt der Auftrag fehl)

Sichert die passive Kopie der Datenbank. Wenn Backup Exec nicht auf die passive Kopie zugreifen kann, schlägt der Auftrag fehl. In diesem Fall wird weder die aktive noch die passive Datenbank gesichert. Wählen Sie diese Option aus, wenn Sie nicht wünschen, dass die Leistung der aktiven Kopie der Datenbank beeinträchtigt wird. Bei Exchange Server 2010 und höher wählt Backup Exec die passive Kopie basierend auf Ihren Einstellungen unter "Bevorzugte Server" aus.

Hinweis: Sie müssen die Einstellungen "Bevorzugter Server" konfiguriert haben, um diese Option zu verwenden.

- Nur von aktiver Kopie sichern (wenn nicht verfügbar, schlägt der Auftrag fehl)

Sichert die aktive Kopie der Datenbank. Wenn Backup Exec nicht auf die aktive Kopie zugreifen kann, schlägt der Auftrag fehl. Daher wird weder die aktive noch die passive Kopie gesichert.

Die aktive Kopie enthält neuere Informationen als die passive Kopie. Wenn Sie also die aktive Kopie sichern, verfügen Sie über ein Backup der neuesten Datenbankdaten.

- Nur aus der bevorzugten Serverkonfiguration sichern (Zuerst mit der passiven Kopie und falls diese nicht verfügbar ist, mit der aktiven Kopie. Der Auftrag schlägt fehl, wenn die Kopien nicht in der bevorzugten Serverkonfiguration verfügbar sind.)

Das Backup kann aus der bevorzugten Serverkonfiguration ausgeführt werden, die Sie als

bevorzugte Backup-Quelle angeben. Backup Exec wählt die passive Kopie der Datenbank als erste Backup-Quelle aus. Steht jedoch die passive Kopie der Datenbank nicht zur Verfügung, wählt Backup Exec die aktive Kopie als Backup-Quelle. Sind keine Kopien der Datenbank zum Sichern auf den konfigurierten bevorzugten Servern verfügbar, schlägt der Auftrag fehl.

Siehe ["So erstellen Sie bevorzugte Server-Konfigurationen für Microsoft Exchange Database Availability Groups \(DAG\)."](#) auf Seite 1279.

Backup-Methode

Geben Sie eine der folgenden Backup-Methoden an, die Sie für diesen Auftrag verwenden möchten:

- **Vollständig – Backup-Datenbanken und Protokolle (Protokolle abschneiden)**
Diese Option sichert die Datenbanken sowie die mit ihnen verknüpften Transaktionsprotokolldateien. Nach dem Sichern der Datenbanken und Transaktionsprotokolle werden die Transaktionsprotokolldateien gelöscht, wenn Transaktionen vollständig in der Datenbank reserviert wurden.
- **Vollständige Kopie – Backup-Datenbanken und Protokolle**
Diese Option sichert die Datenbanken sowie die mit ihnen verknüpften Transaktionsprotokolldateien. Die Transaktionsprotokolle werden nach dem Backup jedoch nicht gelöscht.
Verwenden Sie diese Option, um ein vollständiges Backup einer Datenbank vorzunehmen, ohne den Zustand von derzeit ausgeführten inkrementellen oder differenziellen Backups zu beeinflussen.

Backup Exec Granular Recovery Technology (GRT) zum Aktivieren der Wiederherstellung einzelner Postfächer, E-Mail-Nachrichten und öffentlicher Ordner von Informationsspeicher-Backups verwenden

Wählen Sie diese Option aus, um die Wiederherstellung einzelner Elemente von Backups des Informationsspeichers zu aktivieren. Stellen Sie sicher, dass die Backups die Anforderungen für Granular Recovery Technology erfüllen.

Hinweis: Es wird empfohlen, dass Sie GRT-fähige, inkrementelle Exchange-Backups nicht an Deduplizierungsspeichergeräte senden. Die Transaktionsprotokolle enthalten hauptsächlich eindeutige Daten, die sich nicht gut deduplizieren lassen. Optimale Ergebnisse erhalten Sie, wenn Sie eine Backup-Definition, die ein vollständiges Backup von Exchange auf ein Deduplizierungsspeichergerät und dann ein inkrementelles Backup auf ein Festplattenspeichergerät ausführt, erstellen.

Siehe ["Granular Recovery Technology"](#) auf Seite 737.

Siehe ["Konfigurieren der Optionen für Instant GRT und Vollständige Katalogisierung zum Verbessern der Backup-Leistung von GRT-Aufträgen"](#) auf Seite 656.

Backup-Methode

Wählen Sie eine der folgenden Exchange-spezifischen Backup-Methoden für diesen Auftrag aus:

- **Vollständig – Backup-Datenbanken und Protokolle (Protokolle abschneiden)**
Diese Option sichert die Datenbanken sowie die mit ihnen verknüpften Transaktionsprotokolldateien. Nach dem Sichern der Datenbanken und Transaktionsprotokolle werden die Transaktionsprotokolldateien gelöscht, wenn Transaktionen vollständig in der Datenbank reserviert wurden.
- **Vollständige Kopie – Backup-Datenbanken und Protokolle**
Diese Option sichert die Datenbanken sowie die mit ihnen verknüpften Transaktionsprotokolldateien. Die Transaktionsprotokolle werden nach dem Backup jedoch nicht gelöscht.
Verwenden Sie diese Option, um ein vollständiges Backup einer Datenbank vorzunehmen, ohne den Zustand von derzeit ausgeführten inkrementellen oder differenziellen Backups zu beeinflussen.
- **Differenziell - Protokolle sichern**
Diese Option sichert alle Transaktionsprotokolle, die seit dem letzten vollständigen Backup erstellt oder geändert wurden. Die Transaktionsprotokolle werden nach dem Backup jedoch nicht gelöscht.
Zum Wiederherstellen aus Differenzial-Backups sind das letzte differenzielle und das letzte vollständige Backup erforderlich.
- **Inkrementell – Protokolle sichern (Protokolle kürzen)**
Diese Option sichert alle Transaktionsprotokolle, die seit dem letzten vollständigen oder inkrementellen Backup erstellt oder geändert wurden. Die Transaktionsprotokolle für bereits in der Datenbank reservierte Transaktionen werden anschließend gelöscht.
Um aus inkrementellen Backups wiederherzustellen, sind das letzte vollständige Backup und alle seitdem ausgeführten inkrementellen Backups erforderlich.
Siehe ["Snapshot-Backups und Backups auf einem anderen Host mit dem Exchange Agent"](#) auf Seite 1288.

Wenn die Umlaufprotokollierung aktiviert ist, können keine inkrementellen und differenziellen Backups durchgeführt werden.

Backup Exec Granular Recovery Technology (GRT) zum Aktivieren der Wiederherstellung einzelner Postfächer, E-Mails und öffentlicher Ordner von Informationsspeicher-Backups verwenden

Wählen Sie diese Option, um die Wiederherstellung einzelner Elemente aus inkrementellen Backups des Informationsspeichers zu aktivieren. Stellen Sie sicher, dass die Backups die Anforderungen für Granular Recovery Technology erfüllen.

Hinweis: Es wird empfohlen, dass Sie GRT-fähige, inkrementelle Exchange-Backups nicht an Deduplizierungsspeichergeräte senden. Die Transaktionsprotokolle enthalten hauptsächlich eindeutige Daten, die sich nicht gut deduplizieren lassen. Optimale Ergebnisse erhalten Sie, wenn Sie eine Backup-Definition, die ein vollständiges Backup von Exchange auf ein Deduplizierungsspeichergerät und dann ein inkrementelles Backup auf ein Festplattenspeichergerät ausführt, erstellen.

Siehe ["Granular Recovery Technology"](#) auf Seite 737.

Siehe ["Konfigurieren der Optionen für Instant GRT und Vollständige Katalogisierung zum Verbessern der Backup-Leistung von GRT-Aufträgen"](#) auf Seite 656.

5 Klicken Sie auf "OK".

Wiederherstellen von Exchange-Daten

Die Exchange Agents ermöglicht die Wiederherstellung von Exchange-Datenbanken sowie von einzelnen Postfachelementen. Sie können Elemente an ihrem ursprünglichen Ort wiederherstellen oder die Wiederherstellung an einen neuen Ort umleiten.

Hinweis: Der Wiederherstellungsassistent zeigt nur bis zu 30.000 Elemente an. Wenn Sie Daten aus einer Datenbank oder einem Postfach wiederherstellen möchten, die/der mehr als 30.000 Elemente enthält, sollten Sie das Element suchen, das Sie wiederherstellen möchten. Sie können Suchkriterien wie den Datentyp und das Datum des ursprünglichen Backup verwenden, um die Anzahl der ausgegebenen Elemente zu verringern.

Siehe ["Methoden für das Wiederherstellen von Daten in Backup Exec"](#) auf Seite 258.

Die Anforderungen und Verfahren für das Wiederherstellen von Exchange-Daten variieren abhängig von der verwendeten Backup-Strategie. Bevor Sie Exchange-Daten wiederherstellen, sollten Sie die erforderliche Konfiguration und Aufgaben überprüfen.

Sie können Exchange-Daten auf folgende Weisen wiederherstellen:

- Verwenden Sie die Wiederherstellungsdatenbank für die Wiederherstellung von Daten aus einer älteren Backup-Kopie des Speichers, ohne den Zugriff von Clients auf aktuelle Daten zu behindern.
- Wiederherstellen von Exchange-Daten aus Snapshot-Backups
- Stellen Sie einzelne Austauschfelder von einem Backup zurück, das für granulierte Wiederanlauf-Technologie aktiviert wird (GRT).
Siehe ["Wie Granular Recovery Technology mit dem Exchange-Informationsspeicher funktioniert"](#) auf Seite 1287.
- Wiederherstellen von Exchange-Daten auf einem anderen Server als demjenigen, auf dem gesichert wurde.

Dieses Thema enthält folgende Informationen:

- [Anforderungen für das Wiederherstellen von Exchange](#)
- [Eine Zieldatenbank für Wiederherstellungsdaten in Exchange konfigurieren](#)
- [Wiederherstellen von Daten mit der Wiederherstellungsdatenbank von Exchange Server 2010 und höher](#)
- [Wiederherstellen von Exchange-Daten aus Snapshot-Backups](#)
- [Wiederherstellen einzelner Meldungen aus dem öffentlichen Exchange-Ordner vom Band durch Duplizieren von Backup-Sätzen](#)
- [Umleiten von Exchange-Wiederherstellungsdaten](#)
- [Info zum Umleiten von Exchange-Postfachelementen](#)

Anforderungen für das Wiederherstellen von Exchange

Überprüfen Sie Folgendes, bevor Sie Exchange wiederherstellen:

- Die Datenbanken müssen bereits auf dem Zielsystem vorhanden sein und denselben Namen wie die ursprünglichen Datenbanken haben.
- Der Zielsystem muss denselben Organisations- und Verwaltungsgruppennamen wie der Quellsystem aufweisen.
- Bevor Sie die Wiederherstellung beginnen, konfigurieren Sie die Zieldatenbanken, damit sie durch eine Wiederherstellung überschrieben werden können.
- Sie können E-Mails mit Anhängen nicht wiederherstellen, die Kontaktgruppen und nicht lieferbare Berichte enthalten, da Microsoft Exchange Web Services (EWS) for Microsoft Exchange 2013 die Wiederherstellung von Verteilungslisten und E-Mail-Berichten nicht unterstützt, wenn es sich um Anhänge handelt. Es

wird empfohlen, dass Sie E-Mails, die diese Typen von Anhängen enthalten, in einer PST-Datei wiederherstellen.

Eine Zieldatenbank für Wiederherstellungsdaten in Exchange konfigurieren

Bevor Sie Exchange wiederherstellen, sollten Sie die Zieldatenbank konfigurieren.

So konfigurieren Sie eine Datenbank

1 Sie haben folgende Möglichkeiten:

Für Exchange 2010

Öffnen Sie das Exchange-Verwaltungskonsolen-Dienstprogramm.

Für Exchange 2013 und höher

Öffnen Sie die Exchange-Verwaltungskonsole.

2 Klicken Sie mit der rechten Maustaste auf die Datenbank, die Sie überschreiben möchten.

3 Klicken Sie auf "Eigenschaften".

4 Gehen Sie wie folgt vor:

Exchange Server 2010 und höher

Aktivieren Sie auf der Registerkarte "Wartung" die Option "Diese Datenbank kann bei einer Wiederherstellung überschrieben werden".

Wiederherstellen von Daten mit der Wiederherstellungsdatenbank von Exchange Server 2010 und höher

Exchange 2010 und höher ermöglicht das Bereitstellen einer zweiten Kopie des Exchange-Postfachspeichers auf einem Exchange-Server derselben Exchange-Verwaltungsgruppe, in der sich das Original befindet, während der ursprüngliche Speicher weiterhin zum Verarbeiten der Clients verwendet wird. Dies ermöglicht Ihnen die Wiederherstellung von Daten aus einer älteren Backup-Kopie des Speichers, ohne den Zugriff von Clients auf aktuelle Daten zu behindern.

Exchange Server 2010 und höher nutzt Wiederherstellungsdatenbanken (RDB). Jeder Server hat eine Wiederherstellungsdatenbank und es kann nicht mehr als eine bereitgestellte Wiederherstellungsdatenbank geben.

Beachten Sie Ihre Microsoft Exchange-Dokumentation, um weitere Informationen über RDBs und Wiederherstellungsdatenbanken zu erhalten.

Nachdem die Wiederherstellungsdatenbank erstellt wurde, können Online-Backup-Sätze dort wiederhergestellt werden. Anschließend können Sie die Version des Dienstprogramms "Exchange-Verwaltungsshell" in Exchange verwenden, um Postfachdaten aus den Speichern in PST-Dateien zu extrahieren bzw. die extrahierten Daten in die Online-Speicher zurückzuführen.

Wenn sich die Wiederherstellungsdatenbank auf einem anderen Exchange-Server als die wiederherzustellenden Datenbanken befindet, machen Sie sich mit den Voraussetzungen für die Umleitung von Exchange-Wiederherstellungsdatenbanken vertraut.

Umleiten von Exchange-Wiederherstellungsdaten

Für das Wiederherstellen von Daten unter Verwendung der Wiederherstellungsdatenbank aus Exchange Server 2010 und höher gelten folgende Anforderungen:

- Wenn für die Wiederherstellung mehrere Speicher ausgewählt werden, müssen die Postfachspeicher in der RDB aus der gleichen Datenbank stammen. Zu einer Wiederherstellungsdatenbank können nicht gleichzeitig Postfachspeicher aus verschiedenen Speichergruppen hinzugefügt werden.
- Das Wiederherstellen von Speichern für öffentliche Ordner mithilfe der RDB wird nicht unterstützt.
- Laden Sie vor dem Wiederherstellen keine Postfachspeicher in die Wiederherstellungsdatenbank. Wenn Sie vor der Wiederherstellung die Speicher geladen haben, müssen Sie sie wieder entladen. Wählen Sie auf der Eigenschaftsseite der Datenbank in Exchange System Manager die folgende Option aus:
Diese Datenbank kann bei einer Wiederherstellung überschrieben werden
Löschen Sie dann alle Dateien, die im Dateipfad für die RDB erstellt wurden, sowie hinzugefügte Speicher, bevor Sie mit der Wiederherstellung beginnen.
Alle Dateien, die im Datenpfad für die RDB erstellt wurden, sowie hinzugefügte Speicher sollten ebenfalls gelöscht werden, wenn die Speicher vor der Wiederherstellung geladen wurden.
- Auf dem Host-Server der RDB muss für die wiederherzustellenden Daten eine Datenbank mit dem gleichen Namen wie die ursprüngliche Datenbank vorhanden sein. Wenn auf dem Server keine solche Datenbank vorhanden ist, können Sie diesen Namen für die RDB verwenden, wenn Sie diese erstellen.
- Die Active Directory-Topologie des Exchange-Systems muss intakt und in demselben Zustand wie zum Zeitpunkt des Backup sein. Postfachspeicher, die gelöscht und neu erstellt wurden, können nicht wiederhergestellt werden. Zudem können keine Postfächer aus Speichern wiederhergestellt werden, wenn die Postfächer gelöscht und aus dem System entfernt oder zu anderen Servern oder Postfachspeichern verschoben wurden.

- Wenn die RDB auf einem Server gespeichert ist, sind die darin enthaltenen Postfachspeicher die einzigen Speicher, die standardmäßig auf diesem Server wiederhergestellt werden können. Das Erstellen der RDB empfiehlt sich nur, wenn mithilfe dieser Daten wiederhergestellt werden sollen. Die RDB sollte nach Abschluss der Datenwiederherstellung vom Server gelöscht werden.
- Sie können mehr als eine Wiederherstellungsdatenbank haben, jedoch können Sie nur eine bereitstellen.
- Stellen Sie die Wiederherstellungsdatenbank nicht bereit vor der Wiederherstellung. Wenn Sie die Wiederherstellungsdatenbank bereitstellen vor der Wiederherstellung, müssen Sie die Bereitstellung aufheben. Wählen Sie die Option "Diese Datenbank kann bei einer Wiederherstellung überschrieben werden" auf der Datenbank-Eigenschaftsseite in der Exchange-Management-Konsole aus.

Lesen Sie Ihre Microsoft Exchange Server-Dokumentation, um weitere Informationen zu erhalten über die Anforderungen und die Einschränkungen beim Wiederherstellen von Exchange-Daten.

Wiederherstellen von Exchange-Daten aus Snapshot-Backups

Beachten Sie Folgendes, wenn Sie Exchange-Daten aus Snapshot-Backups wiederherstellen:

- Bei aktivierter Umlaufprotokollierung sind nur Point-In-Time und Verlustwiederherstellungen möglich. Roll-Forwards und Wiederherstellungen ohne Verlust können nicht durchgeführt werden.

Siehe ["Snapshot-Backups und Backups auf einem anderen Host mit dem Exchange Agent"](#) auf Seite 1288.

Wiederherstellen einzelner Meldungen aus dem öffentlichen Exchange-Ordner vom Band durch Duplizieren von Backup-Sätzen

Zum Wiederherstellen einzelner Meldungen aus dem öffentlichen Ordner vom Band müssen die Backup-Sätze, die die Meldungen enthalten, zunächst in einen Datenträgerspeicher kopiert werden. Sie können die Daten aus diesem Datenträgerspeicher dann wiederherstellen.

Das Backup, aus dem Sie wiederherstellen, muss allerdings ein vollständiges Backup oder Kopier-Backup sein. Wenn ein auf das vollständige Backup folgendes inkrementelles oder Differenzial-Backup vorliegt, können Sie einzelne Elemente auch aus dem inkrementellen oder Differenzial-Backup wiederherstellen. Die Backup-Sätze für das vollständige Backup und das inkrementelle oder das Differenzial-Backup müssen sich auf dem gleichen Datenträger befinden.

Es ist nicht möglich, einzelne Meldungen aus öffentlichen Ordnern vom Band wiederherzustellen, die mithilfe der inkrementellen Methode gesichert wurden.

So stellen Sie einzelne Meldungen aus dem öffentlichen Exchange-Ordner vom Band durch Duplizieren von Backup-Sätzen auf Backup-to-Disk wieder her

- 1 Legen Sie das Band/Medium mit den erforderlichen Exchange-Backup-Sätzen in das entsprechende Bandlaufwerk ein.

- 2 Erstellen Sie einen Auftrag zum Duplizieren von Backup-Sätzen.

Siehe ["Manuelles Duplizieren von Backup-Sätzen bzw. Auftragsverläufen"](#) auf Seite 246.

- 3 Führen Sie nach Abschluss des Auftrags einen Wiederherstellungsauftrag aus, um von den Exchange-Backup-Sätzen, die im Datenträgerspeicher dupliziert sind, die einzelnen Meldungen aus dem öffentlichen Ordner wiederherzustellen.

Siehe ["Methoden für das Wiederherstellen von Daten in Backup Exec"](#) auf Seite 258.

Umleiten von Exchange-Wiederherstellungsdaten

Mithilfe von Backup Exec können Exchange-Daten auf dem Server wiederhergestellt werden, auf dem das Backup erstellt wurde, oder an einen anderen Speicherort umgeleitet werden. Zum Umleiten von Daten sollte auf dem ursprünglichen Exchange-Server und auf dem Exchange-Server, an den die Daten umgeleitet wurden, die gleiche Service Pack-Version installiert sein.

Im Folgenden finden Sie Anforderungen zum Umleiten von Exchange-Datenbankwiederherstellungen:

- Die Datenbanken müssen bereits auf dem Zielsystem vorhanden sein.
- Der Zielsystem muss denselben Organisationsgruppennamen wie der Quellsystem aufweisen.
- Die Zieldatenbanken müssen so konfiguriert sein, dass sie überschrieben werden können.

Siehe [„Eine Zieldatenbank für Wiederherstellungsdaten in Exchange konfigurieren“](#) auf Seite 1311.

In folgenden Fällen kann eine Wiederherstellung nicht umgeleitet werden:

- Wiederherstellen einer Exchange Server-Datenbank in eine Datenbank mit einer anderen Exchange-Version. Auch die Versionen der installierten Service Packs müssen für beide Exchange-Server übereinstimmen.
- Wiederherstellen von Standortreplikationsdiensten (SRS) und Schlüsselverwaltungsdiensten (KMS). Diese Dienste sind an den Computer

gebunden, auf dem sie installiert sind. Umleitungen zu einem anderen Computer werden nicht unterstützt und können zu einer Beeinträchtigung der Funktion dieser Dienste führen.

Hinweis: KMS ist in Exchange nicht verfügbar.

Bevor Sie den umgeleiteten Wiederherstellungsauftrag durchführen, machen Sie sich mit dem Auswählen und Anzeigen von wiederherzustellenden Daten sowie den Wiederherstellungsoptionen und das Erstellen von Wiederherstellungsaufträgen vertraut.

Es wird empfohlen, im Anschluss an die Wiederherstellung ein vollständiges Backup der wiederhergestellten Datenbanken durchzuführen.

Siehe "[Sichern von Exchange-Daten](#)" auf Seite 1290.

Info zum Umleiten von Exchange-Postfachelementen

Mit Backup Exec können Sie Postfachelemente wie z. B. Postfächer und öffentliche Ordner in einem anderen Postfach auf demselben Server oder an einem anderen Speicherort wiederherstellen.

Sie können auch Postfächer oder Postfachelemente in einer PST-Datei (einer Microsoft Outlook-Datendatei) wiederherstellen, die mit Microsoft Outlook 2007 oder 2010 kompatibel ist.

Es folgen die Anforderungen zum Umleiten von Exchange-Postfächern und öffentlichen Ordnern und des allgemeinen Ordners zurück in Exchange:

- Der angegebene Speicher für das Postfach bzw. den öffentlichen Ordner muss existieren.
- Das Backup Exec-Login-Konto muss Rechte für das Zielpostfach haben.
- Um Daten des vorhandenen öffentlichen Ordners zu überschreiben, muss das Login-Konto Eigentümer der öffentlichen Daten sein. In dieser seltenen Situation sollten Sie beim Wiederherstellen von Daten aus öffentlichen Ordnern nicht die Wiederherstellungsoption "Vorhandene E-Mails und -Ordner überschreiben" auf der Seite "Wie sollen die Elemente wiederhergestellt werden?" des Wiederherstellungsassistenten verwenden.

Es folgen Anforderungen für das Wiederherstellen in eine PST-Datei:

- Agent for Windows muss auf dem Zielsystem installiert sein, auf dem Sie das Postfach oder die Elemente des öffentlichen Ordners umgeleitet werden.
- Microsoft Outlook 2007 oder 2010 (nur 32 Bi) muss auf dem Zielsystem installiert sein.

Hinweis: Die maximale Größe der .PST-Datei ist 20 GB. Wenn die Wiederherstellung die Maximalgröße übersteigt, werden die Daten auf mehrere PST-Dateien aufgeteilt, die aufeinanderfolgend nummeriert werden.

Notfallwiederherstellung für Exchange-Server

Um Exchange im Notfall schnell und zuverlässig wiederherstellen zu können, ist ein Plan für die Notfallwiederherstellung erforderlich. Da in Exchange die Windows-Sicherheitsoptionen zur Authentifizierung verwendet werden, kann die Notfallwiederherstellung von Exchange nicht von der Notfallwiederherstellung von Windows getrennt ausgeführt werden.

Durch vorausschauende Planung kann die für die Wiederherstellung benötigte Zeit minimiert werden.

Es ist von entscheidender Bedeutung, ein Notfall-Kit mit folgenden Elementen zusammenzustellen:

- Informationen zur Konfiguration des Betriebssystems
- Informationen zur Konfiguration der Festplattenpartition
- Alle RAID-Konfigurationen
- Informationen zur Hardware-Konfiguration
- EISA/MCA-Konfigurationsdisketten
- Informationen zur Exchange-Konfiguration
- Windows-Notfall-CD

Zum Ausführen der eigentlichen Wiederherstellung benötigen Sie folgende Elemente:

- Backup Exec muss installiert sein
- Die zuletzt ausgeführten vollständigen, inkrementellen und differenziellen Backups der wiederherzustellenden Exchange-Datenbanken
- Die Microsoft Exchange Server-Installations-CD
- Alle Service Packs, die auf die ursprüngliche Installation angewendet wurden

Sie können Simplified Disaster Recovery verwenden, um den Exchange-Server wiederherzustellen.

Siehe ["Hinweise zum Einsatz von Simplified Disaster Recovery mit Exchange, SQL, SharePoint, CAS, Hyper-V-Hosts und Deduplication Feature"](#) auf Seite 999.

Im Folgenden werden die Arbeitsschritte für eine vollständige Wiederherstellung von Exchange mithilfe von Backup Exec beschrieben. Sie sollten bereits alle entsprechenden Vorbereitungen getroffen haben.

Verwenden Sie für dieses Verfahren zum Einloggen unter Windows stets das Administratorkonto (oder ein dem Administratorkonto entsprechendes Konto).

Weitere Voraussetzungen:

- Die Datenbanken müssen bereits auf dem Zielsystem vorhanden sein und denselben Namen wie die ursprünglichen Datenbanken haben.
- Der Zielsystem muss denselben Organisations- und Verwaltungsgruppennamen wie der Quellsystem aufweisen.
- Die Zieldatenbanken müssen so konfiguriert sein, dass sie überschrieben werden können.

Siehe "[Wiederherstellen von Exchange-Daten](#)" auf Seite 1309.

So führen Sie eine Notfallwiederherstellung für Exchange aus

- 1** Stellen Sie zunächst den Windows-Server wieder her.

Stellen Sie die Wiederherstellung der Exchange-Server-Dateien sicher, die auf allen Datenträgerpartitionen vorhanden waren.

- 2** Überprüfen Sie im Dienste-Applet, ob die Microsoft Exchange-Informationsspeicherdienste gestartet wurden.

- 3** Starten Sie Backup Exec.

- 4** Katalogisieren Sie die Backup-Sätze der Exchange Server-Datenbanken, die Sie wiederherstellen möchten.

Siehe "[Backup-Sätze](#)" auf Seite 401.

- 5** Führen Sie den Wiederherstellungsassistenten aus und wählen Sie den neuesten vollständigen Backup-Satz jeder Datenbank für die Wiederherstellung aus.

Siehe "[Methoden für das Wiederherstellen von Daten in Backup Exec](#)" auf Seite 258.

- 6** Wählen Sie bei Bedarf alle folgenden inkrementellen Backup-Sätze aus.

Wenn differenzielle Backup-Sätze wiederhergestellt werden sollen, muss nur der neueste Satz ausgewählt werden.

- 7** Es wird empfohlen, im Anschluss an die Wiederherstellung ein vollständiges Backup der wiederhergestellten Datenbanken durchzuführen.

Backup Exec Agent for Microsoft SharePoint

Dieser Anhang enthält folgende Themen:

- [Info zum Microsoft SharePoint-Agent](#)
- [Installieren des Microsoft SharePoint-Agent](#)
- [Anforderungen an den Microsoft SharePoint-Agent](#)
- [Einsatz des Agent for Microsoft SharePoint mit SharePoint Server 2010/2013/2016 und SharePoint Foundation 2010/2013/2016](#)
- [Hinzufügen einer Microsoft SharePoint-Serverfarm zur Serverliste auf der Registerkarte "Backup- und Wiederherstellung"](#)
- [Sichern von Microsoft SharePoint-Daten](#)
- [Wiederherstellen von Microsoft SharePoint-Daten](#)
- [Deaktivieren oder Aktivieren der Verbindung zwischen einem Microsoft SharePoint-Webserver und Backup Exec](#)
- [Anzeigen oder Ändern der Eigenschaften von SharePoint-Farmen](#)
- [Notfallwiederherstellung von Microsoft SharePoint 2010/2013/2016-Daten](#)

Info zum Microsoft SharePoint-Agent

SharePoint Agent ermöglicht Netzwerkadministratoren das Durchführen von Backup- und Wiederherstellungsaufträgen in allen unterstützten Microsoft SharePoint-Installationen, die mit einem Netzwerk verbunden sind. SharePoint-Backups können ohne zusätzlichen Verwaltungsaufwand oder spezielle

Hardware in Netzwerk-Backups integriert werden. Der Agent for Microsoft SharePoint wird als Teil des Agent for Applications and Databases installiert.

Die vom SharePoint Agent unterstützten Plattformen finden Sie in der Liste der mit Backup Exec kompatiblen Software.

Informationen zu den Best Practices zum Einsatz des Backup Exec Agent for Microsoft SharePoint (SharePoint Agent) finden Sie unter *Best Practices für Backup Exec*.

Siehe ["Einsatz des Agent for Microsoft SharePoint mit SharePoint Server 2010/2013/2016 und SharePoint Foundation 2010/2013/2016"](#) auf Seite 1320.

Installieren des Microsoft SharePoint-Agent

Bevor Sie Microsoft SharePoint-Server-Farmen sichern können, müssen Sie den Microsoft SharePoint-Agent (SharePoint Agent) auf dem Backup Exec-Server installieren. Der SharePoint Agent wird als Teil des Agent for Applications and Databases installiert.

Siehe ["Installieren zusätzlicher Agents und Funktionen auf dem lokalen Backup Exec-Server"](#) auf Seite 66.

Siehe ["Installieren von Backup Exec auf Remote-Computern über die Push-Installation"](#) auf Seite 68.

Siehe ["Anforderungen an den Microsoft SharePoint-Agent"](#) auf Seite 1319.

Anforderungen an den Microsoft SharePoint-Agent

Für den Microsoft SharePoint-Agent (SharePoint Agent) müssen die folgenden Anforderungen beachtet werden:

- Der SharePoint Agent muss auf dem Backup Exec-Server installiert werden.
- Agent for Windows muss auf jedem standortfernen SharePoint-Server installiert werden, den Sie schützen möchten. Darüber hinaus muss Agent for Windows auf allen Servern in der Server-Farm installiert werden.
- Sie müssen ein Login-Konto verwenden, das über lokale Administratorrechte verfügt, um SharePoint-Daten zu sichern und wiederherzustellen. Das Konto sollte lokale Administratorrechte auf den Servern besitzen, auf denen die SharePoint-Komponenten installiert sind.
- Das Login-Konto, mit dem Sie Inhalte einer vorhandenen Sammlung wiederherstellen, muss die Berechtigungen zum Erstellen von Objekten in dieser

Sammlung haben. Wenn Sie Inhalt in einer Sammlung installieren, die nicht existiert, wird das Login-Konto zum primären Eigentümer der Sammlung.

- Rechte von Internetinformationsdiensten (IIS) können Backups und Wiederherstellungen einer Datenbank beeinflussen. Das Login-Konto, das Sie für Backup und Wiederherstellung verwenden, muss Zugangsrechte für die IIS-Sites besitzen. Integrierte Windows-Sicherheitsoptionen sollten innerhalb der IIS-Rechte deaktiviert sein.

Anforderungen an das jeweilige Betriebssystem für den SharePoint Agent finden Sie in der Liste der mit Backup Exec kompatiblen Software.

Einsatz des Agent for Microsoft SharePoint mit SharePoint Server 2010/2013/2016 und SharePoint Foundation 2010/2013/2016

Der Agent for Microsoft SharePoint unterstützt Microsoft Office SharePoint Server 2010/2013/2016 und SharePoint Foundation 2010/2013/2016.

SharePoint Server stellt Metadatenfunktionen bereit, einschließlich Tags, Lesezeichen für soziale Netze und Inhaltsbewertungen. Diese Typen von Metadaten werden in den Dienstanwendungen gespeichert, die sich außerhalb der Inhaltsdatenbank befinden. Beispielsweise befinden sich unternehmensweit verwaltete Tags in der Managed Metadata Service-Anwendung. Sie sollten alle Ihre Dienstanwendungen sichern, um zu gewährleisten, dass alle Metadaten geschützt sind.

Außerhalb der Inhaltsdatenbank gespeicherte Metadaten können nicht unter Verwendung der Granular Recovery Technology (GRT) wiederhergestellt werden. Sie können GRT jedoch verwenden, um SharePoint-Daten mit den Metadaten wiederherzustellen, die mit ihnen verknüpft sind. Solange die Metadaten sich in der gleichen Dienstanwendung befinden, hält SharePoint die Verknüpfung zwischen Daten und Metadaten aufrecht.

Sie können die folgenden Typen von SharePoint Server-Daten sichern und wiederherstellen:

- Webanwendungen und die damit verbundenen Datenbanken
- Einzelne Dokumente und Bilder, die in Bibliotheken enthalten sind
- Sites und Teilsites
Einzelne Objekte und ihre Versionen können von den vollständigen Datenbank-Backups wiederhergestellt werden.
- Listen und Listen-Objekte

Einzelne Objekte und ihre Versionen können aus den vollständigen Datenbank-Backups wiederhergestellt werden.

- Konfigurationsdatenbank
Eine Konfigurationsdatenbank enthält alle Konfigurationsinformationen für die gesamte SharePoint-Serverfarm. Gehen Sie bei der Wiederherstellung dieser Datenbank vorsichtig vor. Alle Änderungen, die Sie vor dem Wiederherstellen aus dem Backup an der Farm-Topologie vornehmen, gehen verloren. Die Konfigurationsdatenbank kann nur am ursprünglichen Speicherort wiederhergestellt werden.
- Dienstanwendungen

Siehe ["Notfallwiederherstellung von Microsoft SharePoint 2010/2013/2016-Daten"](#) auf Seite 1334.

Hinzufügen einer Microsoft SharePoint-Serverfarm zur Serverliste auf der Registerkarte "Backup- und Wiederherstellung"

Bevor Sie Microsoft SharePoint-Daten sichern können, müssen Sie auf der Registerkarte "Backup und Wiederherstellung" eine SharePoint-Serverfarm zur Serverliste hinzufügen. Wenn Sie einen einzelnen SharePoint-Server für das Hinzufügen auswählen, fügt Backup Exec die gesamte Farm hinzu, zu dem dieser Server gehört.

Hinzufügen einer Microsoft SharePoint-Serverfarm zur Serverliste auf der Registerkarte "Backup und Wiederherstellung"

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" unter "Server und virtuelle Hosts" auf "Hinzufügen".
- 2 Sie haben folgende Möglichkeiten:

So fügen Sie einen einzelnen SharePoint-Server hinzu	Klicken Sie auf "Microsoft Windows-Computer und -Server".
So fügen Sie eine SharePoint-Serverfarm hinzu	Klicken Sie auf "Microsoft SharePoint-Serverfarmen".
- 3 Klicken Sie auf "Weiter".
- 4 Mit Hilfe des Assistenten "Server hinzufügen" fügen Sie die SharePoint-Serverfarm der Serverliste in der Registerkarte "Backup und Wiederherstellung" hinzu.

Siehe ["Serverliste auf der Registerkarte "Backup und Wiederherstellung""](#) auf Seite 166.

Sichern von Microsoft SharePoint-Daten

Der Agent for Microsoft SharePoint ermöglicht Netzwerkadministratoren das Durchführen von Backup-Aufträgen in allen Microsoft SharePoint-Installationen, die mit einem Netzwerk verbunden sind. SharePoint-Backups können ohne zusätzlichen Verwaltungsaufwand oder spezielle Hardware in Netzwerk-Backups integriert werden.

Weitere Informationen zu bestimmten Typen von SharePoint-Inhalten, die Sie sichern können, finden Sie hier:

Siehe ["Einsatz des Agent for Microsoft SharePoint mit SharePoint Server 2010/2013/2016 und SharePoint Foundation 2010/2013/2016"](#) auf Seite 1320.

Die dynamische Einbeziehungsfunktion von Backup Exec schützt automatisch neue Ressourcen, die hinzugefügt werden, nachdem ein Backup-Auftrag erstellt wurde. Erkennt Backup Exec, dass Sie eine neue Ressource als untergeordnetes Element einer geschützten Ressource hinzugefügt haben, wird die neue Ressource automatisch gesichert. Da der Backup-Auftrag neue Ressourcen enthalten kann, kann das Ausführen des Auftrags mehr Speicherplatz und Zeit erfordern als erwartet.

Sie können Standardoptionen für Backup-Aufträge für alle SharePoint-Backup-Aufträge festlegen. Bei der Erstellung jedes Backup-Auftrags verwendet dieser die Standardoptionen, sofern Sie die Optionen für diesen bestimmten Auftrag nicht ändern.

Hinweis: Viele Backup-Optionen sind verfügbar, die nicht in der folgenden Prozedur beschrieben werden. Informationen zu Backup-Optionen und -Methoden finden Sie im folgenden Thema:

Siehe ["Sichern von Daten"](#) auf Seite 174.

So sichern Sie Microsoft SharePoint-Daten

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" mit der rechten Maustaste auf den zu sichernden SharePoint-Server bzw. die Farm.

Um mehrere Server zu sichern, klicken Sie bei gedrückter Umschalttaste oder Strg-Taste auf die Servernamen und klicken Sie dann mit der rechten Maustaste auf einen der ausgewählten Server.
- 2 Wählen Sie "Backup" und anschließend den Typ des durchzuführenden Backups aus.

- 3 Klicken Sie im Dialogfeld "Eigenschaften der Backup-Definition" im Feld "Auswahl" auf "Bearbeiten".
- 4 Aktivieren Sie im Dialogfeld "Backup-Auswahl" die zu sichernden Ressourcen, und deaktivieren Sie die Ressourcen, die nicht gesichert werden sollen.
- 5 Klicken Sie auf "OK".
- 6 Klicken Sie im Dialogfeld "Eigenschaften der Backup-Definition" im Feld "Backup" auf "Bearbeiten".
- 7 Klicken Sie im Dialogfeld "Backup-Optionen" im linken Teilfenster auf "Planen" und wählen Sie anschließend den Zeitplan für diesen Auftrag aus.
- 8 Klicken Sie im Dialogfeld "Backup-Optionen" im linken Teilfenster auf "Speicher" und wählen Sie dann das Speichergerät aus, das Sie für den Backup-Auftrag verwenden möchten.
- 9 Klicken Sie im Dialogfeld "Backup-Optionen" im linken Teilfenster auf "Microsoft SharePoint".
- 10 Legen Sie eine der folgenden Optionen für diesen Auftrag fest:

Konsistenzprüfung Legen Sie fest, ob eine vollständige Konsistenzprüfung (einschließlich vor dem Backup der in Microsoft SharePoint verwendeten Microsoft SQL-Datenbanken durchgeführt werden soll, bevor Sie die Datenbanken sichern.

Mit Backup fortfahren, wenn Konsistenzprüfung fehlschlägt Legen Sie fest, dass der Backup-Vorgang fortgesetzt werden soll, selbst wenn die Konsistenzprüfung fehlschlägt.

Backup-Methode Geben Sie eine der folgenden Backup-Methoden an, die Sie für diesen Auftrag verwenden möchten:

- **Vollständig - Datenbanken sichern**
Sichert die gesamte Datenbank.
- **Vollständig kopieren – Datenbanken (Kopie) sichern**
Diese Option sichert die gesamte Datenbank, ohne Auswirkung auf zukünftige Differenzial- oder Protokoll-Backups.
Anders als bei vollständigen Backups wird bei der Methode "Vollständig kopieren" der Basis-Backup-Satz für Differenzial-Backups nicht zurückgesetzt. Dieser gibt die seit dem letzten vollständigen Backup geänderten Datenblöcke an.
Nach einem vollständigen Backup können Sie mit der Backup-Methode "Vollständig kopieren" eine Kopie der Datenbank erstellen, ohne dass sich dies auf den für zukünftige Differenzial-Backups erforderlichen Basis-Backup-Satz auswirkt.

Backup Exec Granular Recovery Technology (GRT) Legen Sie fest, ob die Wiederherstellung einzelner Dokumente, Bilder, Sites, Teilsites, Listen und Listeneinträge von Datenbank-Backups ausgeführt werden soll. Es muss eine aktuelle Version von Agent for Windows auf dem SharePoint-Server installiert sein, wenn Sie den GRT-aktivierten Backup-Auftrag ausführen.

verwenden,
um die
Wiederherstellung
einzelner
Elemente des
DatenbankBackups
zu aktivieren

Backup-Methode Geben Sie eine der folgenden SharePoint-spezifischen Backup-Methoden an, die Sie für diesen Auftrag verwenden möchten:

- **Vollständig - Datenbanken sichern**
Sichert die gesamte Datenbank.
- **Vollständig kopieren – Datenbanken (Kopie) sichern**
Diese Option sichert die gesamte Datenbank, ohne Auswirkung auf zukünftige Differenzial- oder Protokoll-Backups.
Anders als bei vollständigen Backups wird bei der Methode "Vollständig kopieren" der Basis-Backup-Satz für Differenzial-Backups nicht zurückgesetzt. Dieser gibt die seit dem letzten vollständigen Backup geänderten Datenblöcke an.
Nach einem vollständigen Backup können Sie mit der Backup-Methode "Vollständig kopieren" eine Kopie der Datenbank erstellen, ohne dass sich dies auf den für zukünftige Differenzial-Backups erforderlichen Basis-Backup-Satz auswirkt.
- **Differenziell - Nur seit dem letzten vollständigen Backup vorgenommene Datenbankänderungen sichern**
Sichert nur die Änderungen, die seit dem letzten vollständigen Backup an der Datenbank vorgenommen wurden.
- **Differenziell (Blockebene) - Sichert Datenbankänderungen seit dem letzten vollständigen Backup.**
Diese Option sichert alle Datenblöcke und Transaktionsprotokolle, die seit dem letzten vollständigen Backup erstellt oder geändert wurden.
- **Inkrementell (Blockebene): Sichert Datenbankänderungen seit dem letzten vollständigen oder inkrementellen Backup.**
Diese Option sichert alle Datenblöcke und Transaktionsprotokolle, die seit dem letzten vollständigen oder inkrementellen Backup erstellt oder geändert wurden.
- **Protokoll - Transaktionsprotokoll sichern und kürzen**
Sichert die Daten im Transaktionsprotokoll. Die Datenbankdaten werden bei dieser Methode nicht gesichert. Nach dem Sichern des Transaktionsprotokolls werden reservierte Transaktionen entfernt (abgeschnitten).
Wenn die Datenbanken für das einfache SQL Server-Wiederherstellungsmodell konfiguriert sind, werden Backups von Protokolldateien nicht unterstützt. Um das Wiederherstellungsmodell zu ändern, verwenden Sie die SQL-Administrationstools, um das Wiederherstellungsmodell auf "Vollständig" festzulegen. Sie sollten ein neues vollständiges Backup ausführen, wenn Sie das Wiederherstellungsmodell ändern, bevor ein Backup von Protokolldateien ausgeführt wird.

Backup Exec Granular Recovery Technology (GRT) verwenden, um die Wiederherstellung einzelner Elemente des Datenbank-Backups zu aktivieren

Legen Sie für diesen Auftrag fest, ob die Wiederherstellung von einzelnen Dokumenten, Bildern, Sites, Subsites, Listen und Listenelementen aus Datenbank-Backups aktiviert werden soll. Es muss eine aktuelle Version von Agent for Windows auf dem SharePoint-Server installiert sein, wenn Sie den GRT-aktivierten Backup-Auftrag ausführen.

Siehe ["Granular Recovery Technology"](#) auf Seite 737.

Siehe ["Konfigurieren der Optionen für Instant GRT und Vollständige Katalogisierung zum Verbessern der Backup-Leistung von GRT-Aufträgen"](#) auf Seite 656.

- 11 Klicken Sie im Dialogfeld "Backup-Optionen" auf eine der für diesen Auftrag festzulegenden optionalen Einstellungen.
 - 12 Klicken Sie auf "OK".
 - 13 Klicken Sie im Dialogfeld "Eigenschaften der Backup-Definition" auf "OK".
- Siehe ["Ändern der Standardeinstellungen für Backup-Aufträge"](#) auf Seite 630.
- Siehe ["Sichern von Daten"](#) auf Seite 174.
- Siehe ["Bearbeiten von Backup-Definitionen"](#) auf Seite 226.

Festlegen der Standard-Backup-Optionen für SharePoint

Sie können die bei der Installation von Backup Exec für alle SharePoint-Aufträge festgelegten Standardeinstellungen verwenden oder eigene Standardeinstellungen wählen. Sie können die Standardeinstellungen übergehen, wenn Sie einzelne Aufträge erstellen.

So legen Sie die Standard-Backup-Optionen für SharePoint fest

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- 2 Wählen Sie "Auftragsstandardeinstellungen" und dann eine Backup-Option.

Beispiel: Wenn Sie die Standardoptionen für SharePoint-Backup-to-Disk einrichten möchten, wählen Sie "Backup-to-Disk". Die Optionen, die angezeigt werden, hängen von den konfigurierten Speichergerätetypen ab. Sie können verschiedene Standardoptionen für die Backup-Aufträge konfigurieren, die Sie an verschiedene Speichergerätetypen senden.
- 3 Klicken Sie im linken Teilfenster auf "Microsoft SharePoint".
- 4 Wählen Sie die entsprechenden Optionen aus.

- Konsistenzprüfung** Wählen Sie die Durchführung einer vollständigen Konsistenzprüfung vor dem Backup der in Microsoft SharePoint verwendeten Microsoft SQL-Datenbanken durchführen (einschließlich der Indizes) der Microsoft SQL-Datenbanken in Microsoft SharePoint aus, bevor Sie die Datenbanken sichern.
- Mit Backup fortfahren, wenn **Konsistenzprüfung** fehlschlägt Legen Sie fest, dass der Backup-Vorgang fortgesetzt werden soll, selbst wenn die Konsistenzprüfung fehlschlägt.
- Backup-Methode** Geben Sie eine der folgenden Backup-Methoden an, die Sie für diesen Auftrag verwenden möchten:
- **Vollständig - Datenbanken sichern**
Sichert die gesamte Datenbank.
 - **Vollständig kopieren – Datenbanken (Kopie) sichern**
Diese Option sichert die gesamte Datenbank, ohne Auswirkung auf zukünftige Differenzial- oder Protokoll-Backups.
Anders als bei vollständigen Backups wird bei der Methode "Vollständig kopieren" der Basis-Backup-Satz für Differenzial-Backups nicht zurückgesetzt. Dieser gibt die seit dem letzten vollständigen Backup geänderten Datenblöcke an.
Nach einem vollständigen Backup können Sie mit der Backup-Methode "Vollständig kopieren" eine Kopie der Datenbank erstellen, ohne dass sich dies auf den für zukünftige Differenzial-Backups erforderlichen Basis-Backup-Satz auswirkt.
- Backup Exec Granular Recovery Technology (GRT)** Legen Sie fest, ob die Wiederherstellung einzelner Dokumente, Bilder, Sites, Teilsites, Listen und Listeneinträge von Datenbank-Backups ausgeführt werden soll. Es muss eine aktuelle Version von Agent for Windows auf dem SharePoint-Server installiert sein, wenn Sie den GRT-aktivierten Backup-Auftrag ausführen.
- Wiederherstellung einzelner Elemente des Datenbank-Backups** zu aktivieren

Backup-Methode Geben Sie eine der folgenden SharePoint-spezifischen Backup-Methoden an, die Sie für diesen Auftrag verwenden möchten:

- **Vollständig - Datenbanken sichern**
Sichert die gesamte Datenbank.
- **Vollständig kopieren – Datenbanken (Kopie) sichern**
Diese Option sichert die gesamte Datenbank, ohne Auswirkung auf zukünftige Differenzial- oder Protokoll-Backups.
Anders als bei vollständigen Backups wird bei der Methode "Vollständig kopieren" der Basis-Backup-Satz für Differenzial-Backups nicht zurückgesetzt. Dieser gibt die seit dem letzten vollständigen Backup geänderten Datenblöcke an.
Nach einem vollständigen Backup können Sie mit der Backup-Methode "Vollständig kopieren" eine Kopie der Datenbank erstellen, ohne dass sich dies auf den für zukünftige Differenzial-Backups erforderlichen Basis-Backup-Satz auswirkt.
- **Differenziell - Nur seit dem letzten vollständigen Backup vorgenommene Datenbankänderungen sichern**
Sichert nur die Änderungen, die seit dem letzten vollständigen Backup an der Datenbank vorgenommen wurden.
- **Differenziell (Blockebene)**
Diese Option sichert alle Datenblöcke und Transaktionsprotokolle, die seit dem letzten vollständigen Backup erstellt oder geändert wurden.
- **Inkrementell (Blockebene)**
Diese Option sichert alle Datenblöcke und Transaktionsprotokolle, die seit dem letzten vollständigen oder inkrementellen Backup erstellt oder geändert wurden.
- **Protokoll - Transaktionsprotokoll sichern und kürzen**
Sichert die Daten im Transaktionsprotokoll. Die Datenbankdaten werden bei dieser Methode nicht gesichert. Nach dem Sichern des Transaktionsprotokolls werden reservierte Transaktionen entfernt (abgeschnitten).
Wenn die Datenbanken für das einfache SQL Server-Wiederherstellungsmodell konfiguriert sind, werden Backups von Protokolldateien nicht unterstützt. Um das Wiederherstellungsmodell zu ändern, verwenden Sie die SQL-Administrationstools, um das Wiederherstellungsmodell auf "Vollständig" festzulegen. Sie sollten ein neues vollständiges Backup ausführen, wenn Sie das Wiederherstellungsmodell ändern, bevor ein Backup von Protokolldateien ausgeführt wird.

Backup Exec Granular Recovery Technology (GRT) verwenden, um die Wiederherstellung einzelner Elemente des Datenbank-Backups zu aktivieren

Legen Sie für diesen Auftrag fest, ob die Wiederherstellung von einzelnen Dokumenten, Bildern, Sites, Subsites, Listen und Listenelementen aus Datenbank-Backups aktiviert werden soll. Es muss eine aktuelle Version von Agent for Windows auf dem SharePoint-Server installiert sein, wenn Sie den GRT-aktivierten Backup-Auftrag ausführen.

Siehe ["Granular Recovery Technology"](#) auf Seite 737.

Siehe ["Konfigurieren der Optionen für Instant GRT und Vollständige Katalogisierung zum Verbessern der Backup-Leistung von GRT-Aufträgen"](#) auf Seite 656.

5 Klicken Sie auf "OK".

Siehe ["Sichern von Microsoft SharePoint-Daten"](#) auf Seite 1322.

Wiederherstellen von Microsoft SharePoint-Daten

Mit Agent for Microsoft SharePoint können Sie folgende Typen von Microsoft SharePoint-Daten im ursprünglichen oder einem anderen Speicherort wiederherstellen:

- Einzelne SharePoint-Elemente wie Dokumente, Bilder, Websites, Unterwebsites, Listen und Listenelemente.
- SharePoint-Webanwendungen oder Portal-Websites und deren Inhalte.
- SharePoint-Farm-Komponenten wie Konfigurationsdatenbanken, Dienstanwendungen, gemeinsam genutzte Dienstanbieter oder andere Komponenten.
- Einzelne SharePoint-Elemente wie Dokumente, Websites und Listenelemente, die über eine Suche gefunden wurden.

Bei der Wiederherstellung von SharePoint-Daten gilt:

- Wenn Sie SharePoint-Daten wiederherstellen, werden einzelne SharePoint-Dokumente immer in den SharePoint-Dokumentbibliotheken wiederhergestellt, aus denen sie ausgecheckt wurden.

Zum Auschecken der Dokumente werden die Anmeldedaten verwendet, die dem für die Wiederherstellung verwendeten Login-Konto entsprechen. Die Dokumente müssen vom entsprechenden Benutzer eingeecheckt oder veröffentlicht werden, bevor sie von anderen Benutzern verwendet werden können.

- Wenn Sie bei der Wiederherstellung versuchen, ein Dokument zu überschreiben, während dieses ausgecheckt ist, kann die Wiederherstellung fehlschlagen. Die Wiederherstellung schlägt fehl, wenn das Dokument von einem anderen als demjenigen Benutzer ausgecheckt wurde, dessen Login-Konto bzw. Anmeldedaten für die Wiederherstellung verwendet wurden.

Siehe ["Methoden für das Wiederherstellen von Daten in Backup Exec"](#) auf Seite 258.

Einzelne Elemente mit Granular Recovery Technology (GRT) wiederherstellen

Backup Exec ermöglicht außerdem die Wiederherstellung einzelner Dokumente, Bilder, Sites, Teilsites, Listen und Listenelemente aus SharePoint-Datenbank-Backups. Um einzelne Elemente aus SharePoint-Datenbank-Backups wiederherzustellen, müssen Sie sicherstellen, dass die folgende Microsoft SharePoint-Option während des Backup-Auftrags ausgewählt ist:

Backup Exec Granular Recovery Technology (GRT) verwenden, um die Wiederherstellung einzelner Elemente des Datenbank-Backups zu aktivieren

Hinweis: Backup Exec unterstützt nicht die Wiederherstellung von granularen Elementen aus komprimierten oder verschlüsselten Datenbanken.

Umgeleitete Wiederherstellungen

In Backup Exec können Sie die Wiederherstellung von folgenden Elementen umleiten:

- Unter SharePoint Server 2016 ermöglicht Backup Exec das Wiederherstellen einzelner Elemente, wie Dokumente und Bilder, auf dem SharePoint-Front-End-Webserver.
- Leiten Sie dateibasierte SharePoint-Daten (z. B. Dokumente und Bilder, die in eine Dokumentbibliothek hochgeladen wurden oder mit Listenelementen verknüpft sind) auf ein NTFS-Dateisystem für SharePoint Server 2010, SharePoint Foundation 2010 und SharePoint Server 2016 um.
Backup Exec kann Dateien direkt in eine SharePoint 2013-Inhaltsdatenbank extrahieren und wieder einfügen. Jedoch können die Dateien nicht für die Umleitung auf Dateisystemebene ausgewählt werden. SharePoint 2013-Inhaltsdatenbankdateien werden als BLOBs in einem geschredderten Format gespeichert. Daher kann Backup Exec die Wiederherstellung der geschredderten BLOBs nicht an ein Dateisystem umleiten.
- Die Wiederherstellung einzelner Elemente wie Dokumente, Websites und Listenelementen von einer auf eine anderen Website.

Hinweis: Diese Funktion wird unter SharePoint Server 2016 nicht unterstützt.

Wenn Sie eine Wiederherstellung von einer Website auf eine andere umleiten, erben die wiederhergestellten Elemente die Sicherheitsberechtigungen des übergeordneten Elements, auf das sie wiederhergestellt werden. Befindet sich die Website in einer anderen SharePoint-Farm, müssen die Versionen von SharePoint identisch sein.

Hinweis: Sie müssen sowohl für den ursprünglichen Webserver als auch den Server in der Website-Sammlung dasselbe Benutzerkonto verwenden, wenn Sie die Wiederherstellung umleiten. Außerdem sollten Sie gewährleisten, dass beide Server denselben NetBIOS-Namen, vollständig qualifizierten Domänenname bzw. IP-Adresse nutzen.

- Wiederherstellen von SharePoint-Datenbanken auf eine andere SQL-Instanz.

Mit der Datenbank haben Sie folgende Möglichkeiten:

- Manuelles Erfassen von Daten mit der Zentraladministrationskonsole von SharePoint 2010/2013/2016
 - Manuelles Anhängen an eine SharePoint-Webanwendung
- Umleiten von SharePoint-Webanwendungsinhaltsdatenbanken auf eine andere Webanwendung.

Das Ziel für die Webanwendung muss online sein und dieselbe Topologie wie die gesicherte Webanwendung haben. Befindet sich die Webanwendung in einer anderen SharePoint-Farm, müssen die Versionen von SharePoint identisch sein.

Vorsicht: Wenn Sie SharePoint Portal-Dokumentbibliotheksdaten wiederherstellen, werden Dokumente am ausgewählten Ziel, die dieselben Namen wie die wiederherzustellenden Dokumente haben, möglicherweise überschrieben. In den Eigenschaften für den Wiederherstellungsauftrag können Sie wählen, ob die Dokumente überschrieben werden sollen.

Weitere Informationen zu den verschiedenen Typen von SharePoint-Inhalten entnehmen Sie der Dokumentation zu Microsoft SharePoint.

Wiederherstellen von Microsoft SharePoint-Daten

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" mit der rechten Maustaste auf den Server, von dem Sie Daten wiederherstellen möchten, und klicken Sie dann auf "Wiederherstellen".
- 2 Wählen Sie "Microsoft SharePoint", und klicken Sie dann auf "Weiter".
- 3 Befolgen Sie die Anweisungen des "Assistenten für Wiederherstellungsaufträge", um die Daten wiederherzustellen.

Siehe ["Einsatz des Agent for Microsoft SharePoint mit SharePoint Server 2010/2013/2016 und SharePoint Foundation 2010/2013/2016"](#) auf Seite 1320.

Deaktivieren oder Aktivieren der Verbindung zwischen einem Microsoft SharePoint-Webserver und Backup Exec

Backup Exec stellt Verbindungen mit den Webservern in Microsoft SharePoint-Serverfarmen her, um die Topologie einer Farm abzurufen. Dieser Vorgang kann einige Zeit in Anspruch nehmen, wenn Backup Exec eine Verbindung zu einem Webserver herzustellen versucht, der nicht verfügbar ist. Wenn ein Webserver in einer Farm für einen bestimmten Zeitraum nicht verfügbar ist, können Sie die Verbindung zwischen diesem Webserver und Backup Exec deaktivieren.

So deaktivieren oder aktivieren Sie die Verbindung zwischen einem SharePoint-Webserver und Backup Exec

- 1 Doppelklicken Sie auf der Registerkarte "Backup und Wiederherstellung" auf die SharePoint-Serverfarm, zu der der Webserver gehört.
- 2 Klicken Sie im linken Teilfenster auf "Eigenschaften".
- 3 Sie haben folgende Möglichkeiten:
 - Wenn die Verbindung zwischen Backup Exec und einem SharePoint-Webserver unterbrochen werden soll, deaktivieren Sie das Kontrollkästchen neben dem Namen des Webserver.
 - Wenn eine Verbindung zwischen Backup Exec und dem SharePoint-Webserver hergestellt werden soll, aktivieren Sie das Kontrollkästchen neben dem Namen des Webserver.
- 4 Klicken Sie auf "Übernehmen".

Anzeigen oder Ändern der Eigenschaften von SharePoint-Farmen

Sie können Eigenschaften für jede SharePoint-Farm anzeigen, die Sie mit Backup Exec überwachen, und einige Eigenschaften ändern. Backup Exec zeigt allgemeine und Systeminformationen über die Farm an.

Sie können über das Dialogfeld mit den SharePoint-Farm-Eigenschaften auch die Verbindung zwischen einem SharePoint-Webserver und Backup Exec aktivieren oder deaktivieren.

Siehe ["Deaktivieren oder Aktivieren der Verbindung zwischen einem Microsoft SharePoint-Webserver und Backup Exec"](#) auf Seite 1332.

Eigenschaften von SharePoint-Farmen anzeigen oder ändern

- 1 Doppelklicken Sie auf der Registerkarte "Backup und Wiederherstellung" auf die SharePoint-Farm, deren Eigenschaften Sie anzeigen möchten.
- 2 Klicken Sie im linken Teilfenster auf "Eigenschaften".

3 Zeigen Sie die Eigenschaften an und ändern Sie sie entsprechend:

SharePoint-Farmname	Zeigt den Namen der SharePoint-Farm an.
Beschreibung	Hier können Sie eine eindeutige Beschreibung eingeben, um die Farm in Backup Exec zu identifizieren. Die Beschreibung ist optional.
Login-Konto	<p>Listet das Login-Konto auf, das Backup Exec für den Zugriff auf die Farm verwendet.</p> <p>Klicken Sie auf "Hinzufügen/Bearbeiten", um ein neues Login-Konto hinzuzufügen bzw. ein vorhandenes Login-Konto zu bearbeiten.</p>
Webserver	<p>Listet die Webserver auf, die zur Farm gehören. Sie können die Verbindung zwischen den Webservern und Backup Exec aktivieren oder deaktivieren.</p> <p>Siehe "Deaktivieren oder Aktivieren der Verbindung zwischen einem Microsoft SharePoint-Webserver und Backup Exec" auf Seite 1332.</p>

4 Wenn Sie Änderungen vorgenommen haben, klicken Sie auf "Übernehmen".

Notfallwiederherstellung von Microsoft SharePoint 2010/2013/2016-Daten

Sie können den Agent for Microsoft SharePoint verwenden, um einen Microsoft SharePoint-Server nach einem Festplattenausfall wiederherzustellen. Bevor Sie die SharePoint-Daten wiederherstellen können, müssen Sie das Betriebssystem des SharePoint-Servers wiederherstellen.

Sie können das Simplified Disaster Recovery Feature aus Backup Exec verwenden oder das Betriebssystem des Servers manuell wiederherstellen.

Weitere Informationen zum Ausführen einer manuellen Wiederherstellung finden Sie in den folgenden Abschnitten:

Siehe ["Durchführen einer manuellen Notfallwiederherstellung eines lokalen Backup Exec-Servers auf einem Windows-Computer"](#) auf Seite 1006.

Siehe ["Manuelles Ausführen der Notfallwiederherstellung eines Remote-Backup Exec-Servers oder Remote-Agent auf einem Windows-Computer"](#) auf Seite 1011.

Siehe ["Info zu Simplified Disaster Recovery"](#) auf Seite 941.

Nachdem der Windows-Server wiederhergestellt wurde, können Sie die SharePoint-Daten wiederherstellen. Führen Sie dazu die Anweisungen in der Tabelle der Reihe nach aus.

Tabelle G-1 So stellen Sie SharePoint-Daten nach einem Notfall wieder her

Schritt	Aktion	Hinweise
Schritt 1	Stellen Sie die Master- und die Modelldatenbanken für die von SharePoint genutzten SQL-Instanzen wieder her. Sie müssen diesen Schritt ausführen, wenn Sie das Betriebssystem des Servers manuell wiederhergestellt haben.	Überspringen Sie diesen Schritt, wenn Sie das Simplified Disaster Recovery Feature aus Backup Exec zum Wiederherstellen des Betriebssystems des Servers verwendet haben. Siehe "Manuelle Wiederherstellung eines SQL Server " auf Seite 1264.
Schritt 2	Wählen Sie die wiederherzustellenden Medien aus.	Siehe "Inventarisieren eines Speichergeräts" auf Seite 550.
Schritt 3	Katalogisieren Sie die wiederherzustellenden Medien.	Siehe "Katalogisieren eines Speichergeräts" auf Seite 548.

Schritt	Aktion	Hinweise
Schritt 4	Stellen Sie die MSDB-Datenbanken für die von SharePoint genutzten SQL-Instanzen wieder her.	<p>Wählen Sie die Backup-Sätze, die MSDB-Datenbanken für die von SharePoint genutzten SQL-Instanzen enthalten.</p> <p>Konfigurieren Sie die folgenden Microsoft SQL-Wiederherstellungsoptionen:</p> <ul style="list-style-type: none"> ■ Benutzen Sie die Standardeinstellungen für alle Wiederherstellungsaufträge. ■ Wählen Sie "Vorhandene Datenbanken automatisch überschreiben" aus. <p>Siehe "Methoden für das Wiederherstellen von Daten in Backup Exec" auf Seite 258.</p>
Schritt 5	Stellen Sie alle Webanwendungen wieder her.	<p>Wählen Sie die Backup-Sätze für alle SharePoint-Webanwendungen aus.</p> <p>Wählen Sie "Ja, bei Wiederherstellung vorhandene Datenbanken überschreiben".</p> <p>Siehe "Methoden für das Wiederherstellen von Daten in Backup Exec" auf Seite 258.</p>

Schritt	Aktion	Hinweise
Schritt 6	Wiederherstellen gemeinsam genutzter Dienstanwendungsdatenbanken.	<p>Stellen Sie die folgenden gemeinsam genutzten Dienstanwendungsdatenbanken wieder her:</p> <ul style="list-style-type: none"> ■ Business Data Connectivity Service ■ Managed Metadata Service ■ PerformancePoint Service Application ■ Search Service Application ■ Secure Store Service ■ User Profile Service Application ■ Web Analytics Service Application ■ Word Automation Services ■ Services\State Services\Service DB 1 <p>Wählen Sie "Ja, bei Wiederherstellung vorhandene Datenbanken überschreiben".</p> <p>Siehe "Methoden für das Wiederherstellen von Daten in Backup Exec" auf Seite 258.</p> <p>Hinweis: Manche der verbleibenden Wiederherstellungsaufträge können fehlschlagen, da die Verbindung mit dem SharePoint-Server noch nicht vollständig aufgebaut wurde. Dies ist zu erwarten. Setzen Sie den Wiederherstellungsvorgang fort, bis alle Schritte abgeschlossen sind.</p>

Schritt	Aktion	Hinweise
Schritt 7	Wiederherstellen von Suchdiensten	<p>Stellen Sie folgende Dienste wieder her:</p> <ul style="list-style-type: none"> ■ SharePoint Foundation Help Search\Search Instance\Index Files 1 ■ Search-DB 1 <p>Wählen Sie "Ja, bei Wiederherstellung vorhandene Datenbanken überschreiben".</p> <p>Siehe "Methoden für das Wiederherstellen von Daten in Backup Exec" auf Seite 258.</p> <p>Hinweis: Sie erhalten möglicherweise die Meldung im Auftragsprotokoll, Ihren Computer neu zu starten. Sie können die Meldung ignorieren.</p>
Schritt 8	Stellen Sie die Ressource "SharePoint-Konfigurationsdatenbank V4/V5-DB" wieder her.	<p>Wählen Sie die Backup-Sätze für die Ressource "SharePoint-Konfigurationsdatenbank V4".</p> <p>Wählen Sie "Ja, bei Wiederherstellung vorhandene Datenbanken überschreiben".</p> <p>Siehe "Methoden für das Wiederherstellen von Daten in Backup Exec" auf Seite 258.</p>
Schritt 9	Starten Sie den SharePoint-Server neu.	<p>Starten Sie nach Abschluss des Wiederherstellungsauftrags den SharePoint-Server neu. Fahren Sie mit dem nächsten Schritt fort.</p>

Schritt	Aktion	Hinweise
Schritt 10	Stellen Sie die verbleibenden SharePoint-Ressourcen wieder her.	Wählen Sie die Backup-Sätze für die SharePoint-Ressource "Globale Einstellungen". Siehe "Methoden für das Wiederherstellen von Daten in Backup Exec" auf Seite 258.
Schritt 11 (für SharePoint 2013/2016-Multiserverfarmen)	Gewährleisten Sie, dass die Server in der SharePoint-Farm nach der Wiederherstellung richtig konfiguriert werden.	Führen Sie den Assistenten zum Konfigurieren von SharePoint-Produkten aus.
Schritt 12	Sichern Sie den SharePoint-Server.	Nach Abschluss der Notfallwiederherstellung sollten Sie so bald wie möglich einen Backup-Auftrag auszuführen. Siehe "Sichern von Daten" auf Seite 174.

Backup Exec Agent for Oracle auf Windows- oder Linux-Servern

Dieser Anhang enthält folgende Themen:

- [Info zu Backup Exec Oracle Agent](#)
- [Installieren des Oracle Agents](#)
- [Konfigurieren des Oracle Agent auf Windows-Computern und -Linux-Servern](#)
- [Informationen zu Authentifizierungsinformationen auf dem Backup Exec-Server](#)
- [Info zur Änderung von Informationen der Oracle-Instanz](#)
- [Sichern von Oracle-Datenbanken](#)
- [Wiederherstellen von Oracle-Ressourcen](#)
- [Best Practices für Backup Exec Agent for Oracle auf Windows- und Linux-Servern](#)

Info zu Backup Exec Oracle Agent

Backup Exec Agent for Oracle on Windows Servers or Linux Servers (Oracle Agent) verwendet den Recovery Manager (RMAN) von Oracle, um Oracle-Datenbanken zu schützen. RMAN ist ein Tool, das Backup und Wiederherstellung von Oracle-Datenbanken verwaltet.

Folgende Funktionen sind zusammen mit dem Oracle Agent verfügbar:

- Möglichkeit, als Datenbankadministrator (DBA) Backup- und Wiederherstellungsvorgänge aus Backup Exec oder der RMAN-Konsole einzuleiten.
Vom DBA auf der RMAN-Konsole ausgeführte Vorgänge werden als von DBA gestartete bzw. DBA-initiierte Vorgänge bezeichnet. Informationen über RMAN finden Sie in der Oracle-Dokumentation.
- Unterstützung mehrerer Datenströme zur Steigerung der Leistung bei Backup- und Wiederherstellungsvorgängen.
- RMAN-Wiederherstellungskatalog zur Verwaltung des Backup und Wiederherstellung von Oracle-Datenbanken
- Unterstützung für Oracle Real Application Cluster (RAC)

Informationen zu den Best Practices zum Einsatz des Backup Exec Agent for Oracle auf Windows- oder Linux-Servern (Oracle Agent) finden Sie unter *Best Practices für Backup Exec*.

Hinweise zu Oracle 12c

Backup Exec unterstützt folgende neue Funktionen von Oracle 12c:

- Unterstützung der mehrinstanzfähigen Architektur
Backup Exec unterstützt die mehrinstanzfähige Architektur, die in Oracle 12c eingeführt wurde. In dieser neuen Architektur funktioniert die Oracle-Datenbank als mehrinstanzfähige Containerdatenbank (CDB), die keine, eine oder mehr PDBs enthält. Eine PDB ist ein vom Benutzer erstellter Satz von Schemas, Objekten und zugehörigen Strukturen, der in einer Anwendung als separate Datenbank angezeigt wird. Oracle-Datenbanken vor Version 12c waren keine CDBs.
- Neues Recht (SYSBACKUP) für RMAN
Ab Oracle 12c unterstützt der Oracle-Agent die Backup- und Wiederherstellungsaufgaben nur mit einem Benutzer, der das Recht "SYSBACKUP" hat.
- Unterstützung eines nicht-Administratorbenutzers für ORACLE_HOME unter Windows
Ab Oracle 12c können die Oracle-Dienste von einem Oracle-Benutzer ohne Administratorrechte ausgeführt werden. Jedoch kann die Installation nur von einem Benutzer mit Administratorrechten ausgeführt werden.

Folgendes wird nicht unterstützt:

- TSM-Geräte (Tivoli Storage Manager) als Speicher für Backup-Aufträge in Oracle
- Oracle Management Server

Siehe ["Installieren des Oracle Agents"](#) auf Seite 1342.

Siehe ["Konfigurieren des Oracle Agent auf Windows-Computern und -Linux-Servern"](#) auf Seite 1342.

Installieren des Oracle Agents

Der Oracle Agent wird als Teil des Agent for Applications and Databases installiert und kann lokale oder Remote-Oracle-Instanzen schützen.

Um lokale oder externe Oracle-Instanzen zu schützen, müssen Sie die folgenden Backup Exec-Optionen installieren:

- Backup Exec Agent for Windows auf Remote-Windows-Computern

Hinweis: Wenn Sie eine ältere Version des Agent for Windows auf einem Oracle-Server aktualisieren, müssen Sie den Oracle-Server nach dem Upgrade neu starten. Backup Exec-Aufträge können erst erfolgreich abgeschlossen werden, wenn Sie den Oracle-Server neu starten.

Siehe ["Methoden für die Installation von Agent for Windows"](#) auf Seite 77.

- Backup Exec Agent for Linux auf Remote-Linux-Computern
Siehe ["Installieren von Agent for Linux"](#) auf Seite 1561.
- Der Agent for Applications and Databases auf dem Backup Exec-Server.
Siehe ["Installieren zusätzlicher Agents und Funktionen auf dem lokalen Backup Exec-Server"](#) auf Seite 66.

Konfigurieren des Oracle Agent auf Windows-Computern und -Linux-Servern

Bevor Sie Oracle-Datenbanken sichern oder wiederherstellen können, müssen Sie folgende Schritte durchführen:

Tabelle H-1 Konfigurieren des Oracle Agent auf Windows-Computern und -Linux-Servern

Schritt	Aktion
Schritt 1	<p>Konfigurieren Sie Informationen über die Oracle-Instanzen für den Oracle Agent.</p> <p>Siehe "Konfigurieren einer Oracle-Instanz auf Windows-Computern" auf Seite 1345.</p> <p>Siehe "Konfigurieren einer Oracle-Instanz auf Linux-Servern" auf Seite 1353.</p>

Schritt	Aktion
Schritt 2	<p>Aktivieren Sie den Datenbankzugriff für den Backup Exec-Server.</p> <p>Immer wenn sich Oracle-Instanzinformationen ändern oder eine neue Konfiguration hinzugefügt wird, müssen Sie Backup Exec Agent Utility aktualisieren. Wenn Anmeldedaten nicht aktualisiert werden, falsch sind, oder der Server heruntergefahren ist, wird beim Ausführen eines Backup-Auftrags möglicherweise die Fehlermeldung "Verbinden mit dieser Ressource nicht möglich..." angezeigt. Wenn diese Meldung angezeigt wird, müssen Sie den Server online schalten und die Informationen konfigurieren.</p> <p>Führen Sie für Oracle RAC Backup Exec Agent Utility auf jedem Knoten aus und fügen Sie den Instanzen Informationen hinzu. Wenn Oracle RAC-Knoten hinzugefügt oder entfernt werden, müssen Sie Informationen zu allen Änderungen der Instanzen in Backup Exec Agent Utility eingeben.</p> <p>Hinweis: Wenn Sie Backup Exec Agent Utility verwenden, sollte das Benutzerkonto, mit dem Sie eingeloggt sind, ein Mitglied der Oracle DBA-Gruppe sein.</p> <p>Sie benötigen Administratorrechte zum Ausführen von Backup Exec Agent Utility.</p> <p>Siehe "Aktivieren des Datenbankzugriffs für Oracle-Vorgänge auf Windows-Computern" auf Seite 1351.</p> <p>Siehe "Aktivieren des Datenbankzugriffs für Oracle-Vorgänge auf Linux-Servern" auf Seite 1358.</p>
Schritt 3	<p>Legen Sie Authentifizierung-Anmeldedaten für Oracle fest.</p> <p>Siehe "Informationen zu Authentifizierungsinformationen auf dem Backup Exec-Server" auf Seite 1359.</p>

Konfigurieren einer Oracle-Instanz auf Windows-Computern

Sie können Backup Exec Agent Utility verwenden, um Informationen zu Oracle-Instanzen für den Oracle Agent auf Windows-Computern zu konfigurieren.

So konfigurieren Sie eine Oracle-Instanz auf Windows-Computern

- 1
- Klicken Sie auf dem Computer mit dem Agent for Windows in der Taskleiste auf "Start > Alle Programme > Veritas Backup Exec > Backup Exec Agent Utility".

Wenn Backup Exec Agent Utility ausgeführt wird, wird ein Symbol in der Taskleiste eingeblendet. Durch Doppelklicken auf das Symbol können Sie das Dienstprogramm anzeigen.
- 2
- Klicken Sie auf der Registerkarte "Oracle" auf "Neu".

Alle derzeit auf dem Computer vorhandenen Instanzen werden auf der Registerkarte angezeigt.
- 3
- Schließen Sie die Auswahl der passenden Optionen ab.

Siehe ["Optionen für die Oracle Agent-Konfiguration"](#) auf Seite 1345.
- 4
- Klicken Sie auf "OK".

Optionen für die Oracle Agent-Konfiguration

Sie können die folgenden Oracle Agent-Konfigurationsoptionen festlegen.

Siehe ["Konfigurieren einer Oracle-Instanz auf Windows-Computern"](#) auf Seite 1345.

Siehe ["Bearbeiten einer Oracle-Instanz auf Windows-Computern"](#) auf Seite 1350.

Tabelle H-2 Optionen für die Oracle Agent-Konfiguration

Element	Beschreibung
Lokaler Instanzname	<p>Zeigt den Namen der Oracle-Instanz an. Wenn Sie eine Instanz bearbeiten, können Sie ihren Namen nicht ändern.</p> <p>Für Oracle RAC-Knoten geben Sie den vollständig qualifizierten Domänennamen für den jeden Knoten.</p> <p>Der vollständig qualifizierte Domänennamen des Knotens wird in der Liste von Servern auf der Registerkarte "Backup und Wiederherstellung" angezeigt.</p> <p>Der Name hat folgendes Format: RAC-<dbname>-<dbid>, wobei dbname für den Datenbanknamen und dbid für die Datenbank-ID steht.</p>

Element	Beschreibung
Benutzername	<p>Zeigt den Benutzernamen für die Oracle-Instanz an.</p> <p>Wenn sich die Anmeldedaten für die Oracle-Instanz ändern, müssen Sie einen Benutzer mit SYSDBA-Berechtigung zur Oracle-Instanz hinzufügen.</p> <p>Geben Sie für alle Oracle RAC-Knoten den gleichen Satz der Login-Daten ein.</p> <p>Für eine Oracle 12c-Datenbank müssen Sie einen Benutzernamen eingeben, der SYSBACKUP-Rechte hat.</p>
Kennwort	Zeigt das Kennwort für den Benutzernamen der Oracle-Instanz an.
Kennwort bestätigen	Zeigt das Kennwort erneut an, um es zu bestätigen.
Oracle Home User erhält die Berechtigungen für die Backup Exec-Ordner "Logs" und "Data"	<p>Unter Oracle 12c und höher unterstützt die Oracle-Datenbank die Verwendung von Oracle Home User. Dieser Benutzer hat keine Administratorrechte und benötigt daher Zugriffsrechte auf die Backup Exec-Ordner "Logs" und "Data".</p> <p>Hinweis: Dieses Feld ist nur für Datenbanken aus Oracles 12c und höher verfügbar.</p>

Element	Beschreibung
Zusätzlicher Instanzpfad für PDB-Wiederherstellungen	<p>Für eine zeitgenaue Wiederherstellung einer Plug-fähigen Datenbank (PDB), stellt RMAN zuerst die PDB-Dateien aus dem entsprechenden Backup wieder her. Für diese Wiederherstellung benötigt RMAN eine Kopie des Undo-Tablespace des Stammbehälters, im Zustand zum angegebenen Zeitpunkt. Für diese Wiederherstellung erstellt RMAN eine vorübergehende zusätzliche Datenbank, die aus dem Undo-, System- und Sysaux-Tablespace des Stammcontainers besteht.</p> <p>Wenn die wiederherzustellende Datenbank einen Schnellwiederherstellungsbereich enthält, erstellt RMAN die zusätzlichen Datenbankdateien in diesem Bereich im Ordner "<FRA>/<SID>/datafile". It in diesem Bereich jedoch nicht genügend Speicherplatz verfügbar, zeigt RMAN den folgenden Fehler an:</p> <p>ORA-19809: Limit für Wiederherstellungsdateien überschritten</p> <p>Wenn die wiederherzustellende Datenbank einen Schnellwiederherstellungsbereich enthält, erstellt RMAN die zusätzlichen Datenbankdateien in dem Speicherort, den Sie im Feld für den zusätzlichen Instanzpfad für PDF-Wiederherstellungen angegeben haben.</p> <p>Agent for Windows verifiziert den angegebenen zusätzlichen Pfad. Ist dieser Pfad nicht verfügbar, erstellt der Agent einen zusätzlichen Pfad. Wenn Sie diesen Pfad nicht angeben, geht RMAN davon aus, dass der Schnellwiederherstellungsbereich konfiguriert ist und genügend Speicherplatz hat.</p> <p>Agent Utility kann einen Pfad nicht validieren, der auf dem ASM-Datenträger angegeben wird und akzeptiert den Pfad wie angegeben. Deshalb müssen Sie sicherstellen, dass der Pfad, den Sie eingaben, richtig und zugänglich ist.</p> <p>Hinweis: Dieses Feld ist nur für Datenbanken aus Oracles 12c und höher verfügbar.</p>

Element	Beschreibung
Wiederherstellungskatalog verwenden	<p>Gibt an, dass Sie planen, den Oracle-Wiederherstellungskatalog zu verwenden.</p> <p>Der Oracle Agent unterstützt die Verwendung des RMAN-Wiederherstellungskatalogs zur Verwaltung des Backup und der Wiederherstellung von Oracle-Datenbanken. Falls Sie den Wiederherstellungskatalog nicht verwenden möchten, nutzt RMAN die Steuerdatei der Quelldatenbank als alleinigen Speicher für Metadaten.</p> <p>Das Ziel für die RMAN-Verbindung ist entweder eine Zieldatenbank (Steuerdatei) oder ein Wiederherstellungskatalog. In Orakel 12c stellt RMAN eine Verbindung zur Containerdatenbank her, wenn der Wiederherstellungskatalog nicht konfiguriert ist.</p>
TNS-Name	Zeigt den Oracle Net Service-Namen an.
Benutzername	Zeigt den Benutzernamen für den Oracle-Wiederherstellungskatalog an.
Kennwort	Zeigt das Kennwort für den Oracle-Wiederherstellungskatalog an.
Kennwort bestätigen	Zeigt das Kennwort für den Wiederherstellungskatalog erneut an, um es zu bestätigen.
Name oder IP-Adresse des Backup Exec-Servers	<p>Zeigt den Namen oder die IP-Adresse des Backup Exec-Servers an, an den von DBA gestartete Backup-Aufträge gesendet werden sollen.</p> <p>Sie müssen für alle Vorgänge dieselbe Form der Namensauflösung verwenden.</p>
Auftragsvorlagenname	<p>Zeigt den Namen der Backup Exec-Auftragsvorlage an, den der von DBA gestartete Auftrag für Backup- und Wiederherstellungsvorgänge verwenden soll. Sie erstellen die Auftragsvorlage im Dialogfeld "Einstellungen für von DBA gestartete Aufträge" auf dem Backup Exec-Server. Wenn Sie keine Auftragsvorlagen angeben, wird die Standardauftragsvorlage aktiviert.</p> <p>Siehe "DBA-initiierte Auftragsvorlagen" auf Seite 746.</p>

Anzeigen einer Oracle-Instanz auf Windows-Computern

Sie können Backup Exec Agent Utility verwenden, um Informationen zu Oracle-Instanzen für den Oracle Agent auf Windows-Servern anzuzeigen.

So zeigen Sie eine Oracle-Instanz auf Windows-Computern an

- Klicken Sie auf dem Computer mit dem Agent for Windows in der Taskleiste auf "Start > Alle Programme > Veritas Backup Exec > Backup Exec Agent Utility".
- Zeigen Sie auf der Registerkarte "Oracle" die Instanzen an, die derzeit auf dem Computer vorhanden sind.

Siehe ["Oracle-Optionen für Backup Exec Agent Utility"](#) auf Seite 1349.
- Klicken Sie auf "OK".

Oracle-Optionen für Backup Exec Agent Utility

Sie können die folgenden Oracle-Optionen für Backup Exec Agent Utility festlegen:

Siehe ["Anzeigen einer Oracle-Instanz auf Windows-Computern"](#) auf Seite 1349.

Tabelle H-3 Oracle-Optionen für Backup Exec Agent Utility

Element	Beschreibung
Instanz	Zeigt den Namen der Oracle-Instanz an.
Benutzername	Zeigt den Benutzernamen für die Oracle-Instanz an.
Wiederherstellungskatalog	Zeigt den Namen des Wiederherstellungskatalogs an.
Backup Exec-Server	Zeigt den Namen oder die IP-Adresse des Backup Exec-Servers an, an den von DBA gestartete Backup-Aufträge gesendet werden sollen.
Auftragsvorlage	Zeigt den Namen der von DBA gestarteten Vorlage an. Siehe "Informationen über die Durchführung eines von DBA gestarteten Backup-Auftrags für Oracle" auf Seite 1366.
Neu	Ermöglicht das Hinzufügen einer Oracle-Instanz.
Bearbeiten	Ermöglicht das Ändern einer Oracle-Instanz.

Element	Beschreibung
Löschen	Ermöglicht das Löschen einer Oracle-Instanz.

Bearbeiten einer Oracle-Instanz auf Windows-Computern

Sie können Backup Exec Agent Utility verwenden, um Informationen zu Oracle-Instanzen für den Oracle Agent auf Windows-Computern zu ändern.

So bearbeiten Sie eine Oracle-Instanz auf Windows-Computern

- 1 Klicken Sie auf dem Computer mit dem Agent for Windows in der Taskleiste auf "Start > Alle Programme > Veritas Backup Exec > Backup Exec Agent Utility".

Wenn Backup Exec Agent Utility ausgeführt wird, wird ein Symbol in der Taskleiste eingeblendet. Durch Doppelklicken auf das Symbol können Sie das Dienstprogramm anzeigen.

- 2 Klicken Sie auf der Registerkarte "Oracle" auf "Bearbeiten".

Alle derzeit auf dem Computer vorhandenen Instanzen werden auf der Registerkarte angezeigt.

- 3 Ändern Sie die entsprechenden Optionen.

Siehe ["Optionen für die Oracle Agent-Konfiguration"](#) auf Seite 1345.

- 4 Klicken Sie auf "OK".

Löschen einer Oracle-Instanz auf Windows-Computern

Sie können Backup Exec Agent Utility verwenden, um eine Oracle-Instanz für den Oracle Agent auf Windows-Computern zu entfernen.

So löschen Sie eine Oracle-Instanz auf Windows-Computern

- 1 Klicken Sie auf dem Computer mit dem Agent for Windows in der Taskleiste auf "Start > Alle Programme > Veritas Backup Exec > Backup Exec Agent Utility".

Wenn Backup Exec Agent Utility ausgeführt wird, wird ein Symbol in der Taskleiste eingeblendet. Durch Doppelklicken auf das Symbol können Sie das Dienstprogramm anzeigen.

- 2 Klicken Sie auf der Registerkarte "Oracle" auf "Löschen".

Alle derzeit auf dem Computer vorhandenen Instanzen werden auf der Registerkarte angezeigt.

- 3 Klicken Sie auf "OK".

Aktivieren des Datenbankzugriffs für Oracle-Vorgänge auf Windows-Computern

Sie können Backup Exec Agent Utility verwenden, um nach der Konfiguration einer Oracle-Instanz Datenbankzugriff für den Windows-Computer zu aktivieren.

Siehe ["Sichern von Oracle-Datenbanken"](#) auf Seite 1362.

Siehe ["Sichern von Oracle RAC-Datenbanken"](#) auf Seite 1364.

Siehe ["DBA-initiierte Auftragsvorlagen"](#) auf Seite 746.

Siehe ["Ändern der Standardeinstellungen für Backup-Aufträge"](#) auf Seite 630.

So aktivieren Sie Datenbankzugriff für Oracle-Vorgänge auf Windows-Computern

- 1 Klicken Sie auf dem Computer mit dem Agent for Windows in der Taskleiste auf "Start > Alle Programme > Veritas Backup Exec > Backup Exec Agent Utility".

Wenn Backup Exec Agent Utility ausgeführt wird, wird ein Symbol in der Taskleiste eingeblendet. Durch Doppelklicken auf das Symbol können Sie das Dienstprogramm anzeigen.

- 2 Klicken Sie auf die Registerkarte "Datenbankzugriff".

(Optional) Klicken Sie beim ersten Starten von Backup Exec Agent Utility auf "Einstellungen ändern", um diese Optionen zu aktivieren.

3 Legen Sie die gewünschten Optionen fest, um den Datenbankzugriff zu konfigurieren:

Backup Exec-Server kann Oracle-Vorgänge authentifizieren	Aktivieren Sie diese Option, um Oracle-Vorgänge zwischen dem Backup Exec-Server und diesem Computer zu ermöglichen.
Benutzername	<p>Geben Sie einen Benutzernamen an, der Administratorrechte für diesen Computer hat. Dieses Login-Konto wird vom Backup Exec-Server beim Herstellen einer Verbindung zu diesem Computer genutzt.</p> <p>Wenn Sie im Benutzernamen eine IP-Adresse oder einen voll qualifizierten Computernamen angeben, kann Backup Exec Agent Utility das Benutzerkonto möglicherweise nicht verifizieren. Wenn die Login-Daten falsch sind, wird bei der Ausführung eines Backup- oder Wiederherstellungsauftrags möglicherweise die Fehlermeldung "Verbindung zu Ressource nicht möglich..." angezeigt.</p> <p>Sie müssen diesen Computernamen und das Login-Konto der Liste von Authentifizierungsdaten für Oracle-Server auf dem Backup Exec-Server hinzufügen. Wenn bei dem Backup der Oracle-Ressourcen die Authentifizierung fehlschlägt, schlägt auch der Backup-Auftrag fehl. Wenn die Authentifizierung bei der Suche nach den Backup-Sätzen eines Wiederherstellungsauftrags fehlschlägt, sind die Backup-Sätze nicht mehr verfügbar, und Sie müssen einen DBA-initiierten Wiederherstellungsauftrag durchführen, um Daten zu sichern.</p>
Kennwort	<p>Geben Sie das Kennwort für dieses Login-Konto an.</p> <p>Hinweis: Login-Daten werden aus Sicherheitsgründen nicht auf dem Remote-Computer gespeichert.</p>
Kennwort bestätigen	Geben Sie das Kennwort zum Bestätigen erneut ein.

Benutzerdefinierten Port für die Verbindung des Backup Exec-Servers bei Oracle-Vorgängen verwenden	<p>Aktivieren Sie diese Option, um den Port zu ändern, der für die Kommunikation zwischen diesem Computer und dem Backup Exec-Server bei Oracle-Vorgängen genutzt wird. Standardmäßig wird Port 5633 verwendet.</p> <p>Wenn Sie die Port-Nummer auf diesem Computer ändern, müssen Sie sie auch auf dem Backup Exec-Server ändern und anschließend den Backup Exec Job Engine-Dienst auf dem Backup Exec-Server erneut starten.</p>
Port-Nummer	Geben Sie die Port-Nummer ein, die für die Verbindung zwischen diesem Computer und dem Backup Exec-Server verwendet werden soll.

4 Klicken Sie auf "OK".

5 Geben Sie für Oracle RAC-Installationen den vollständig qualifizierten Domänennamen zur Bereitstellung von Informationen ein.

Der Backup Exec-Server, auf dem Sie bereitstellen, listet die RAC-Datenbanken in der Serverliste auf der Registerkarte "Backup und Wiederherstellung" auf.

Wenn Sie keinen vollständig qualifizierten Domänennamen für die Bereitstellung eingeben, werden die RAC-Datenbanken nicht in der Serverliste aufgeführt.

Siehe ["Info zum Veröffentlichen von Agent for Windows auf den Backup Exec-Servern"](#) auf Seite 1035.

6 Fügen Sie auf dem Backup Exec-Server den Oracle-Servernamen und den für den Datenbankzugriff angegebenen Benutzernamen zur Liste der Authentifizierungsdaten des Backup Exec-Servers hinzu.

Siehe ["Informationen zu Authentifizierungsinformationen auf dem Backup Exec-Server"](#) auf Seite 1359.

Konfigurieren einer Oracle-Instanz auf Linux-Servern

Sie können Backup Exec Agent Utility verwenden, um Informationen zu Oracle-Instanzen für den Oracle Agent auf Linux-Servern zu konfigurieren.

So konfigurieren Sie eine Oracle-Instanz auf Linux-Servern

- 1 Öffnen Sie auf dem Linux-Server, auf dem die Oracle-Instanzen installiert sind, ein Terminalfenster.

Hinweis: Wenn die Oracle-Instanz, die Sie schützen möchten, ein Teil von Oracle RAC mit Version 12c ist, wechseln zum Oracle-Benutzer mit dem Befehl `su - <Oracle-Benutzer>`.

- 2 Wechseln Sie zum folgenden Verzeichnis:

cd /opt/VRTSralus/bin

- 3 Starten Sie Backup Exec Agent Utility:

./AgentConfig

- 4 Geben Sie **2** ein, um "Konfigurieren der Oracle-Instanz" auszuwählen und drücken Sie die **Eingabetaste**.
- 5 Geben Sie **1** ein, um die Option "Neue Oracle-Instanz hinzufügen" auszuwählen und drücken Sie die **Eingabetaste**.
- 6 Geben Sie den Namen der Oracle-Instanz in Großbuchstaben ein.
Beispiel: ORACLENAME
- 7 Geben Sie den Benutzernamen für die Oracle-Instanz ein.

Wenn die Login-Daten für die Oracle-Instanz geändert werden, müssen Sie die Login-Daten in diesem Feld ändern. Geben Sie für alle Oracle RAC-Knoten den gleichen Satz der Login-Daten ein.

Wenn Sie Backup Exec Agent Utility verwenden, um Oracle-Login-Daten für eine Instanz einzugeben, können die Login-Daten nicht überprüft werden, wenn das Benutzerkonto, mit dem Sie eingeloggt sind, ein Mitglied der Oracle DBA-Gruppe ist. Sind die Einloggdaten falsch, wird bei Ausführung eines Backup-Auftrags die Fehlermeldung "Anhängen an eine Ressource nicht möglich..." angezeigt.

Hinweis: Für Oracle 12c benötigt der Benutzer das Recht SYSBACKUP.

- 8 Geben Sie unter Oracle 12c und höher, wenn Sie dazu aufgefordert werden, den zusätzlichen Instanzpfad für PDB-Wiederherstellung ein.

Wenn die Datenbank, die Sie wiederherstellen, keinen Schnellwiederherstellungsbereich nutzt, erstellt RMAN die zusätzlichen Datenbankdateien im angegebenen Speicherort.

Agent Utility kann einen Pfad nicht validieren, der auf dem ASM-Datenträger angegeben wird und akzeptiert den Pfad wie angegeben. Deshalb müssen Sie sicherstellen, dass der Pfad, den Sie eingaben, richtig und zugänglich ist.

Hinweis: Die Datenbankinstanz wird mit dem Oracle-Benutzer konfiguriert; deshalb muss der Oracle-Benutzer Zugriffsrechte auf das Verzeichnis haben, das im zusätzlichen Instanzpfad angegeben ist. Sonst kann das Agent Utility das zusätzliche Verzeichnis nicht erstellen und Sie müssen das Verzeichnis manuell erstellen und dem Oracle-Benutzer Lese-/Schreibzugriff zuweisen.

Siehe ["Optionen für die Oracle Agent-Konfiguration"](#) auf Seite 1345.

- 9 Um die Oracle-Datenbank in der Serverliste des Backup Exec-Servers auf der Registerkarte "Backup und Wiederherstellung" anzuzeigen, geben Sie den Backup Exec-Servernamen oder die IP-Adresse ein, auf denen der Remote-Computer veröffentlichen soll.
- 10 Geben Sie den zu verwendenden Wiederherstellungskatalog an, wenn eine entsprechende Aufforderung angezeigt wird.

Der Oracle Agent unterstützt die Verwendung des RMAN-Wiederherstellungskatalogs zur Verwaltung des Backup und der Wiederherstellung von Oracle-Datenbanken. Falls Sie den Wiederherstellungskatalog nicht verwenden möchten, nutzt RMAN die Steuerdatei der Quelldatenbank als alleinigen Speicher für Metadaten.

Das Ziel für die RMAN-Verbindung ist entweder eine Zieldatenbank (Steuerdatei) oder ein Wiederherstellungskatalog. In Oracle 12c stellt RMAN eine Verbindung zur Containerdatenbank her, wenn der Wiederherstellungskatalog nicht konfiguriert ist.

Wenn Sie einen Wiederherstellungskatalog angeben, muss jede zu sichernde Datenbank im Wiederherstellungskatalog registriert sein, bevor Sie Backup-Aufträge über den Backup Exec-Server ausführen können.

- 11 Um einen Wiederherstellungskatalog zu verwenden, geben Sie den Namen des Katalogs sowie einen Benutzernamen und ein Kennwort für den Katalog ein.

- 12** Um eine benutzerdefinierte Vorlage mit Einstellungen für von DBA gestartete Aufträge zu verwenden, geben Sie den Namen der Vorlage ein.
 Siehe ["DBA-initiierte Auftragsvorlagen"](#) auf Seite 746.
- 13** Um den neuen Eintrag in der Konfigurationsdatei festzulegen, geben Sie **Y** ein und drücken Sie dann die **Eingabetaste**.

Anzeigen einer Oracle-Instanz auf Linux-Servern

Sie können Backup Exec Agent Utility verwenden, um Informationen zu Oracle-Instanzen für den Oracle Agent auf Linux-Servern anzuzeigen.

Folgende Informationen werden aufgelistet:

- Name der Instanz
- Login-Name für die Instanz
- IP-Adresse des standardmäßigen Backup Exec-Servernamens für die von DBA gestarteten Vorgänge
- Name der von DBA gestarteten Auftragsvorlage
- Der zusätzliche Instanzpfad für eine Oracle 12c-Datenbank (optional)

So zeigen Sie eine Oracle-Instanz auf Linux-Servern an

- 1** Öffnen Sie auf dem Linux-Server, auf dem die Oracle-Instanzen installiert sind, ein Terminalfenster.
- 2** Wechseln Sie zum folgenden Verzeichnis:

```
cd /opt/VRTSralus/bin
```
- 3** Starten Sie Backup Exec Agent Utility:

```
./AgentConfig
```
- 4** Geben Sie **4** ein.

Bearbeiten einer Oracle-Instanz auf Linux-Servern

Sie können Backup Exec Agent Utility verwenden, um Informationen zu Oracle-Instanzen für den Oracle Agent auf Linux-Servern zu ändern.

So bearbeiten Sie eine Oracle-Instanz auf Linux-Computern

- 1** Öffnen Sie auf dem Linux-Server, auf dem die Oracle-Instanzen installiert sind, ein Terminalfenster.
- 2** Wechseln Sie zum folgenden Verzeichnis:

```
cd /opt/VRTSralus/bin
```


- 3 Starten Sie Backup Exec Agent Utility:

```
./AgentConfig
```

- 4 Geben Sie **2** ein, um "Konfigurieren der Oracle-Instanz" auszuwählen, und drücken Sie die **Eingabetaste**.

Alle derzeit auf dem Computer vorhandenen Instanzen werden erkannt.

Hinweis: Wenn die Oracle-Instanz, die Sie euch schützen möchten, ein Teil von Oracle RAC 12c ist, wechseln Sie zum Oracle-Benutzer, bevor Sie die Option "Konfigurieren der Oracle-Instanz" wählen.

- 5 Geben Sie **2** ein.
- 6 Folgen Sie den Eingabeaufforderungen.

Löschen einer Oracle-Instanz auf Linux-Servern

Sie können Backup Exec Agent Utility verwenden, um eine Oracle-Instanz für den Oracle Agent auf Linux-Servern zu entfernen.

Siehe ["Konfigurieren des Oracle Agent auf Windows-Computern und -Linux-Servern"](#) auf Seite 1342.

So löschen Sie eine Oracle-Instanz für den Oracle Agent auf Linux-Servern

- 1 Öffnen Sie auf dem Linux-Server, auf dem die Oracle-Instanzen installiert sind, ein Terminalfenster.

- 2 Wechseln Sie zum folgenden Verzeichnis:

```
cd /opt/VRTSralus/bin
```

- 3 Starten Sie Backup Exec Agent Utility:

```
./AgentConfig
```

- 4 Geben Sie **2** ein, um "Konfigurieren der Oracle-Instanz" auszuwählen, und drücken Sie die **Eingabetaste**.

Alle derzeit auf dem Computer vorhandenen Instanzen werden erkannt.

- 5 Geben Sie **3** ein.
- 6 Folgen Sie den Eingabeaufforderungen.

Aktivieren des Datenbankzugriffs für Oracle-Vorgänge auf Linux-Servern

Sie können Backup Exec Agent Utility verwenden, um Datenbankzugriff für den Linux-Server zu aktivieren, nachdem Sie eine Oracle-Instanz konfiguriert haben.

Siehe ["Einstellung von Authentifizierungs-Identifikationsdaten auf dem Backup Exec-Server für Oracle-Vorgänge"](#) auf Seite 1360.

Siehe ["Sichern von Oracle-Datenbanken"](#) auf Seite 1362.

Siehe ["Sichern von Oracle RAC-Datenbanken"](#) auf Seite 1364.

Siehe ["DBA-initiierte Auftragsvorlagen"](#) auf Seite 746.

Siehe ["Ändern der Standardeinstellungen für Backup-Aufträge"](#) auf Seite 630.

So aktivieren Sie den Datenbankzugriff für Oracle-Vorgänge auf Linux-Servern

- 1 Öffnen Sie auf dem Linux-Server, auf dem die Oracle-Instanzen installiert sind, ein Terminalfenster.

- 2 Wechseln Sie zum folgenden Verzeichnis:

```
cd /opt/VRTSralus/bin
```

- 3 Starten Sie Backup Exec Agent Utility:

```
./AgentConfig
```

- 4 Geben Sie **1** ein, um "Datenbankzugriff konfigurieren" auszuwählen, und drücken Sie anschließend die **Eingabetaste**.

- 5 Geben Sie den Benutzernamen ein, der sich in der Gruppe "beoper" auf dem Linux-System befindet.

Siehe ["Info zur Backup Exec-Operator-Gruppe \(beoper\) für den Agent for Linux"](#) auf Seite 1565.

Wenn bei dem Backup der Oracle-Ressourcen die Authentifizierung fehlschlägt, schlägt auch der Backup-Auftrag fehl. Wenn die Authentifizierung bei der Suche nach den Backup-Sätzen eines Wiederherstellungsauftrags fehlschlägt, sind die Backup-Sätze nicht mehr verfügbar, und Sie müssen einen von DBA gestarteten Wiederherstellungsauftrag durchführen, um Daten zu sichern.

- 6 Geben Sie das Kennwort für dieses Login-Konto ein und bestätigen Sie es.
Die Login-Daten werden nicht auf diesem Computer gespeichert.

- 7 Geben Sie bei entsprechender Aufforderung an, ob Sie bei Oracle-Vorgängen einen benutzerdefinierten Anschluss zur Verbindung der Backup Exec-Server-Kommunikation zwischen dem Backup Exec-Server mit diesem Computer verwenden möchten.

Standardmäßig wird Port 5633 verwendet. Wenn Sie die Port-Nummer auf diesem Computer ändern, müssen Sie sie auch auf dem Backup Exec-Server ändern und anschließend den Backup Exec Job Engine-Dienst auf dem Backup Exec-Server erneut starten. Wenn eine Windows-Firewall aktiviert ist, müssen Sie diesen Port als Ausnahme hinzufügen.

Siehe ["Netzwerk- und Sicherheitsoptionen für Backup Exec ändern"](#) auf Seite 713.

- 8 Um die Oracle-Einstellungen in der Konfigurationsdatei zu speichern, geben Sie **"Y"** ein und drücken Sie dann die **Eingabetaste**.

Informationen zu Authentifizierungsinformationen auf dem Backup Exec-Server

Sie müssen den vollständig qualifizierten Oracle-Domännennamen und den Namen des Login-Kontos in die Liste der Oracle-Server und Authentifizierungsinformationen des Backup Exec-Servers aufnehmen. Der Backup Exec-Server hat Datenbankzugriff für Vorgänge auf Oracle-Instanzen, die in der Authentifizierungsliste enthalten sind. Vergewissern Sie sich vor dem Start von Backup- oder Wiederherstellungsvorgängen auf dem Computer, auf dem die Oracle-Instanzen installiert sind, dass Instanzinformationen und Datenbankzugriff mit Backup Exec Agent Utility konfiguriert werden.

Der Name des Login-Kontos muss Administratorrechte für den Oracle-Server haben. Wenn der Benutzername falsch ist, fehlt oder nicht über die erforderlichen Rechte verfügt, können Sie auf diesem Computer keine Oracle-Backup- oder -Wiederherstellungsvorgänge ausführen.

Hinweis: Bei Oracle RAC-Knoten geben Sie den vollständig qualifizierten Domännennamen für den Namen des Login-Konten ein. Sie können den vollständig qualifizierten Domännennamen des Knotens in der Serverliste auf der Registerkarte "Backup und Wiederherstellung" anzeigen. In folgendem Format:
RAC-**<Datenbankname>**-**<Datenbank-ID>**.

Siehe ["Konfigurieren des Oracle Agent auf Windows-Computern und -Linux-Servern"](#) auf Seite 1342.

Siehe ["Einstellung von Authentifizierungs-Identifikationsdaten auf dem Backup Exec-Server für Oracle-Vorgänge"](#) auf Seite 1360.

Siehe ["Löschen eines Oracle-Servers aus der Liste der Authentifizierungsdaten des Backup Exec-Servers"](#) auf Seite 1362.

Einstellung von Authentifizierungs-Identifikationsdaten auf dem Backup Exec-Server für Oracle-Vorgänge

Sie müssen den Oracle-Server der Liste hinzufügen, damit der Backup Exec-Server für die Vorgänge auf die Datenbank zugreifen kann.

Siehe ["Informationen zu Authentifizierungsinformationen auf dem Backup Exec-Server"](#) auf Seite 1359.

Siehe ["Info zur Änderung von Informationen der Oracle-Instanz"](#) auf Seite 1362.

So stellen Sie die Authentifizierungs-Identifikationsdaten auf dem Backup Exec-Server für Oracle-Vorgänge ein:

- 1 Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Backup Exec-Einstellungen".
- 2 Klicken Sie im linken Teilfenster auf "Oracle".
- 3 Geben Sie den Namen des Oracle-Servers ein, auf dem die Instanz installiert ist.

Der Name des Oracle-Servers sollte dem Namen des Servers entsprechen, auf dem sich die Oracle-Ressource befindet. Es wird empfohlen, dass Sie den vollständig qualifizierten Domänennamen eingeben. Beispiel:

"Servername.domain.com" ist der voll qualifizierte Domänenname und der Servername ist der NETBIOS-Name. Für Oracle RAC-Knoten geben Sie RAC-<Datenbankname>-<Datenbank-ID> für jeden Knoten in der Liste ein.

- 4 Klicken Sie auf "Hinzufügen".

- Um den Namen des Login-Kontos hinzuzufügen, führen Sie einen der folgenden Schritte aus:

Auf den Pfeil klicken	Wählen Sie den Namen des Login-Kontos aus, das Sie hinzufügen möchten.
Klicken Sie auf <neues Login-Konto>.	Geben Sie die entsprechenden Optionen ein.

Verwenden Sie für das Login-Konto das gleiche Format wie bei Eingabe des Login-Kontonamens auf der Registerkarte "Datenbankzugriff" im Backup Exec Agent Utility. Wenn Sie im Backup Exec Agent Utility beispielsweise Domänenname/Benutzername eingegeben haben, müssen Sie dieses Format auch in der Liste der Authentifizierungs-Identifikationsdaten verwenden.

- Klicken Sie auf "OK".

Optionen zu Einstellungen für Oracle-Aufträge

Sie können den vollständig qualifizierten Oracle-Domännennamen und den Namen des Login-Kontos in die Liste der Oracle-Server und Authentifizierungsdaten des Backup Exec-Servers aufnehmen.

Siehe ["Informationen zu Authentifizierungsinformationen auf dem Backup Exec-Server"](#) auf Seite 1359.

Tabelle H-4 Authentifizierungsdaten für Oracle-Serveroptionen

Element	Beschreibung
Servename	Zeigt den Namen des Oracle-Servers an.
Login-Konto	Zeigt den Namen des Einlogggkontos mit Zugriffsrechten auf den Oracle-Server an.
Hinzufügen	Ermöglicht das Hinzufügen des vollständig qualifizierten Domännennamens und der Einlogggkontodaten.
Löschen	Ermöglicht das Entfernen des vollständig qualifizierten Domännennamens und der Login-Kontodaten

Löschen eines Oracle-Servers aus der Liste der Authentifizierungsdaten des Backup Exec-Servers

Sie können einen Oracle-Servernamen oder ein Oracle-Login-Konto aus der Liste der Authentifizierungsdaten des Backup Exec-Servers löschen.

Siehe ["Informationen zu Authentifizierungsinformationen auf dem Backup Exec-Server"](#) auf Seite 1359.

So löschen Sie einen Oracle-Server aus der Liste der Authentifizierungsdaten des Backup Exec-Servers

- 1 Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Backup Exec-Einstellungen".
- 2 Klicken Sie im linken Teilfenster auf "Oracle".
- 3 Wählen Sie das Element aus, das den zu löschenden Servernamen oder das zu löschende Login-Konto enthält.
- 4 Klicken Sie auf "Löschen".
- 5 Klicken Sie auf "OK".

Info zur Änderung von Informationen der Oracle-Instanz

Sobald sich Informationen zur Oracle-Instanz wie Benutzername oder Kennwort der Instanz ändern, muss Backup Exec Agent Utility aktualisiert werden.

Wenn Oracle RAC-Knoten hinzugefügt oder entfernt werden, müssen Sie Informationen zu allen Änderungen der Instanzen in Backup Exec Agent Utility eingeben. Nachdem die Änderungen eingegeben wurden, werden sie vom Backup Exec-Server erkannt.

Wenn die Änderungen im Backup Exec Agent Utility nicht eingegeben werden, wird bei der Ausführung eines Backup-Auftrags möglicherweise die Fehlermeldung "Verbinden mit dieser Ressource nicht möglich..." angezeigt.

Siehe ["Konfigurieren des Oracle Agent auf Windows-Computern und -Linux-Servern"](#) auf Seite 1342.

Sichern von Oracle-Datenbanken

Bevor Sie Oracle-Datenbanken sichern, sollten Sie Folgendes prüfen:

- Führen Sie Backup Exec Agent Utility auf dem Oracle-Server aus und fügen Sie Informationen zu den Instanzen hinzu. Erst dann können Sie Backup- oder Wiederherstellungsvorgänge ausführen.
Bei jeder Änderung der Oracle-Instanzinformationen müssen Sie Backup Exec Agent Utility aktualisieren. Nachdem die Änderungen eingegeben wurden, werden sie vom Backup Exec-Server erkannt.
Siehe ["Konfigurieren des Oracle Agent auf Windows-Computern und -Linux-Servern"](#) auf Seite 1342.
- Bei einem Backup-Vorgangs kann sich die Menge der gesicherten Daten von der Größe der Oracle-Dateien auf dem Datenträger unterscheiden. Dies ist normal. Backup Exec sichert die ausgewählten Datendateien sowie eine Kopie der Steuerdatei.
- In einer Central Admin Server Feature-Umgebung müssen alle Backup-Aufträge einer bestimmten Oracle-Instanz an denselben verwalteten Backup Exec-Server delegiert werden. Wenn Sie den Backup-Auftrag nicht auf denselben verwalteten Backup Exec-Server beschränken, müssen Sie das physische Medium mit den Backup-Sätzen auf einen einzigen verwalteten Backup Exec-Server übertragen, bevor Sie Daten wiederherstellen können.
Siehe ["Auswählen eines Backup Exec-Server-Pools für Backups"](#) auf Seite 1499.
- Wenn sich die Oracle-Datenbank auf Datenträgern befindet, die mit Oracle Automatic Storage Management (ASM) konfiguriert sind, können Sie diese Datenträger nicht als Teil eines Dateisystem-Backup auswählen.
Sobald Sie versuchen, diese Datenträger auszuwählen, wird die folgende Meldung angezeigt:

```
An error was encountered while attempting to browse the  
contents of <drive>. A device-specific error occurred.
```
- Die Datenbank muss geladen oder geöffnet sein, bevor Sie Backup-Auswahlen vornehmen können.
- Die Datenbank muss im Modus ARCHIVELOG sein, bevor der Knoten "Archivierte Protokolle" unter der Oracle-Ressource des Oracle-Servers angezeigt werden kann.

Hinweise zu Oracle 12c

Bevor Sie eine Oracles 12c-Datenbank sichern, überprüfen Sie Folgendes:

- Zum Ausführen von Sicherungs- und Wiederherstellungsfunktionen für eine Oracle 12c-Datenbank muss der Benutzer das Recht SYSBACKUP haben. Für frühere Datenbankversionen ist das Recht SYSDBA und der Benutzer für die RMAN-Verbindung SYS.

- Das Ziel für die RMAN-Verbindung ist entweder eine Zieldatenbank (Steuerdatei) oder ein Wiederherstellungskatalog. In Orakel 12c stellt RMAN eine Verbindung zur Containerdatenbank her, wenn der Wiederherstellungskatalog nicht konfiguriert ist.
- Selbst wenn Sie eine einzelne PDB oder einen einzelnen Tablespace oder eine Datendatei zum Sichern auswählen, verwendet der Oracle-Agent die CDB als RMAN-Ziel, wenn der Wiederherstellungskatalog nicht konfiguriert ist. Wenn Sie mehrere PDBs oder eine ganze CDB oder archivierte Protokolle zum Sichern auswählen, verwendet auch der Oracle-Agent die CDB als Ziel. Auf diese Weise ist das Ziel für RMAN immer die CDB. Alle Backups und Wiederherstellungen werden ausgeführt, indem sie eine Verbindung zur CDB herstellen.
- Wenn Sie den Knoten "Oracle Database" zum Sichern auswählen, werden alle Datendateien von PDBs (einschließlich Datendateien des Stammverzeichnisses), archivierten Protokollen und der Steuerdatei gesichert. Wenn Sie den Knoten "Plug-fähige Datenbanken" auswählen, wird die ganze CDB einschließlich der Archivprotokolle gesichert. Archivprotokolle werden nur gesichert, wenn die Datenbank im Archivprotokollmodus ausgeführt wird.
- Jeder PDB-Knoten listet alle Tablespaces dieser PDB auf. Wird eine PDB zum Sichern ausgewählt, werden alle Tablespaces und die archivierten Protokolle zusammen mit der Steuerdatei gesichert. Archivprotokolle werden nur gesichert, wenn die CDB im Archivprotokollmodus ausgeführt wird.

Sie können eine Oracle-Datenbank der Liste von Servern auf der Registerkarte "Backup und Wiederherstellung" hinzufügen, damit die Datenbank für Backup-Aufträge ausgewählt werden kann. Sie können Standardoptionen für Backup-Aufträge für alle Oracle-Backup-Aufträge festlegen. Bei der Erstellung jedes Backup-Auftrags verwendet dieser die Standardoptionen, sofern Sie die Optionen für den bestimmten Auftrag nicht ändern.

Siehe ["Serverliste auf der Registerkarte "Backup und Wiederherstellung"](#) auf Seite 166.

Siehe ["Sichern von Daten"](#) auf Seite 174.

Siehe ["Backup-Optionen für Oracle"](#) auf Seite 1367.

Siehe ["Sichern von Oracle RAC-Datenbanken"](#) auf Seite 1364.

Siehe ["Informationen über die Durchführung eines von DBA gestarteten Backup-Auftrags für Oracle"](#) auf Seite 1366.

Sichern von Oracle RAC-Datenbanken

Oracle Real Application Cluster (RAC) ist ein aktiver Cluster mit gemeinsam genutztem Speicher, in dem mehrere Instanzen gemeinsam eine einzige physische

Datenbank verwenden. Da alle Knoten des Clusters auf die Datenbank zugreifen können, können Sie über alle Knoten ein Backup oder Wiederherstellung starten.

Der Oracle RAC-Datenbank-Ressourcencontainer wird der Registerkarte "Backup und Wiederherstellung" automatisch hinzugefügt, nachdem

- Sie installieren den Remote Agent for Windows und konfigurieren Backup Exec Agent Utility auf einem Oracle-Server mit Windows.
- Sie den Remote Agent for Linux and UNIX installieren und das Dienstprogramm "AgentConfig" auf einem Oracle-Server mit Linux oder Unix konfigurieren.

Folgende Voraussetzungen gelten für das Sichern von Oracle RAC-Ressourcen:

- Führen Sie Backup Exec Agent Utility auf jedem Knoten aus und fügen Sie Informationen über die Instanzen hinzu. Erst dann können Sie Backup- oder Wiederherstellungsvorgänge ausführen.
Wenn RAC-Knoten hinzugefügt oder entfernt werden, muss Backup Exec Agent Utility mit Informationen zu den betroffenen Instanzen aktualisiert werden. Nachdem die Änderungen eingegeben wurden, werden sie vom Backup Exec-Server erkannt.
Siehe ["Konfigurieren des Oracle Agent auf Windows-Computern und -Linux-Servern"](#) auf Seite 1342.
- Sie müssen den vollständig qualifizierten RAC-Domännennamen auswählen, wenn Sie Backup-Auswahlen machen.
Jeder Knoten im Cluster verwendet den gleichen vollständig qualifizierten Domännennamen. Der vollständig qualifizierte Domänenname des Knotens wird in der Liste von Servern auf der Registerkarte "Backup und Wiederherstellung" angezeigt. Sie haben folgendes Format:
RAC-<Datenbankname>-<Datenbank-ID>.

Oracle RAC-Backups werden ähnlich wie Backups standardmäßiger Oracle-Datenbanken durchgeführt.

Es gibt jedoch folgende Unterschiede:

- Standardmäßig speichert jeder Knoten in einem Oracle RAC seine Archivprotokolle lokal. Sichern Sie die Archivprotokolle einzeln, um eindeutige Backups zu erhalten. Alternativ können Sie die Archivprotokolle auf gemeinsam genutzte Speicher für Backup verschieben.
- Jedem Knoten, der Teil des Clusters ist, wird eine Priorität zugewiesen. Bei Datenbank-Backups stellt Backup Exec eine Verbindung zu dem Knoten mit der höchsten Priorität her. Backup Exec verwendet den vollständig qualifizierten Domännennamen, um zum Knoten eine Verbindung herzustellen.

Siehe ["Serverliste auf der Registerkarte "Backup und Wiederherstellung"](#) auf Seite 166.

Siehe ["Sichern von Daten"](#) auf Seite 174.

Siehe ["Backup-Optionen für Oracle"](#) auf Seite 1367.

Siehe ["Sichern von Oracle-Datenbanken"](#) auf Seite 1362.

Siehe ["Informationen über die Durchführung eines von DBA gestarteten Backup-Auftrags für Oracle"](#) auf Seite 1366.

Informationen über die Durchführung eines von DBA gestarteten Backup-Auftrags für Oracle

Ein Datenbankadministrator (DBA) kann einen Backup- oder Wiederherstellungsvorgang für Oracle über die RMAN-Konsole ausführen. Beispielskripts für Backup- und Wiederherstellungsvorgänge, die Sie über die RMAN-Konsole ausführen können, finden Sie in dem folgenden Verzeichnis:

```
<Backup Exec install path>\Backup Exec\scripts\Oracle
```

Weitere Informationen zur Verwendung der RMAN-Konsole finden Sie in der Oracle-Dokumentation.

Lesen Sie folgende Hinweise, bevor Sie Backup-Aufträge für Oracle über die RMAN-Konsole starten.

- Stellen Sie sicher, dass Sie alle vorbereitenden Maßnahmen für die Konfiguration des Oracle Agents ausgeführt haben.
Siehe ["Konfigurieren des Oracle Agent auf Windows-Computern und -Linux-Servern"](#) auf Seite 1342.
- Der Kanal wird erst freigegeben, wenn die RMAN-Konsole beendet oder ein neuer manueller Kanal auf dieser Konsole zugeordnet wird.
- Mithilfe der Option SKIP INACCESSIBLE in RMAN können beschädigte Daten und Protokolldateien übersprungen werden. Aufträge, bei denen diese Option verwendet wurde, können erfolgreich abgeschlossen werden. Es ist jedoch wahrscheinlich, dass die Datenbank nach Wiederherstellung der Daten funktionsunfähig ist. Die Option "SKIP INACCESSIBLE" steht nicht für Backup Exec-Server-Vorgänge zur Verfügung. Werden bei einem Backup-Auftrag beschädigte Daten oder Protokolldateien erkannt, schlägt der Auftrag fehl. Es wird empfohlen, diese Option nicht zu verwenden.
- Bei DBA-initiierten Aufträgen in einer Central Admin Server Feature-Umgebung (CAS) muss der in der Vorlage angegebene Zielspeicher lokal an den zentralen Administrationsserver angehängt werden.
Wenn der Zielspeicher einen Speichergerätepool einschließt, müssen alle Geräte im Pool lokal an den zentralen Administrationsserver angeschlossen sein.

Siehe ["Info zur Änderung von Informationen der Oracle-Instanz"](#) auf Seite 1362.

Siehe ["Info zur Änderung von Informationen der Oracle-Instanz"](#) auf Seite 1362.

Siehe ["Sichern von Oracle-Datenbanken"](#) auf Seite 1362.

Siehe ["DBA-initiierte Auftragsvorlagen"](#) auf Seite 746.

Backup-Optionen für Oracle

Für Backup-Aufträge in Oracle stehen die folgenden Optionen zur Verfügung. Diese Optionen werden angezeigt, wenn Sie in den Dialogfeldern Backup-Auftragsstandards und Backup-Optionen eines Backup-Auftrags die Oracle-Option auswählen.

Siehe ["Sichern von Oracle-Datenbanken"](#) auf Seite 1362.

Siehe ["Sichern von Daten"](#) auf Seite 174.

Siehe ["Ändern der Standardeinstellungen für Backup-Aufträge"](#) auf Seite 630.

Tabelle H-5 Backup-Optionen für Oracle

Element	Beschreibung
Maximale Anzahl zu verwendender Geräte für Ressourcen, die mehrere Datenströme unterstützen	<p>Gibt die maximale Anzahl der verfügbaren Geräte für den Backup-Auftrag an.</p> <p>Wenn Sie mehr als ein Gerät angeben, müssen Sie eines der folgenden Elemente als Zielspeicher für den Backup-Auftrag auswählen:</p> <ul style="list-style-type: none">■ Einen Speicherpool.■ Einen veralteten Backup-to-Disk-Ordner, für den mindestens zwei Vorgänge gleichzeitig aktiviert sind. <p>Wenn nur ein Speichergerät für den Backup-Auftrag zur Verfügung steht, werden die Datenströme von RMAN auf dem Medium seriell gesichert.</p> <p>Diese Option steht für von DBA gestartete Aufträge nicht zur Verfügung.</p>
Minimum an erforderlichen Geräten. Auftrag als fehlgeschlagen kennzeichnen, wenn weniger Geräte zur Verfügung stehen.	<p>Gibt die Mindestanzahl der verfügbaren Speichergeräte für den Auftrag an.</p> <p>Wenn der Auftrag die Mindestanzahl Geräte nicht abrufen kann, schlägt der Auftrag fehl.</p> <p>Diese Option steht für von DBA gestartete Aufträge nicht zur Verfügung.</p>

Element	Beschreibung
Archivierte Protokolldateien löschen	Ermöglicht das automatische Löschen der archivierten Protokolldateien nach dem Backup.
Bereits gesicherte archivierte Protokolldateien nicht sichern	Backup Exec überspringt alle archivierten Protokolldateien, die vorher gesichert worden sind.
Backup offline durchführen	<p>Backup Exec schaltet die Datenbank offline, bevor Sie den Backup-Auftrag beginnen. Nachdem der Backup-Auftrag beendet ist, schaltet Backup Exec die Datenbank wieder online.</p> <p>Wählen Sie diese Option aus, wenn die Oracle-Datenbank eine nicht archivierte Datenbank mit Protokollierung ist.</p>

Wiederherstellen von Oracle-Ressourcen

Der Oracle Agent ermöglicht das Wiederherstellen von Oracle-Datenbanken, Tablespace oder Datendateien. Sie können Elemente an ihrem ursprünglichen Speicherort oder an einem neuen Speicherort wiederherstellen. Die in Backup Exec vorgenommene Wiederherstellungsauswahl liegt als Skript vor. RMAN verwendet das Skript zur Auswahl der wiederherzustellenden Daten aus dem Backup-Satz von Backup Exec. Nachdem die Daten auf dem Oracle-Server wiederhergestellt wurden, führt RMAN alle angeforderten Wiederherstellungsvorgänge durch. Die ausgewählte Optionen bestimmen die Wiederherstellungsvorgänge.

Für einige Wiederherstellungsvorgänge sind keine Medien des Backup Exec-Servers erforderlich. Die Log-Dateien können sich beispielsweise noch auf dem Oracle-Server befinden. Bei einem Wiederherstellungsvorgang werden nicht immer genauso viele Daten wiederhergestellt, wie gesichert wurden. In manchen Fällen wird die Menge der wiederhergestellten Daten mit 0 Byte angezeigt. Dies ist normal, da Oracle Datendateien eventuell überspringt, die auf dem Datenträger bereits auf dem neuesten Stand sind.

Hinweis: Backup Exec Agent für Oracle unterstützt das Wiederherstellen einer Ressource nicht, wenn Sie die Ressource auf verschiedenen Datenträgern sichern. Beispiel: Sie können eine Oracle-Datenbank nicht wiederherstellen, wenn Sie ein vollständiges Backup der Oracle-Datenbank mit der Option "Backup-to-Disk" auf einem Gerät, das am Backup Exec-Server angeschlossen ist, und ein inkrementelles Backup einer Oracle-Datenbank auf einem Remote Media Agent-Gerät ausgeführt haben.

Zur vollständigen Wiederherstellung von einer Datenbank, einem Tablespace oder einer Datendatei müssen Sie ein Backup der gewünschten Datenbank oder der Dateien verwenden. Wenden Sie anschließend Online- oder archivierte Log-Dateien oder beides an. Für die vom Backup Exec-Server und einem DBA aus gestarteten Aufträge ermittelt RMAN, welche Backup Exec-Daten für die gewünschte Wiederherstellung erforderlich sind.

Hinweis: Backup Exec bietet keine Unterstützung für Point-in-Time-Wiederherstellungen von Oracle-Tablespaces (TSPITR) über serverinitiierte Vorgänge.

Backup Exec unterstützt das Wiederherstellen aus Speichergeräten und Backup-Sätzen für den Oracle Agent nicht, da RMAN während der Wiederherstellung entscheidet, welche Backup-Sätze für den Wiederherstellungsauftrag benötigt werden.

Für Datenbanken aus Oracle 12c und höher unterstützt Backup Exec die plug-fähige Database Point-In-Time Restore (DBPITR) durch von Server und DBA initiierten Vorgänge.

Der PIT-Wiederherstellungsauftrag des Stammverzeichnisses schlägt mit folgendem Fehler fehl: "Das Angeben einer CDB\$ROOT-Datenbank wird nicht unterstützt". Diese Funktion wird von Oracle nicht unterstützt.

Für Oracle 12c und höher wird das Stammverzeichnis als Knoten mit der Bezeichnung Tablespaces in der Ansicht zum Sichern, Durchsuchen und Wiederherstellen angezeigt. Wählen Sie zum Wiederherstellen des Stammverzeichnisses den Knoten "Tablespaces" unter dem Knoten "control file" in der Ansicht "Details File".

Sie können das Stammverzeichnis nur wiederherstellen, wenn ein Datenbeschädigungs- oder Benutzerfehler auftritt, der nur das Stammverzeichnis betrifft. Jedoch empfiehlt Oracle, dass Sie alles PDBs wiederherstellen, nachdem Sie das Stammverzeichnis wiederhergestellt haben, um Inkonsistenzen in den Metadaten im Stammverzeichnis und in den PDBs zu verhindern. In solch einem Fall ist es vorzuziehen, die CDB vollständig wiederherzustellen.

Der Oracle Agent behält den Zustand der Plug-fähigen Datenbanken (PDBs) vor dem Wiederherstellungsauftrag bei. Nach der Wiederherstellung, bringt der Agent die PDBs in den Zustand vor dem Wiederherstellungsauftrag.

Hinweis: Die Zustände "Offen", "Geladen", "Schreibgeschützt" und "Lesen/Schreiben" bleiben erhalten, "Migrieren" nicht. Hatte eine PDB im Zustand "Migrieren" vor dem Wiederherstellungsauftrag, wird der Zustand nach der Wiederherstellung in "Geladen" geändert.

Sie können eine Oracle-Wiederherstellungsauswahl nur über die Ansicht nach Ressourcen im Wiederherstellungsassistenten vornehmen. Die Detailansicht zeigt Backup-Sätze an, aber Sie können deren Inhalt nicht durchsuchen oder auswählen.

In der Ansicht nach Ressourcen können Sie eine Wiederherstellungsauswahl aus der Online-Datenbank oder den Steuerdateien treffen.

Tabelle H-6 Wiederherstellungsauswahlen für Oracle-Ressourcen

Anzeigen der Wiederherstellungsauswahl in	Beschreibung
Online-Datenbank	<p>Bietet eine Ansicht der Live-Datenbank (sofern verfügbar). Sie können eine ganze Datenbank oder einzelne Tablespaces und Datendateien auswählen.</p> <p>Für eine Oracle 12c-Datenbank zeigt diese Ansicht die PDBs, den Tablespace-Knoten und die archivierten Protokolle auf derselben Ebene an. In dieser Ansicht können Sie zwar den ganzen Tablespace und die einzelnen Datendateien zur Wiederherstellung auswählen, aber nicht die PDBs und die archivierten Protokollknoten.</p> <p>Für Oracle 12c unterstützt Backup Exec die Wiederherstellung einer oder mehrerer Tablespaces und Datendateien eines PDB. Das Umleiten einer Wiederherstellung einer PDB auf demselben Host in einen anderen Pfad wird unterstützt. Jedoch wird zeitgenaue Wiederherstellung von Tablespaces und die umgeleitete Wiederherstellung einer PDB auf einem neuen Host nicht unterstützt.</p> <p>Hinweis: Bei Oracle RAC wird die Oracle-Datenbank unter ihrem vollständigen Domänenname (FQDN) aufgelistet. Sie haben folgendes Format: RAC-<i><Datenbankname></i>-<i><Datenbank-ID></i>.</p>

Anzeigen der Wiederherstellungsdaten in	Beschreibung
Steuerdateien	<p>Zeigt eine Liste aller gesicherten Steuerdateien an. Für jede Steuerdatei wird das Backup-Datum und die Piece-ID aufgeführt.</p> <p>Sie können keine einzelnen Tablespaces oder Datendateien zur Wiederherstellung auswählen.</p> <p>Für eine Oracle 12-Datenbank in dieser Ansicht können Sie nur den Steuerdateiknoten und die PDB-Knoten zur Wiederherstellung auswählen. Wenn Sie den Steuerdateiknoten zur Wiederherstellung auswählen, wird die gesamte CDB wiederhergestellt. Dabei werden alle Daten der CDB und aller PDBs wiederhergestellt. Diese Daten werden in der im Wiederherstellungsauftrag angegebenen PIT wiederhergestellt. Die Funktionsweise ist mit der der Steuerdateiwiederherstellung einer nicht-CDB-Datenbank identisch.</p> <p>Wenn Sie eine einzelne PDB auswählen, wird nur diese wiederhergestellt.</p> <p>Hinweis: Wenn Sie mit einer Steuerdatei Daten bis zu einem bestimmten Zeitpunkt wiederherstellen möchten, stellen Sie sicher, dass das Datum der gesicherten Steuerdatei vor dem angegebenen Wiederherstellungszeitpunkt liegt. Die Datenbankstruktur sollte sich zwischen zwei Zeitpunkten nicht geändert haben. Außerdem wird bei der Wiederherstellung einer Steuerdatei die gesamte Datenbank auf den Zeitpunkt zurückgesetzt, zu dem die gewählte Steuerdatei gesichert wurde.</p>

Siehe ["Methoden für das Wiederherstellen von Daten in Backup Exec"](#) auf Seite 258.

DBA-initiierte Wiederherstellungen für Oracle

DBAs können Wiederherstellungsaufträge direkt über die RMAN-Konsole starten. Sie können beispielsweise angeben, welche Ressourcen wiederhergestellt werden sollen und wie viele Kanäle dem Wiederherstellungsauftrag zugewiesen werden sollen. Weitere Informationen zur Verwendung der RMAN-Konsole finden Sie in der Oracle-Dokumentation.

Alle von DBA gestarteten Wiederherstellungsaufträge werden nach Beendigung gelöscht.

Hinweis: Wenn Sie einen von DBA gestarteten Wiederherstellungsauftrag zur Wiederherstellung einer Datendatei, einem Tablespace oder einer Datenbank verwenden, die gerade online geschaltet sind, wird auf der RMAN-Konsole eine Meldung angezeigt. Die Meldung gibt an, dass die Wiederherstellung nicht durchgeführt werden kann, da Oracle keine Online-Elemente wiederherstellen kann. Die Meldung wird jedoch nicht an Backup Exec weitergegeben. Daher wird der von DBA gestartete Auftrag in Backup Exec als erfolgreich abgeschlossen gemeldet.

Wiederherstellungsoptionen für Oracle

Die folgenden Optionen sind verfügbar, wenn Sie Oracle-Daten wiederherstellen.

Tabelle H-7 Wiederherstellungsoptionen für Oracle

Element	Beschreibung
Bis zum letzten verfügbaren Zeitpunkt	Stellt die Oracle-Datenbank auf die aktuellen vollständigen und inkrementellen Backups wieder her.
Bis zu einem bestimmten Zeitpunkt und einschließlich dieses Zeitpunkts	<p>Stellt Daten bis zu einem bestimmten Zeitpunkt und einschließlich dieses Zeitpunkts wieder her. Nach diesem Zeitpunkt wird die Wiederherstellung gestoppt.</p> <p>Geben Sie ein Datum und Uhrzeit ein oder klicken Sie auf den Pfeil, um einen Kalender anzuzeigen, in dem Sie ein Datum und eine Uhrzeit auswählen können.</p>
Auf bestimmte SCN	Führt eine Wiederherstellung bis zu und einschließlich einer bestimmten SCN (System Control Number) durch. Geben Sie die SCN in das vorgesehene Feld ein.

Informationen zum Umleiten einer Wiederherstellung von Oracle-Daten

In Backup Exec haben Sie folgende Möglichkeiten zur Umleitung einer Oracle-Instanz oder deren Dateien:

- Umleiten einer Oracle-Instanz an einen anderen Oracle-Server

Hinweis: Wenn Sie die Instanz an einen anderen Oracle-Server umleiten, vergewissern Sie sich, dass eine Instanz mit demselben Namen und derselben Datenbank-ID (DBID) auf diesem Server eingerichtet ist. Die Datenbank sollte sich im Status "Nomount" befinden. Weitere Informationen zur Erstellung einer Instanz mit demselben Namen und derselben Datenbank-ID finden Sie in der Oracle-Dokumentation.

- Umleiten einer Oracle-Instanz an einen anderen Oracle-Server und Angeben alternativer Pfade für die Oracle-Dateien
- Umleiten von Tablespace, Datendateien und archivierte Protokolldateien an einen alternativen Speicherort desselben Servers
- Für Oracle 12c unterstützt Backup Exec die umgeleitete Wiederherstellung einer CDB bzw. PDB auf demselben Host in einem anderen Pfad. Backup Exec unterstützt die umgeleitete Wiederherstellung einer PDB auf einen neuen Host nicht.

Es wird empfohlen, dass Sie nur eine Instanz für jeden umgeleiteten Wiederherstellungsvorgang auswählen.

Siehe ["Methoden für das Wiederherstellen von Daten in Backup Exec"](#) auf Seite 258.

Erweiterte Wiederherstellungsoptionen in Oracle

Die folgenden erweiterten Optionen sind verfügbar, wenn Sie Oracle-Daten wiederherstellen.

Tabelle H-8 Erweiterte Wiederherstellungsoptionen in Oracle

Element	Beschreibung
Datenbank nach dem Wiederherstellen öffnen	Stellt sicher, dass die Datenbank geöffnet wird, sobald die Wiederherstellung fertig gestellt ist. Aktivieren Sie diese Option, wenn die Datenbank nach der Wiederherstellung online geschaltet werden soll.
Schreibgeschützte Dateien wiederherstellen, wenn sie nicht aktuell sind	Ermöglicht, dass RMAN die Header aller schreibgeschützten Datendateien überprüft und alle nicht aktuellen wiederherstellt.

Element	Beschreibung
Nur Überprüfung; keine Wiederherstellung von Daten	<p>Lädt alle erforderlichen Medien und liest sie bei Bedarf. RMAN wählt die für den Vorgang erforderlichen Backup-Sätze aus und scannt sie, um sicherzustellen, dass sie verfügbar und nicht beschädigt sind. Es werden keine Daten auf den Datenbankserver geschrieben oder wiederhergestellt. Eine Überprüfung der Steuerdatei wird nicht unterstützt.</p> <p>Es wird empfohlen, dass Sie diese Option aktivieren, um sicherzustellen, dass alle erforderlichen Medien verfügbar sind, bevor Sie die Datenbank wiederherstellen.</p>
Daten wiederherstellen, wenn die Überprüfung ohne Fehler abgeschlossen wurde	<p>Ermöglicht die sofortige Ausführung des Wiederherstellungsauftrags, wenn die Prüfung erfolgreich war.</p> <p>Alle Optionen, die Sie für die Wiederherstellung ausgewählt haben, werden angewendet.</p>
Nur die Steuerdatei wiederherstellen	Stellt die Steuerdatei für die Oracle-Datenbank wieder her, ohne die Tablespace oder die verbundenen Datendateien einzuschließen.
Nach dem Wiederherstellen nicht mehr benötigte archivierte Protokolle löschen	Löscht ältere Protokolldateien und gibt Speicherplatz auf der Festplatte frei.
Maximale Anzahl zu verwendender Geräte für Ressourcen, die mehrere Datenströme unterstützen	<p>Gibt die maximale Anzahl verfügbarer Geräte für den Backup-Auftrag an.</p> <p>Wenn Sie mehr als ein Gerät angeben, müssen Sie eines der folgenden Elemente als Zielspeicher für den Backup-Auftrag auswählen:</p> <ul style="list-style-type: none"> ■ Einen Speicherpool. ■ Einen veralteten Backup-to-Disk-Ordner, für den mindestens zwei Vorgänge gleichzeitig aktiviert sind. <p>Wenn nur ein Speichergerät für den Backup-Auftrag zur Verfügung steht, werden die Datenströme von RMAN auf dem Medium seriell gesichert.</p> <p>Diese Option steht für von DBA gestartete Aufträge nicht zur Verfügung.</p>

Ausführen einer umgeleiteten Wiederherstellung einer Oracle 12c-Datenbank unter Verwendung von Backup Exec

Szenarien für umgeleitete Datenbankwiederherstellungen

- Datenbank mit einer OMF (Oracle Managed File)
 - Wiederherstellen der Datenbank im selben Pfad auf einem neuen Host
Bevor Sie den Wiederherstellungsauftrag ausführen, stellen Sie sicher, dass die Ordnerstruktur auf dem neuen Oracle-Server mit der der ursprünglichem Datenbank identisch ist. Bei einer OMF-Datenbank werden PDB-Ordner als GUIDs erstellt. Sie müssen daher dieselbe Ordnerstruktur wie die der ursprünglichen Datenbank manuell erstellen.
 - Wiederherstellen der Datenbank in einem anderen Pfad auf einem neuen Host
Sie können den Pfad für die umgeleitete Wiederherstellung in der Benutzeroberfläche von Backup Exec angeben. Oracle Agent erstellt die Ordnerstruktur mit PDB-Namen im angegebenen Pfad und stellt die Daten in den entsprechenden Ordnern wieder her.
Beispiel: Der Pfad für die in Backup Exec angegebenen umgeleitete Wiederherstellung lautet `C:\Redirect`. Die CDB, die Sie wiederherstellen möchten, hat zwei PDBs: PDB1 und PDB2. Diese PDBs haben GUID-basierte Ordner in der ursprünglichen Datenbank. Nach der Wiederherstellung werden Daten in den folgenden Ordnern wiederhergestellt:
 - Daten aus PDB1 werden in `C:\Redirect\PDB1` wiederhergestellt.
 - Daten aus PDB2 werden in `C:\Redirect\PDB2` wiederhergestellt.
 - Daten aus PDB\$SEED werden in `C:\Redirect\PDB$SEED` wiederhergestellt.
 - Daten aus ROOT werden in `C:\Redirect\ROOT` wiederhergestellt.

Hinweis: Wenn der Oracle Agent die Verzeichnisstruktur nicht erstellen kann, schlägt der Wiederherstellungsauftrag fehl und der Benutzer wird aufgefordert, die Struktur manuell zu erstellen.

- Datenbank ohne OMF
 - Wiederherstellen der Datenbank im selben Pfad auf einem neuen Host
Bevor Sie den Wiederherstellungsauftrag ausführen, stellen Sie sicher, dass die Ordnerstruktur auf dem neuen Oracle-Server mit der der ursprünglichem Datenbank identisch ist.

- Wiederherstellen der Datenbank in einem anderen Pfad auf einem neuen Host
Sie können den Pfad für die umgeleitete Wiederherstellung in der Benutzeroberfläche von Backup Exec angeben. Oracle Agent erstellt die Ordnerstruktur mit PDB-Namen im angegebenen Pfad und stellt die Daten in den entsprechenden Ordnern wieder her.
Beispiel: Der Pfad für die in Backup Exec angegebenen umgeleitete Wiederherstellung lautet `C:\Redirect`. Die CDB, die Sie wiederherstellen möchten, hat zwei PDBs: PDB1 und PDB2. Diese PDBs haben namensbasierte Ordner in der ursprünglichen Datenbank. Nach der Wiederherstellung werden Daten in den folgenden Ordnern wiederhergestellt:
 - Daten aus PDB1 werden in `C:\Redirect\PDB1` wiederhergestellt.
 - Daten aus PDB2 werden in `C:\Redirect\PDB2` wiederhergestellt.
 - Daten aus PDB\$SEED werden in `C:\Redirect\PDB$SEED` wiederhergestellt.
 - Daten aus ROOT werden in `C:\Redirect\ROOT` wiederhergestellt.

Hinweis: Wenn der Oracle Agent die Verzeichnisstruktur nicht erstellen kann, schlägt der Wiederherstellungsauftrag fehl und der Benutzer wird aufgefordert, die Struktur manuell zu erstellen.

Hinweis: Backup Exec unterstützt die umgeleitete Wiederherstellung einer PDB auf einen neuen Host nicht. Das Umleiten einer Wiederherstellung einer PDB auf demselben Host in einen anderen Pfad wird jedoch von Backup Exec unterstützt.

Wichtige Punkte beim Umleiten einer Wiederherstellung

- Standardmäßig stellt RMAN die Dateien in demselben Speicherort wieder her, aus dem sie gesichert wurden.
- Die Datenbankverzeichnisse und -pfade werden nicht von RMAN erstellt, müssen aber bereits existieren.
- Löschen Sie die Wiederholen-Protokolle, bevor Sie den Wiederherstellungsauftrag starten, da datenträgerbasierte Protokolle nicht nützlich sind. Wenn Sie die Wiederholen-Protokolle nicht löschen, kann der Wiederherstellungsauftrag mit dem folgenden Fehler fehlschlagen:
ORA-19698: C:\APP\ORAUSER\ORADATA\STRING\REDO01.LOG stammt aus einer anderen Datenbank: id=nnnnnn, db_name=STRING

- Wenn Sie die Datenbank im selben Pfad auf einem neuen Host wiederherstellen möchten, stellen Sie sicher, dass die Verzeichnisstruktur mit der ursprünglichen Datenbank identisch ist. Wird die Wiederherstellung jedoch in einem anderen Pfad auf einem neuen Host umgeleitet, erstellt der Oracle Agent die Verzeichnisse im neuen Pfad.

Verwenden Sie das Verfahren zum Einsatz eines neuen Oracle-Servers, um die vollständige Oracle-Instanz oder -Datenbank wiederherzustellen, nachdem sie verloren gegangen, gelöscht oder zerstört wurde.

Ausführen einer umgeleiteten Wiederherstellung einer Oracle 12c-Datenbank unter Verwendung von Backup Exec

- 1 Erstellen Sie die Oracle-Datenbank mit dem Namen der ursprünglichen Datenbank, die nicht mehr verfügbar ist.
- 2 Benennen Sie die Datei `pwd<SID>.ora` um. Notieren Sie sich den Pfad zu dieser Datei für die Verwendung im Schritt 3b.
- 3 Erstellen Sie eine neue Version der Datei `pwd<SID>.ora`:
 - Öffnen Sie eine Eingabeaufforderung.
 - Geben Sie folgenden Befehl ein:
`orapwd file="path from Step 2"\pwd<sid>.ora password=<Kennwort>`
Beispiel: `C:\> orapwd file=c:\oracle\product\12.1.0\db_1\database\pwdORCL1.ora password=NEWpassword`

Hinweis: Backup Exec Remote Agent muss für den Zugriff auf die Oracle-Datenbank installiert und konfiguriert sein.

- 4 Geben in der Eingabeaufforderung folgenden Befehl ein:
`SQLplus / as SYSDBA`
- 5 Geben Sie `SHUTDOWN IMMEDIATE;` ein.
- 6 Geben Sie `STARTUP NOMOUNT;` ein.
- 7 Schließen Sie `Sqlplus` und starten Sie `RMAN` über die Eingabeaufforderung.
- 8 Geben Sie `SET DBID=dbid ID;` ein.

Hinweis: Diese `dbid` muss mit der `dbid` der ursprünglichen Oracle-Instanz identisch sein. Geben Sie schließlich `EXIT` ein.

- 9 Klicken Sie auf dem Backup Exec-Server in der Navigationsleiste auf den Pfeil neben "Wiederherstellen" und dann auf "Neuer Wiederherstellungsauftrag".
- 10 Klicken Sie im Bereich "Eigenschaften" unter "Quelle" auf "Auswählen".
- 11 Wählen Sie die entsprechende Steuerdatei zum Wiederherstellen aus.
- 12 Klicken Sie im Teilfenster "Wiederherstellungsauftrag – Eigenschaften" unter "Ziel" auf "Oracle-Umleitung".
- 13 Aktivieren Sie das Kontrollkästchen "Oracle-Instanz auf Server wiederherstellen". Geben Sie die Identifikationsdaten für das Konto ein, um auf den neuen oder alternativen Oracle-Server zuzugreifen.

Wenn die Oracle-Dateien und Archivprotokolle auf einem anderen Speicherort auf dem Zielsystem gespeichert sind, aktivieren Sie die Option "Oracle-Dateien in Pfad umleiten" und geben Sie die gültigen Pfade für die Dateien und Archivprotokolle ein. Klicken Sie auf "Jetzt ausführen", um den Wiederherstellungsauftrag zu starten.

Hinweis: Der Wiederherstellungsauftrag schlägt fehl, weil der Wiederherstellungsanteil inkonsistente Archivprotokolle erkennt. Dies ist ein normaler Vorgang bei einer Notfallwiederherstellung.

- 14 Starten Sie auf dem Oracle-Server in der Eingabeaufforderung "SQLplus/as SYSDBA".
- 15 Geben Sie `alter database open resetlogs; ein.`

Tritt ein Fehler auf, während Oracle versucht, die Datenbank zu öffnen, dokumentieren Sie den Online-Wiederhol-Protokollpfad, und aktualisieren Sie dann den Pfad:

- Öffnen Sie auf dem Oracle-Server die Eingabeaufforderung und geben Sie den folgenden Befehl ein: `SQLPLUS /nolog`
- Geben Sie `connect<sys/password@SID>; ein.`
- Geben Sie folgenden SQLPlus-Befehl ein:

`SQLPLUS ALTER DATABASE RENAME FILE <alter Pfad aus Backup auf einen beliebigen Wiederhol-Protokolldateinamen> to <Pfad zum Namen des erwarteten wiederhergestellten Wiederhol-Protokolls>;`

Beispiel: `ALTER DATABASE RENAME FILE`

`'D:\ORACLE\ORADATA\JACOB\REDO01.LOG' to`
`'C:\ORACLE\ORADATA\JACOB\REDO01.LOG';`

- In der Eingabeaufforderung geben Sie "RMAN" und dann in der RMAN-Eingabeaufforderung den folgenden Befehl ein:

```
alter database open resetlogs;
```

- Schließen Sie die Eingabeaufforderung.

ist die Wiederherstellung abgeschlossen.

Anforderungen zum Wiederherstellen der vollständigen Oracle-Instanz und -Datenbank unter Verwendung des ursprünglichen Oracle-Servers

Wenn die Oracle-Instanz oder -Datenbank vollständig gelöscht oder unbrauchbar werden, können Sie den gleichen Oracle-Server für die Wiederherstellung verwenden. Sie können diese Anweisungen auch verwenden, wenn Sie einen neuen physischen Server konfigurieren, der den gleichen Servernamen und SID-Namen verwendet.

Für eine erfolgreiche Wiederherstellung entsprechend dieses Fallbeispiels müssen Sie über Folgendes verfügen:

Tabelle H-9 Anforderungen für die Wiederherstellung anhand des ursprünglichen Oracle-Servers

Element	Beschreibung
DBID	Wenn Sie die DBID nicht kennen, können Sie diese nach dem Einloggen im Backup Exec-Auftragsprotokoll oder in RMAN nachschlagen.
ControlFile Piece-ID	Sie können die ControlFile Piece-ID im Unterknoten "Steuerdateien" des Oracle-Knotens in der Backup Exec-Wiederherstellungsansicht feststellen.
Vollständiges Oracle-System-Backup	Das vollständige Oracle-System-Backup muss Folgendes umfassen: <ul style="list-style-type: none">■ Steuerdatei■ Datendateien■ Archivierungsprotokolle Für Oracle 12c müssen Sie ein vollständiges Backup der Containerdatenbank durchführen.
Der ursprüngliche Oracle-Server	Um das Oracle-System nach einem Notfall wiederherzustellen, muss die Wiederherstellung auf dem ursprünglichen Oracle-Server erfolgen.

Wiederherstellen der vollständigen Oracle-Instanz und -Datenbank unter Verwendung des ursprünglichen Oracle-Servers

Sie können den gleichen Oracle-Server für eine Wiederherstellung verwenden, wenn ein vollständiger Verlust, eine vollständige Löschung oder Zerstörung der Oracle-Instanz oder -Datenbank auftritt.

Siehe ["Anforderungen zum Wiederherstellen der vollständigen Oracle-Instanz und -Datenbank unter Verwendung des ursprünglichen Oracle-Servers"](#) auf Seite 1379.

So stellen Sie die vollständige Oracle-Instanz oder -Datenbank unter Verwendung des ursprünglichen Oracle-Servers wieder her

- 1 Erstellen Sie die Oracle-Datenbank erneut mit demselben Namen, den Sie für die verloren gegangene ursprüngliche Datenbank verwendet hatten.
- 2 Suchen Sie die Datei "pwd<SID>.ora" und benennen Sie sie um.
- 3 Gehen Sie entsprechend der folgenden Anweisungen und in der angegebenen Reihenfolge vor, um eine neue pwd-<SID>.ora-Datei zu erstellen:
 - Öffnen Sie eine Eingabeaufforderung.
 - Geben Sie folgenden Befehl ein:
`orapwd file=path\pwdsid.ora password=<password>`
- 4 Geben Sie die folgenden Befehle in der angegebenen Reihenfolge ein:
 - `RMAN`
 - Geben Sie `CONNECT TARGET <sys/password@sid>;` ein.
 - `SHUTDOWN ABORT;`
 - `STARTUP NOMOUNT;`
 - `SET DBID<dbid ID>;`
- 5 Starten Sie auf dem Backup Exec-Server den Backup Exec-Wiederherstellungsassistenten.
- 6 Wählen Sie das entsprechende ControlFile für die Wiederherstellung aus.
Der Wiederherstellungsauftrag schlägt fehl, da Archivierungsprotokolle gefunden werden, die nicht miteinander vereinbar sind. Dies ist ein normaler Vorgang bei einer Notfallwiederherstellung.
- 7 Beenden Sie nach Fertigstellung des Wiederherstellungsauftrags Backup Exec.
- 8 Geben Sie an der Oracle-Server-Eingabeaufforderung Folgendes ein:
Alter database open resetlogs;
- 9 Schließen Sie die Eingabeaufforderung.

Anforderungen für die Wiederherstellung der vollständigen Oracle-Instanz oder -Datenbank auf einen anderen als den ursprünglichen Oracle-Server-Computer.

Wenn eine Oracle-Instanz oder Datenbank vollständig verloren geht, gelöscht oder zerstört wird, können Sie die Instanz und die Datenbank auf einem anderen Computer als den ursprünglichen Oracle-Server wiederherstellen.

Siehe ["Wiederherstellen der vollständigen Oracle-Instanz und -Datenbank unter Verwendung des ursprünglichen Oracle-Servers"](#) auf Seite 1380.

Für eine erfolgreiche Wiederherstellung entsprechend dieses Fallbeispiels müssen Sie über Folgendes verfügen:

Tabelle H-10 Anforderungen bei der Wiederherstellung mit einem neuen oder alternativen Oracle-Server

Element	Beschreibung
DBID	Wenn Sie die DBID nicht kennen, können Sie diese nach dem Einloggen im Backup Exec-Auftragsprotokoll oder in RMAN nachschlagen.
ControlFile Piece-ID	Sie können die ControlFile Piece-ID im Unterknoten "Steuerdateien" des Oracle-Knotens in der Backup Exec-Wiederherstellungsansicht feststellen.
Vollständiges Oracle-System-Backup	Das vollständige Oracle-System-Backup muss Folgendes umfassen: <ul style="list-style-type: none">■ Steuerdatei■ Datendateien■ Archivierungsprotokolle

Wiederherstellen der vollständigen Oracle-Instanz oder -Datenbank auf einem anderen als den ursprünglichen Oracle-Server

Sie können eine Oracle-Instanz oder -Datenbank auf einem anderen Computer als dem ursprünglichen Oracle-Server wiederherstellen.

Siehe ["Anforderungen für die Wiederherstellung der vollständigen Oracle-Instanz oder -Datenbank auf einen anderen als den ursprünglichen Oracle-Server-Computer."](#) auf Seite 1381.

So stellen Sie die vollständige Oracle-Instanz und -Datenbank auf einem anderen als dem ursprünglichen Oracle-Server wieder her

- 1 Erstellen Sie die Oracle-Instanz erneut mit demselben Namen, den Sie für die verloren gegangene ursprüngliche Instanz verwendet hatten.
- 2 Suchen Sie die Datei "pwd<SID>.ora" und benennen Sie sie um.
- 3 Gehen Sie entsprechend der folgenden Anweisungen und in der angegebenen Reihenfolge vor, um eine neue pwd-<SID>.ora-Datei zu erstellen:
 - Öffnen Sie eine Eingabeaufforderung.
 - Geben Sie folgenden Befehl ein:

```
orapwd file=path\pwdsid.ora password=<Kennwort>
```
- 4 Geben Sie die folgenden Befehle in der angegebenen Reihenfolge ein:
 - RMAN
 - Geben Sie `CONNECT TARGET <sys/password@sid>;` ein.
 - `SHUTDOWN ABORT;`
 - `STARTUP NOMOUNT;`
 - `SET DBID<dbid ID>;`
- 5 Starten Sie auf dem Backup Exec-Server den Backup Exec-Wiederherstellungsassistenten.
- 6 Wählen Sie das entsprechende ControlFile für die Wiederherstellung aus.
- 7 Wählen Sie die Option zum Wiederherstellen "Auf einem anderen Oracle-Server" und die entsprechenden Optionen aus.
- 8 Beenden Sie nach Fertigstellung des Wiederherstellungsauftrags Backup Exec.
Der Wiederherstellungsauftrag schlägt fehl, da Archivierungsprotokolle gefunden werden, die nicht miteinander vereinbar sind. Dies ist ein normaler Vorgang bei einer Notfallwiederherstellung.
- 9 Wechseln Sie zum Oracle-Server.

10 Geben Sie **Alter database open resetlogs;** ein.

11 Sie haben folgende Möglichkeiten:

Es tritt ein Fehler auf, während Oracle versucht, die Datenbank zu öffnen.	Notieren Sie sich den Online-Redo-Protokollpfad und aktualisieren Sie dann den Pfad.
--	--

Es tritt kein Fehler auf.	Keine Aktion. Die Notfallwiederherstellung ist abgeschlossen.
---------------------------	---

Best Practices für Backup Exec Agent for Oracle auf Windows- und Linux-Servern

Best Practices sind Tipps und Empfehlungen, die Ihnen helfen können, Backup Exec Agent for Oracle auf Windows- und Linux-Servern (Oracle Agent) effektiv zu verwenden. Weitere Informationen zum Oracle Agent finden Sie im *Administratorhandbuch zu Backup Exec*.

Die folgenden empfohlenen Verfahren helfen Ihnen, den Oracle Agent effektiv zu verwenden:

- Aktivieren Sie den Oracle-Archivprotokollmodus und die automatische Archivierung für Protokolldateien von Oracle.
- Kennen Sie die DBID und andere wichtige Konfigurationsdetails der Datenbank.
- Kennen Sie die Namen von init<SID>.ora und die spfiles für die Instanzen auf dem Oracle-Server.
- Speichern Sie das RMAN-Repository nicht auf dem gleichen Server, auf dem sich die zu sichernde Datenbank befindet.
- Sichern Sie Ihre aktuelle Steuerdatei, wenn Sie einen vom Datenbankadministrator (DBA) initiierten Auftrag ausführen. Wenn ein Backup der aktuellen Steuerdatei vorliegt, müssen Sie Medien nicht durchsuchen, um eine Steuerdatei zu finden, die zur Wiederherstellung verfügbar ist.
- Prüfen Sie Wiederherstellungsszenarien häufig, um mit den Wiederherstellungsverfahren vertraut zu werden. Die Oracle-Wiederherstellung kann komplex sein und ist aufgrund der Art der betroffenen Daten häufig zeitempfindlich. Es wird empfohlen, dass Sie Testpläne und Konfigurationsaktivitäten mit Ihrem Oracle DBA koordinieren, um sicherzustellen, dass die Wiederherstellungsverfahren bestätigt sind.

- Verwenden Sie RMAN-Skripts, um folgende Schritte durchzuführen:
 - Löschen Sie alle Archivprotokollkopien in einer gemultiplexten Archivprotokollkonfiguration.

Hinweis: Sie können Backup Exec verwenden, um alle nicht gemultiplexten, einzelnen Speicherortarchivprotokolle zu löschen.

- Führen Sie die RMAN-Optimierung aus.

Berücksichtigen Sie die folgenden Verfahren, wenn Sie Oracle-Datenbanken sichern:

- Führen Sie ein vollständiges Backup durch, wenn Sie Strukturveränderungen an einer Datenbank vornehmen.
- Löschen Sie archivierte Protokolldateien nicht, es sei denn, Sie haben zwei bestätigte Backups jedes Protokolls.
- Erstellen Sie aus folgenden Gründen Oracle-spezifische Mediensätze und Backup-Aufträge:
 - RMAN kann die Aufbewahrung von Medien verwalten und dem Backup Exec-Server mitteilen, dass Backup-Sätze abgelaufen sind. RMAN kann den Aufbewahrungszeitraum der Medien erfolgreich verwalten, solange keine nicht zusammenhängenden Backup-Sätze vorhanden sind. Nicht zusammenhängende Backup-Sätze haben Aufbewahrungszeiträume, die länger als der RMAN-Aufbewahrungszeitraum sind.
 - Mediensätze für Oracle-Backups sollten einen Aufbewahrungszeitraum haben, der größer als die Einstellung für `CONTROL_FILE_RECORD_KEEP_TIME` ist. Standardmäßig ist `CONTROL_FILE_RECORD_KEEP_TIME` 7 Tage. Wenn die Mediensätze für die Oracle-Backups einen größeren Aufbewahrungszeitraum haben, werden Backup-Sätze nicht überschrieben und RMAN wird nicht aktualisiert.
 - Wenn Sie mehrere Auftragsströme in Oracle konfigurieren, können zusätzliche Ressourcen wie Dateisysteme dazu führen, dass mehr Geräte als erwartet Laufwerke zuordnen.
- Verteilen Sie die Last von Oracle-Aufträgen zwischen verwalteten Backup Exec-Servern in einer CASO-Umgebung. Jedoch bedeutet dieses Szenario, dass archivierte Protokolldatei-Backups sich auf mehreren verwalteten Backup Exec-Servern befinden können. Dies erschwert die Wiederherstellung.

- Erwägen Sie Neuzuweisungen von Ports, wenn Sie RALUS in einer Linux-Umgebung verwenden. Anwendungen wie zum Beispiel Webmin, die Port 10000 verwenden, können RALUS-Vorgänge behindern.
- Aktivieren Sie Oracle Block Change Tracking für schnellere inkrementelle Backups.
- Aktivieren Sie Backup Exec-Komprimierung, wenn Sie allgemeine Optionen für Backup-Aufträge konfigurieren.
- Stellen Sie sicher, dass Sie den vollständig qualifizierten Domännennamen des Oracle-Servers eingeben, wenn Sie ihn der Liste von Servern auf der Registerkarte "Backup und Wiederherstellung" hinzufügen.
- Stellen Sie sicher, dass Sie den vollqualifizierten Domännennamen des Oracle-Servers und den Namen des Login-Kontos in die Liste der Oracle-Server und Authentifizierungsdaten des Backup Exec-Servers aufnehmen.

Die folgenden Best Practices müssen beachtet werden, wenn Sie eine Oracles 12c-Datenbank verwenden:

- Erstellen Sie ein vollständiges Backup einer Container-Datenbank (CDB), wann immer es eine Strukturveränderungen gibt, wie zum Beispiel die Ergänzung einer neuen Plug-fähigen Datenbank (PDB).
- Schließen Sie das Stammverzeichnis der CDB in die Backups ein, um sicherzustellen, dass Metadaten der CDB immer gesichert werden.
- Führen Sie die Datenbank im Archivprotokollmodus aus, um sicherzustellen, dass die Datenbank zum Zeitpunkt wiederhergestellt werden kann.
- Wenn sich die CDB im Modus "No Archive Log" befindet, fahren Sie vor dem Sichern der PDB die CDB herunter. Um das Herunterfahren der CDB zu vermeiden, können Sie entweder die Datenbank im Archivprotokollmodus ausführen oder ein DBA-initiiertes Backup der PDBs ausführen.
- Oracle empfiehlt, nicht nur das Stammverzeichnis wiederherzustellen, da dies Inkonsistenzen in den Metadaten verursachen kann. Stattdessen sollten Sie die gesamte CDB wiederherstellen.
- Wenn die PIT-Wiederherstellung (point in time) der PDB fehlschlägt, schlagen möglicherweise auch nachfolgende Aufträge mit der folgenden Fehlermeldung fehl:
ORA-19852: Error creating services for auxiliary instance.
Dieser Fehler tritt auf, weil die vorherigen fehlgeschlagenen PIT-Wiederherstellungsversuche nicht richtig bereinigt wurden. Um dieses Problem zu beheben, müssen Sie die fehlgeschlagenen PIT-Datenbankwiederherstellungsversuche bereinigen. Führen Sie die folgenden

Schritte durch, um die fehlgeschlagenen Erstellungsversuche für zusätzliche Dienste zu bereinigen:

- Verwenden Sie das Datenbank (DB)-PIT-Wiederherstellungspaket, um die zusätzliche Instanz im Falle fehlgeschlagener PIT-Aufträge zu bereinigen:

```
SQL> exec dbms_backup_restore.manageauxinstance ('DBPITR',1);
```

- Führen Sie den obigen Satz von Befehlen im RMAN-Skript aus, um die RMAN-Konfiguration zu bereinigen.

```
CONFIGURE CHANNEL DEVICE TYPE 'SBT_TAPE' CLEAR;
```

```
CONFIGURE AUXILIARY CHANNEL DEVICE TYPE 'SBT_TAPE' CLEAR;
```

Backup Exec Agent for Enterprise Vault

Dieser Anhang enthält folgende Themen:

- [Info zu Agent for Enterprise Vault](#)
- [Anforderungen für Enterprise Vault Agent](#)
- [Installieren von Enterprise Vault Agent](#)
- [Info zu Backup-Methoden für Enterprise Vault-Backup-Aufträge](#)
- [Info zum Sichern von Enterprise Vault-Komponenten](#)
- [Konsistenzprüfungen für Enterprise Vault-Datenbanken und Compliance and Discovery Accelerator-Datenbanken](#)
- [Wiederherstellen von Enterprise Vault](#)
- [Konfigurieren von Enterprise Vault für die Verwendung des Namens des neuen SQL-Servers mit der Verzeichnisdatenbank](#)
- [Best Practices für den Enterprise Vault Agent](#)
- [Info zu Backup Exec Migrator for Enterprise Vault](#)
- [Enterprise Vault-Login-Konto](#)
- [Optionen zu Enterprise Vault](#)

Info zu Agent for Enterprise Vault

Backup Exec Agent for Enterprise Vault (Enterprise Vault Agent) wird als Teil des Agents for Applications and Databases installiert.

Enterprise Vault Agent bietet Datenschutz für die folgenden Enterprise Vault-Komponenten:

- Standorte
- Vault-Speichergruppen
- Datenbanken
- Indizes
- Speicherpartitionen

Enterprise Vault Agent kann helfen, eine Notfallwiederherstellungslösung für Daten zur Verfügung zu stellen, die mit Enterprise Vault archiviert werden. Die Wiederherstellung der archivierten Daten hängt nicht von der Archivquelle, beispielsweise Exchange Server oder einem spezifischen Dateisystem, ab.

Enterprise Vault Agent lässt Sie folgende Aktionen durchführen:

- Enterprise Vault-Archive aus geöffneten oder geschlossenen Speicherpartitionen sichern oder wiederherstellen
- Einzelne Enterprise Vault-Speichergruppen über eine Enterprise Vault-Site sichern und wiederherstellen
- Backups von Enterprise Vault-Speicherorten, -Datenbanken und -Index-Speicherorten erstellen und wiederherstellen

Beim Sichern von Enterprise Vault-Servern können die folgenden Enterprise Vault-Komponenten zusammen mit den Speicherpartitionen gesichert werden:

- Enterprise Vault-Verzeichnis- und Überwachungsdatenbanken
- Enterprise Vault-Prüfung, FSA-Berichterstellung und Fingerabdruckdatenbanken
- Enterprise Vault-Speicherdatenbanken
- Enterprise Vault-Indexdateien

Wenn Sie die Enterprise Vault Compliance and Discovery Accelerator-Produkte installieren, können die folgenden Komponenten gesichert werden:

- Enterprise Vault Compliance Accelerator- und Discovery Accelerator-Konfigurationsdatenbanken
- Enterprise Vault Compliance and Discovery Accelerator-Kundendatenbanken
- Enterprise Vault Discovery Accelerator Custodian -Datenbank

Enterprise Vault Agent verwendet den Enterprise Vault-Backup-Modus, um Enterprise Vault-Komponenten zu sichern. Mithilfe des Backup-Modus kann Enterprise Vault Agent Enterprise Vault-Komponenten sichern, ohne Enterprise Vault-Archivierungsvorgänge unterbrechen zu müssen.

Beispielsweise wenn Sie eine Speichergruppe oder eine Site für die Sicherung auswählen, wird der jeweilige Speicher oder Indizes in den Backup-Modus versetzt. Backup-Modus lässt Enterprise Vault mit der Archivierung in anderen Speichergruppen oder Sites fortfahren. Nachdem der Backup-Auftrag erfolgreich abgeschlossen wurde, nimmt Enterprise Vault Agent die Enterprise Vault-Komponenten aus dem Backup-Modus, damit diese Komponenten die Archivierung weiterhin durchführen können.

Während Enterprise Vault-Versionen 8.x, 9.x und 10.x den Backup-Modus implementieren, bieten Ihnen Enterprise Vault 9.x und 10.x mehr Flexibilität bei Ihren Backup-Aufträgen für Speicher. Mit Enterprise Vault 9.x und 10.x können Sie mehrere Backup-Aufträge des gleichen Speichers aus Enterprise Vault 9.x und 10.x gleichzeitig ausführen. In Enterprise Vault 8.x müssen mehrere Speicher-Backup-Aufträge nacheinander ausgeführt werden.

Beispielsweise können Sie zum Sichern eines Speichers mehrere Backup-Aufträge erstellen. Die Auswahlliste aller Backup-Aufträge enthält eine oder mehrere Partitionen des Speichers. Unter Enterprise Vault 9.x und 10.x werden die Partitionen gleichzeitig gesichert, wenn verschiedene Backup-Aufträge gleichzeitig auf sie zugreifen. Unter Enterprise Vault 8.x werden die Partitionen zwar in beiden Backup-Aufträgen gesichert, allerdings nacheinander. Der erste Backup-Auftrag muss beendet sein, bevor der zweite Auftrag beginnt. Andernfalls schlägt der Backup-Auftrag fehl.

Hinweis: In allen Versionen von Enterprise Vault sichert Enterprise Vault Agent jedes Mal automatisch die Speicherdatenbank, wenn eine geöffnete Partition gesichert wird.

Enterprise Vault Agent führt Backups der Compliance Accelerator- und Discovery Accelerator- Anwendungsdatenbanken durch, während sie online sind. Es legt die Datenbanken nicht im schreibgeschützten Modus oder im Backup-Modus ab, bevor es die Backups durchführt.

Enterprise Vault Agent führt eine physische Überprüfung auf allen Enterprise Vault-Datenbanken aus, bevor sie gesichert werden. Enterprise Vault Agent führt auch eine physikalische Überprüfung auf jeder Datenbank aus, bevor Sie sie wiederherstellen.

Hinweis: Enterprise Vault Agent verwendet physikalische Datenbankkonsistenzüberprüfungen, weil physikalische Überprüfungen weniger Systemressourcen als andere Typen von Datenbankkonsistenzüberprüfungen verbrauchen.

Das Sichern und Wiederherstellen von Enterprise Vault-Datenbanken und den zugehörigen Komponenten erfordert bestimmte Benutzerkontendaten für jede Enterprise Vault-Komponente, die Sie schützen.

Tabelle I-1 Unterstützte Benutzerkonten, die erforderlich sind, um Enterprise Vault-Komponenten zu sichern und wiederherzustellen

Enterprise Vault-Komponenten	Benutzer-Anmeldeinformationen
Enterprise Vault-Datenbanken und -Komponenten (Speicher, Indexe, Partitionen, Speicherdatenbank, Verzeichnis, Überwachung, Fingerabdruck, FSA-Berichterstellung- und Prüfungsdatenbanken)	<p>Die folgenden Anmeldedaten sind erforderlich:</p> <ul style="list-style-type: none">■ Vault-Dienstkonto■ Domänenadministratorkonto mit rollenbasierten Administratorrechten <p>Sie können auch jedes Domänenbenutzerkonto verwenden, das die folgenden Bedingungen erfüllt:</p> <ul style="list-style-type: none">■ Das Benutzerkonto muss in der Administratorgruppe auf allen Servern enthalten sein, auf denen sich Enterprise Vault-Partitionen und Enterprise Vault-Datenbanken befinden.■ Das Benutzerkonto muss Backup-bezogene, rollenbasierte Administratorrechte für den Speicher und den Index-Standort haben. Backup-bezogene rollenbasierte Administratorrechte umfassen:<ul style="list-style-type: none">■ EVT Speicher-Backupmodus verwalten■ EVT Indexort-Backup-Modus verwalten <p>Um rollenbasierte Administratorrechte für einen Windows-Domänen-Administratorkonto zu konfigurieren, konsultieren Sie Ihre Enterprise Vault-Dokumentation.</p>

Enterprise Vault-Komponenten	Benutzer-Anmeldeinformationen
Compliance Accelerator und Discovery Accelerator	Die folgenden Anmeldedaten sind erforderlich: <ul style="list-style-type: none">■ Vault-Dienstkonto■ Domänenadministratorkonto Ein Benutzerkonto, das Mitglied der Gruppe des Administrators auf den Computern ist, auf denen sich die Anwendungen "Compliance" und "Discovery Accelerator" sich befinden.

Beim Sichern bestimmter Enterprise Vault-Komponenten werden automatisch auch andere Enterprise Vault-Komponenten gesichert. Backup Exec schließt diese Komponenten mit ein, um eine eventuelle Wiederherstellung von Enterprise Vault zu beschleunigen.

Tabelle I-2 Enterprise Vault-Datenbanken, die automatisch gesichert werden

Backup durch Benutzer:	Automatisches Backup durch Backup Exec:	Beschreibung
Enterprise Vault-Standort	Verzeichnisdatenbank	Backup Exec sichert automatisch auch die mit dem Enterprise Vault-Standort verbundene Verzeichnisdatenbank.
Geöffnete Partition	Speicherdatenbank	Backup Exec sichert automatisch auch die mit der geöffneten Partition verbundene Speicherdatenbank.

Im Laufe der Zeit wächst die Menge der Daten, die Enterprise Vault speichert. Irgendwann beobachten sie möglicherweise, dass Sie, während die Daten ihren Nutzungslebenszyklus durchlaufen, nicht mehr so häufig darauf zugreifen. Sie können Backup Exec Migrator verwenden, damit Enterprise Vault automatisch die älteren Enterprise Vault-Daten zu den Speichergeräten migriert, die Backup Exec verwaltet.

Siehe ["Info zu Backup Exec Migrator for Enterprise Vault"](#) auf Seite 1413.

Anforderungen für Enterprise Vault Agent

Überprüfen Sie die folgenden Anforderungen, bevor Sie Agent for Enterprise Vault (Enterprise Vault Agent) verwenden.

- Auf dem Enterprise Vault-Server muss mindestens eine Partition vorhanden sein, damit die Serverankündigung bei Backup Exec erfolgen kann.
- Sie müssen Backup Exec Agent for Windows installieren und Enterprise Vault Agent auf jedem Computer lizenzieren, auf dem eine Enterprise Vault-Komponente vorhanden ist.

Hinweis: Enterprise Vault Agent nutzt den Agent for Windows zum Sichern aller NTFS-Freigaben auf einem Remote-Computer mit Enterprise Vault-Daten. Wenn Agent for Windows jedoch nicht installiert ist, verwendet Enterprise Vault Agent das Microsoft Common Internet File System (CIFS) zum Sichern der Daten.

Bei einem Gerät oder einem Filter, der Agent for Windows nicht unterstützt, verwendet Enterprise Vault Agent CIFS zum Sichern der Daten. Es wird empfohlen, für NDMP-Backups von Enterprise Vault-Daten getrennte Backup-Aufträge zu erstellen. Mit NDMP Feature von Backup Exec kann eine deutliche Leistungssteigerung bei NDMP-Backups erzielt werden.

Installieren von Enterprise Vault Agent

Der Agent for Enterprise Vault (Enterprise Vault Agent) wird als Teil des Agent for Applications and Databases installiert. Um alle Enterprise Vault-Server zu sichern, muss der Enterprise Vault Agent auf jedem Enterprise Vault-Server in Ihrer Umgebung installiert werden. Darüber hinaus muss der Enterprise Vault Agent auch auf jedem Remote-Computer installiert werden, auf dem Enterprise Vault-Komponenten installiert sind. Wenn die Compliance- und Discovery-Accelerators auf Remote-Computern installiert werden, muss der Enterprise Vault Agent ebenfalls auf diesen Computern installiert werden.

Sie haben bei der Installation des Enterprise Vault Agent folgende Möglichkeiten:

- Automatisch über den Backup Exec-Server als Teil einer Installation von Agent for Windows auf dem lokalen Enterprise Vault-Server. Nach der Installation müssen Sie Enterprise Vault Agent möglicherweise so konfigurieren, dass es sich auf dem Backup Exec-Server Ihrer Wahl veröffentlichen lässt. Siehe ["Info zum Veröffentlichen von Agent for Windows auf den Backup Exec-Servern"](#) auf Seite 1035.

- Installieren Sie die erforderlichen Enterprise Vault Agent-Lizenzen auf dem Backup Exec-Server.
Nachdem Sie die Lizenzen installiert haben, können Sie über eine Push-Installation Backup Exec Agent for Windows auf allen Enterprise Vault-Servern und den Computern installieren, auf denen andere Enterprise Vault-Komponenten installiert sind.

Siehe ["Installieren zusätzlicher Agents und Funktionen auf dem lokalen Backup Exec-Server"](#) auf Seite 66.

Siehe ["Installieren von Agent for Windows auf Remote-Computern über eine Push-Installation"](#) auf Seite 78.

Info zu Backup-Methoden für Enterprise Vault-Backup-Aufträge

Sie können eine Backup-Methode auswählen, die vom Enterprise Vault-Objekt abhängt, das Sie sichern möchten.

Die folgende Tabelle beschreibt den Typ von Enterprise Vault-Backup-Aufträgen, die Sie ausführen können. Die Tabelle beschreibt auch die Backup-Methoden, die für jeden Backup-Auftragstyp verfügbar sind.

Tabelle I-3 Für Enterprise Vault-Backup-Aufträge verfügbare Backup-Methoden

Zu sicherndes Element	Wählen Sie aus.	Beschreibung
Verzeichnis- und Überwachungsdatenbank Prüfungsdatenbank und FSA-Berichterstellungsdatenbank	Vollständige, Differenzial- oder inkrementelle Backup-Methode	Backups der Verzeichnis-, Überwachungs-, Überprüfungs- und FSA-Berichts-Datenbanken können mit der vollständigen und inkrementellen Backupmethode durchgeführt werden. Ein Backup dieser Datenbanken mit der Differenzial-Backup-Methode ist nicht möglich. Wenn Sie die Differential-Backup-Methode wählen, führt Backup Exec stattdessen ein vollständiges Backup durch. Hinweis: Bei Auswahl der inkrementellen Backup-Methode werden die Datenbank-Transaktionsprotokolle gesichert und aufgeteilt.
Speicherdatenbank und Abdruckdatenbank	Vollständige, Differenzial- oder inkrementelle Backup-Methode	Speicherdatenbank- und Abdruckdatenbank-Backups können mit jeder der drei Backup-Methoden durchgeführt werden: vollständig, differenzial und inkrementell. Hinweis: Bei Auswahl der inkrementellen Backup-Methode werden die Datenbank-Transaktionsprotokolle gesichert und aufgeteilt.
Speicherpartitionen und Indexorte	Backup-Methode "Vollständig", "Differenziell" oder "inkrementell"	Für Standard-Backup-Aufträge des Dateisystems können alle verfügbaren Backup-Methoden eingesetzt werden.

Wenn in einem Backup-Auftrag mehrere Enterprise Vault-Komponenten vorhanden sind, benötigt jede einzelne möglicherweise eine Methode, die von jener des ganzen Auftrags abweicht. Angenommen, Sie erstellen einen Auftrag, mit dem über ein Differenzial-Backup sowohl eine Verzeichnisdatenbank als auch eine Partition gesichert werden sollen. Weil jedoch eine Verzeichnisdatenbank nicht mit der Differenzial-Methode gesichert werden kann, verwendet Backup Exec die

vollständige Backup-Methode, um die Verzeichnisdatenbank zu sichern. Dies ermöglicht schnelle und einfache Wiederherstellungen. Nachdem die Verzeichnisdatenbank gesichert ist, verwendet Backup Exec die Differenzial-Backup-Methode, um die Partition zu sichern.

Die folgende Tabelle unterstützt Sie bei der Auswahl.

Tabelle I-4 Tatsächlich verwendete Backup-Methoden für Enterprise Vault-Komponenten

Enterprise Vault-Komponente	Vollständig (G)	Differenzial (D)	Inkrementell (Z)
Verzeichnis- und Überwachungsdatenbank	D	D	Z Kürzt Transaktionsprotokolle immer
Speicherdatenbank	D	D	Z Kürzt Transaktionsprotokolle immer
Prüfungsdatenbank	D	D	Z Kürzt Transaktionsprotokolle immer
FSA-Berichtsdatenbank	D	D	Z Kürzt Transaktionsprotokolle immer
Abdruckdatenbank	D	D	Z Kürzt Transaktionsprotokolle immer
Partition	D	D	Z
Indexstammpfad	D	D	Z

Enterprise Vault-Komponente	Vollständig (G)	Differenzial (D)	Inkrementell (Z)
Compliance Accelerator/Discovery Accelerator-Datenbank Hinweis: Schließt auch die Compliance Accelerator- und Discovery Accelerator-Datenbanken ein, die mit Laufzeitversionen von Enterprise Vault installiert werden.	D	D	Z Kürzt Transaktionsprotokolle immer
Compliance Accelerator/Discovery Accelerator-Kunden-Datenbank Hinweis: Schließt auch die Compliance Accelerator- und Discovery Accelerator-Datenbanken ein, die mit Laufzeitversionen von Enterprise Vault installiert werden.	D	D	Z Kürzt Transaktionsprotokolle immer
Discovery Accelerator Custodian-Datenbank Hinweis: Schließt auch die Discovery Accelerator Custodian-Datenbanken ein, die mit Laufzeitversionen von Enterprise Vault installiert werden.	D	D	Z Kürzt Transaktionsprotokolle immer

Siehe ["Backup-Methoden in Backup Exec"](#) auf Seite 205.

Siehe ["Info zum Sichern von Enterprise Vault-Komponenten"](#) auf Seite 1397.

Backup-Optionen für Enterprise Vault

Sie können eine Backup-Methode auswählen, die auf dem Typ von Enterprise Vault-Datenbank basiert, den Sie sichern möchten.

Siehe ["Info zu Backup-Methoden für Enterprise Vault-Backup-Aufträge"](#) auf Seite 1393.

Siehe ["Sichern von Daten"](#) auf Seite 174.

Siehe ["Info zum Sichern von Enterprise Vault-Komponenten"](#) auf Seite 1397.

Info zum Sichern von Enterprise Vault-Komponenten

Sie können beliebige oder alle Enterprise Vault-Komponenten für das Backup auswählen, wenn Sie einen Backup-Auftrag erstellen. Wenn Sie alle Komponenten für das Backup in ein und demselben Auftrag auswählen, erfolgt die Wiederherstellung schneller. Wenn Sie jedoch mehrere Backup-Aufträge für die Komponenten erstellen, werden die Backup-Aufträge schneller ausgeführt.

Die folgende Tabelle zeigt die Enterprise Vault-Komponenten, die Sie auswählen können, sowie jeweils mit Empfehlungen für das Backup:

Tabelle I-5 Enterprise Vault-Komponenten

Enterprise Vault-Komponente	Beschreibung
Verzeichnisdatenbank	<p>Die Verzeichnisdatenbank ist eine Microsoft SQL Server-Datenbank, die Konfigurationsdaten enthält.</p> <p>Nachdem Daten in die Datenbank eingegeben wurden, ändert sich die Datenmengen in der Verzeichnisdatenbank nur geringfügig.</p> <p>Sie sollten die Verzeichnisdatenbank sichern, nachdem Sie Enterprise Vault-Komponenten hinzugefügt oder entfernt haben. Sie sollten die Verzeichnisdatenbank auch sichern, wenn Sie den Speicherort einer Komponente ändern. Konfigurationsänderungen können das Erstellen von Speichern und Speicherpartitionen und das Ändern von Speicherpartitionsstatus betreffen.</p>

Enterprise Vault-Komponente	Beschreibung
Überwachungsdatenbank	<p>Enterprise Vault schließt einen Überwachungsagent auf jedem Enterprise Vault-Server ein. Der Überwachungsagent überwacht Folgendes:</p> <ul style="list-style-type: none"> ■ Status von Enterprise Vault-Diensten und von Aufgaben. ■ Leistungszähler für Speicher, Speicherplatz, Arbeitsspeicher und Prozessoren. ■ Status der Archivierungsziele für protokollierte Exchange Server-Mailbox-Ziele, darunter Zählungen der Objekte im Posteingang, für ausstehende Archivierung und für fehlgeschlagene Vorgänge, z. B. DL Expansion-Fehler. <p>Der Überwachungsagent sammelt Überwachungsdaten in geplanten Abständen, gewöhnlich alle paar Minuten.</p> <p>Alle Informationen, die der Überwachungsagent sammelt, werden in einer Microsoft SQL Server-Datenbank gespeichert, die als Überwachungsdatenbank bezeichnet wird.</p>
Fingerabdruckdatenbank	<p>Die Fingerabdruckdatenbanken enthalten die zur Einzelinstanzspeicherung gehörigen Informationen für alle Speicher in der Speichergruppe.</p> <p>Wenn Sie die Einzelinstanzspeicherung der archivierten Elemente aktivieren, sollten Sie die Fingerabdruckdatenbanken regelmäßig sichern.</p>

Enterprise Vault-Komponente	Beschreibung
Indextpeicherort	<p>Der Indexspeicherort speichert den gesamten archivierten Dateninhalt, der indiziert wird, um ein schnelles Suchen und Abrufen von archivierten Elementen zu ermöglichen. Die Indexdaten werden in Indexdateien an dem Speicherort gespeichert, der bei der Installation von Enterprise Vault angegeben wird.</p> <p>Sie sollten den Indexspeicherort regelmäßig sichern.</p>
Speicherdatenbankgruppe	<p>Die Speichergruppe ist eine logische Entität. Wenn Sie sie für ein Backup auswählen, werden alle Speicherdatenbanken, Speicherpartitionen und Fingerabdruckdatenbanken gesichert. Weil diese Komponenten sehr ähnlich sind, sollten Sie die Speichergruppe auswählen, um alle Komponenten zusammen zu sichern.</p>
Speicher	<p>Die Speicherdatenbank ist eine logische Entität. Wenn Sie sie für ein Backup auswählen, werden alle Speicherdatenbanken und Speicherpartitionen gesichert.</p>
Alle Partitionen	<p>Eine Speicherdatenbank-Partition stellt den physischen Speicherort dar, an dem die archivierten Elemente gespeichert werden. Eine Speicherdatenbank kann eine oder mehrere Speicherpartitionen enthalten. Wenn Sie "Alle Partitionen" für das Backup auswählen, dann werden alle Speicherpartitionen im Speicher für das Backup ausgewählt.</p> <p>Hinweis: Wenn Sie eine geöffnete Partition sichern, sichert Backup Exec automatisch die Speicherdatenbank.</p>
Site	<p>Eine Enterprise Vault-Site ist eine logische Darstellung einer Installation von Enterprise Vault. Wenn Sie diese Komponente für das Backup auswählen, wird die Verzeichnisdatenbank auch automatisch gesichert.</p>

Enterprise Vault-Komponente	Beschreibung
Compliance Accelerator-Datenbank und Discovery Accelerator-Datenbank	Diese Datenbanken werden als optionale Zusätze für Enterprise Vault installiert und sind ein Teil der Discovery Accelerator- und Compliance Accelerator-Produkte.

Siehe ["Sichern von Daten"](#) auf Seite 174.

Siehe ["Bearbeiten von Backup-Definitionen"](#) auf Seite 226.

Siehe ["Hinzufügen einer Stufe zu einer Backup-Definition"](#) auf Seite 244.

Konsistenzprüfungen für Enterprise Vault-Datenbanken und Compliance and Discovery Accelerator-Datenbanken

Backup Exec führt automatisch vor einem Backup-Auftrag und nach einem Wiederherstellungsauftrag eine physische Konsistenzprüfung der jeweiligen Enterprise Vault-Datenbank durch. Außerdem wird die Konsistenz der Compliance and Discovery-Datenbanken vor einem Backup-Auftrag und nach einem Wiederherstellungsauftrag geprüft. Backup Exec verwendet das Dienstprogramm "Nur physische Überprüfung" von Microsoft SQL Server für die Konsistenzprüfungen für die Datenbanken. Schlägt eine Konsistenzprüfung fehl, setzt Backup Exec den Auftrag fort und zeichnet die fehlgeschlagenen Konsistenzprüfungen im Backup Exec-Auftragsprotokoll auf.

Weitere Informationen über das Dienstprogramm "Nur physische Überprüfung" finden Sie in der Dokumentation zu Microsoft SQL Server-Dokumentation.

Wiederherstellen von Enterprise Vault

Beachten Sie folgende Hinweise, bevor Sie mit einer Enterprise Vault-Wiederherstellung beginnen.

- Beim Wiederherstellen einer Enterprise Vault-Installation sollte die Wiederherstellung der Verzeichnisdatenbank in einem separaten Auftrag erfolgen. Erst nach der Wiederherstellung der Verzeichnisdatenbank sollten Sie die Enterprise Vault-Komponenten und -Partitionen wiederherstellen.
- Wenn Sie Enterprise Vault-Datenbanken wiederherstellen, können Sie die Optionen auswählen, die Datenbanken entweder in einem betriebsbereiten oder einem nicht betriebsbereiten Zustand versetzen. Die Optionen für den nicht betriebsbereiten Zustand, die Sie auswählen, werden auf alle Enterprise

Vault-Datenbanken außer der Speicherdatenbank angewendet. Wenn Sie eine Enterprise Vault-Speicherdatenbank wiederherstellen, versetzt Enterprise Vault Agent die Speicherdatenbank in den Enterprise Vault-Backup-Modus. Falls die Speicherdatenbank nach Abschluss der Wiederherstellung in einem nicht betriebsfähigen Zustand verbleibt, kann Enterprise Vault Agent sie nicht vom Backup-Modus entfernen.

- Wenn Sie die Option auswählen, die die Datenbanken einsatzfähig hält, stellt Enterprise Vault Agent die Vault Store-Datenbank in einem einsatzfähigen Zustand wieder her. Der Betriebsstatus der Speicherdatenbank wird aufrechterhalten, selbst wenn Sie zusätzliche Backup-Sätze für die Wiederherstellung im selben Wiederherstellungsauftrag auswählen. Zusätzliche Backup-Sätze können die Backup-Methoden "Vollständig", "Differenzial" und "Inkrementell" umfassen.
- Wenn Sie die Option auswählen, die die Datenbanken nicht betriebsbereit hält, fordert Enterprise Vault Agent Sie auf, den Enterprise Vault-Speicherdienst zu beenden, bevor Sie die Vault Store-Datenbank-Wiederherstellung starten. Sie können die Wiederherstellung der Speicherdatenbank erneut starten, nachdem der Enterprise Vault-Speicherdienst beendet wurde.

Als optimales Verfahren wird empfohlen, dass Sie die Speicherdatenbank im betriebsbereiten Zustand wiederherstellen. Wenn Sie die Speicherdatenbank in einem nicht betriebsbereiten Zustand wiederherstellen, kann Enterprise Vault sie nicht vom Backup-Modus entfernen, nachdem der Wiederherstellungsvorgang abgeschlossen ist.

Siehe ["Enterprise Vault-Wiederherstellungsoptionen"](#) auf Seite 1402.

- Sie können Enterprise Vault-Komponenten einzeln wiederherstellen. Bevor Sie mit der Wiederherstellung beginnen, können die Datenbanken und andere Komponenten auf dem Enterprise Vault-Zielservers vorhanden sein oder nicht. Falls die Datenbanken nicht vorhanden sind, können Sie sie mithilfe von Enterprise Vault Agent wiederherstellen. Nachdem der Wiederherstellungsauftrag abgeschlossen ist, müssen Sie Enterprise Vault konfigurieren, damit es die wiederhergestellten Datenbanken verwendet.

Um Enterprise Vault zu konfigurieren, damit es die wiederhergestellten Datenbanken verwendet, konsultieren Sie Ihre Enterprise Vault-Dokumentation.

Folgende Elemente sind verfügbar:

- Enterprise Vault 8.x-/9.x-/10.x-Verzeichnis-, Überwachungs-, Überprüfungs-, FSA-Bericht- und Fingerabdruckdatenbanken.
- Speicherdatenbanken, Indizes und Partitionen.
- Compliance- und Discovery Accelerator-Konfiguration und Kundendatenbanken.

- Discovery Accelerator Custodian-Datenbank
- Es wird die Verwendung eines Enterprise Vault-Dienstkontos oder eines Kontos mit Zugriffsberechtigung auf die Wiederherstellungsauswahl als Standard-Login-Konto empfohlen. Andernfalls müssen Sie möglicherweise für jede zu sichernde Enterprise Vault-Ressource die entsprechenden Anmeldedaten eingeben.
- Nachdem Sie Enterprise Vault wiederhergestellt haben, erscheint eine Meldung, die Sie informiert, dass Sie Enterprise Vault-Wiederherstellungstools ausführen müssen. Diese gewährleisten die Neusynchronisierung von Enterprise Vault mit den eben wiederhergestellten Datenbanken.
Für Informationen über das Ausführen der Enterprise Vault-Wiederherstellungstools konsultieren Sie Ihre Enterprise Vault-Dokumentation.

Vor der Wiederherstellung von Enterprise Vault-Standorten, -Servern oder anderen Komponenten sollten folgende Elemente auf dem Zielcomputer installiert sein:

- Enterprise Vault
- Backup Exec Agent for Windows

Hinweis: Sie müssen den Agent for Windows auf den Enterprise Vault-Remote-Computern installieren, auf denen die Enterprise Vault-Komponenten wiederhergestellt werden sollen.

Siehe "[Methoden für das Wiederherstellen von Daten in Backup Exec](#)" auf Seite 258.

Enterprise Vault-Wiederherstellungsoptionen

Wählen Sie in der folgenden Tabelle die Wiederherstellungsoption, die Sie verwenden möchten, wenn Sie die Enterprise Vault-Datenbanken wiederherstellen.

Tabelle I-6 Enterprise Vault-Wiederherstellungsoptionen

Element	Beschreibung
Enterprise Vault-Datenbanken beim Wiederherstellen ausgewählter Datenbanken automatisch offline schalten	

Element	Beschreibung
	<p>Schaltet die gemeinsam genutzten Enterprise Vault-Verzeichnis-, Überwachungs-, Überprüfungs-, FSA-Bericht- und Fingerabdruckdatenbanken offline, damit Backup Exec sie während eines Wiederherstellungsauftrags ersetzen kann.</p> <p>Hinweis: Wenn Sie diese Option nicht verwenden, müssen Sie das Verzeichnis und die Admin-Dienste auf allen Enterprise Vault-Servern beenden, bevor Sie die vorher erwähnten Datenbanken wiederherstellen. Darüber hinaus müssen Sie auch den Accelerator Manager-Server auf allen Compliance Accelerator-Servern und den Discovery-Servern beenden. Erst nachdem Sie den Accelerator Manager beendet haben, können Sie die Kunden-, Konfigurations- und Custodian-Datenbanken wiederherstellen.</p> <p>Außerdem werden die Verbindungen mit folgenden Elementen beendet:</p> <ul style="list-style-type: none">■ Überwachungsdatenbank■ Überprüfungs-, Fingerabdruck- und FSA-Berichtdatenbanken (nur Enterprise Vault 8.x, 9.x, 10.x)■ Konfigurations-, Kunden- und Custodian-Datenbanken <p>Nach Beendigung der Wiederherstellung müssen Sie die Enterprise Vault-Verzeichnis- und Administratordienste auf Ihrem Enterprise Vault-Server manuell neu starten. Die Dienste stellen eine neue Verbindung mit den wiederhergestellten Datenbanken her und die Archivierung in Enterprise Vault wird wieder aufgenommen.</p> <p>Hinweis: Diese Option hat zur Folge, dass die Verbindungen zur von Ihnen wiederhergestellten Verzeichnisdatenbank in den Enterprise Vault-Administrator- und -Verzeichnisdiensten auf allen Enterprise Vault-Servern beendet werden. Sie beendet auch die Verbindungen zur Enterprise Vault Accelerator Manager-Datenbank.</p>

Element	Beschreibung
Enterprise Vault-Datenbanken nicht offline schalten	<p>Lässt alle Enterprise Vault-Datenbanken online.</p> <p>Wenn Sie diese Option verwenden, müssen Sie das Verzeichnis und die Admin-Dienste auf allen Enterprise Vault-Servern beenden, bevor Sie die vorher erwähnten Datenbanken wiederherstellen. Darüber hinaus müssen Sie auch den Accelerator Manager-Server auf allen Compliance Accelerator-Servern und den Discovery-Servern beenden. Erst nachdem Sie den Accelerator Manager beendet haben, können Sie die Kunden-, Konfigurations- und Custodian-Datenbanken wiederherstellen.</p>
Datenbank betriebsbereit halten. Wiederher. zusätz. Transaktionsprot. oder Diff.-Backups nicht möglich.	<p>Setzt alle unvollständigen Transaktionen zurück, wenn Sie die letzte Datenbank, das Differenzial- oder das Protokoll-Backup wiederherstellen. Nach der Wiederherstellung ist die Datenbank betriebsbereit. Wenn Sie diese Option nicht auswählen, verbleibt die Datenbank in einem Zwischenstadium und kann nicht verwendet werden.</p> <p>Wenn Sie diese Option auswählen, können Sie nicht mit dem Wiederherstellen von Backups fortfahren. Sie müssen den Wiederherstellungsvorgang von vorn beginnen.</p>
Datenbank außer Betrieb halten. Wiederher. zusätz. Transaktionsprot. oder Diff.-Backups möglich.	<p>Erstellt und verwaltet eine Datenbank im Standby-Modus.</p> <p>Indem Sie diese Option verwenden, können Sie mit der Wiederherstellung anderer Backup-Sätze für nicht-betriebsbereite Datenbanken fortfahren.</p> <p>Weitere Informationen zu Standby-Datenbanken finden Sie in der SQL-Dokumentation.</p>

Hinweis: Es wird empfohlen, dass Sie alle erforderlichen Backup-Sätze wählen, wenn Sie einen einzelnen Wiederherstellungsauftrag für eine Vault Store-Datenbank ausführen. Zu allen erforderlichen Backup-Sätzen können vollständige, Differenzial- und inkrementelle Backup-Sätze gehören. Die Speicherdatenbank sollte nach Abschluss des Wiederherstellungsauftrags auch in einem betriebsbereiten Zustand wiederhergestellt werden.

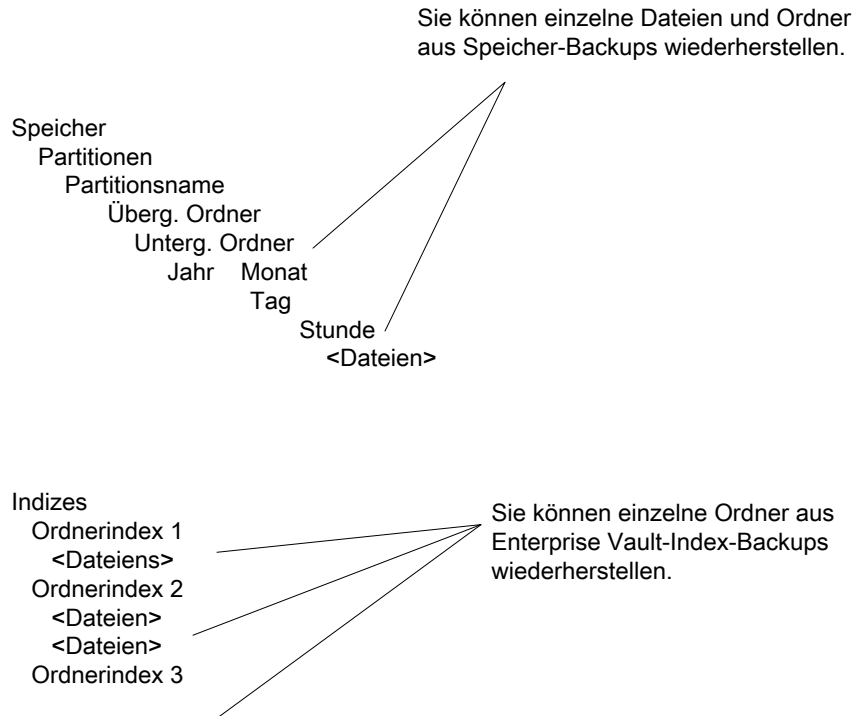
Siehe ["Methoden für das Wiederherstellen von Daten in Backup Exec"](#) auf Seite 258.

Info zum Wiederherstellen einzelner Dateien und Ordner mit Enterprise Vault Agent

Agent for Enterprise Vault (Enterprise Vault Agent) unterstützt das Wiederherstellen einzelner Dateien und Ordner aus den Backups von Speicherpartitionen. Sie können auch komplette Indexspeicherorte oder einzelne Ordner aus Enterprise Vault-Index-Backups wiederherstellen.

Siehe ["Methoden für das Wiederherstellen von Daten in Backup Exec"](#) auf Seite 258.

Abbildung I-1 Wiederherstellen einzelner Dateien aus Vault-Speicherpartitionen und vollständiger Ordner aus einem Enterprise Vault-Index



Info zur automatischen Umleitung von Enterprise Vault-Komponenten unter einem Enterprise Vault-Server

Sie können den Speicherort der Speicherdatenbanken, Fingerabdruckdatenbanken oder Partitionen in einen anderen als den Backup-Speicherort ändern. Während der Wiederherstellung der Speicherdatenbank, Fingerabdruckdatenbanken oder Partitionen erkennt Agent for Enterprise Vault (Enterprise Vault Agent) die Änderung des Speicherorts. Die Komponentenwiederherstellungen werden dann automatisch an den neuen Speicherort umgeleitet.

Hinweis: Automatisch umgeleitete Wiederherstellungen der Speicherdatenbanken, Partitionen oder Fingerabdruckdatenbanken treten auf, wenn Sie nur den Speicherort dieser Enterprise Vault-Komponenten ändern. Die Namen der Partitionen, der Speicher und der Speichergruppen dürfen nicht ab dem Zeitpunkt geändert werden, zu der die Partition ursprünglich gesichert wurde.

Siehe "[Wiederherstellen von Enterprise Vault](#)" auf Seite 1400.

Umleiten einer Wiederherstellung für eine Enterprise Vault-Komponente

Sie können die Wiederherstellung der Enterprise Vault-Komponenten umleiten.

Die folgende Tabelle beschreibt die Anforderungen für das Umleiten einer Wiederherstellung für eine Enterprise Vault-Komponente:

Tabelle I-7 Anforderungen für das Umleiten einer Wiederherstellung für eine Enterprise Vault-Komponente

Komponente	Anforderung
Alle Enterprise Vault-Komponenten	<p>Im Folgenden sehen Sie die Anforderungen für das Umleiten der Wiederherstellung von allen Enterprise Vault-Komponenten:</p> <ul style="list-style-type: none">■ Alle Enterprise Vault-Komponenten müssen bereits auf dem Server bereits vorhanden sein, an die Sie die Wiederherstellung umleiten. Wenn sie nicht existieren, müssen sie erstellt werden. <p>Weitere Informationen hierzu erhalten Sie in Ihrer Dokumentation zu Enterprise Vault.</p> <ul style="list-style-type: none">■ Das Backup Exec-Einlogkonto, das Sie verwenden, muss die gleichen Anmeldedaten wie das Speicherdienstkonto haben.
Enterprise Vault-Datenbanken	<p>Im Folgenden sehen Sie Anforderungen für das Umleiten der Wiederherstellung der Datenbanken:</p> <ul style="list-style-type: none">■ Sie müssen einen separaten Auftrag für jede Datenbank erstellen, die Sie umleiten möchten.■ Sie müssen alle Datenbanken zum gleichen SQL-Server umleiten.

Komponente	Anforderung
Speicherdatenbanken	<p>Im Folgenden sehen Sie zusätzliche Anforderungen für das Umleiten der Wiederherstellung einer Speicherdatenbank:</p> <ul style="list-style-type: none">■ Stellen Sie sicher, dass die Verzeichnisdatenbank bereits auf dem Server vorhanden ist, an die Sie die Wiederherstellung umleiten.■ Stellen Sie sicher, dass die Verzeichnisdatenbank einen Eintrag für den Speicher enthält, der den neuen SQL-Server-Namen verwendet.
Speicherpartition	<p>Im Folgenden sehen Sie zusätzliche Anforderungen für das Umleiten der Wiederherstellung einer Speicherpartition:</p> <ul style="list-style-type: none">■ Der Speicher muss bereits eine Speicherpartition mit demselben Namen enthalten. Wenn keine Speicherpartition vorhanden ist, müssen Sie sie erstellen.
Indexspeicherort	<p>Die Verzeichnisdatenbank muss bereits mit dem neuen Indexspeicherort konfiguriert werden.</p> <p>Weitere Informationen hierzu erhalten Sie in Ihrer Dokumentation zu Enterprise Vault.</p>

Umleitungsoptionen für Enterprise Vault

Sie können einen Wiederherstellungsauftrag für Enterprise Vault-Komponenten umleiten.

Siehe ["Umleiten einer Wiederherstellung für eine Enterprise Vault-Komponente"](#) auf Seite 1408.

Tabelle I-8 Umleitungsoptionen für Enterprise Vault

Element	Beschreibung
Auf einen neuen Microsoft SQL Server	<p>Leitet die Wiederherstellungsaufträge von Enterprise Vault-Datenbanken und Accelerator-Datenbanken auf einen anderen SQL Server um.</p> <p>Zeigt den Namen des Servers an, auf den Sie den Wiederherstellungsauftrag für einen Speicher umleiten möchten.</p> <p>Hinweis: Speicherdatenbanken werden nur für Enterprise Vault 8.x, 9.x und 10.x wiederhergestellt.</p>
Instanz	<p>Zeigt den Namen der SQL-Serverinstanz an, zu der Sie den Wiederherstellungsauftrag für einen Speicher umleiten möchten.</p>
Indexstamm auf einem neuen Speicherort wiederherstellen	<p>Leitet den Wiederherstellungsauftrag für den Indexstamm zu einem neuen Speicherort um.</p> <p>Wenn Sie die Wiederherstellung des Enterprise Vault-Servers umleiten, können Sie einen alternativen Pfad auf dem Zielsystem angeben. Außerdem können Sie den Indexstammspeicherort an einen alternativen Pfad auf dem ursprünglichen Server umleiten.</p>
Pfad	<p>Zeigt den Pfadnamen an, zu dem Sie den Wiederherstellungsauftrag für einen Indexstamm umleiten möchten.</p>
Partitionsstamm an neuem Speicherort wiederherstellen	<p>Leitet den Wiederherstellungsauftrag für eine Speicherpartition an einen neuen Speicherort um.</p> <p>Partitionen werden nur für Enterprise Vault 8.x, 9.x und 10.x wiederhergestellt.</p>
Pfad	<p>Zeigt den Pfadnamen an, zu dem Sie den Wiederherstellungsauftrag für eine Speicherpartition umleiten möchten.</p>
Enterprise Vault-Login-Konto	<p>Gibt das Login-Konto an, das verwendet werden soll.</p>

Konfigurieren von Enterprise Vault für die Verwendung des Namens des neuen SQL-Servers mit der Verzeichnisdatenbank

Gehen Sie wie folgt vor, um Enterprise Vault so zu konfigurieren, dass der Name des neuen SQL-Servers mit der Verzeichnisdatenbank verwendet wird.

So konfigurieren Sie Enterprise Vault für die Verwendung des Namens des neuen SQL-Servers mit der Verzeichnisdatenbank

- 1 Ändern Sie dazu auf jedem Enterprise Vault-Server mithilfe von Enterprise Vault den Namen des vorherigen SQL Server-Computers. Ändern Sie den Namen zu dem Namen des SQL-Server-Computers, auf dem die Verzeichnisdatenbank jetzt gespeichert ist.

Weitere Informationen hierzu erhalten Sie in Ihrer Dokumentation zu Enterprise Vault.

- 2 Starten Sie den Enterprise Vault-Administratordienst auf allen Enterprise Vault-Servern, die die Verzeichnisdatenbank verwenden.

Nach dem Neustart des Enterprise Vault-Administratordiensts auf dem Enterprise Vault-Server werden zwei Verzeichnisnamen angezeigt.

Beispiel: "Verzeichnis auf <OldSQL_Computername >" und "Verzeichnis auf <NewSQL_Computername >".

- 3 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" mit der rechten Maustaste auf den zu sichernden Server.
- 4 Wählen Sie im Menü "Backup" die Backup-Definition, die Sie verwenden möchten.
- 5 Klicken Sie im Dialogfeld "Auswahl" auf "Bearbeiten".
- 6 Erweitern Sie "Verzeichnis auf <SQL Server-Computer, auf den Sie die Verzeichnisdatenbank verschoben haben>".

- 7 Erweitern Sie alle Elemente unter "Verzeichnis auf <SQL Server-Computer, auf den Sie die Verzeichnisdatenbank verschoben haben >".

Die Verzeichnis - und Überwachungs -Datenbanken, Enterprise Vault 8.x-, 9.x-, oder 10.x- FSA-Berichts - und Prüfungs -Datenbanken und die Enterprise Vault-Sites sollten angezeigt werden. Darüber hinaus sollte die Verzeichnisdatenbank den neuen Namen und die neue Instanz des SQL-Servers enthalten, auf den sie umgeleitet wurde.

Beim Konfigurieren eines neuen Auftrags für das Verzeichnisdatenbank-Backup müssen Sie die Verzeichnisdatenbank im aktuellen Verzeichnisserver auswählen. 13 Tage nach dem Verschieben der Verzeichnisdatenbank entfernt Backup Exec den vorherigen Verzeichnisservernamen automatisch.

- 8 Um den vorherigen Servernamen manuell zu entfernen, klicken Sie mit der rechten Maustaste auf "Verzeichnis auf <OldSQL_computer_name >".
- 9 Klicken Sie auf "Entfernen".

Weitere Informationen hierzu erhalten Sie in Ihrer Dokumentation zu Enterprise Vault.

Best Practices für den Enterprise Vault Agent

Bei Verwendung von Agent for Enterprise Vault (Enterprise Vault Agent) werden die folgenden Best Practices empfohlen.

- Sichern Sie die Enterprise Vault-Verzeichnisdatenbank, nachdem Sie Konfigurationsänderungen in Enterprise Vault vorgenommen haben.
- Stellen Sie die Enterprise Vault-Verzeichnisdatenbank in einem separaten Backup Exec-Wiederherstellungsauftrag wieder her.
- Stellen Sie alle vollständigen, differenzialen und inkrementellen Backup-Sätze der Speicherdatenbank in ein und demselben Wiederherstellungsauftrag wieder her.
- Achten Sie darauf, dass die Zeitrahmen für das Backup und für die Archivierung nicht überlappen.
- Achten Sie darauf, dass die Zeitrahmen für das Backup und für die Migration nicht überlappen.
- Stellen Sie sicher, dass die Komponenten von Enterprise Vault sich nicht im Backup-Modus befinden, bevor Sie die Enterprise Vault-Verzeichnisdatenbank sichern.

- Wenn Sie sowohl Backup Exec NDMP Feature als auch Enterprise Vault Agent installieren, wählen Sie nur ein Produkt aus, um eine Enterprise Vault-Partition zu schützen, die sich auf NDMP-Dateien befindet.
- Ändern Sie nicht das Wiederherstellungsmodell der von Enterprise Vault erstellten Datenbanken. Bei der Erstellung der einzelnen Datenbanken konfiguriert Enterprise Vault diese im Modus für die vollständige Wiederherstellung.

Informationen zu den Best Practices zum Einsatz des Backup Exec Agent for Enterprise Vault und Backup Exec Migrator finden Sie unter *Best Practices für Backup Exec*.

Siehe ["Info zu Agent for Enterprise Vault"](#) auf Seite 1387.

Info zu Backup Exec Migrator for Enterprise Vault

Backup Exec Migrator für Enterprise Vault (Backup Exec Migrator) ermöglicht Ihnen die automatische Migration archivierter Enterprise Vault-Daten auf die von Backup Exec verwalteten Speichergeräte. Durch Migration der archivierten Enterprise Vault-Daten von einer Partition können Sie Speicherplatz auf dem Enterprise Vault-Server zurückgewinnen, ohne dass Kosten für zusätzliche Hardware entstehen.

Indem Sie Enterprise Vault-Archivdaten auf die Speichergeräte des Backup Exec-Servers migrieren, sorgen Sie außerdem für eine höhere Speicherredundanz durch Verwendung einer Off-Host-Umgebung.

Siehe ["Funktionsweise des Backup Exec Migrator"](#) auf Seite 1414.

Siehe ["Konfigurieren von Backup Exec Migrator"](#) auf Seite 1423.

Anforderungen für Backup Exec Migrator for Enterprise Vault

Bevor Sie Backup Exec Migrator konfigurieren, stellen Sie sicher, dass Ihr Enterprise Vault-Server die folgenden Anforderungen erfüllt:

- Backup Exec Agent für Enterprise Vault muss auf dem Enterprise Vault-Server installiert sein.
- Enterprise Vault-Migration und -Sammlungen müssen für die Enterprise Vault-Partition aktiviert sein, von der Sie Daten migrieren möchten.
- Enterprise Vault 8.0 SP3 oder höher muss auf dem Enterprise Vault-Server installiert sein.

Funktionsweise des Backup Exec Migrator

Enterprise Vault initiiert automatisch alle Datenmigrationsvorgänge vom Enterprise Vault-Server aus, nachdem Sie Backup Exec Migrator konfiguriert haben. Enterprise Vault trifft Entscheidungen darüber, was migriert werden soll, basierend auf den Archivierungsrichtlinien und den Datenaufbewahrungsrichtlinien, die Sie in der Enterprise Vault-Administratorkonsole konfigurieren. Der Backup Exec Migrator migriert dann die archivierten Daten auf einen Backup Exec-Server, nachdem Enterprise Vault die geeigneten Daten aus den Speicherpartitionen gesammelt hat. Wenn Sie Migrationsoptionen für eine Partition konfigurieren, können Sie den Migrationszeitraum festlegen. Alle Migrationsoptionen werden auf dem Enterprise Vault Server konfiguriert.

Tabelle I-9 Enterprise Vault-Datenmigration

Aktion	Hinweise
Enterprise Vault archiviert geeignete Partitionsdaten basierend auf der Dateigröße oder dem Dateierstellungsdatum.	<p>Alle Daten, die für das Archiv geeignet sind, werden in der Partition festgelegt, in die Sie Daten migrieren möchten.</p> <p>Weitere Informationen hierzu erhalten Sie in Ihrer Dokumentation zu Enterprise Vault.</p>
Nachdem Enterprise Vault den Archivierungsvorgang abgeschlossen hat, sammelt ein Enterprise Vault-Sammelvorgang die archivierten Daten.	<p>Beim Sammelvorgang werden die archivierten Daten in Windows-CAB-Dateien abgelegt. Die CAB-Dateien werden in der Partition gespeichert, in der die Migration vorgenommen wird.</p> <p>Geeignete Daten können Enterprise Vault-Dateien mit den folgenden Erweiterungen umfassen:</p> <ul style="list-style-type: none">■ .dvf■ .dvssp■ .dvsc■ .dvs <p>Hinweis: Einige der geeigneten Daten können wegen Einschränkungen der Dateigröße nicht in CAB-Dateien komprimiert werden. Der Backup Exec Migrator migriert die Daten jedoch während des Migrationsvorgangs.</p> <p>Weitere Informationen hierzu erhalten Sie in Ihrer Dokumentation zu Enterprise Vault.</p>

Aktion	Hinweise
Der Backup Exec Migrator initiiert die Migration der archivierten Datendateien in einen Backup Exec-Server.	

Aktion	Hinweise
	<p>Migrationszeitpläne werden festgelegt, wenn Sie die Migration für eine Partition konfigurieren und wenn Sie einen Sammlungszeitplan für die Partition konfigurieren.</p> <p>Siehe "Konfigurieren von Enterprise Vault-Sammlungen" auf Seite 1424.</p> <p>Siehe "Konfigurieren des Backup Exec Migrator zur Kommunikation mit Enterprise Vault" auf Seite 1428.</p> <p>Gemäß den Konfigurationsempfehlungen für die Backup Exec Migrator- und Enterprise Vault-Partitionen soll ein Migrationsauftrag pro Partition während eines Migrationszeitraums laufen. Der Backup Exec Migrator kann jedoch auch separate Migrationsaufträge für jeden Partitionsordner erstellen, wenn Sie den Konfigurationsempfehlungen nicht folgen. Wenn separate Aufträge erstellt werden, führt der sich daraus ergebende Mehraufwand, der zur Durchführung der Aufträge erforderlich ist, zu einer herabgesetzten Migrations- und Abrufleistung.</p> <p>Hinweis: Wenn Sie eine Anforderung zum Dateiabruf vom Enterprise Vault-Server aus zwischen Migrationszeiträumen einplanen, werden separate Aufträge erstellt, obwohl Sie den Konfigurationsempfehlungen folgen. In diesem Fall erstellt der Backup Exec Migrator automatisch separate Aufträge, um den Abruf der angeforderten Datei zu ermöglichen. Während eines Migrationsvorgangs kann der Wiederherstellungsauftrag eingeplant werden, um zwischen Migrationsaufträgen durchgeführt zu werden.</p> <p>Wenn Sie den Konfigurationsempfehlungen nicht folgen, kann dies sich negativ auf die Leistung beim Dateiabruf auswirken.</p> <p>Um die möglichst effizienteste Migrations- und Abrufleistung sicherzustellen, folgen Sie</p>

Aktion	Hinweise
	den Empfehlungen, wenn Sie den Backup Exec Migrator und die Enterprise Vault-Partitionen konfigurieren. Siehe "Konfigurieren von Backup Exec Migrator" auf Seite 1423.
Backup Exec schließt den Migrationsvorgang ab, indem alle migrierten Dateien auf Speichergeräte verschoben werden.	Es wird das Konfigurieren von zwei Speichergeräten für gestaffelte Migrationsvorgänge empfohlen. Siehe "Info zur Verwendung gestaffelter Migrationen mit Backup Exec und dem Backup Exec Migrator" auf Seite 1417. Siehe "Konfigurieren von Backup Exec Migrator" auf Seite 1423.

Nachdem Backup Exec die CAB-Dateien auf die Speichergeräte migriert hat, können Sie Migrationsdetails in den Auftragsverlaufdetails für jeden Enterprise Vault-Server anzeigen, auf dem die Migration ausgeführt wird.

Siehe ["Informationen zum Auftragsverlauf"](#) auf Seite 302.

Info zur Verwendung gestaffelter Migrationen mit Backup Exec und dem Backup Exec Migrator

Wenn Sie Backup Exec konfigurieren, um den Backup Exec Migrator einzusetzen, empfiehlt es sich, dass Sie zwei Speichergeräte für gestaffelte Migrationsvorgänge konfigurieren. Erwägen Sie beim Auswählen der zu nutzenden Geräte einen leistungsstarken plattenbasierten Speicher und ein Bandgerät mit niedrigerer Leistung. Indem Sie zwei Geräte verwenden, können archivierte Daten in zwei Stufen migriert werden.

Während der ersten Phase migriert Backup Exec die Daten, die es von Backup Exec Migrator erhält, in einen Backup-to-Disk-Ordner auf einer leistungsstarken Festplatte. Durch die Verwendung eines Backup-to-Disk-Ordners können Sie die für die erste Migration benötigte Zeitdauer minimieren. Während der zweiten Migrationsphase erstellt Backup Exec einen Duplizierungsauftrag, um die archivierten Daten aus dem Backup-to-Disk-Ordner auf ein Bandgerät zu migrieren. Sie können den duplizierten Auftrag entsprechend einplanen, um die archivierten Daten dann auf ein Bandgerät zu verschieben, wenn die Aktivität des Backup Exec-Servers gering ist.

Siehe ["Konfigurieren des Backup Exec Migrator zur Verwendung eines Backup Exec-Servers"](#) auf Seite 1425.

Siehe ["Konfigurieren des Backup Exec Migrator zur Kommunikation mit Enterprise Vault"](#) auf Seite 1428.

Info zu Backup Exec Migrator-Ereignissen

Backup Exec Migrator generiert Ereignisse, die den Status der von ihm ausgeführten Aufgaben angeben. Die Ereignisse liefern auch nützliche Informationen für die Fehlerbehebung. Sie können die Ereignisse auf dem Computer anzeigen, auf dem Sie den Enterprise Vault-Speicherdienst installiert haben. Verwenden Sie dazu die Windows-Ereignisanzeige. In der Ereignisanzeige können Sie die Ereignisse unter "Enterprise Vault" sehen. Sie können die Ereignisse auch im Dienstprogramm Enterprise Vault Dtrace anzeigen.

Weitere Informationen zum Dienstprogramm Enterprise Vault Dtrace finden Sie in der Dokumentation zu Enterprise Vault.

Siehe ["Info zu Backup Exec Migrator-Protokollen"](#) auf Seite 1418.

Info zu Backup Exec Migrator-Protokollen

Backup Exec Migrator kann Protokolldateien erstellen, die die gesamte Migrationsaktivität protokollieren. Die Protokolldateien befinden sich auf dem Enterprise Vault-Server und auf dem Backup Exec-Server. Backup Exec Migrator-Protokolldateien können Ihnen bei der Behebung von Problemen im Zusammenhang mit der Migration helfen.

Bevor Sie die Protokolldateien anzeigen können, müssen Sie die Backup Exec Migrator-Protokollierung auf dem Enterprise Vault-Server und auf dem Backup Exec-Server aktivieren. Um die Backup Exec Migrator-Protokolle auf dem Enterprise Vault-Server zu aktivieren, bearbeiten die Windows-Registrierung.

Siehe ["So aktivieren Sie die Backup Exec Migrator-Protokollierung"](#) auf Seite 1420.

Sie müssen außerdem die Backup Exec Migrator-Protokollierung auf dem Backup Exec-Server aktivieren.

Siehe ["Verwenden von Backup Exec Debug Monitor zur Fehlerbehebung"](#) auf Seite 910.

Hinweis: Die Protokolldateien des Dienstprogramms zum Wiederherstellen von Partitionen sind standardmäßig aktiviert.

Nachdem Sie die Protokollierung auf dem Enterprise Vault-Server und auf dem Backup Exec-Server aktiviert haben, werden die folgenden Typen von Protokolldateien erstellt:

- VxBSA-Protokolldateien
Beispiel: <computer_name>-vxbsa<00>.log
- Protokolldateien des Dienstprogramms zum Wiederherstellen von Partitionen
Beispiel: partitionrecovery<00>.log
- Backup Exec-Server-Protokolldateien
Beispiel: <computer_name>-bengine<00>.log

Jedes Mal, wenn Backup Exec Migrator gestartet wird, werden separate VxBSA-Protokolldateien erstellt. Infolgedessen wird die Folgenummer jeder neuen Protokolldatei jeweils um eins erhöht.

Beispiel: <computer_name>vxbsa00.log, <computer_name>vxbsa01.log.

In ähnlicher Weise wird jedes Mal, wenn das Dienstprogramm zum Wiederherstellen von Partitionen gestartet wird, eine neue Protokolldatei erstellt. Infolgedessen wird die Folgenummer jeder neuen Protokolldatei für das Dienstprogramm zum Wiederherstellen von Partitionen jeweils um eins erhöht.

Beispiel: partitionrecovery00.log, partitionrecovery01.log

Die Folgenummern der Protokolldateien auf dem Backup Exec-Server werden ebenfalls jeweils um eins erhöht, wenn mehrere Protokolldateien erstellt werden.

Beispiel: <computer_name>-bengine00.log, <computer_name>-bengine01.log

Sie können die Protokolldateien an den folgenden Speicherorten finden.

Tabelle I-10 Speicherorte der Protokolldateien für Backup Exec Migrator und das Dienstprogramm zum Wiederherstellen von Partitionen

Protokolldatei	Computer	Verzeichnisort
VxBSA-Protokolldateien Protokolldateien des Dienstprogramms zum Wiederherstellen von Partitionen	Enterprise Vault-Server	C:<Backup Exec-Installationsordner>\Backup Exec\RAWS\logs
Backup Exec-Server-Protokolldateien	Backup Exec-Server	C:<Backup Exec-Installationsordner>\Backup Exec\Logs

Siehe ["Info zu Backup Exec Migrator-Ereignissen"](#) auf Seite 1418.

So aktivieren Sie die Backup Exec Migrator-Protokollierung

Führen Sie die folgenden Schritte aus, um die Backup Exec Migrator VxBSA-Protokollierung für den Backup Exec-Remote Agent auf einem Enterprise Vault-Server zu aktivieren.

Warnung: Ein falscher Einsatz des Windows-Registrierungseditors kann dazu führen, dass das Betriebssystem nicht mehr richtig funktioniert. Gehen Sie bei Änderungen an der Windows-Registrierung vorsichtig vor. Änderungen an der Registrierung sollten nur von erfahrenen Benutzern durchgeführt werden. Um Datenkontinuität zu gewährleisten, sollten Sie ein vollständiges Backup der Registrierung und des Systems erstellen, bevor Sie Änderungen an der Registrierung vornehmen.

1. Wählen Sie auf dem Enterprise Vault-Server "Start" und dann "Ausführen".
2. Geben Sie `regedit` ein und drücken Sie die **Eingabetaste**.
3. Öffnen Sie im Registrierungseditor den Ordner "Arbeitsplatz" und dann "HKEY_LOCAL_MACHINE > SOFTWARE > Symantec > Backup Exec for Windows > Backup Exec > Debug".
4. Doppelklicken Sie auf den Schlüssel "VXBSAlevel".
5. Ändern Sie das Datenfeld "Wert" in 6. Dies ermöglicht die vollständige ausführliche Protokollierung.
6. Klicken Sie auf "OK".
7. Aktivieren Sie die Protokollierung für den Remote-Agent durch Festlegen des folgenden Registrierungswerts auf 1: HKLM\SOFTWARE\Symantec\Backup Exec For Windows\Backup Exec\Engine\Logging\CreateDebugLog.
8. Schließen Sie den Windows-Registrierungseditor.

Auf dem Backup Exec-Medienserver aktivieren Sie die Protokollierung für den Engine-Dienst durch Festlegen der folgenden Registrierungsschlüssel:

- Setzen Sie den Schlüssel "HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Backup Exec For Windows\Backup Exec\Debug\Enabled" auf 1.
- Setzen Sie den Schlüssel "HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Backup Exec For Windows\Backup Exec\Debug\Verbose" auf 6.

Nach Aktivierung der Backup Exec Migrator-Protokollierung finden Sie die Protokolldateien im folgenden Ordner auf dem Enterprise Vault-Server: C:<Backup Exec-Installationsordner>\BACKUP EXEC\RAWS\logs

Folgende Protokolldateien werden erzeugt:

- ComputerName-vxbsa<XX>.log
- ComputerName-bengine<XX>Log (Wenn der Backup Exec-Medienserver auf dem Enterprise Vault-Server installiert ist.)
- ComputerName-beremote<XX>.log
- ComputerName-TAOSrv<XX>.log
- ComputerName-TAOCli<XX>.log

Um die Protokollierung von Migrator-Ereignissen in der Enterprise Vault-Serveranwendung zu aktivieren, führen Sie folgende Schritte auf dem Enterprise Vault-Server aus:

1. Öffnen Sie eine Eingabeaufforderung und wechseln Sie in den Installationsordner von Enterprise Vault. Dieser Ordner enthält die Datei "Dtrace.exe".
2. Führen Sie die Anwendung "Dtrace.exe" aus.
3. Aktivieren Sie die ausführliche Protokollierung für die Prozesse "StorageFileWatch" und "EVStgOfflineOps", indem Sie die folgenden Befehle ausführen:
 - `set StorageFileWatch verbose`
 - `set EVStgOfflineOps verbose`
4. Geben Sie den Befehl `view` zum Anzeigen einer Liste von Prozessen ein, für die Sie die ausführliche Protokollierung aktivieren können.
5. Legen Sie die Protokolldatei mit dem Befehl `log [Name_der_Protokolldatei]` fest
6. Um die Überwachung der Konsole selbst zu aktivieren, geben Sie den Befehl `mon` ein.
7. Führen Sie die Migrator-Aufgaben aus, für die Protokolle erforderlich sind.
8. Drücken Sie `Strg+C`, um die Überwachungsphase zu beenden.
9. Deaktivieren Sie die Protokollierung, um sicherzustellen, dass alle Einträge in der Protokolldatei gespeichert werden. Verwenden Sie den Befehl `log`, um die Protokollierung zu deaktivieren. Dann können Sie die Protokolldatei mit der Datei "Name_der_Protokolldatei" erfassen, die Sie zuvor im Befehl `log` festgelegt haben.

Info zum Löschen der von Backup Exec Migrator migrierten Dateien

Enterprise Vault löscht archivierte Elemente automatisch, wenn ihre Enterprise Vault-Aufbewahrungszeiträume ablaufen. Ein Enterprise Vault-Aufbewahrungszeitraum gibt an, wie lange archivierte Elemente in Enterprise Vault erhalten bleiben, bevor sie gelöscht werden.

Backup Exec Migrator behält die bestehenden Enterprise Vault-Aufbewahrungszeiträume für archivierte Elemente bei, wenn die archivierten Elemente auf Band migriert werden. Infolgedessen gibt Enterprise Vault beim Ablauf des Aufbewahrungszeitraums für die Daten eines Elements den Befehl aus, das Element von dem von Backup Exec verwalteten Speicherband zu löschen. Um das abgelaufene Archivelement zu löschen, muss die .cab Datei, in der es sich befindet, vom Band gelöscht werden.

Hinweis: Obgleich Backup Exec Migrator die bestehenden Enterprise Vault-Aufbewahrungszeiträume beibehält, initiiert es nicht den Löschvorgang der abgelaufenen archivierten Elemente oder archivierten Partitionen vom Band. Nur Enterprise Vault kann den Löschvorgang der abgelaufenen Elemente und Partitionen initiieren.

Weitere Informationen zum Löschen abgelaufener Elemente finden Sie in der Dokumentation zu Enterprise Vault.

Weil die .cab-Dateien archivierte Elemente mit verschiedenen Aufbewahrungszeiträumen enthalten können, kann ein abgelaufenes Element in den Backup Exec-Katalogen als gelöscht markiert werden. Es wird jedoch möglicherweise nicht sofort vom Band gelöscht. Die Aufbewahrungszeiträume aller archivierten Elemente in einer .cab-Datei müssen abgelaufen sein, bevor Enterprise Vault einen Befehl ausgibt, die .cab-Datei vom Band zu löschen.

Enterprise Vault kann auch gesamte archivierte Speicherpartitionen vom Band löschen. Nachdem Sie mithilfe der Enterprise Vault-Verwaltungskonsolle eine aktive Enterprise Vault-Speicherpartition löschen, löscht Enterprise Vault die dazugehörige archivierte Partition vom Band.

In Backup Exec werden die Bänder automatisch wiederverwendet, wenn alle auf dem Band vorhandenen Elemente in den Katalogen als gelöscht markiert wurden. Backup Exec sucht einmal alle 24 Stunden nach abgelaufenen Enterprise Vault Migrator-Medien. Wenn Backup Exec solche Medien erkennt, verschiebt es sie logisch in den temporären Mediensatz und generiert dann eine Informationsmeldung, die Sie auf den Vorgang hinweist.

Hinweis: Als abgelaufene Enterprise Vault Migrator-Medien werden Medien definiert, die ausschließlich migrierte Enterprise Vault-Daten enthalten, die in den Backup Exec-Katalogen als gelöscht markiert wurden.

Siehe ["Verwalten von Bändern"](#) auf Seite 472.

Hinweis: Stellen Sie sicher, dass migrierte Enterprise Vault-Daten auf den Bändern zugänglich verbleiben, die für Migrationszwecke verwendet werden, bis die Enterprise Vault-Daten-Aufbewahrungszeiträume ablaufen. Daher wird empfohlen, einen Aufbewahrungszeitraum von 999 Jahren für alle Bänder zu konfigurieren, die zu Migrationszwecken verwendet werden.

Siehe ["Überschreibschutzzeiträume und Anhängenzeiträume in Mediensätzen"](#) auf Seite 476.

Konfigurieren von Backup Exec Migrator

Alle für die Ausführung von Backup Exec Migrator erforderlichen Programmdateien werden installiert, wenn Sie Agent for Enterprise Vault (Enterprise Vault Agent) auf dem Enterprise Vault-Server installieren. Bevor Sie jedoch Backup Exec Migrator verwenden können, müssen Sie das Programm konfigurieren, damit ein Backup Exec-Server und der Enterprise Vault-Server als Ziel verwendet werden können.

Tabelle I-11 Enterprise Vault-Konfigurationsprozess

Schritt	Beschreibung
Schritt 1	Konfigurieren Sie Enterprise Vault-Sammlungen. Siehe "Konfigurieren von Enterprise Vault-Sammlungen" auf Seite 1424.
Schritt 2	Konfigurieren Sie Backup Exec Migrator zur Verwendung eines Backup Exec-Servers. Siehe "Konfigurieren des Backup Exec Migrator zur Verwendung eines Backup Exec-Servers" auf Seite 1425.
Schritt 3	Konfigurieren Sie Backup Exec Migrator zur Verwendung von Enterprise Vault. Siehe "Konfigurieren des Backup Exec Migrator zur Kommunikation mit Enterprise Vault" auf Seite 1428.

Verwenden Sie die folgenden Konfigurationsempfehlungen für Backup Exec Migrator und die Enterprise Vault-Partitionen:

- Konfigurieren Sie die Enterprise Vault-Partitionen so, dass migrierte Daten lokal gespeichert werden.
Konfigurieren Sie Enterprise Vault-Partitionen nicht so, dass Dateien unmittelbar nach Abschluss einer Migration gelöscht werden.
In Ihrer Enterprise Vault-Dokumentation finden Sie weitere Einzelheiten zum Konfigurieren einer Partition für die Migration.
- Konfigurieren Sie die Backup Exec-Servervorlage für die Ausführung gestaffelter Migrationen.
Siehe ["Info zur Verwendung gestaffelter Migrationen mit Backup Exec und dem Backup Exec Migrator"](#) auf Seite 1417.

Die Nichtbeachtung der Konfigurationsempfehlungen führt zu Leistungseinbußen bei Migration und Abruf.

Konfigurieren von Enterprise Vault-Sammlungen

Bevor Sie den Backup Exec Migrator zum Migrieren von mit Enterprise Vault archivierten Daten aus einer Partition verwenden können, muss Enterprise Vault zunächst die Daten sammeln.

So konfigurieren Sie Enterprise Vault-Sammlungen

- 1 Navigieren Sie von der Enterprise Vault-Konsole zu einer Speicherpartition, von der Sie Daten migrieren möchten.
- 2 Klicken Sie mit der rechten Maustaste auf die Partition und klicken Sie anschließend auf "Eigenschaften".
- 3 Auf der Registerkarte "Sammlungen" aktivieren Sie "Sammlungsdateien benutzen".
- 4 Legen Sie die Sammlungsoptionen entsprechend fest.
Siehe ["Speicherpartitionseigenschaften – Sammlungen"](#) auf Seite 1424.
- 5 Klicken Sie auf "OK".

Speicherpartitionseigenschaften – Sammlungen

Bevor Sie den Backup Exec Migrator zum Migrieren von mit Enterprise Vault archivierten Daten aus einer Partition verwenden können, muss Enterprise Vault die zu migrierenden Daten sammeln.

Siehe ["Konfigurieren von Enterprise Vault-Sammlungen"](#) auf Seite 1424.

Tabelle I-12 Speicherpartitionseigenschaften – Sammlungsoptionen

Element	Beschreibung
Sammlungsdetails verwenden	Lässt Sie Enterprise Vault als Collector festlegen.
Start um	Gibt die Ortszeit an, zu der Sie die Sammlung beginnen möchten.
Ende um	Gibt die Ortszeit an, zu der Sie die Sammlung beenden möchten. Enterprise Vault beendet das Sammeln zu diesem Zeitpunkt oder sobald keine zu sammelnden Dateien mehr vorhanden sind, je nachdem, was zuerst eintritt.
Begrenzen Sie die Sammlungsdateien auf <Anzahl> Megabyte.	Gibt die maximale Größe für die Sammlungsdateien an. Die Standardgröße ist 10 MB; Sie können jedoch eine Dateigröße von 1 MB bis zu 99 MB angeben. Sie können diesen Wert ändern, um die Verwendung Ihrer Backup-Medien zu optimieren.
Sammeln von Dateien, die älter sind als	Gibt die Zeitdauer an, die nach der Archivierung der Elemente vergehen muss, bevor diese für die Sammlung geeignet sind.

Konfigurieren des Backup Exec Migrator zur Verwendung eines Backup Exec-Servers

Führen Sie die folgenden Schritte aus, um Backup Exec Migrator zur Verwendung eines Backup Exec-Servers als Ziel zu konfigurieren.

Hinweis: Es wird die Konfiguration von zwei Server-Speichergeräten empfohlen, wenn Sie Backup Exec Migrator für Backup Exec konfigurieren. Bei Konfiguration von zwei Speichergeräten können Sie eine gestaffelte Migration für Ihre archivierten Enterprise Vault-Daten durchführen.

Siehe ["Info zur Verwendung gestaffelter Migrationen mit Backup Exec und dem Backup Exec Migrator"](#) auf Seite 1417.

Siehe ["Konfigurieren des Backup Exec Migrator zur Kommunikation mit Enterprise Vault"](#) auf Seite 1428.

So konfigurieren Sie Backup Exec Migrator zur Verwendung eines Backup Exec-Servers

- 1 Starten Sie Backup Exec auf dem Backup Exec-Server.
- 2 Erstellen Sie ein Einloggkonto, das die Anmeldedaten des Dienstkontos des Enterprise Vault-Servers verwendet.

Speicherdienstkonto-Identifikationsdaten werden verwendet, damit Backup Exec und Backup Exec Migrator den Migrationsvorgang abschließen können

Siehe ["Backup Exec-Login-Konten"](#) auf Seite 762.
- 3 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- 4 Klicken Sie auf "Backup Exec-Einstellungen" und klicken Sie dann auf "Einstellungen für von DBA gestartete Aufträge".
- 5 Wählen Sie die Vorlage STANDARD aus, und klicken Sie dann auf "Bearbeiten".

Sie können auch eine vorhandene Vorlage verwenden, oder Sie können eine neue Vorlage speziell für Enterprise Vault-Migrationen erstellen.
- 6 Wählen Sie unter "Speicher" "Beliebiger Festplattenspeicher" als primären Speicherort für migrierte Daten und legen Sie die Optionen für das Gerät fest.
- 7 Unter "Migrator for Enterprise Vault" klicken Sie auf den Pfeil nach unten neben dem Feld für "Speicherdienstkonto-Login-Daten".
- 8 Wählen Sie das Login-Konto aus, das Sie in Schritt 2 erstellt haben.

Siehe ["Optionen von Migrator for Enterprise Vault"](#) auf Seite 1427.
- 9 Legen Sie im Dialogfeld "Einstellungen für von DBA gestartete Aufträge" andere Optionen nach Bedarf fest.

Siehe ["DBA-initiierte Auftragsvorlagen"](#) auf Seite 746.
- 10 Sie haben folgende Möglichkeiten:

Wenn Sie gestaffelte Migrationen konfigurieren möchten:

Gehen Sie wie folgt vor:

- Aktivieren Sie unter "Auftragseinstellungen duplizieren" das Kontrollkästchen "Einstellungen zum Duplizieren von Backup-Sätzen für diesen Auftrag aktivieren".
 - Wählen Sie in der Liste "Speicher" einen Speichertyp.
 - Legen Sie andere Optionen nach Bedarf fest.
- Siehe ["Duplizieren von Auftragseinstellungen für DBA-initiierte Aufträge"](#) auf Seite 755.
- Klicken Sie auf "OK".

Siehe ["Info zur Verwendung gestaffelter Migrationen mit Backup Exec und dem Backup Exec Migrator"](#) auf Seite 1417.

Wenn Sie keine gestaffelten Migrationen konfigurieren möchten:

Fahren Sie mit Schritt 12 fort.

11 Klicken Sie auf "OK".

12 Konfigurieren Sie Backup Exec Migrator zur Verwendung von Enterprise Vault.

Siehe ["Konfigurieren des Backup Exec Migrator zur Kommunikation mit Enterprise Vault"](#) auf Seite 1428.

Optionen von Migrator for Enterprise Vault

Backup Exec Migrator verwendet das Enterprise Vault-Server-Speicherdienstkonto während des Authentifizierungsprozesses zwischen Backup Exec Migrator und Backup Exec-Server.

Tabelle I-13 Optionen von Migrator for Enterprise Vault

Element	Beschreibung
Speicherdienstkonto-Login-Daten	<p>Gibt die zu verwendenden Anmeldedaten des Speicherdienstkontos von Enterprise Vault-Server an, damit Backup Exec und Backup Exec Migrator den Migrationsvorgang abschließen können.</p> <p>Das Speicherdienstkonto muss entweder in der Administratorengruppe oder in der Backup-Operatorengruppe auf dem Backup Exec-Server enthalten sein.</p> <p>Hinweis: Wenn sich der Enterprise Vault-Server und der Backup Exec-Server in verschiedenen Domänen befinden, muss Vertrauen zwischen den Domänen festgelegt werden. Bei dem Benutzer des Speicherdienstkontos muss es sich um einen vertrauenswürdigen Benutzer auf dem Backup Exec-Server handeln. Vertrauensverhältnisse sind erforderlich, damit die Microsoft Security Support Provider Interface (SSPI) den Benutzer des Speicherdienstkontos authentifizieren kann.</p> <p>Weitere Informationen zu Domänen-Vertrauensverhältnissen finden Sie in der Microsoft-Dokumentation.</p>
Neu	<p>Lässt Sie ein neues Login-Konto erstellen oder ein vorhandenes Konto bearbeiten.</p> <p>Siehe "Backup Exec-Login-Konten" auf Seite 762.</p>

Siehe "[Konfigurieren des Backup Exec Migrator zur Verwendung eines Backup Exec-Servers](#)" auf Seite 1425.

Konfigurieren des Backup Exec Migrator zur Kommunikation mit Enterprise Vault

Führen Sie die folgenden Schritte aus, um Backup Exec Migrator zur Kommunikation mit Enterprise Vault zu konfigurieren.

Siehe "[Konfigurieren von Backup Exec Migrator](#)" auf Seite 1423.

So konfigurieren Sie Backup Exec Migrator zur Kommunikation mit Enterprise Vault

- 1** Navigieren Sie auf dem Enterprise Vault-Server zu einer Speicherpartition, von der Daten migriert werden sollen.
- 2** Klicken Sie mit der rechten Maustaste auf die Speicherpartition, und klicken Sie dann auf "Eigenschaften".
- 3** Aktivieren Sie auf der Registerkarte "Migration" die Option "Dateien migrieren".
- 4** Legen Sie im Feld "Sammlungs-Dateien vom Hauptspeicher entfernen" einen Zeitraum von mehr als 0 Tagen für diese Option fest.

Legen Sie den Zeitraum nicht auf 0 Tage fest. Bei einem Zeitraum von 0 Tagen löscht Enterprise Vault die migrierten Daten sofort von der Partition. Wichtiger noch, diese Einstellung veranlasst Backup Exec Migrator, separate Migrationsaufträge für jeden Partitionsordner zu erstellen, der während eines Migrationszeitraums migriert wird. Wenn separate Aufträge erstellt werden, führt der sich daraus ergebende Mehraufwand, der zur Durchführung der Aufträge erforderlich ist, zu einer herabgesetzten Migrations- und Abrufleistung.

Siehe ["Konfigurieren von Backup Exec Migrator"](#) auf Seite 1423.

- 5** Legen Sie nach Bedarf andere Migrationsoptionen fest.
Siehe ["Eigenschaften der Speicherpartition – Migrationsoptionen"](#) auf Seite 1430.
- 6** Vergewissern Sie sich, dass auf der Registerkarte "Erweitert" der Eintrag "Backup Exec" im Feld "Einstellung auflisten von" angezeigt wird.
- 7** Wählen Sie im Fenster unterhalb des Felds "Einstellung auflisten von" die Option "Backup Exec-Server".
- 8** Klicken Sie auf "Ändern".
- 9** Geben Sie den Namen oder die IP-Adresse des Backup Exec-Zielservers ein.
- 10** Klicken Sie auf "OK".
- 11** Wählen Sie "Backup Exec DBA-initiierte Vorlage".
- 12** Klicken Sie auf "Ändern".

- 13** Geben Sie den Namen einer vorhandenen Vorlage ein, die die Vault-Dienstkonto-Anmeldedaten für Enterprise Vault Server verwendet.

Die Vorlage, die Sie auswählen, muss für die Verwendung des Vault-Dienstkontos des Enterprise Vault-Servers konfiguriert sein. Die Vorlage, die Sie verwenden, muss auch dem Vorlagennamen entsprechen, den Sie verwendeten, als Sie Backup Exec Migrator zur Verwendung mit einem Backup Exec-Server konfigurierten.

Siehe ["Konfigurieren des Backup Exec Migrator zur Verwendung eines Backup Exec-Servers"](#) auf Seite 1425.
- 14** Klicken Sie auf "OK".
- 15** Vergewissern Sie sich, dass der Name der Vorlage, die das Dienstkonto des Enterprise Vault-Servers enthält, im Teilfenster "Einstellung" angezeigt wird.

Siehe ["Konfigurieren des Backup Exec Migrator zur Verwendung eines Backup Exec-Servers"](#) auf Seite 1425.
- 16** Um die Kommunikation zwischen dem Enterprise Vault-Server und dem Backup Exec-Server zu prüfen, klicken Sie auf "Konfiguration testen".
- 17** Wenn der Test fehlschlägt, stellen Sie sicher, dass Sie die richtigen Anmeldedaten für das Vault-Dienstkonto verwendet haben, und klicken Sie dann erneut auf "Konfiguration testen".
- 18** Klicken Sie auf "OK", nachdem der Test erfolgreich abgeschlossen wurde.
- 19** Klicken Sie auf "OK".

Eigenschaften der Speicherpartition – Migrationsoptionen

Wählen Sie die gewünschten Optionen für Enterprise Vault-Migrationseigenschaften aus.

Tabelle I-14 Eigenschaften der Speicherpartition – Migrationsoptionen

Element	Beschreibung
Dateien migrieren	<p>Ermöglicht das Migrieren archivierter Enterprise Vault-Daten zu einem Backup Exec-Speichergerät.</p> <p>Durch Migration können Speicherkosten reduziert werden, indem Sammlungsdateien auf tertiäre Speichergeräte verschoben werden. Jedoch können sich Abrufzeiten erhöhen.</p> <p>Weitere Informationen hierzu erhalten Sie in Ihrer Dokumentation zu Enterprise Vault.</p>

Element	Beschreibung
Migrator	<p>Gibt den Namen der Migrationsanwendung an.</p> <p>Backup Exec muss in diesem Feld angezeigt werden.</p>
Dateien migrieren, die älter sind als	<p>Gibt den Zeitraum an, der seit der letzten Änderung von Dateien vergangen sein muss, bevor diese migriert werden können.</p> <p>Weitere Informationen hierzu erhalten Sie in Ihrer Dokumentation zu Enterprise Vault.</p>
Sammlungsdateien aus dem Hauptspeicher entfernen	<p>Gibt das Alter an, in dem migrierte Sammlungsdateien aus dem primären Speicherort entfernt werden.</p> <p>Dateien, die zu Backup Exec-Speichermedien migriert wurden, können für den angegebenen Zeitraum an ihrem primären Speicherort verbleiben.</p> <p>Hinweis: Es wird empfohlen, den Zeitraum für diese Option auf einen höheren Wert als 0 Tage festzulegen, wobei ein längerer Zeitraum am besten ist. Legen Sie den Zeitraum nicht auf 0 Tage fest. Bei einem Zeitraum von 0 Tagen erstellt Backup Exec Migrator für jede migrierte Partition separate Migrationsaufträge in einem Migrationszeitraum. Wenn separate Aufträge erstellt werden, führt der sich daraus ergebende Mehraufwand, der zur Durchführung der Aufträge erforderlich ist, zu einer herabgesetzten Migrations- und Abrufleistung.</p> <p>Siehe "Konfigurieren von Backup Exec Migrator" auf Seite 1423.</p>

Siehe ["Konfigurieren des Backup Exec Migrator zur Kommunikation mit Enterprise Vault"](#) auf Seite 1428.

Info zum Anzeigen migrierter Enterprise Vault-Daten

In der Backup Exec-Ansicht "Backup-Sätze" werden die migrierten Elemente für die Enterprise Vault-Partition angezeigt. Backup-Sätze, die die migrierten

CAB-Dateien enthalten, werden in der Ansicht "Backup-Sätze" unter einem Partitionsnamen angezeigt, der die Enterprise Vault-Partition widerspiegelt, von der die Daten migriert wurden. Da die Ansicht "Backup-Sätze" die archivierten Daten in einem schreibgeschützten Modus anzeigt, können Sie die Daten nicht für die Wiederherstellung auswählen. Jedoch können Sie die Daten in der Anwendung abrufen, in der sich die Daten befinden.

Siehe ["Backup-Sätze"](#) auf Seite 401.

Hinweis: Sie können alle archivierten Elemente vollständig abrufen, die in der Ansicht "Backup-Sätze" angezeigt werden, indem Sie das Dienstprogramm zum Wiederherstellen von Partitionen verwenden.

Siehe ["Info über das Dienstprogramm zum Wiederherstellen von Partitionen"](#) auf Seite 1433.

Siehe ["Info zum Abrufen migrierter Enterprise Vault-Daten"](#) auf Seite 1432.

Info zum Abrufen migrierter Enterprise Vault-Daten

Sämtliche Vorgänge zum Abrufen von Dateien gehen von der Enterprise Vault-Serverkonsole aus. Sie können keine archivierten Enterprise Vault-Daten von Backup Exec aus wiederherstellen.

Wenn Dateien aus einer Partition migriert werden, erstellt Enterprise Vault in der Partition eine Verknüpfung, die die migrierte Datei ersetzt. Die Verknüpfung erstellt auch einen Link zum Speicherort der migrierten Datei. Sie können Dateien abrufen, indem Sie auf ihre Verknüpfungen in der Enterprise Vault-Partition selbst doppelklicken. Wenn eine Partition eine lokale Kopie der migrierten Dateien aufbewahrt, ruft Enterprise Vault die Dateien von den lokalen Kopien ab. Wenn Enterprise Vault die migrierten Dateien löscht, weil der Dateiaufbewahrungszeitraum der Partition abläuft, müssen die angeforderten Dateien aus den Backup Exec-Speichermedien abgerufen werden.

Hinweis: Backup Exec unterstützt keine Wiederherstellungen von Speichergeräten und von Backup-Sätzen für Backup Exec Migrator for Enterprise Vault, da die Wiederherstellung von Daten auf dem Enterprise Vault oder dort, wo sich die Daten befinden, initiiert wird. Die Ansicht "Backup-Sätze" zeigt die archivierten Daten in einem schreibgeschützten Modus an, deshalb können Sie die Daten nicht für die Wiederherstellung auswählen.

Backup Exec Migrator for Enterprise Vault unterstützt das Wiederherstellen einer Ressource nicht, wenn Sie die Ressource auf verschiedenen Datenträgern sichern.

Tabelle I-15 Abruf von migrierten Daten

Aktion	Hinweise
Enterprise Vault interagiert mit Backup Exec Migrator, um den Prozess zu beginnen.	Der Backup Exec Migrator identifiziert den Backup Exec-Server, auf dem die Dateien gespeichert sind.
Der Backup Exec Migrator plant einen Backup Exec-Wiederherstellungsauftrag am Server ein.	Backup Exec stellt die angeforderten Dateien wieder her.
Der Backup Exec Migrator migriert die wiederhergestellten Dateien vom Backup Exec-Server zur Enterprise Vault-Serverpartition.	Backup Exec Migrator verschiebt die wiederhergestellten Dateien an einen von Enterprise Vault angegebenen Speicherort unter Verwendung des von Enterprise Vault angegebenen Namens.

Der Abrufprozess läuft automatisch ab, nachdem Sie den Vorgang am Enterprise Vault-Server starten. Ein Benutzereingriff ist nicht erforderlich, außer um eventuell ein Band in das Bandgerät einzulegen, wenn Sie Speichermedien entfernt haben.

Siehe ["Abrufen von migrierten Enterprise Vault-Daten"](#) auf Seite 1433.

Abrufen von migrierten Enterprise Vault-Daten

Führen Sie die folgenden Schritte durch, um migrierte Enterprise Vault-Dateien wiederherzustellen.

Hinweis: Um die gewünschten Dateien erfolgreich abzurufen, legen Sie ein Band in ein Bandlaufwerk am Backup Exec-Server ein.

So rufen Sie migrierte Enterprise Vault-Daten ab

- 1 Am Enterprise Vault Server navigieren Sie zu der Partition, aus der Sie die Daten abrufen möchten.
- 2 Doppelklicken Sie auf die Datei, die Sie abrufen möchten.

Info über das Dienstprogramm zum Wiederherstellen von Partitionen

Das Dienstprogramm zum Wiederherstellen von Partitionen ist eine Kommandozeilenanwendung, die automatisch installiert wird, wenn Sie Backup Exec Agent for Windows installieren. Mit dem Dienstprogramm können Sie alle archivierten Dateien einer Partition aus den Backup Exec-Speichermedien in einem einzelnen Vorgang wiederherstellen. Sie können es auch verwenden, um die

archivierten Partitionsdaten für jede der Enterprise Vault-Partitionen in einer Notfallwiederherstellungssituation wiederherzustellen.

Nachdem Sie das Dienstprogramm zum Wiederherstellen von Partitionen verwendet haben, können Sie Wiederherstellungsdetails überprüfen, indem Sie den Backup Exec-Auftragsverlauf für jeden Enterprise Vault-Server betrachten, auf dem die Wiederherstellung erfolgt.

Siehe ["Anforderungen für das Dienstprogramm zum Wiederherstellen von Partitionen"](#) auf Seite 1434.

Siehe ["Suchen einer Archiv-ID"](#) auf Seite 1434.

Siehe ["Starten des Dienstprogramms zum Wiederherstellen von Partitionen"](#) auf Seite 1435.

Anforderungen für das Dienstprogramm zum Wiederherstellen von Partitionen

Sie müssen folgende Informationen kennen, wenn Sie das Dienstprogramm zum Wiederherstellen von Partitionen verwenden:

- Den Namen der Speicherpartition für die Daten, die Sie wiederherstellen möchten
- Die Archiv-ID der Partitionsdaten, die Sie wiederherstellen möchten
- Ein Enterprise Vault-Server-Benutzerkonto mit Speicherdienstkonto-Berechtigungen

Hinweis: Wenn Sie das Dienstprogramm zum Wiederherstellen von Partitionen auf einem Computer mit Windows Server 2008/2008 R2 ausführen, sind Administratorrechte erforderlich.

Darüber hinaus muss das Dienstprogramm zum Wiederherstellen von Partitionen auf dem Enterprise Vault-Server laufen, von dem die Daten, die Sie wiederherstellen möchten, ursprünglich migriert wurden.

Siehe ["Suchen einer Archiv-ID"](#) auf Seite 1434.

Siehe ["Starten des Dienstprogramms zum Wiederherstellen von Partitionen"](#) auf Seite 1435.

Suchen einer Archiv-ID

Sie verwenden die Archiv-ID der Daten, die Sie wiederherstellen möchten, zusammen mit dem Speicherpartitionsnamen, wenn Sie das Dienstprogramm zum Wiederherstellen von Partitionen ausführen. Die Archiv-ID ist eine alphanumerische Zeichenfolge beträchtlicher Länge.

Beispielsweise 1D69957C6D917714FB12FEA54C9A8299A1110000ev8archive.EVMBE

Die Archiv-ID wird bei den Eigenschaften eines archivierten Dateisatzes aufgelistet.

So suchen Sie eine Archiv-ID

- 1 In der linken Ansicht der Enterprise Vault-Verwaltungskonsole erweitern Sie "Archive".
- 2 Navigieren Sie in der Ordnerstruktur und wählen Sie den Ordner des Datentyps aus, den Sie wiederherstellen möchten.
- 3 Klicken Sie in der rechten Ansicht mit der rechten Maustaste auf ein Archiv und wählen Sie dann "Eigenschaften" aus.
- 4 Die Archiv-ID befindet sich auf der Registerkarte "Erweitert" im unteren Bereich.

Siehe ["Starten des Dienstprogramms zum Wiederherstellen von Partitionen"](#) auf Seite 1435.

Starten des Dienstprogramms zum Wiederherstellen von Partitionen

Führen Sie die folgenden Schritte aus, um das Dienstprogramm zum Wiederherstellen von Partitionen zu starten.

So starten Sie das Dienstprogramm zum Wiederherstellen von Partitionen

- 1 Über den Enterprise Vault-Server öffnen Sie eine Windows-Eingabeaufforderung.
- 2 Navigieren Sie zum Enterprise Vault Agent-Installationsverzeichnis.
Beispiel: C:<Backup Exec-Installationsordner>\Backup Exec\RAWS
- 3 Gehen Sie wie folgt vor:

So starten Sie das Dienstprogramm zum Wiederherstellen von Partitionen auf einem Computer mit Windows Server 2008/2008 R2

Geben Sie folgenden Befehl ein:

```
runas  
/Benutzer:<Domäne\Administrator>  
partitionrecovery.exe -vs  
<Speichername> -ap <Archiv-ID>
```

So starten Sie das Dienstprogramm zum Wiederherstellen von Partitionen auf Computern mit anderen unterstützten Versionen von Windows

Geben Sie folgenden Befehl ein:

```
partitionrecovery.exe -vs  
<Speichername> -ap <Archiv-ID>
```

- 4 Drücken Sie die **Eingabetaste**.

Siehe ["Info über das Dienstprogramm zum Wiederherstellen von Partitionen"](#) auf Seite 1433.

Best Practices für die Verwendung von Backup Exec Migrator

Sie können die folgenden Best Practices befolgen, wenn Sie Backup Exec Migrator verwenden:

- Es wird empfohlen, regelmäßig die Backup Exec-Kataloge zu sichern. Falls die Kataloge beschädigt werden, können Sie sie aus den Backups wiederherstellen. Nachdem Sie die Kataloge wiederhergestellt haben, müssen Sie die Speichermedien neu katalogisieren, auf denen Backup Exec Migrator-Daten gespeichert werden. Durch erneutes Katalogisieren der Speichermedien wird sichergestellt, dass die neuesten Katalogeinträge verfügbar sind.
- Optimale Leistung erzielen Sie, indem Sie Backup Exec Migrator so konfigurieren, dass Daten in einen Backup-to-Disk-Ordner und dann auf ein Bandgerät migriert werden. Verwenden Sie dazu einen Duplizierungsauftrag. Siehe ["Info zur Verwendung gestaffelter Migrationen mit Backup Exec und dem Backup Exec Migrator"](#) auf Seite 1417.
Siehe ["Manuelles Duplizieren von Backup-Sätzen bzw. Auftragsverläufen"](#) auf Seite 246.
- Legen Sie auf der Registerkarte mit den Optionen für "Migration" von Enterprise Vault den Zeitraum für "Sammlungs-Dateien vom Hauptspeicher entfernen" auf einen längeren Wert als 0 Tage fest.
Bei einem Zeitraum von 0 Tagen löscht Enterprise Vault die migrierten Daten sofort von der Partition.

Wenn Sie 0 Tage als Zeitraum eingestellt haben, werden die folgenden Schritte empfohlen:

- Erhöhen Sie die Zahl gleichzeitiger Aufträge, die für den Backup-to-Disk-Ordner zulässig sind, den Sie für die Migration benutzen. Erhöhen Sie die Zahl der gleichzeitigen Aufträge entsprechend der folgenden Formel:
$$<\text{Anzahl empfohlene gleichzeitige Aufträge}> = <\text{Anzahl installierter Bandlaufwerke plus zwei}>$$

Sind beispielsweise zwei Bandlaufwerke installiert, sollten Sie den Backup-to-Disk-Ordner so konfigurieren, dass vier gleichzeitige Aufträge möglich sind.

Mit gleichzeitigen Aufträgen kann Backup Exec Migrator die Migration von Daten zum Magnetplattenspeicher fortsetzen, während Bandlaufwerke Duplizierungsaufträge in einer Umgebung für gestaffelte Migration verarbeiten.

Hinweis: Sie können die Zahl gleichzeitig laufender Aufträge erhöhen, indem sie die Gesamtgleichzeitigkeitsstufe der Backup-to-Disk-Geräte erhöhen.

- Es wird empfohlen, dass Sie zuerst alle archivierten Dateien in einem Erfassungs- und Migrationsvorgang erfassen und sie dann im nächsten Vorgang migrieren. Dieser Prozess hilft sicherzustellen, dass Backup Exec Migrator einen einzelnen Auftrag für jeden Migrationsvorgang erstellt, wodurch die Migrationsleistung sich verbessert.

Siehe ["Info zu Backup Exec Migrator for Enterprise Vault"](#) auf Seite 1413.

Fehlerbehebung bei Backup Exec Migrator und dem Dienstprogramm zum Wiederherstellen von Partitionen

Überprüfen Sie die folgenden Fehlermeldungen auf mögliche Lösungen zu den Fehlern, die auftreten können:

- Backup Exec Migrator protokolliert Migrationsaktivitäten in der Windows-Ereignisanzeige und im Dienstprogramm Enterprise Vault Dtrace auf dem Enterprise Vault Server. Es protokolliert auch Migrationsaktivitäten auf dem Backup Exec-Medienserver.
Die Einzelheiten, die in den Protokolldateien bereitgestellt werden, können Ihnen dabei helfen, Probleme mit Backup Exec Migrator zu beheben.
Siehe ["Info zu Backup Exec Migrator-Ereignissen"](#) auf Seite 1418.
Siehe ["Info zu Backup Exec Migrator-Protokollen"](#) auf Seite 1418.
- Das Dienstprogramm zum Wiederherstellen von Partitionen kann keine Dateien zum Abrufen finden.
Es gibt keine Dateien, die mit der Archiv-ID, die Sie zur Verfügung stellten, aus der Speicherdatenbank abgerufen werden können.
- Der Vorgang des Dienstprogramms zum Wiederherstellen von Partitionen wird aufgrund einer Benutzeranforderung beendet.
Sie haben möglicherweise den Vorgang des Dienstprogramms zum Wiederherstellen von Partitionen beendet, indem Sie **Strg + C** oder **Strg + Pause** gedrückt haben.
- Der Name der migrierten Datei `<file_name>` mit der ID `<migrated_file_id>` wurde in den Backup Exec-Backup-Sätzen nicht gefunden. Der Abruf wird für diese Datei übersprungen.
Das Dienstprogramm zum Wiederherstellen von Partitionen überspringt Sammlungsdateien, wenn sie bereits in der Speicherdatenbank existieren. Um die Dateien wiederherzustellen, löschen Sie sie aus der Speicherdatenbank und führen Sie dann das Dienstprogramm zum Wiederherstellen von Partitionen erneut aus.

- Das Dienstprogramm zum Wiederherstellen von Partitionen kann keine Partitionen finden. Stellen Sie sicher, dass der Name des Speichers gültig ist und dass es Partitionen im Speicher gibt.

Der Speichername, den Sie angegeben haben, ist möglicherweise ungültig.

Siehe ["Info zu Backup Exec Migrator for Enterprise Vault"](#) auf Seite 1413.

Siehe ["Info über das Dienstprogramm zum Wiederherstellen von Partitionen"](#) auf Seite 1433.

Enterprise Vault-Login-Konto

Um Enterprise Vault-Daten zu sichern und wiederherzustellen, muss Backup Exec den Benutzernamen und das Kennwort für das Konto kennen, das zum Anmelden am Enterprise Vault-Server verwendet wird. Backup Exec verwendet auch das Login-Konto, um mit der Enterprise Vault-SQL-Datenbank zu kommunizieren.

Das Enterprise Vault-Login-Konto muss über folgende Berechtigungen verfügen:

- Sichern und Wiederherstellen von SQL-Datenbanken.
- Kommunizieren mit den Enterprise Vault-Diensten und Ablegen von Enterprise Vault im Backup-Modus.

Das Login-Konto muss über Berechtigungen zum Lesen und Schreiben in Enterprise Vault-Dateisystem-Pfaden wie Enterprise Vault-Partitionen und -Indexspeicherorten. Die Dateipfade können entweder umfassend gekennzeichnete UNC-Pfade sein oder Pfade, die sich auf dem lokalen Laufwerk befinden.

Optionen zu Enterprise Vault

Im Feld "Backup-Methode" können Sie eine Backup-Methode zum Sichern von Enterprise Vault-Daten angeben.

Siehe ["Backup-Methoden in Backup Exec"](#) auf Seite 205.

Backup Exec Agent for Microsoft Active Directory

Dieser Anhang enthält folgende Themen:

- [Info zum Agent for Microsoft Active Directory](#)
- [Anforderungen für Agent for Microsoft Active Directory](#)
- [Info zum Sichern von Active Directory und ADAM/AD LDS](#)
- [Infos zum Wiederherstellen von einzelnen Active Directory- und ADAM/AD LDS-Objekten](#)

Info zum Agent for Microsoft Active Directory

Der Backup Exec Agent for Microsoft Active Directory verwendet vollständige Backups, für die Granular Recovery Technology (GRT) aktiviert wird, um Sie einzelne Active Directory-Objekte und -Attribute wiederherstellen zu lassen, ohne eine autoritative oder nicht-autoritativer vollständige Wiederherstellung durchzuführen. Außerdem können Sie einzelne Objekte und Attribute aus Active Directory Application Mode (ADAM) bzw. Active Directory Lightweight Directory Services (AD LDS) wiederherstellen.

Der Agent for Microsoft Active Directory wird als Teil des Agent for Applications and Databases installiert.

Der Agent for Microsoft Active Directory funktioniert mit Backups des Windows-Systemzustands, in dem Active Directory installiert wird, und mit ADAM/AD LDS. Bei dem Backup des Windows-Systemstatus umfasst der Backup-Auftrag Active Directory, da Active Directory Bestandteil des Windows-Systemstatus ist. Sie können den Agent auch zur Wiederherstellung einzelner ADAM/AD LDS-Objekte und -Attribute verwenden. Bei dem Backup mehrerer ADAM/AD LDS-Instanzen

werden alle Instanzen unter dem Knoten "Active Directory-Anwendungsmodus" angezeigt.

Siehe ["Installieren zusätzlicher Agents und Funktionen auf dem lokalen Backup Exec-Server"](#) auf Seite 66.

Siehe ["Infos zum Wiederherstellen von einzelnen Active Directory- und ADAM/AD LDS-Objekten"](#) auf Seite 1446.

Anforderungen für Agent for Microsoft Active Directory

Überprüfen Sie die folgenden Anforderungen für den Agent for Microsoft Active Directory:

- Der Agent for Windows muss auf dem Computer installiert werden, auf dem das Active Directory installiert wird.
- Anforderungen an das jeweilige Betriebssystem für den Agent for Microsoft Active Directory finden Sie in der Liste der mit Backup Exec kompatiblen Software.
- Stellen Sie sicher, dass die folgende Option auf den Backup-Auftragseigenschaften ausgewählt wird: "Backup Exec Granular Recovery Technology (GRT) zum Aktivieren der Wiederherstellung einzelner Objekte aus Active Directory-Backups verwenden (für schreibgeschützte Domänencontroller nicht unterstützt)". Dies ist die Standardeinstellung. Diese Option muss ausgewählt werden, damit Sie einzelne Attribute und Eigenschaften vom vollständigen Active Directory und den ADAM/AD LDS-Backups wiederherstellen können.
- Um ein GRT-Backup eines Windows Server 2012 R2 Active Directory Server durchzuführen, müssen Sie einen Backup Exec-Server verwenden, auf dem Windows Server 2012 R2 ausgeführt wird.

Dies sind die Anforderungen für die Wiederherstellung von einzelnen Objekten und von Attributen von Backup-Aufträgen, die den Agent for Microsoft Active Directory verwendeten:

- Sie benötigen ein vollständiges Backup des Windows-Systemzustands (wo Active Directory installiert ist) oder von ADAM/AD LDS.
- Auf dem Backup Exec-Server, der den Wiederherstellungsauftrag ausführt, muss ein Windows-Betriebssystem mit Unterstützung für Minifilter-Treiber installiert sein.

- Sie müssen einen Speicherort auf dem Datenträger des Backup Exec-Servers festlegen, an dem Backup Exec die wiederherzustellenden Objekte und Attribute bei der Wiederherstellung von einem Band vorübergehend ablegen kann.

Siehe ["Infos zum Wiederherstellen von einzelnen Active Directory- und ADAM/AD LDS-Objekten"](#) auf Seite 1446.

Info zum Sichern von Active Directory und ADAM/AD LDS

Es wird empfohlen, Active Directory- und ADAM/AD LDS-Backups auf Festplattenspeicher auszuführen und die Backups dann auf Band zu kopieren. Diese Strategie führt zu kürzeren Backup-Zeiträumen, und Festplattenspeicher bieten die effizienteste Speichermethode für GRT-aktivierte Backups und die effizienteste Methode der Wiederherstellung. Außerdem können Sie mit dieser Methode auch Active Directory oder ADAM/AD LDS verwalten, ohne die einzelnen gesicherten Objekte und Eigenschaften katalogisieren zu müssen.

Wenn Sie beispielsweise auf einem Band sichern, müssen Sie einen temporäre Festplattenbereitstellungsort auf einem lokalen NTFS-Datenträger erstellen, um einzelne Elemente von GRT-aktivierten Backups auf Band wiederherzustellen. Die Daten werden zunächst vom Band an den temporären Staffelspeicherort kopiert und erst in einem zweiten Schritt wiederhergestellt. Daher ist die Wiederherstellung von Band zeitaufwändiger. Für beste Ergebnisse sollten Sie Datenträgerspeicher speziell auswählen, wenn Sie Ihre GRT-aktivierten Backup-Aufträge konfigurieren.

Hinweis: Sie können Datenbanken nicht auf Geräten sichern, die an einem Computer angehängt werden, auf dem Remote Media Agent for Linux installiert ist.

Mit Granular Recovery Technology (GRT) können Sie einzelne Objekte und Attribute aus Active Directory- und ADAM/AD LDS-Backups wiederherstellen, ohne eine autoritative oder nicht-autoritative vollständige Wiederherstellung durchführen zu müssen. Die Funktion "Granular Recovery Technology" wird standardmäßig aktiviert, wenn Sie einen Backup-Auftrag erstellen. Um ein GRT-Backup eines Windows Server 2012 R2 Active Directory Server durchzuführen, müssen Sie einen Backup Exec-Server verwenden, auf dem Windows Server 2012 R2 ausgeführt wird.

Beim direkten Sichern beliebiger Anwendungsdatenbanken von Windows Active Directory oder ADAM/AD LDS auf Band stimmen die während des Sicherns hinzugefügten oder gelöschten Objekte und Eigenschaften nicht mit den einzelnen Objekten und Eigenschaften überein, die für eine Wiederherstellung mithilfe des Backup-Satzes verfügbar sind. Das Backup der Datenbank ist ein Snapshot-Backup

der tatsächlichen Active Directory- oder ADAM/AD LDS-Datenbank, und die einzelnen Active Directory- oder ADAM/AD LDS-Objekte werden nach Ausführung des Snapshot katalogisiert. Da bei diesem Katalogisierungsvorgang Objekte und Eigenschaften aus der tatsächlichen Active Directory- oder ADAM/AD LDS-Datenbank erfasst werden, kann es nach Erstellung des Snapshot zu Änderungen an diesen kommen.

Siehe ["Sichern von Daten"](#) auf Seite 174.

Siehe ["Bearbeiten von Backup-Definitionen"](#) auf Seite 226.

Siehe ["Hinzufügen einer Stufe zu einer Backup-Definition"](#) auf Seite 244.

Siehe ["Optionen für Backup-Aufträge von Microsoft Active Directory"](#) auf Seite 1444.

Siehe ["Granular Recovery Technology"](#) auf Seite 737.

Optionen für Active Directory und ADAM/AD LDS-Backup-Aufträge bearbeiten

Sie können die Standardeinstellungen für alle Backup-Aufträge von Active Directory und ADAM/AD LDS bearbeiten.

Siehe ["Infos zum Wiederherstellen von einzelnen Active Directory- und ADAM/AD LDS-Objekten"](#) auf Seite 1446.

So bearbeiten Sie Optionen der Backup-Aufträge von Active Directory und ADAM/AD LDS

- 1 Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und dann "Auftragsstandardeinstellungen".
- 2 Wählen Sie eine Backup-Option aus.
- 3 Klicken Sie auf der linken Seite auf Microsoft Active Directory.

4 Bearbeiten Sie die folgenden Backup-Optionen für den Agent for Microsoft Active Directory wie gewünscht:

Backup Exec Granular Recovery Technology (GRT) verwenden, um Wiederherstellung einzelner Objekte von Active Directory-Backups zu aktivieren (wird bei schreibgeschützten Domänencontrollern nicht unterstützt)

Aktiviert die Wiederherstellung einzelner Elemente aus vollständigen Backups von Active Directory oder ADAM/AD LDS.

Dies ist die Standardeinstellung. Diese Option muss ausgewählt werden, damit Sie einzelne Attribute und Eigenschaften vom vollständigen Active Directory und den ADAM/AD LDS-Backups wiederherstellen können.

Hinweis: Einzelne Objekte und Attribute aus Active Directory-Backups für schreibgeschützte Domänencontroller (RODC) können nicht wiederhergestellt werden. Führen Sie GRT-Backups und -Wiederherstellungen von Active Directory auf einem beschreibbaren, zentralisierten Rechenzentrum-Domänencontroller durch.

Stellen Sie sicher, dass Sie die Anforderungen für Granular Recovery Technology erfüllen.

Um ein GRT-aktiviertes Backup eines Windows Server 2012 R2 Active Directory Application Server durchzuführen, müssen Sie einen Backup Exec-Server verwenden, der Windows Server 2012 R2 ausführt.

Siehe "[Granular Recovery Technology](#)" auf Seite 737.

Bei Verwendung des Snapshot-Providers von Microsoft Volume Shadow Copy Service (VSS) Konsistenzprüfung vor dem Backup durchführen (Windows Server 2008)

Überprüft Snapshots auf beschädigte Daten. Diese Option bezieht sich ausschließlich auf Snapshots und wird von Microsoft Volume Shadow Copy Services (VSS) ausgeführt.

Mit Backup fortfahren, wenn
Konsistenzprüfung fehlschlägt

Ermöglicht dem Backup-Auftrag, selbst bei nicht bestandener Konsistenzprüfung weiter ausgeführt zu werden. Dies kann vor allem dann sinnvoll sein, wenn auch ein fehlerhaftes Backup der Datenbank besser ist als gar keines oder beim Sichern einer großen Datenbank lediglich ein kleines Problem auftritt.

5 Klicken Sie auf "OK".

Optionen für Backup-Aufträge von Microsoft Active Directory

Sie können die Standardeinstellungen für Backup-Aufträge von Active Directory und ADAM/AD LDS bearbeiten.

Hinweis: Nur vollständige Backups von Active Directory sind zulässig

Siehe ["Optionen für Active Directory und ADAM/AD LDS-Backup-Aufträge bearbeiten"](#) auf Seite 1442.

Tabelle J-1 Standardoptionen für Backup von Microsoft Active Directory

Element	Beschreibung
Backup Exec Granular Recovery Technology (GRT) verwenden, um Wiederherstellung einzelner Objekte von Active Directory-Backups zu aktivieren (wird bei schreibgeschützten Domänencontrollern nicht unterstützt)	<p>Aktiviert die Wiederherstellung einzelner Elemente aus vollständigen Backups von Active Directory oder ADAM/AD LDS.</p> <p>Dies ist die Standardeinstellung. Diese Option muss ausgewählt werden, damit Sie einzelne Attribute und Eigenschaften vom vollständigen Active Directory und den ADAM/AD LDS-Backups wiederherstellen können.</p> <p>Hinweis: Einzelne Objekte und Attribute aus Active Directory-Backups für schreibgeschützte Domänencontroller (RODC) können nicht wiederhergestellt werden. Führen Sie GRT-Backups und -Wiederherstellungen von Active Directory auf einem beschreibbaren, zentralisierten Rechenzentrum-Domänencontroller durch.</p> <p>Stellen Sie sicher, dass Sie die Anforderungen für Granular Recovery Technology erfüllen.</p> <p>Um ein GRT-aktiviertes Backup eines Windows Server 2012 R2 Active Directory Server durchzuführen, müssen Sie einen Backup Exec-Server verwenden, der Windows Server 2012 R2 ausführt.</p> <p>Siehe "Granular Recovery Technology" auf Seite 737.</p>
Bei Verwendung des Snapshot-Providers von Microsoft Volume Shadow Copy Service (VSS) Konsistenzprüfung vor dem Backup durchführen (Windows Server 2008)	<p>Überprüft Snapshots auf beschädigte Daten. Diese Option gilt nur für Active Directory-Snapshots, die vom Microsoft Volumenschattenkopie-Dienst (VSS) durchgeführt werden.</p>

Element	Beschreibung
Mit Backup fortfahren, wenn Konsistenzprüfung fehlschlägt	Ermöglicht dem Backup-Auftrag, selbst bei nicht bestandener Konsistenzprüfung weiter ausgeführt zu werden. Dies kann vor allem dann sinnvoll sein, wenn ein Backup des Active Directory im aktuellen Zustand besser ist als gar keines oder beim Sichern eines großen Active Directory, in der lediglich ein geringfügiges Problem vorliegt.

Siehe ["Info zum Sichern von Active Directory und ADAM/AD LDS"](#) auf Seite 1441.

Infos zum Wiederherstellen von einzelnen Active Directory- und ADAM/AD LDS-Objekten

Wenn Sie Active Directory- und ADAM/AD LDS-Objekte von Band wiederherstellen, müssen Sie einen Stagingspeicherort auf dem Datenträger angeben, in dem die Objekte vor der Wiederherstellung abgelegt werden. Der Speicherort muss sich auf einem lokalen NTFS-Datenträger auf dem Backup Exec-Server befinden, auf dem der Wiederherstellungsauftrag ausgeführt wird, und das Backup Exec-Dienstkonto muss darauf zugreifen können.

Standardmäßig stellt der Agent for Microsoft Active Directory gelöschte Active Directory- oder ADAM/AD LDS-Objekte vom Active Directory-Container für gelöschte Objekte wieder her, wenn ihre Tombstone-Verfallszeiten nicht abgelaufen sind.

Wenn Objekte in Active Directory gelöscht werden, werden sie aus ihrem aktuellen Active Directory- oder ADAM/AD LDS-Container entfernt, in Tombstones umgewandelt und dann im Container für gelöschte Objekte von Active Directory abgelegt, wo ihre Tombstone-Verfallszeit überwacht wird. Nach Ablauf ihrer Tombstone-Verfallszeit werden die Tombstones aus dem Active Directory-Container für gelöschte Objekte entfernt, wodurch die Objekte dauerhaft aus den Active Directory- und ADAM/AD LDS-Datenbanken gelöscht werden.

Mit dem Agent for Microsoft Active Directory können auch Tombstone-Objekte aus dem Active Directory-Container der gelöschten Objekte wiederhergestellt werden, wenn folgende Bedingungen erfüllt sind:

- Die Tombstone-Verfallszeit ist noch nicht abgelaufen.
- Sie wurden nicht aus dem Container für gelöschte Objekte entfernt.
- Sie stellen auf einem Computer mit Windows Server 2008/2008 R2 x64 wieder her.

Bei der Wiederherstellung von Active Directory-Benutzerobjekten müssen Sie das Benutzerkennwort des Objekts zurücksetzen und anschließend das Benutzerkonto des Objekts erneut aktivieren. Bei ADAM/AD LDS-Benutzerobjekten müssen Sie das Benutzerkennwort des Objekts zurücksetzen und anschließend das Benutzerkonto des Objekts erneut aktivieren. Verwenden Sie für Active Directory-Benutzerobjekte die Microsoft-Anwendung Active Directory-Benutzer und -Computer. Verwenden Sie für ADAM/AD LDS-Benutzerobjekte die Anwendung "ADSI Edit".

Bei Active Directory-Computerobjekten muss das Konto des Objekts zurückgesetzt werden.

Einige Objekte im Knoten der Active Directory-Konfigurationspartition können nicht über den Active Directory-Container für gelöschte Objekte reanimiert werden. Neu erstellte Objekte werden jedoch von manchen Anwendungen nicht erkannt.

Hinweis: Beim Wiederherstellen von ADAM/AD LDS-Daten beendet Backup Exec die wiederherzustellende ADAM/AD LDS-Instanz, bevor der Auftrag gestartet wird. Die ADAM/AD LDS-Instanz wird jedoch nach Abschluss des Wiederherstellungsauftrags nicht neu gestartet, da möglicherweise weitere Aufträge (z. B. autoritative Wiederherstellungen miti "Adamutil.exe") erforderlich sind. Sie müssen die ADAM/AD LDS-Instanz neu starten. Wenn Backup Exec die ADAM/AD LDS-Instanz nicht beenden kann, oder wenn Backup Exec nicht alle ADAM/AD LDS-Daten wiederherstellen kann, schlägt die Wiederherstellung fehl.

Informationen dazu finden Sie in der Microsoft-Dokumentation zu Active Directory.

Zurücksetzen des Active Directory-Computerobjekts und des Computerobjekt-Kontos

Computerobjekte in Active Directory leiten sich von Benutzerobjekten ab. Manche Attribute, die mit einem Computerobjekt verknüpft sind, können nicht wiederhergestellt werden, wenn Sie ein gelöscht Computerobjekt wiederherstellen. Die Attribute können nur wiederhergestellt werden, wenn die Attribute durch Schemaänderungen gespeichert wurden, bevor das Computerobjekt ursprünglich gelöscht wurde. Da sich die Anmeldedaten von Computerobjekten alle 30 Tage ändern, stimmen die Daten des Backup ggf. nicht mit den Daten überein, die auf dem jeweiligen Computer gespeichert sind.

Hinweis: Damit Sie ein Computerobjekt zurücksetzen können, müssen Sie die Microsoft-Anwendung "Active Directory-Benutzer und -Computer" verwenden.

Weitere Informationen zum Zurücksetzen von Computerobjekten finden Sie in der Dokumentation zu "Active Directory-Benutzer und -Computer".

Wurde das Attribut "userAccountControl" eines Computerobjekts nicht beibehalten, bevor das Objekt gelöscht wurde, müssen Sie das Konto des Objekts zurücksetzen, nachdem Sie das Objekt wiederhergestellt haben.

Zurücksetzen des Active Directory-Computerobjektkontos

- 1** Entfernen Sie den Computer aus der Domäne.
- 2** Fügen Sie den Computer wieder der Domäne hinzu. Die SID für den Computer bleibt gleich, da sie beibehalten wird, wenn Sie ein Computerobjekt löschen. Wenn der Tombstone des Objekts abläuft und ein neues Computerobjekt erstellt wird, ändert sich die SID.

Neuerstellen von bereinigten Active Directory- und ADAM/AD LDS-Objekten

Sie können versuchen, gelöschte Active Directory-Objekte und ADAM-/LDSobjekte neu zu erstellen, nachdem sie vom Container "Active Directory Deleted Objects" gereinigt wurden, indem das Objekt von einem vorherigen Active Directory-Backup wiederhergestellt wird.

Sie können versuchen, gelöschte Objekte erneut zu erstellen, wenn deren Tombstone-Verfallszeiten abgelaufen sind und die Objekte aus dem Active Directory-Container für gelöschte Objekte entfernt wurden.

Beachten Sie jedoch Folgendes:

- Die meisten Anwendungen werden ein neu erstelltes Objekt nicht erkennen, da neu erstellte Objekte nicht mit dem ursprünglichen, gelöschten Objekt identisch sind. Neu erstellten Objekten werden neue GUIDs (Global Unique Identifiers) und Sicherheits-IDs zugewiesen, die von den Anwendungen, die das ursprüngliche Objekt erstellt haben, nicht erkannt werden können.
- Vom Windows-Betriebssystem erstellte Attribute können beim Neuerstellen eines gelöschten Objekts nicht neu erstellt werden. Objekte, für die vom Betriebssystem festgelegte Attribute erforderlich sind, werden daher nicht von Windows erkannt, wenn die Objekte neu erstellt werden.

Siehe ["Methoden für das Wiederherstellen von Daten in Backup Exec"](#) auf Seite 258.

Siehe ["Infos zum Wiederherstellen von einzelnen Active Directory- und ADAM/AD LDS-Objekten"](#) auf Seite 1446.

Backup Exec Central Admin Serverfunktion

Dieser Anhang enthält folgende Themen:

- [Infos zu Central Admin Server Feature](#)
- [Anforderungen zum Installieren von CAS](#)
- [Auswählen des Speicherorts für CAS-Speicher- und Mediendaten](#)
- [Installieren von Central Admin Server Feature](#)
- [Aktualisieren einer vorhandenen CAS-Installation](#)
- [Umwandlung eines Backup Exec-Servers in einen zentralen Administrationsserver](#)
- [Umwandlung eines Backup Exec-Servers in einen verwalteten Backup Exec-Server](#)
- [Löschen eines verwalteten Backup Exec-Servers aus einer CAS-Umgebung](#)
- [Umbenennen eines zentralen Administrationsservers](#)
- [Umbenennen eines verwalteten Backup Exec-Servers](#)
- [Reduzieren des Netzwerkverkehrs in CAS](#)
- [Mit CAS bereitgestellte, zentralisierte und replizierte Katalogspeicherorte](#)
- [Ändern der Einstellungen für einen verwalteten Backup Exec-Server](#)
- [Erreichen der CAS-Kommunikationsschwellenwerte](#)
- [Warnmeldungen und Benachrichtigungen in CAS](#)

- Aktivieren verwalteter Backup Exec-Server für die Verwendung einer verfügbaren Netzwerkkarte
- Info zur Auftragsdelegierung in CAS
- Info zum Hinzufügen von Speichergeräten in einer CAS-Umgebung
- Funktionsweise von Data Lifecycle Management (DLM) in einer CAS-Umgebung
- Abrufen von Medienüberwachungsinformationen für einen verwalteten Backup Exec-Server
- Verwenden von Backup Exec-Server-Pools in CAS
- Funktionsweise der zentralisierten Wiederherstellung in CAS
- Info zum Wiederherstellen fehlgeschlagener Aufträge in CAS
- Anhalten oder Wiederaufnehmen eines verwalteten Backup Exec-Servers
- Beenden oder Starten von Backup Exec-Diensten für einen verwalteten Backup Exec-Server
- Anzeigen von verwalteten Backup Exec-Servereigenschaften
- Anzeigen der Einstellungen für einen zentralen Administrationsserver
- Notfallwiederherstellung in CAS
- Fehlerbehebung in CAS
- Ausführen von Backup Exec Utility für CAS-Vorgänge
- Deinstallieren von Backup Exec vom zentralen Administrationsserver
- Deinstallieren von Backup Exec von einem verwalteten Backup Exec-Server

Infos zu Central Admin Server Feature

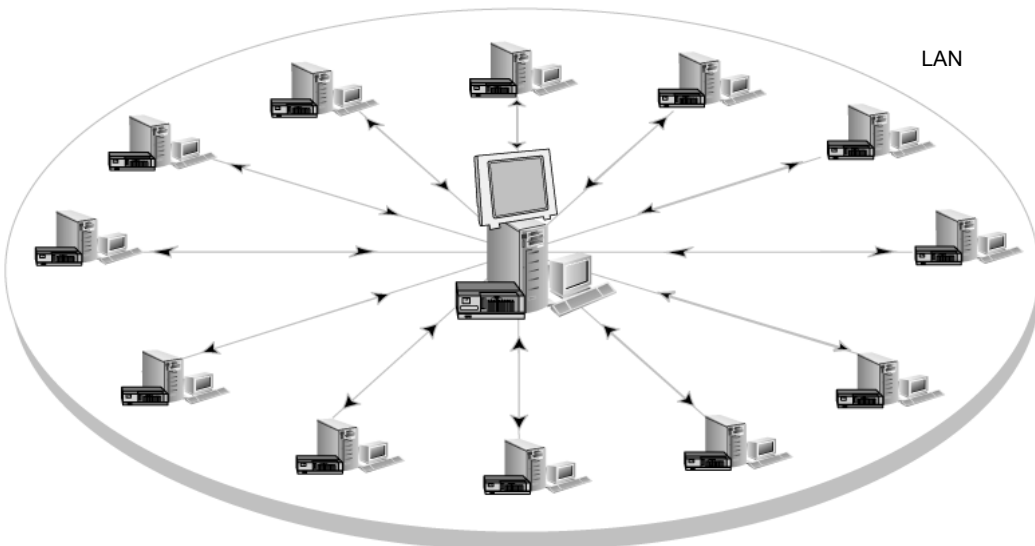
Backup Exec Central Admin Server Feature (CAS) ermöglicht, dass ein zentraler Administrationsserver Aufträge an verwaltete Backup Exec-Server im Netzwerk delegiert. Durch die Auftragsdelegierung wird für die Aufträge automatisch eine Lastverteilung auf sämtliche verfügbaren verwalteten Backup Exec-Server in der CAS-Umgebung durchgeführt. Wenn im Unternehmen mehrere Backup Exec-Server vorhanden sind, können Sie die Vorteile von CAS nutzen. Weitere Informationen dazu, welche Backup Exec-Editionen die Funktion "CAS" unterstützen, finden Sie im Preisgestaltungs- und Lizenzierungshandbuch.

Alle Backup-Informationen in der CAS-Umgebung können auf dem zentralen Administrationsserver zentralisiert werden. Die verwalteten Backup Exec-Server führen die tatsächliche Verarbeitung von Backup- und Wiederherstellungsaufträgen durch. Sie erstellen Aufträge auf dem zentralen Administrationsserver und delegieren dann die Aufträge an einen verwalteten Backup Exec-Server. Die Aufträge werden an die verfügbaren Speichergeräte auf dem verwalteten Backup Exec-Server delegiert oder verteilt. Mehrere Backup Exec-Server können ein Speichergerät gemeinsam verwenden, wenn die gemeinsame Nutzung aktiviert ist. Zentralisierte Wiederherstellungsaufträge können auch an verwaltete Backup Exec-Server delegiert werden. Darüber hinaus kann ein zentraler Administrationsserver ebenfalls als verwalteter Backup Exec-Server fungieren und delegierte Aufträge verarbeiten. Ein verwalteter Backup Exec-Server kann auch Aufträge ausführen, die lokal auf seiner Administratorkonsole erstellt werden.

Informationen zu den Best Practices zum Einsatz von Backup Exec Central Admin Server Option finden Sie unter *Best Practices für Backup Exec*.

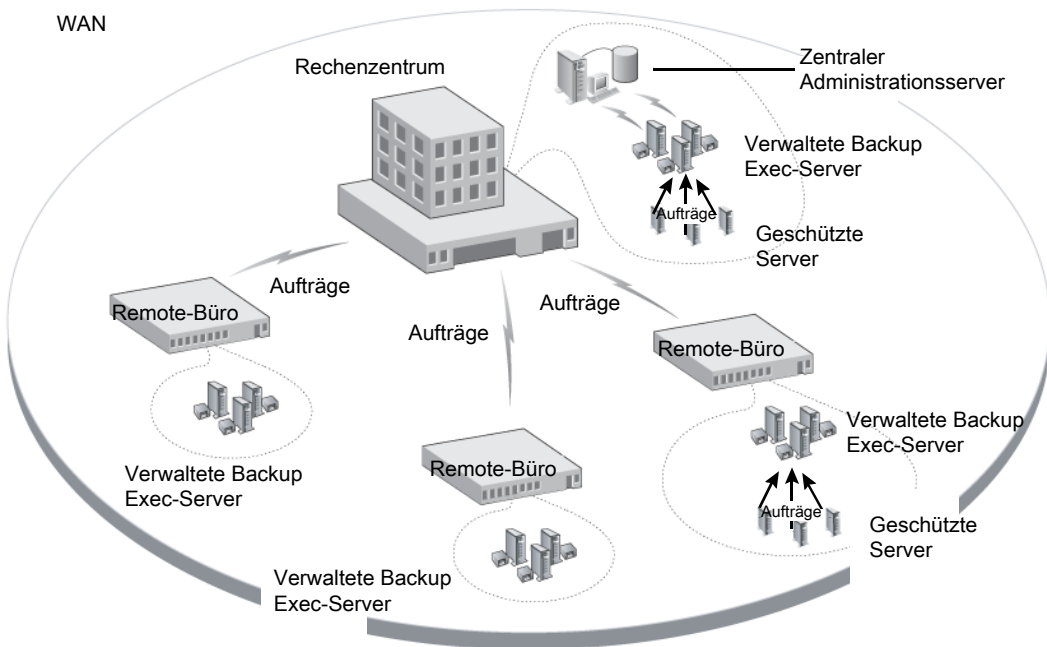
Die folgende Grafik zeigt eine LAN-Umgebung (Local Area Network) mit einem zentralen Administrationsserver und mehreren verwalteten Backup Exec-Servern.

Abbildung K-1 Mit CAS konfigurierte Backup Exec-Umgebung – LAN



Die Kommunikation, die über LAN zwischen dem zentralen Administrationsserver und den verwalteten Backup Exec-Servern erfolgt, findet auch über WAN statt.

Abbildung K-2 Mit CAS konfigurierte Backup Exec-Umgebung – WAN



Siehe ["Freigeben von Speichergeräten"](#) auf Seite 544.

Siehe ["Auswählen des Speicherorts für CAS-Speicher- und Mediendaten"](#) auf Seite 1453.

Siehe ["Installieren von Central Admin Server Feature"](#) auf Seite 1455.

Siehe ["Aktualisieren einer vorhandenen CAS-Installation"](#) auf Seite 1466.

Anforderungen zum Installieren von CAS

Die Systemanforderungen für die Central Admin Server Feature (CAS) entsprechen den Mindestanforderungen für Backup Exec mit Ausnahme des RAM. Die Anforderungen an Prozessorgeschwindigkeit, Arbeitsspeicher und Speicherplatz sind jedoch möglicherweise höher je nach Anzahl der verwalteten Backup Exec-Servern, der zu sichernden Server und des erforderlichen Katalogspeicherplatzes.

Auf dem Computer, auf dem Sie den zentralen Administrationsserver installieren, ist 1 GB RAM erforderlich, obgleich 2 GB RAM oder mehr für bessere Leistung empfohlen wird. Andere Anwendungen auf dem Backup Exec-Server erfordern

ebenfalls eine bestimmte Menge an RAM, um richtig zu funktionieren. Die Anforderungen für RAM-Kapazität können sich auch erhöhen, wenn der zentrale Administrationsserver weitere Backup Exec-Server oder Band-Hardware verwaltet.

Führen Sie vor dem Installieren von CAS folgende Schritte aus:

- Vergewissern Sie sich, dass Sie Administratorrechte auf den Computern besitzen, auf denen Sie CAS installieren möchten.
- Stellen Sie beim Installieren von CAS auf Backup Exec-Servern in mehreren Domänen sicher, dass sich das Backup Exec-Dienstkonto in der vertrauenswürdigen Domäne befindet und Administratorrechte auf allen Backup Exec-Servern besitzt, die Sie als verwaltete Backup Exec-Server verwenden möchten.
 Wird die Backup Exec-Datenbank für den zentralen Administrationsserver auf einer SQL Server-Instanz auf einem anderen Computer installiert, muss das Konto ein Domänenkonto mit lokalen administrativen Berechtigungen auch auf diesem Computer sein.
- Vergewissern Sie sich, dass der zentrale Administrationsserver und die verwalteten Backup Exec-Server Teil einer Domäne bzw. von Domänen sind. CAS wird in einer Arbeitsgruppe nicht unterstützt.
- Verwenden Sie nur NetBIOS-Computernamen für verwaltete Backup Exec-Server und zentrale Administrationsserver. Sie können keine voll qualifizierten Domännennamen oder IP-Adressen als Servernamen eingeben.
- Stellen Sie sicher, dass Sie über die entsprechenden Lizenzen für Backup Exec verfügen. Zusätzlich zu einer Lizenz für CAS ist eine Lizenz für Backup Exec erforderlich.
- Gewährleisten Sie, dass beim Installieren eines verwalteten Backup Exec-Servers der eingeloggte Benutzer und das Backup Exec-Dienstkonto für den verwalteten Backup Exec-Server Administratorrechte auf dem zentralen Administrationsserver haben.

Siehe ["Systemanforderungen für Backup Exec"](#) auf Seite 51.

Siehe ["Installieren von Central Admin Server Feature"](#) auf Seite 1455.

Auswählen des Speicherorts für CAS-Speicher- und Mediendaten

Während der Installation der Funktion eines verwalteten Backup Exec-Servers können Sie den Speicherort für Speicher- und Mediendaten des Backup Exec-Servers festlegen.

In der folgenden Tabelle wird verglichen, wie CAS-Aufgaben je nach Speicherort der Speicher- und Mediendaten des verwalteten Backup Exec-Servers ausgeführt werden:

Tabelle K-1 Vergleich von CAS-Aufgaben

Aufgabe	Speicher- und Mediendaten auf dem zentralen Administrationsserver	Speicher- und Mediendaten auf dem verwalteten Backup Exec-Server
Delegieren von Aufträgen vom zentralen Administrationsserver an den verwalteten Backup Exec-Server	Ja	Nein. Stattdessen können Sie Aufträge auf dem zentralen Administrationsserver erstellen und dann auf den verwalteten Backup Exec-Server kopieren.
Verwalten von Speichergeräten und Medien auf dem verwalteten Backup Exec-Server vom zentralen Administrationsserver aus	Ja	Nein
Anhalten, Löschen, Ausführen und Abbrechen kopierter Aufträge sowie Ändern der zugehörigen Priorität vom zentralen Administrationsserver aus, bei aktivierter Auftragsüberwachung auf dem verwalteten Backup Exec-Server	Ja	Ja
Überwachen von Aufträgen, die auf dem lokalen verwalteten Backup Exec-Server erstellt werden, falls die Option zur Überwachung von Aufträgen auf dem verwalteten Backup Exec-Server aktiviert ist	Ja	Ja

Aufgabe	Speicher- und Mediendaten auf dem zentralen Administrationsserver	Speicher- und Mediendaten auf dem verwalteten Backup Exec-Server
Senden von Auftragsstatusaktualisierungen, Auftragsprotokollen und Auftragsverläufen an den zentralen Administrationsserver bei aktivierter Auftragsüberwachungsoption auf dem verwalteten Backup Exec-Server	Ja	Ja
Zentralisieren, Verteilen oder Replizieren des Katalogs	Ja	Nein Es kann nur ein verteilter Katalogspeicherort ausgewählt werden.
Ausführen zentralisierter Wiederherstellungen	Ja	Ja Sie können die Backup-Sätze durchsuchen und vom zentralen Administrationsserver aus Wiederherstellungsvorgänge für den verwalteten Backup Exec-Server ausführen.

Hinweis: In einer CAS-Umgebung können Sie einem zentralen Administrationsserver oder einem verwalteten Backup Exec-Server nur einen NDMP-Server hinzufügen, auf dem sich die Speicher- und Mediendatenbank befindet.

Siehe ["Aktualisieren einer vorhandenen CAS-Installation"](#) auf Seite 1466.

Siehe ["Infos zu Central Admin Server Feature"](#) auf Seite 1450.

Siehe ["Ausführen von Backup Exec Utility für CAS-Vorgänge"](#) auf Seite 1516.

Installieren von Central Admin Server Feature

Die Central Admin Server Feature wird als Teil der Enterprise Server Feature installiert. Nachdem Sie die Lizenz für Backup Exec eingegeben haben, müssen

Sie im Bereich "Funktionen konfigurieren" das Element "Backup Exec-Funktionen" erweitern und dann das Element "Enterprise Server Feature", um Central Admin Server Feature zum Installieren auszuwählen. Wenn Sie die Installation von Central Admin Server Feature auswählen, wird der zentrale Administrationsserver installiert. Nach der Installation des zentralen Administrationsservers können Sie verwaltete Backup Exec-Server installieren.

Hinweis: Sie müssen zum Installieren von CAS die benutzerdefinierte Installation im Installationsassistenten verwenden. Die Standardinstallation unterstützt die Installation von CAS nicht.

Siehe ["Push-Installation eines verwalteten Backup Exec-Server vom zentralen Administrationsserver aus "](#) auf Seite 1456.

Lesen Sie vor der Installation die Hinweise zu den Speicherorten von Speicher- und Mediendaten.

Siehe ["Auswählen des Speicherorts für CAS-Speicher- und Mediendaten "](#) auf Seite 1453.

Ein verwalteter Backup Exec-Server kann außerhalb der Firewall installiert werden, in der der zentrale Administrationsserver installiert ist, oder innerhalb einer anderen Firewall. Jedoch müssen Sie einen statischen Port für SQL Server einrichten und einen Alias für den verwalteten Backup Exec-Server erstellen.

Siehe ["Installieren eines verwalteten Backup Exec-Servers über eine Firewall "](#) auf Seite 1463.

Push-Installation eines verwalteten Backup Exec-Server vom zentralen Administrationsserver aus

Nachdem Sie den zentralen Administrationsserver installiert haben, können Sie die Funktion eines verwalteten Backup Exec-Servers über eine Push-Installation auf einem eigenständigen Server installieren.

Legen Sie vor der Installation eines verwalteten Backup Exec-Servers den Speicherort für dessen Speicher- und Mediendatenbank fest. Während der Installation des verwalteten Backup Exec-Servers können Sie den Speicherort der Speicher- und Mediendaten des Backup Exec-Servers festlegen. Ihre Wahl wirkt sich auf die Art und Weise aus, wie Sie Ihre Aufträge in der CAS-Umgebung verwalten können.

Siehe ["Auswählen des Speicherorts für CAS-Speicher- und Mediendaten "](#) auf Seite 1453.

So installieren Sie einen verwalteten Backup Exec-Server über eine Push-Installation vom zentralen Administrationsserver aus

- 1** Klicken Sie auf dem zentralen Administrationsserver auf die Backup Exec-Schaltfläche und wählen Sie anschließend die Option "Installation und Lizenzierung" aus.
- 2** Wählen Sie "Agents und Backup Exec-Server auf anderen Servern installieren".
- 3** Klicken Sie im Installationsassistenten auf "Hinzufügen" und wählen Sie dann "Einzelcomputer hinzufügen" oder "Mehrere Computer mit den gleichen Einstellungen hinzufügen".
- 4** Wählen Sie "Backup Exec" und klicken auf dann "Weiter".
- 5** Geben Sie im Feld "Remote-Computer" den Namen des verwalteten Backup Exec-Servers ein, der hinzugefügt werden soll, oder klicken Sie auf "Remote-Computer durchsuchen", um den Server zu suchen.
- 6** Klicken Sie auf "Zur Liste hinzufügen".

Diese Option ist nicht erforderlich, wenn Sie in Schritt 3 "Einzelcomputer hinzufügen" ausgewählt haben.

- 7** Füllen Sie die Felder unter "Identifikationsdaten für Remote-Computer" folgendermaßen aus:

Benutzername	Geben Sie den Benutzernamen für ein Konto mit Administratorrechten auf dem Remote-Computer ein.
Kennwort	Geben Sie das Kennwort für ein Konto mit Administratorrechten auf dem Remote-Computer ein.
Domäne	Wählen Sie die Domäne des Remote-Computers.

- 8** Klicken Sie auf "Weiter".
- 9** Wählen Sie für die Eingabe der Lizenzschlüssel eine der folgenden Methoden:

So geben Sie Berechtigungs-IDs manuell ein	Geben Sie im Feld "Berechtigungs-ID eingeben" die entsprechende ID aus Ihrem Zertifikat ein und klicken Sie auf "Hinzufügen".
So importieren Sie eine Lizenzdatei	Klicken Sie auf "Lizenzdatei importieren" und navigieren Sie dann zum Speicherort Ihrer SLF-Datei.
So installieren Sie eine Testversion	Geben Sie keine Berechtigungs-IDs ein und importieren Sie keine Lizenzdateien. Fahren Sie mit dem nächsten Schritt fort.

- 10** Klicken Sie auf "Weiter".
- 11** Nachdem Ihre Berechtigungs-IDs validiert wurden, klicken Sie auf "Weiter".
- 12** Erweitern Sie in der Liste der zu installierenden Funktionen "Backup Exec " und wählen Sie dann "Verwalteter Backup Exec-Server" aus.
- 13** Sie haben folgende Möglichkeiten:

Sie möchten das Verzeichnis ändern, in dem die Backup Exec-Dateien installiert sind. Geben Sie im Feld "Zielordner" den Namen des Verzeichnisses ein.

So übernehmen Sie das Standardverzeichnis (empfohlen) Fahren Sie mit dem nächsten Schritt fort.

Es wird empfohlen, keinen Bereitstellungspunkt als Zielordner auszuwählen, da Backup Exec beim Löschen des Bereitstellungspunkts deinstalliert wird.

- 14** Klicken Sie auf "Weiter".
- 15** Geben Sie einen Benutzernamen, ein Kennwort und eine Domäne für ein Administratorenkonto ein, das die Backup Exec-Systemdienste verwenden können, und klicken Sie dann auf "Weiter".
- 16** Wählen Sie im Fenster "SQL Server auswählen" den Speicherort der Backup Exec-Datenbank aus und klicken Sie dann auf "Weiter".
- 17** Geben Sie in das Feld "Zentraler Administrationsserver" den Namen des zentralen Administrationsservers ein, der diesen verwalteten Backup Exec-Server verwalten soll.

Verwenden Sie nur NetBIOS-Computernamen für verwaltete Backup Exec-Server und zentrale Administrationsserver. Sie können keine voll qualifizierten Domännennamen oder IP-Adressen als Servernamen eingeben.

- 18** Wählen Sie eine der folgenden Optionen, um festzulegen, wie Speichergeräte und Daten verwaltet werden:

Siehe "[Optionen im Dialogfeld "Verwalteten Backup Exec-Server konfigurieren"](#)" auf Seite 1461.

Zentral verwalteter Backup Exec-Server Wählen Sie diese Option aus, damit der zentrale Administrationsserver diesen Backup Exec-Server, seine Speichergeräte, Medien und Auftragsdelegierung verwalten kann. Diese Option ermöglicht außerdem, dass der Backup Exec-Server Speichergeräte mit anderen verwalteten Backup Exec-Servern gemeinsam nutzt.

Uneingeschränkter Zugriff auf Kataloge und Backup-Sätze für Wiederherstellung Wählen Sie diese Option aus, damit dieser verwaltete Backup Exec-Server uneingeschränkten Zugriff auf alle zentral gespeicherten Kataloge hat. Diese Option legt auch fest, dass dieser verwaltete Backup Exec-Server Daten aus jedem Backup-Satz auf allen freigegebenen Speichergeräten wiederherstellt.

Diese Option kann nur ausgewählt werden, wenn die Option "Zentral verwalteter Backup Exec-Server" ausgewählt ist. Durch das Auswählen beider Optionen geben Sie dem zentralen Administrationsserver die größtmögliche Kontrolle über den verwalteten Backup Exec-Server.

Lokal verwalteter Backup Exec-Server Wählen Sie diese Option aus, damit der zentrale Administrationsserver diesen verwalteten Backup Exec-Server überwachen und Wiederherstellungsaufträge für ihn erstellen kann. Jedoch werden der Server und seine Geräte, Medien und Backup-Aufträge lokal gesteuert.

- 19** Klicken Sie auf "Weiter".
- 20** Wählen Sie die gewünschten Gerätetreiber aus und klicken Sie auf "Weiter".
- 21** Wenn die Remote-Computer von Backup Exec validiert wurden, können Sie die Liste wie folgt ändern:

So fügen Sie einen Remote-Computer manuell hinzu	Klicken Sie auf "Hinzufügen" und dann auf "Einzelserver hinzufügen".
So fügen Sie mehrere Remote-Computer manuell hinzu	Klicken Sie auf "Hinzufügen" und dann auf "Mehrere Server mit den gleichen Einstellungen hinzufügen".
So fügen Sie mehrere Remote-Computer durch das Importieren einer vorhandenen Liste der Computer hinzu	<p>Klicken Sie auf "Importieren und exportieren", und wählen Sie dann eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> ■ Wählen Sie "Aus Datei importieren", um Backup Exec zum Hinzufügen der Namen der Remote-Computer aus einer ausgewählten Liste zu aktivieren. ■ Wählen Sie "Auf diesem Backup Exec-Server veröffentlichte Server importieren", damit Backup Exec die Namen aller Remote-Computer hinzufügen kann, die für die Veröffentlichung auf diesem Backup Exec-Server eingerichtet sind. <p>Sie müssen Remote-Computer-Identifikationsdaten für die Liste der Remote-Computer eingeben.</p>
So ändern Sie das Produkt, das Sie zum Installieren oder Ändern anderer Installationseigenschaften ausgewählt haben	Wählen Sie den Remote-Computer aus, den Sie ändern möchten, und klicken Sie dann auf "Bearbeiten".
So löschen Sie einen Remote-Computer aus der Liste	Wählen Sie den Remote-Computer aus, den Sie löschen möchten, und klicken Sie dann auf "Löschen".
So sichern Sie die Liste der Remote-Computer und der verbundenen Remote-Computer-Identifikationsdaten	<p>Überprüfen Sie, dass "Serverliste für zukünftige Remote-Installationssitzungen speichern" markiert ist.</p> <p>Diese Option aktiviert die Namen aller automatisch hinzugefügten Remote-Computer und ihrer Identifikationsdaten, wenn Sie Backup Exec oder Optionen auf diesen Remote-Computern installieren möchten.</p>

So speichern Sie diese Liste der Remote-Computer in einer XML-Datei

Klicken Sie auf "Importieren und exportieren" und klicken Sie dann auf "In Datei exportieren".

Sie können den Speicherort auswählen, um die XML-Datei zu speichern. Diese Option ist nützlich, wenn Sie dieselbe Liste für mehrere Backup Exec-Server benutzen möchten. Wenn Sie die Liste importieren, müssen Sie die Remote-Computer-Identifikationsdaten erneut eingeben.

So beheben Sie die Fehler, die während der Validierung gefunden wurden

Klicken Sie mit der rechten Maustaste auf den Namen des Computers und klicken Sie dann auf "Fehler beheben".

So aktivieren Sie Backup Exec, um einen ungültigen Remote-Computer erneut zu validieren

Klicken Sie mit der rechten Maustaste auf den Namen des Computers, und klicken Sie dann auf Validierung erneut vornehmen.

22 Nachdem alle Computer validiert wurden, klicken Sie auf "Weiter".

23 Lesen Sie die Backup Exec-Installationszusammenfassung und klicken Sie dann auf "Installieren".

24 Klicken Sie auf "Weiter", und klicken Sie dann auf "Fertigstellen".

Wenn Sie den Remote-Computer noch nicht neu gestartet haben, müssen Sie den Neustart jetzt durchführen, damit die Konfigurationseinstellungen wirksam werden.

Optionen im Dialogfeld "Verwalteten Backup Exec-Server konfigurieren"

Die folgenden Informationen können Ihnen helfen, zu entscheiden, welche Konfigurationsoptionen Sie bei der Installation eines verwalteten Backup Exec-Servers wählen sollten.

Die folgenden Informationen treffen zu, wenn Sie die Optionen "Zentral verwalteter Backup Exec-Server" und "Uneingeschränkter Zugriff auf Kataloge und Backup-Sätze für Wiederherstellung" auswählen:

- Dieser Backup Exec-Server wird ein verwalteter Backup Exec-Server.
- Eine dauerhafte Netzwerkverbindung zwischen dem verwalteten Backup Exec-Server und dem zentralen Administrationsserver ist erforderlich.

- Die Kataloge werden zentralisiert und auf dem zentralen Administrationsserver gespeichert. Beachten Sie, dass diese Kombination von Optionen möglicherweise nicht geeignet ist, wenn Sie eine Netzwerkverbindung mit niedriger Bandbreite zum zentralen Administrationsserver haben.
- Dieser verwaltete Backup Exec-Server kann auf Backup-Sätze für alle Speichergeräte zugreifen, die er mit anderen Backup Exec-Servern gemeinsam nutzt, und diese auch wiederherstellen.

Hinweis: Ein verwalteter Backup Exec-Server, der mit dem Katalogmodus als "zentralisiert unbeschränkt" konfiguriert wurde, kann nur eigene Sätze durchsuchen. Backup-Sätze, die von anderen verwalteten Backup Exec-Servern oder dem zentralen Administrationsserver erstellt wurden, können nicht durchsucht werden.

- Für die Backup-Aufträge, die auf dem zentralen Administrationsserver erstellt werden, ist eine Lastverteilung möglich, und sie können an diesen verwalteten Backup Exec-Server weitergeleitet werden.
- Ein paralleles Upgrade kann mit dieser Konfiguration nicht durchgeführt werden. Dieser verwaltete Backup Exec-Server muss zur gleichen Zeit wie der zentrale Administrationsserver aktualisiert werden.

Die folgenden Informationen gelten, wenn Sie die Option "Zentral verwalteter Backup Exec-Server", aber nicht die Option "Uneingeschränkter Zugriff auf Kataloge und Backup-Sätze für Wiederherstellung" auswählen:

- Dieser Backup Exec-Server wird ein verwalteter Backup Exec-Server.
- Eine dauerhafte Netzwerkverbindung zwischen dem verwalteten Backup Exec-Server und dem zentralen Administrationsserver ist erforderlich.
- Die Kataloge sind standardmäßig im verteilten Modus, können aber geändert werden. Die Kataloge für die Aufträge, die auf diesen verwalteten Backup Exec-Server ausgeführt werden, werden lokal gespeichert.
- Dieser verwaltete Backup Exec-Server kann auf alle Backup-Sätze zugreifen, die auf den Speichergeräten gespeichert sind, die er hostet, und diese auch wiederherstellen. Es spielt dabei keine Rolle, welcher Backup Exec-Server den Backup-Auftrag ausgeführt hat. Für die Geräte mit gemeinsam genutzten Speicher, die andere Backup Exec-Server hosten, kann dieser verwaltete Backup Exec-Server jedoch nur auf die Backup-Sätze zugreifen, die von ihm ausgeführten Backup-Aufträgen erstellt wurden, und diese auch wiederherstellen.
- Für die Backup-Aufträge, die auf dem zentralen Administrationsserver erstellt werden, ist eine Lastverteilung möglich, und sie können an diesen verwalteten Backup Exec-Server weitergeleitet werden.

- Es wird empfohlen, diese Option bei der privaten Cloud-Konfiguration zu verwenden.

Die folgenden Informationen treffen zu, wenn Sie die Option "Lokal verwalteter Backup Exec-Server" auswählen:

- Dieser Backup Exec-Server wird ein verwalteter Backup Exec-Server.
- Eine dauerhafte Netzwerkverbindung zwischen dem verwalteten Backup Exec-Server und dem zentralen Administrationsserver ist nicht erforderlich. Daher kann diese Option nützlich sein, wenn eine Verbindung mit sehr niedriger Bandbreite zwischen dem verwalteten Backup Exec-Server und dem zentralen Administrationsserver besteht. Sie ist möglicherweise auch nützlich, wenn der verwaltete Backup Exec-Server nicht immer eine Verbindung zum zentralen Administrationsserver herstellen kann.
- Die Kataloge sind standardmäßig im verteilten Modus. Die Kataloge für die Aufträge, die auf diesen verwalteten Backup Exec-Server ausgeführt werden, werden lokal gespeichert.
- Der zentrale Administrationsserver leitet Aufträge nicht an diesen verwalteten Backup Exec-Server weiter.
- Dieser verwaltete Backup Exec-Server kann nicht in einer privaten Cloud-Konfiguration verwendet werden

Siehe ["Push-Installation eines verwalteten Backup Exec-Server vom zentralen Administrationsserver aus "](#) auf Seite 1456.

Installieren eines verwalteten Backup Exec-Servers über eine Firewall

Ein verwalteter Backup Exec-Server kann außerhalb der Firewall installiert werden, in der der zentrale Administrationsserver installiert ist, oder innerhalb einer anderen Firewall.

Folgende Regeln gelten für die verwalteten Backup Exec-Server, die über eine Firewall installiert werden:

- Port 3527 muss in beide Richtungen offen sein, um eine Verbindung für den Backup Exec-Serverdienst zu ermöglichen.
- Port 10000 muss für Agent for Windows geöffnet sein, um das Suchen nach Remote-Auswahlen zu ermöglichen.
- Es muss ein in beide Richtungen offener SQL-Anschluss zur Datenbank des Administrationsservers vorliegen, um Datenbankverbindungen zu ermöglichen.
- Es muss ein statischer Anschluss verwendet werden.

Die Backup Exec-SQL-Instanz wird standardmäßig zur Verwendung eines dynamischen Ports konfiguriert. Die Portnummer kann sich bei jedem Start des

SQL-Servers ändern. Der dynamische Port muss in einen statischen Port geändert werden. Nach der Änderung der Port-Konfiguration von dynamisch zu statisch muss der statische Port der Windows-Firewall-Liste für Ausnahmen hinzugefügt werden.

Informationen hierzu erhalten Sie in der Dokumentation zu Ihrem Windows-Betriebssystem.

Siehe ["So ändern Sie den dynamischen Port einer SQL Express-Instanz in einen statischen Port und erstellen einen Alias für den verwalteten Backup Exec-Server"](#) auf Seite 1464.

Siehe ["So öffnen Sie einen SQL-Port für ein SQL 2008-Instanz und erstellen einen Alias für einen verwalteten Backup Exec-Server"](#) auf Seite 1465.

So ändern Sie den dynamischen Port einer SQL Express-Instanz in einen statischen Port und erstellen einen Alias für den verwalteten Backup Exec-Server

- 1 Klicken Sie auf dem zentralen Administrationsserver auf "Start > Alle Programme > Microsoft SQL Server 2014 > Konfigurationstools > SQL Server Configuration Manager".
- 2 Erweitern Sie "SQL Server -Netzwerkconfiguration".
- 3 Klicken Sie auf "Protokolle für BKUPEXEC" und führen Sie im rechten Teilfenster einen Doppelklick auf "TCP/IP" aus.
- 4 Klicken Sie im Dialogfeld "TCP/IP-Eigenschaften" auf die Registerkarte "IP-Adressen".
- 5 Entfernen Sie in "TCP Dynamische Ports" unter "IPAll" den Wert und lassen Sie das Feld leer.
- 6 Geben Sie unter "IPAll" in "TCP-Port" eine Port-Nummer ein.
Die Port-Nummer kann zwischen 1025 und 65535 liegen und darf nicht von einer anderen Anwendung verwendet werden.
- 7 Ändern Sie unter der Überschrift der verwendeten spezifischen Netzwerkkarte (z. B. IP1 oder IP2) den Eintrag unter "Aktiviert" von "Nein" zu "Ja".
- 8 Entfernen Sie in "TCP Dynamische Ports" unter derselben Überschrift den Wert "0" und geben Sie die gleiche Port-Nummer ein, die Sie für den TCP-Port eingegeben haben.
- 9 Klicken Sie auf "Übernehmen".
- 10 Starten Sie Backup Exec und die SQL-Dienste neu.
- 11 Klicken Sie auf dem verwalteten Backup Exec-Server auf "Start > Alle Programme > Microsoft SQL Server 2014 > Konfigurationstools > SQL Server Configuration Manager".

- 12 Erweitern Sie "SQL Native Client-Konfiguration".
- 13 Klicken Sie auf "Aliase" und doppelklicken Sie auf den Aliasnamen, der den Namen des zentralen Administrationsservers und der Backup Exec-SQL-Instanz enthält.
- 14 Geben Sie im Dialogfeld "Aliaseigenschaften" die erforderlichen Informationen entsprechend der folgenden Tabelle ein:

Aliasname	Geben Sie den Namen des zentralen Administrationsservers und der Backup Exec-SQL-Instanz im Format "Servername\Instanzname" ein.
Port-Nummer	Geben Sie die Port-Nummer der Remote-Backup Exec-SQL Server-Instanz ein, die Sie sich zuvor notiert haben.
Protokoll	Wählen Sie "TCP/IP".
Server	Geben Sie den Namen des zentralen Administrationsservers und der Backup Exec-SQL-Instanz im Format "Servername\Instanzname" ein.

- 15 Klicken Sie auf "Übernehmen" und dann auf "OK".
- 16 Schließen Sie das Dienstprogramm "SQL Server Configuration Manager".

So öffnen Sie einen SQL-Port für ein SQL 2008-Instanz und erstellen einen Alias für einen verwalteten Backup Exec-Server

- 1 Klicken Sie auf dem zentralen Administrationsserver auf "Start > Alle Programme > Microsoft SQL Server 2014 > Konfigurationstools > SQL Server Configuration Manager".
- 2 Erweitern Sie "SQL Server-Netzwerkkonfiguration" und klicken Sie dann auf "Protokolle" für die SQL Server-Instanz, die durch den zentralen Administrationsserver verwendet wird.
- 3 Wählen Sie unter "Aktivierte Protokolle" die Option "TCP/IP" aus und klicken Sie auf "Eigenschaften".
- 4 Doppelklicken Sie auf "TCP/IP" und klicken Sie anschließend auf die Registerkarte "IP-Adressen".
- 5 Notieren Sie die dynamische TCP-Portnummer.
- 6 Gehen Sie zur Erstellung eines Alias für den verwalteten Backup Exec-Server auf diesem zu "`%SystemRoot%\System32`" und doppelklicken Sie auf "`cliconfg.exe`".
- 7 Klicken Sie auf der Registerkarte "Alias" auf "Hinzufügen".

- 8 Geben Sie im Feld "Serveralias" Folgendes ein: "*Servername\Instanzname*"
- 9 Wählen Sie unter "Netzwerkbibliotheken" die Option "TCP/IP".
- 10 Geben Sie im Feld "Servername" Folgendes ein: "*Servername\Instanzname*"
- 11 Heben Sie die Markierung von "Anschluss dynamisch bestimmen" auf.
- 12 Geben Sie im Feld "Portnummer" die Portnummer für die Remote Backup Exec-SQLServer-Instanz ein.

Aktualisieren einer vorhandenen CAS-Installation

Aktualisieren Sie in einer bestehenden CAS-Umgebung den zentralen Administrationsserver und anschließend die verwalteten Backup Exec-Server. Sie können aus Backup Exec 2014 oder höher aktualisieren.

Falls erforderlich, können Sie in der CAS-Umgebung parallele Aktualisierungen vornehmen. Sie können mithilfe eines parallelen Upgrades über einen Zeitraum hinweg zuerst den zentralen Administrationsserver und dann die verwalteten Backup Exec-Server von der vorherigen auf die aktuelle Version aktualisieren. Beachten Sie, dass ein rollendes Upgrade nur aus Backup Exec 16 Feature Pack 2 oder höher durchgeführt werden kann. Rollende Upgrades werden in Versionen vor Backup Exec 15 nicht unterstützt. Sie müssen zum Durchführen von parallelen Aktualisierungen das aktuellste Backup Exec-Service Pack installiert haben.

Hinweis: Aufwärtskompatibilität wird bei parallelen Aktualisierungen nicht unterstützt. Deshalb kann kein System, das die vorherige Version ausführt, ein System nicht schützen, das die aktuelle Version ausführt.

Es wird empfohlen, in einer CAS-Installation längerfristig keine gemischten Versionen zu verwenden. In einer Umgebung mit gemischten Versionen fehlt die Hauptfunktion für die Verwaltung verwalteter Backup Exec-Server. Die Fähigkeit, die CAS-Umgebung ordnungsgemäß zu verwalten, wird dadurch beeinträchtigt.

Hinweis: Benennen Sie keine verwalteten Backup Exec-Server oder den zentralen Administrationsserver während des Upgrade-Vorgangs um. Obgleich Sie die Server vor einem Upgrade umbenennen können, sollten Sie sie umbenennen, nachdem das Upgrade abgeschlossen ist.

Nachdem Sie eine Aktualisierung des zentralen Administrationsservers auf die aktuelle Version durchgeführt haben, werden die folgenden Vorgänge auf verwalteten Backup Exec-Servern unterstützt, die die vorherige Version ausführen:

- Backup

- Wiederherstellung
- Inventarisierung
- Katalog

So aktualisieren Sie eine vorhandene CAS-Installation

- 1** Stellen Sie sicher, dass das neueste Service Pack für Backup Exec installiert ist.
- 2** Halten Sie alle geplanten Aufträge auf dem zentralen Administrationsserver und den verwalteten Backup Exec-Servern an.
Siehe ["Aufträge anhalten"](#) auf Seite 292.
- 3** Lassen Sie alle aktiven Aufträge zu einem Ende kommen.
- 4** Führen Sie einen Datenbankwartungsauftrag aus, um nicht mehr benötigte Auftragsverläufe und Kataloge zu löschen und die Aktualisierungsdauer somit zu verkürzen.
- 5** Beenden Sie alle Backup Exec-Dienste auf jedem verwalteten Backup Exec-Server.
- 6** Wählen Sie im Installationsmedien-Browser die Option für die Installation von Backup Exec aus.
- 7** Klicken Sie im Begrüßungsbildschirm auf "Weiter".
- 8** Wählen Sie "Ich nehme die Bedingungen der Lizenzvereinbarung an" aus, und klicken Sie anschließend auf "Weiter".
- 9** Aktivieren Sie die Option "Lokale Installation" und klicken Sie anschließend auf "Backup Exec-Software und -Funktionen installieren".
- 10** Klicken Sie auf "Weiter".
- 11** Folgen Sie den Aufforderungen im Assistenten.
- 12** Geben Sie auf der Seite "Bestehende Daten und Kataloge sichern" ein Verzeichnis ein oder wählen Sie ein Verzeichnis aus, in dem alle vorhandenen Kataloge und Daten gesichert werden sollen. Standardmäßig wird folgendes Verzeichnis verwendet:

`C:<Backup Exec install path>\Backup Exec\Data`

Klicken Sie auf "Ältere Daten und Kataloge nicht sichern", wenn frühere Kataloge und Daten nicht beibehalten werden sollen.

- 13** Klicken Sie zum Fortfahren auf "Weiter".

Eine Übersicht der Aktualisierung wird angezeigt. Nach Beendigung der Aktualisierung wird die Kommunikation mit den verwalteten Backup Exec-Servern automatisch aktiviert.

- 14** Nehmen Sie alle Aufträge aus der Wartestellung.

Siehe ["Aufheben der Wartestellung von Aufträgen"](#) auf Seite 294.

- 15** Aktualisieren Sie einige oder alle verwalteten Backup Exec-Server.

Hinweis: Wenn Sie den zentralen Administrationsserver von Backup Exec 16 Feature Pack 2 auf Backup Exec aktualisieren und einige der verwalteten Backup Exec-Servers vorher nicht gesichert wurden, werden diese erst dann auf der Registerkarte "Backup und Wiederherstellung" angezeigt, wenn Sie sie auf Backup Exec 16 Feature Pack 2 aktualisieren oder sie unter Verwendung des Assistenten "Server hinzufügen" manuell hinzufügen.

Siehe ["Mit CAS bereitgestellte, zentralisierte und replizierte Katalogspeicherorte"](#) auf Seite 1476.

Siehe ["Ändern der Einstellungen für einen verwalteten Backup Exec-Server"](#) auf Seite 1479.

Umwandlung eines Backup Exec-Servers in einen zentralen Administrationsserver

Sie können einen eigenständigen Backup Exec-Server in einen zentralen Administrationsserver umwandeln.

So wandeln Sie einen Backup Exec-Server in einen zentralen Administrationsserver um

- 1** Starten Sie Backup Exec auf dem Backup Exec-Server, den Sie in einen zentralen Administrationsserver umwandeln möchten.
- 2** Klicken Sie auf die Backup Exec-Schaltfläche und dann auf "Installation und Lizenzierung" und "Funktionen und Lizenzen auf diesem Backup Exec-Server installieren".
- 3** Wählen Sie eine der folgenden Methoden aus, um Lizenzen einzugeben:

So geben Sie Lizenzen
manuell ein

Gehen Sie dazu in folgender Reihenfolge vor:

- Geben Sie im Feld "Berechtigungs-ID eingeben" eine ID ein.
- Klicken Sie auf "Zur Liste hinzufügen".
- Wiederholen Sie diesen Vorgang für jede Berechtigungs-ID der einzelnen Funktionen oder Agents, die Sie hinzufügen möchten.

So importieren Sie Lizenzen
aus einer Datei

Gehen Sie dazu in folgender Reihenfolge vor:

- Klicken Sie auf "Lizenzdatei importieren".
- Wählen Sie die Lizenzdatei aus.

So installieren Sie eine
Testversion

Fahren Sie mit dem nächsten Schritt fort.

Für die vollständig funktionsfähige Testversion ist kein Lizenzschlüssel erforderlich.

- 4 Klicken Sie auf "Weiter".
- 5 Erweitern Sie in der Liste von Funktionen "Backup Exec-Optionen", erweitern Sie "Enterprise Server Feature" und wählen Sie dann "Central Admin Server Feature".
- 6 Klicken Sie auf "Weiter".
- 7 Lesen Sie die Backup Exec-Installationszusammenfassung und klicken Sie dann auf "Installieren".
- 8 Klicken Sie auf "Fertigstellen".

Siehe ["Umwandlung eines Backup Exec-Servers in einen verwalteten Backup Exec-Server"](#) auf Seite 1469.

Umwandlung eines Backup Exec-Servers in einen verwalteten Backup Exec-Server

Um einen Backup Exec-Server in einen verwalteten Backup Exec-Server zu ändern, legen Sie den zentralen Administrationsserver fest, der den Backup Exec-Server verwalten soll.

Wird der verwaltete Backup Exec-Server nach dem Befolgen dieser Anweisungen nicht auf der Registerkarte "Speicher" angezeigt und ist Ihr Netzwerk mit Firewalls ausgestattet, müssen Sie möglicherweise Ports zwischen dem zentralen Administrationsserver und dem verwalteten Backup Exec-Server öffnen.

So wandeln Sie einen Backup Exec-Server in einen verwalteten Backup Exec-Server um

- 1** Klicken Sie bei dem eigenständigen Backup Exec-Server auf die Schaltfläche "Backup Exec" und wählen Sie zuerst "Installation und Lizenzierung" und dann "Funktionen und Lizenzen auf diesem Backup Exec-Server installieren".
- 2** Klicken Sie im Bereich "Lizenzen hinzufügen" auf "Weiter".
- 3** Wählen Sie im Bereich "Funktionen konfigurieren", unter "Backup Exec " die Option "Verwalteter Backup Exec-Server" aus und klicken Sie dann auf "Weiter".
- 4** Wenn Sie aufgefordert werden, eine zusätzliche Sprache auszuwählen, klicken Sie auf "Weiter".
- 5** Geben Sie den Namen des zentralen Administrationsservers ein, der diesen Backup Exec-Server verwalten soll.

- 6** Wählen Sie unter "Verwaltete Backup Exec-Server-Konfiguration" die entsprechende Option aus und klicken Sie dann auf "Weiter".

Zentral verwalteter Backup Exec-Server	Wählen Sie diese Option aus, damit der zentrale Administrationsserver diesen Backup Exec-Server, seine Speichergeräte, Medien und Auftragsdelegierung verwalten kann. Diese Option ermöglicht außerdem, dass der Backup Exec-Server Speichergeräte mit anderen verwalteten Backup Exec-Servern gemeinsam nutzt.
Uneingeschränkter Zugriff auf Kataloge und Backup-Sätze für Wiederherstellung	<p>Wählen Sie diese Option aus, damit dieser verwaltete Backup Exec-Server uneingeschränkten Zugriff auf alle zentral gespeicherten Kataloge hat. Diese Option legt auch fest, dass dieser verwaltete Backup Exec-Server Daten aus jedem Backup-Satz auf allen freigegebenen Speichergeräten wiederherstellt.</p> <p>Diese Option kann nur ausgewählt werden, wenn die Option "Zentral verwalteter Backup Exec-Server" ausgewählt ist. Durch das Auswählen beider Optionen geben Sie dem zentralen Administrationsserver die größtmögliche Kontrolle über den verwalteten Backup Exec-Server.</p>
Lokal verwalteter Backup Exec-Server	Wählen Sie diese Option aus, damit der zentrale Administrationsserver diesen verwalteten Backup Exec-Server überwachen und Wiederherstellungsaufträge für ihn erstellen kann. Jedoch werden der Server und seine Geräte, Medien und Backup-Aufträge lokal gesteuert.

- 7** Klicken Sie auf "Installieren".
- 8** Klicken Sie auf "Fertigstellen", sobald die Installation abgeschlossen ist.

Siehe ["Umwandlung eines Backup Exec-Servers in einen zentralen Administrationsserver"](#) auf Seite 1468.

Löschen eines verwalteten Backup Exec-Servers aus einer CAS-Umgebung

Wenn Verbindungen zwischen dem verwalteten Backup Exec-Server und dem zentralen Administrationsserver noch aktiv sind, können Sie einen verwalteten Backup Exec-Server entfernen, indem Sie ihn von der Registerkarte "Speicher" löschen. Wenn Sie einen verwalteten Backup Exec-Server aus der Registerkarte "Speicher" löschen, wird der Server in einen eigenständigen Backup Exec-Server geändert. Nachdem der verwaltete Backup Exec-Server aus der CAS-Umgebung entfernt ist, verbleibt er weiterhin auf der Liste von Servern auf der Registerkarte "Backup und Wiederherstellung", also kann er als eigenständiger Server noch gesichert werden und wiederhergestellt werden.

Hinweis: Wenn der zentrale Administrationsserver einen Systemausfall erfährt, gehen die Verbindungen zwischen dem verwalteten Backup Exec-Server und dem zentralen Administrationsserver verloren. Der verwaltete Backup Exec-Server kann nicht von der Registerkarte "Speicher" gelöscht werden. Jedoch können Sie den verwalteten Backup Exec-Server in einen eigenständigen Backup Exec-Server ändern, indem Sie die Windows-Funktion "Programm ändern" verwenden.

Siehe ["Notfallwiederherstellung in CAS"](#) auf Seite 1513.

So löschen Sie einen verwalteten Backup Exec-Server aus einer CAS-Umgebung

- 1 Wenn die Speichergeräte auf dem verwalteten Backup Exec-Server, der gelöscht werden soll, gemeinsam mit anderen verwalteten Backup Exec-Servern genutzt werden, klicken Sie auf der Registerkarte "Speicher" mit der rechten Maustaste auf das Gerät und anschließend auf "Freigabe". Deaktivieren Sie die Server, die das Gerät gemeinsam nutzen.

Sie müssen den Freigabeverweis entfernen, um das Überschreiben der Medien zu vermeiden.

Hinweis: Wenn bestimmte Geräte von Fibre Channel-SAN gemeinsam genutzt werden, trennen Sie die Geräte auf dem verwalteten Backup Exec-Server, bevor Sie sie löschen.

- 2 Klicken Sie auf der Registerkarte "Speicher" des zentralen Administrationsservers mit der rechten Maustaste auf den verwalteten Backup Exec-Server, den Sie aus der CAS-Umgebung löschen und in einen eigenständigen Backup Exec-Server konvertieren möchten.

- 3 Wählen Sie die Option "Löschen".
- 4 Klicken Sie auf "Ja", um zu bestätigen, dass Sie den Server in einen eigenständigen Backup Exec-Server konvertieren möchten.
- 5 Nachdem Sie eine Warnmeldung auf dem zentralen Administrationsserver erhalten, der den Löschvorgang des Servers bestätigt, starten Sie den Server, der in einen eigenständigen Backup Exec-Server umgewandelt wurde, neu.

Hinweis: Wenn Backup Exec nicht in der Lage ist, die Anfrage abzuschließen, können Sie den Verweis auf dem verwalteten Backup Exec-Server aus der Datenbank des zentralen Administrationsservers entfernen. Wenn der verwaltete Backup Exec-Server dann wieder online ist, fügt Backup Exec automatisch den verwalteten Backup Exec-Server wieder der Datenbank des zentralen Administrationsservers hinzu. Zu diesem Zeitpunkt können Sie dieses Verfahren wiederholen.

Siehe ["Umwandlung eines Backup Exec-Servers in einen verwalteten Backup Exec-Server"](#) auf Seite 1469.

Umbenennen eines zentralen Administrationsservers

Wenn Sie einen Server sichern und dann umbenennen, werden sowohl der neue als auch der alte Servername auf der Registerkarte "Backup und Wiederherstellung" angezeigt. Klicken Sie auf das Symbol mit dem alten Servernamen, um Daten wiederherzustellen, die Sie gesichert haben, bevor der Servername geändert wurde. Klicken Sie auf das Symbol mit dem neuen Servernamen, um Daten wiederherzustellen, die Sie gesichert haben, nachdem der Servername geändert wurde.

Nachdem Sie einen zentralen Administrationsserver umbenannt haben, verwendet der Katalogordner den neuen Server. Die "Katalogselbstheilung", ein automatischer Vorgang, ändert die Katalogdateien auf dem Server und die Katalogmetadaten in der Backup Exec-Datenbank.

Hinweis: Wenn Sie einen zentralen Administrationsserver umbenennen möchten, mit dem keine verwalteten Backup Exec-Server verknüpft sind, brauchen Sie diesen Vorgang nicht durchzuführen. Stattdessen können Sie Standardfunktion von Windows zum Umbenennen verwenden.

So benennen Sie einen zentralen Administrationsserver um

- 1 Klicken Sie auf dem zentralen Administrationsserver auf der Registerkarte "Speicher" mit der rechten Maustaste auf einen verwalteten Backup Exec-Server und klicken Sie auf "Löschen".

Der verwaltete Backup Exec-Server wird nicht aus Backup Exec gelöscht. Er wird nur aus der CAS-Umgebung gelöscht, und wird ein eigenständiger Backup Exec-Server.

- 2 Wiederholen Sie Schritt 1 für jeden verwalteten Backup Exec-Server, der vom zentralen Administrationsserver verwaltet wird.
- 3 Verwenden Sie zum Umbenennen des Servers die entsprechende Standardfunktion von Windows.
- 4 Um den verwalteten Backup Exec-Server wieder mit dem zentralen Administrationsserver zu verbinden, installieren Sie die verwaltete Backup Exec-Serverfunktion auf den Servern, die aus der Registerkarte "Speicher" gelöscht wurden.

Hinweis: Starten Sie den Server neu, wenn die Installation abgeschlossen ist.

- 5 Überprüfen Sie, ob die verwalteten Backup Exec-Server wieder mit dem umbenannten zentralen Administrationsserver verbunden ist.

Umbenennen eines verwalteten Backup Exec-Servers

Bevor Sie einen verwalteten Backup Exec-Server umbenennen können, müssen Sie ihn aus der CAS-Umgebung löschen, damit er ein eigenständiger Backup Exec-Server wird. Nachdem Sie den Server umbenannt haben, müssen Sie die verwaltete Backup Exec-Funktion auf dem Server erneut installieren und dann alle Aufträge auf den neuen verwalteten Backup Exec-Server umleiten.

Wenn Sie einen Server sichern und dann umbenennen, werden sowohl der neue als auch der alte Servername auf der Registerkarte "Backup und Wiederherstellung" angezeigt. Klicken Sie auf das Symbol mit dem alten Servernamen, um Daten wiederherzustellen, die Sie gesichert haben, bevor der Servername geändert wurde. Klicken Sie auf das Symbol mit dem neuen Servernamen, um Daten wiederherzustellen, die Sie gesichert haben, nachdem der Servername geändert wurde.

Nachdem Sie einen verwalteten Backup Exec-Server umbenannt haben, verwendet der Katalogordner den neuen verwalteten Backup Exec-Server. Die

"Katalogselbstheilung", ein automatischer Vorgang, ändert die Katalogdateien auf dem Server und die Katalogmetadaten in der Backup Exec-Datenbank.

So benennen Sie einen verwalteten Backup Exec-Server um

- 1** Klicken Sie auf dem zentralen Administrationsserver auf der Registerkarte "Speicher" mit der rechten Maustaste auf den verwalteten Backup Exec-Server, den Sie umbenennen möchten.
- 2** Klicken Sie auf "Löschen", um den verwalteten Backup Exec-Server aus der CAS-Umgebung zu löschen.

Der verwaltete Backup Exec-Server wird nicht aus Backup Exec gelöscht. Er wird nur aus der CAS-Umgebung gelöscht, und wird ein eigenständiger Backup Exec-Server. Der Server muss aus der CAS-Umgebung entfernt werden, bevor er umbenannt werden kann.

- 3** Starten Sie die Dienste auf dem Server neu, den Sie umbenennen möchten.
- 4** Verwenden Sie zum Umbenennen des Servers die entsprechende Standardfunktion von Windows.
- 5** Starten Sie den Server neu.

Nachdem der Server neu gestartet wurde, fordert Sie Backup Exec möglicherweise auf, die Backup Exec-Dienste und die Backup Exec-Deduplizierungsdienste neu zu starten. Sie müssen im Dialogfeld "Backup Exec-Dienstmanager" einen neuen Servernamen wählen.

- 6** Um den Server mit dem zentralen Administrationsserver zu verbinden, installieren Sie den verwalteten Backup Exec-Server auf dem umbenannten Server.

Hinweis: Starten Sie den Server neu, wenn die Installation abgeschlossen ist.

- 7** Überprüfen Sie, ob der umbenannte verwaltete Backup Exec-Server wieder mit dem zentralen Administrationsserver verbunden ist.
- 8** Leiten Sie alle Aufträge, die vor der Umbenennung mit dem verwalteten Backup Exec-Server verknüpft waren, auf den umbenannten Server um.

Reduzieren des Netzwerkverkehrs in CAS

Um eine Netzwerkverbindung mit geringer Bandbreite nutzen zu können oder den Netzwerkverkehr zu verringern, stehen Ihnen folgende Möglichkeiten zur Verfügung:

- Verringern der Häufigkeit, mit der Aktualisierungen des Auftragsstatus von den verwalteten Backup Exec-Servern an den zentralen Administrationsserver gesendet werden
- Verhindern, dass der zentrale Administrationsserver die Aufträge überwacht, die auf den lokalen verwalteten Backup Exec-Servern erstellt werden.
- Verringern der Häufigkeit, mit der Auftragsprotokolle und -verläufe von den verwalteten Backup Exec-Servern an den zentralen Administrationsserver gesendet werden
- Verringern der Zeit, die Backup Exec wartet, bevor es den Status des verwalteten Backup Exec-Servers ändert, wenn der Backup Exec-Server nicht mehr reagiert
- Bewahren Sie die Kataloge auf dem verwalteten Backup Exec-Server (verteilt) auf. Besteht eine permanente Netzwerkverbindung zwischen dem zentralen Administrationsserver und dem verwalteten Backup Exec-Server, können Sie den Katalog durchsuchen und, unabhängig vom Katalogspeicherort, Wiederherstellungsvorgänge von beiden Servern aus ausführen.

Siehe ["Ändern der Einstellungen für einen verwalteten Backup Exec-Server"](#) auf Seite 1479.

Mit CAS bereitgestellte, zentralisierte und replizierte Katalogspeicherorte

In der CAS-Umgebung können Sie den Katalogspeicherort auswählen. Besteht unabhängig vom Katalogspeicherort eine permanente Netzwerkverbindung zwischen dem zentralen Administrationsserver und dem verwalteten Backup Exec-Server, können Sie den Katalog nach Backup-Sätzen durchsuchen und Wiederherstellungsvorgänge von beiden Servern aus ausführen.

Die folgenden Katalogspeicherorte sind verfügbar:

Tabelle K-2

Element	Beschreibung
Verteilt	<p>Image-Dateien (kleine Dateien mit Informationen über den Backup-Satz) werden von jedem verwalteten Backup Exec-Server auf den zentralen Administrationsserver verteilt. Protokolldateien, die detaillierte Informationen zum Backup-Satz enthalten, verbleiben auf dem verwalteten Backup Exec-Server.</p> <p>Hinweis: Es ist wichtig, die Katalogdateien auf dem verwalteten Backup Exec-Server zu sichern, da der Großteil der Kataloginformationen hier aufbewahrt wird, wenn die Option des verteilten Katalogspeicherorts angewendet wird.</p> <p>Wenn der Katalog verteilt vorliegt, zeigt die Ansicht "Auswahl für die Wiederherstellung" auf dem zentralen Administrationsserver die Backup-Sätze nur auf Datenträgerebene an. Backup-Satz-Details werden nicht angezeigt, wenn der verwaltete Backup Exec-Server, der diesen Backup-Satz erstellt hat, nicht verfügbar ist. Es kann jedoch der gesamte Datenträger vom zentralen Administrationsserver aus wiederhergestellt werden.</p> <p>Verteilte Kataloge ermöglichen Leistungssteigerungen, zentralisierte Standard-Wiederherstellungsfunktionen und die Verminderung des Netzwerkverkehrs. Hat ein verwalteter Backup Exec-Server keine permanente Verbindung zum zentralen Administrationsserver, werden bei jeder Herstellung der Verbindung die Image-Dateien im Katalog automatisch auf den zentralen Administrationsserver verteilt. Die durch diese Katalogverteilung verursachte temporäre Zunahme des Netzwerkverkehrs ist gering.</p>

Element	Beschreibung
Zentralisiert	Alle Katalogdateien und -informationen des verwalteten Backup Exec-Servers werden auf dem zentralen Administrationsserver aufbewahrt.
Repliziert	<p>Alle Katalogdateien werden vom verwalteten Backup Exec-Server auf den zentralen Administrationsserver repliziert. Sowohl der verwaltete Backup Exec-Server als auch der zentrale Administrationsserver speichern die Kataloge, der vom verwalteten Backup Exec-Server erstellt werden.</p> <p>Löschungen von Katalogdateien werden nur dann vom verwalteten Backup Exec-Server auf den zentralen Administrationsserver repliziert, wenn Backup Exec die Katalogdateien entsprechend der Katalogeinstellungen löscht. Wenn Katalogdateien auf dem verwalteten Backup Exec-Server als Ergebnis eines Backup-Auftrags oder manuell gelöscht werden, werden die Löschungen bei der nächsten Synchronisierung der Kataloge repliziert.</p>

Beachten Sie bei Auswahl des Katalogspeicherorts Folgendes:

- Der verwaltete Backup Exec-Server sollte über ausreichend Festplattenspeicherplatz für einen verteilten oder replizierten Katalog verfügen.
- Die Netzwerkbandbreite sollte dem durch einen zentralisierten oder replizierten Katalog ausgelösten Netzwerkverkehr gerecht werden. Zentralisierte und replizierte Kataloge erfordern eine Netzwerkverbindung mit großer Bandbreite.
- Im Hinblick auf die Datenwiederherstellungsanforderungen ist es relevant, Kataloginformationen an einem Speicherort aufzubewahren. Wenn der Katalogspeicherort zentralisiert oder repliziert wird, werden alle Kataloginformationen an einem Speicherort aufbewahrt. Dies ist für Backup-Zwecke unkomplizierter. Ist der Katalogspeicherort verteilt, werden die meisten Kataloginformationen auf dem verwalteten Backup Exec-Server aufbewahrt.

Siehe ["Ändern der Einstellungen für einen verwalteten Backup Exec-Server"](#) auf Seite 1479.

Ändern der Einstellungen für einen verwalteten Backup Exec-Server

Die Einstellungen für einen verwalteten Backup Exec-Server legen fest, wie der verwaltete Backup Exec-Server mit dem zentralen Administrationsserver kommuniziert und interagiert. Beispielsweise können Sie den Verbindungstyp, den Katalogspeicherort und die Funktionen der Auftragsberichterstellung- und -überwachung ändern. Sie können die Einstellungen für einen verwalteten Backup Exec-Server jederzeit ändern.

Hinweis: Sie müssen möglicherweise die Dienste auf dem verwalteten Backup Exec-Server neu starten, nachdem Sie die Einstellungen ändern. Wenn Sie beispielsweise den Katalogspeicherort ändern, müssen Sie die Dienstleistungen neu starten, damit die Änderung in Kraft treten.

So ändern Sie die Einstellungen für einen verwalteten Backup Exec-Server

- 1 Doppelklicken Sie auf dem zentralen Administrationsserver auf der Registerkarte "Speicher" auf einen verwalteten Backup Exec-Server.
- 2 Klicken Sie im linken Teilfenster auf "Einstellungen".
- 3 Wählen Sie die entsprechenden Optionen aus.

Verbindungseinstellungen

Wählen Sie eine der folgenden Verbindungstypen mit dem zentralen Administrationsserver:

- **Schnelle Verbindung**
Bestimmt, dass der zentrale Administrationsserver häufig mit dem verwalteten Backup Exec-Server kommunizieren soll. Wenn Sie diese Einstellung auswählen, werden Aktualisierungen des Auftragsstatus standardmäßig alle 10 Sekunden an den zentralen Administrationsserver gesendet. Auftragsprotokolle und Auftragsverläufe werden immer dann gesendet, wenn ein Auftrag auf dem verwalteten Backup Exec-Server fertiggestellt wird.
- **Langsame Verbindung**
Bestimmt, dass der zentrale Administrationsserver weniger häufig mit dem verwalteten Backup Exec-Server kommunizieren soll. Wenn Sie diese Einstellung auswählen, werden Aktualisierungen des Auftragsstatus standardmäßig alle 120 Sekunden an den zentralen Administrationsserver gesendet. Auftragsprotokolle und Auftragsverläufe werden nur dann gesendet, wenn ein Auftrag auf dem verwalteten Backup Exec-Server fehlschlägt.
- **Benutzerdefiniert**
Ermöglicht die Änderung der Schwellenwerte, die die Kommunikationsstatus auslösen, wenn verwaltete Backup Exec-Server nicht mehr reagieren. Sie können auch einstellen, wie häufig der verwaltete Backup Exec-Server Statusaktualisierungen für aktive Aufträge an den zentralen Administrationsserver sendet. Die eingestellte Häufigkeit wirkt sich auf den Netzwerkverkehr aus.

Verbindung verzögert

Hinweis: Diese Option wird nur angezeigt, wenn im Feld "Verbindungseinstellungen" die Option "Benutzerdefiniert" ausgewählt ist.

Geben Sie die Wartezeit an, bis der Status des verwalteten Backup Exec-Servers in "Verbindung verzögert" geändert wird, wenn der verwaltete Backup Exec-Server nicht reagiert.

Der zentrale Administrationsserver delegiert keine Aufträge an den verwalteten Backup Exec-Server, wenn dieser den Status "Verbindung verzögert" aufweist. Die Auftragsdelegierung wird wieder aufgenommen, wenn der verwaltete Backup Exec-Server wieder den Status "Aktiviert" annimmt, bevor der Schwellenwert überschritten wird.

Der Standardschwellenwert beträgt fünf Minuten.

Keine Verbindung

Hinweis: Diese Option wird nur angezeigt, wenn im Feld "Verbindungseinstellungen" die Option "Benutzerdefiniert" ausgewählt ist.

Geben Sie die Wartezeit an, bis der Status des verwalteten Backup Exec-Servers von "Verbindung verzögert" zu "Keine Verbindung" geändert wird.

Ändert sich der Status des verwalteten Backup Exec-Servers von "Verbindung verzögert" in "Keine Verbindung", markiert der zentrale Administrationsserver die aktiven Aufträge auf dem verwalteten Backup Exec-Server als "Fehlgeschlagen". Die benutzerdefinierte Fehlerbehandlungsregel "Wiederhergestellte Aufträge" wird auf jeden Auftrag angewendet, der bei Auftreten des Status "Keine Verbindung" aktiv ist.

Der Standardschwellenwert beträgt 15 Minuten.

Statusinformationen zu aktiven Aufträgen
an zentralen Administrationsserver senden

Hinweis: Diese Option wird nur
angezeigt, wenn im Feld
"Verbindungseinstellungen" die Option
"Benutzerdefiniert" ausgewählt ist.

Wählen Sie diese Option, damit der
verwaltete Backup Exec-Server ein
Auftragsstatus-Update an den zentralen
Administrationsserver zu schicken. Sie
können die Anzahl der Sekunden
festlegen, die der verwaltete Backup
Exec-Server wartet, bis Aktualisierungen
des Auftragsstatus an den zentralen
Administrationsserver gesendet werden.
Um die Netzwerkbandbreite bei
Ausführung vieler Aufträge beizubehalten,
erhöhen Sie den Zeitraum zwischen den
Aktualisierungen des Auftragsstatus.
Verkürzen Sie den Zeitraum, wenn Sie
mehr Aktualisierungen senden möchten.

Die Standardeinstellung ist zehn
Sekunden. Mit diesem Wert wird praktisch
eine Überwachung in Echtzeit
gewährleistet. Diese Einstellung wird nur
für schnelle Netzwerkverbindungen
empfohlen.

Statusinformationen an zentralen
Administrationsserver senden

Hinweis: Diese Option wird nur angezeigt, wenn im Feld "Verbindungseinstellungen" die Option "Benutzerdefiniert" und im Feld "Statusinformationen zu aktiven Aufträgen an zentralen Administrationsserver senden" die Option "Aktiviert" ausgewählt ist.

Legen Sie den Zeitraum fest, den ein verwalteter Backup Exec-Server zwischen dem Senden von Auftragsstatusinformationen zum zentralen Administrationsserver wartet. Um die Netzwerkbandbreite bei Ausführung vieler Aufträge beizubehalten, erhöhen Sie den Zeitraum zwischen den Aktualisierungen des Auftragsstatus. Verkürzen Sie den Zeitraum, wenn Sie mehr Aktualisierungen senden möchten.

Die Standardeinstellung ist zehn Sekunden. Mit diesem Wert wird praktisch eine Überwachung in Echtzeit gewährleistet. Diese Einstellung wird nur für schnelle Netzwerkverbindungen empfohlen.

Für Netzwerkverbindungen mit geringerer Bandbreite empfiehlt sich ein Wert von 120 Sekunden. Mit dieser Frequenz können Aktualisierungen für mittelgroße Aufträge angezeigt werden, wobei der durch Aktualisierungen des Auftragsstatus entstehende Netzwerkverkehr zugleich deutlich gesenkt werden kann.

Wenn Sie das Kontrollkästchen deaktivieren, werden keine Statusaktualisierungen gesendet. Die Fortschrittsanzeige für Aufträge wird nicht auf dem zentralen Administrationsserver angezeigt. Ist der Auftrag abgeschlossen, wird auf dem zentralen Administrationsserver der "Auftragsverlauf" aktualisiert.

Auftragsprotokolldetails an den zentralen
Administrationsserver senden

Wählen Sie, wann das Auftragsprotokoll für den verwalteten Backup Exec-Server an den zentralen Administrationsserver gesendet wird. Sie können wählen, ob das Auftragsprotokoll einmal täglich, nach dem Abschließen eines Auftrags oder nie gesendet wird.

Folgende Optionen sind verfügbar:

- Nie
Wenn Sie diese Option auswählen, werden Auftragsprotokolle lokal auf dem verwalteten Backup Exec-Server gespeichert.
- Einmal täglich
Wenn Sie diese Option auswählen, wird das Feld "Auftragsprotokolle senden um" angezeigt. Sie müssen die Zeit auswählen, um die das Auftragsprotokoll an den zentralen Administrationsserver gesendet wird.
- Bei Auftragsabschluss
Wenn Sie diese Option auswählen, wird das Feld "Auftragsprotokolle nur senden, wenn Auftrag fehlschlägt" angezeigt. Wählen Sie "Ja" aus, um das Auftragsprotokoll nur für fehlgeschlagene Aufträge zu senden. Wählen Sie "Nein" aus, um das Auftragsprotokoll unabhängig von der Auftragsbehandlung zu senden.

Auftragsprotokolle senden um

Wählen Sie die Zeit, zu der Backup Exec die Auftragsprotokolle für den verwalteten Backup Exec-Server an den zentralen Administrationsserver sendet. Diese Option wird nur angezeigt, wenn für die Option "Auftragsprotokolldetails an den zentralen Administrationsserver senden" die Option "Einmal täglich" ausgewählt ist.

Auftragsprotokolle nur senden, wenn
Auftrag fehlschlägt

Wählen Sie, ob das Auftragsprotokoll nur für fehlgeschlagene oder für alle Aufträge gesendet werden soll. Wählen Sie "Ja" aus, um das Auftragsprotokoll nur für fehlgeschlagene Aufträge zu senden. Wählen Sie "Nein" aus, um das Auftragsprotokoll unabhängig von der Auftragsbehandlung zu senden. Diese Option wird nur angezeigt, wenn für die Option "Auftragsprotokolldetails an den zentralen Administrationsserver senden" die Option "Bei Auftragsabschluss" ausgewählt ist.

Auftragsverlaufdetails an den zentralen
Administrationsserver senden

Wählen Sie, wann der Auftragsverlauf für den verwalteten Backup Exec-Server an den zentralen Administrationsserver gesendet wird.

Folgende Optionen sind verfügbar:

- Nie
Wenn Sie diese Option auswählen, werden Auftragsverläufe lokal auf dem verwalteten Backup Exec-Server gespeichert.
- Einmal täglich
Wenn Sie diese Option auswählen, wird das Feld "Auftragsverlauf senden um" angezeigt. Sie müssen die Zeit auswählen, um die der Auftragsverlauf an den zentralen Administrationsserver gesendet wird.
- Bei Auftragsabschluss
Wenn Sie diese Option auswählen, wird das Feld "Auftragsverlauf nur senden, wenn Auftrag fehlschlägt" angezeigt. Wählen Sie "Ja" aus, um den Auftragsverlauf nur für fehlgeschlagene Aufträge zu senden. Wählen Sie "Nein" aus, um den Auftragsverlauf unabhängig von der Auftragsbehandlung zu senden.

Auftragsverlauf senden um	Wählen Sie die Zeit, zu der Backup Exec den Auftragsverlauf für den verwalteten Backup Exec-Server an den zentralen Administrationsserver sendet. Diese Option wird nur angezeigt, wenn für die Option "Auftragsverlaufdetails an zentralen Administrationsserver senden" die Option "Einmal täglich" ausgewählt ist.
Auftragsverlauf nur senden, wenn Auftrag fehlschlägt	Wählen Sie, ob der Auftragsverlauf nur für fehlgeschlagene oder alle Aufträge gesendet werden soll. Wählen Sie "Ja" aus, um die Auftragsverlaufsdetails nur für fehlgeschlagene Aufträge zu senden. Wählen Sie "Nein" aus, um die Auftragsverlaufsdetails unabhängig von der Auftragsbehandlung zu senden. Diese Option wird nur angezeigt, wenn für die Option "Auftragsverlaufdetails an zentralen Administrationsserver senden" die Option "Bei Auftragsabschluss" ausgewählt ist.
Aufträge überwachen, die lokal auf dem verwalteten Backup Exec-Server erstellt wurden	<p>Wählen Sie diese Option, wenn Sie delegierte Aufträge und die Aufträge anzeigen möchten, die auf dem lokalen verwalteten Backup Exec-Server erstellt werden.</p> <p>Darüber hinaus können Sie Aufträge, die auf dem lokalen verwalteten Backup Exec-Server erstellt oder dort kopiert wurden, zurückhalten, löschen, ausführen, abbrechen und ihre Priorität ändern.</p>

Warnmeldungen anzeigen, wenn sich die Zeit zwischen dem verwalteten Backup Exec-Server und dem zentralen Administrationsserver unterscheidet

Wählen Sie diese Option, damit Backup Exec eine Warnmeldung erstellen kann, wenn die Uhr auf dem verwalteten Backup Exec-Server von der auf dem zentralen Administrationsserver abweicht. Eine Meldung wird erstellt, wenn die angegebene Anzahl von Sekunden überschritten wird.

CAS überwacht die internen Computeruhren sowohl der verwalteten Backup Exec-Server als auch des zentralen Administrationsservers. Wenn Zeitunterschiede zwischen dem zentralen Administrationsserver und den verwalteten Backup Exec-Servern auftreten, werden Aufträge möglicherweise zu einem unerwarteten Zeitpunkt ausgeführt. Um Probleme zu vermeiden, muss die Zeit der verwalteten Backup Exec-Server mit der des zentralen Administrationsservers übereinstimmen. Wenn Sie Warnmeldungen zum Zeitunterschied erhalten, setzen Sie die Uhr auf dem verwalteten Backup Exec-Server zurück, damit sie mit der Systemuhr auf dem zentralen Administrationsserver übereinstimmt.

Wenn Sie Änderungen an der Systemzeit des verwalteten Backup Exec-Servers oder des zentralen Administrationsservers vornehmen, müssen Sie die Backup Exec-Dienste auf diesem Server neu starten.

Die Warnmeldung senden, nachdem die Server nicht synchronisiert sind

Geben Sie die Anzahl von Sekunden an, um die sich die Uhren auf dem verwalteten Backup Exec-Server und dem zentralen Administrationsserver unterscheiden müssen, bevor Backup Exec eine Warnmeldung sendet.

Hinweis: Diese Option wird nur angezeigt, wenn im Feld "Warnmeldungen anzeigen, wenn sich die Zeit zwischen dem verwalteten Backup Exec-Server und dem zentralen Administrationsserver unterscheidet" die Option "Aktiviert" ausgewählt ist.

Speicherort für Speicher- und Mediendatenbank

Geben Sie an, ob die Speicher- und Mediendatenbank auf dem zentralen Administrationsserver oder auf einem verwalteten Backup Exec-Server liegt.

Katalog vorhalten in

Wählen Sie einen der folgenden Speicherorte für den Katalog:

- **Verwalteter Backup Exec-Server (verteilt)**
Verteilt die Katalogdateien zwischen dem zentralen Administrationsserver und dem verwalteten Backup Exec-Server. Wenn Speicher- und Mediendaten in einer lokalen Datenbank auf dem verwalteten Backup Exec-Server gespeichert sind, dann ist der verteilte Speicherort der einzige verfügbare Katalogspeicherort. Wählen Sie diese Option, wenn Ihre Netzwerkverbindung eine niedrige Bandbreite aufweist.
- **Zentraler Administrationsserver (zentral)**
Behält alle Katalogdateien auf dem zentralen Administrationsserver. Eine Netzwerkverbindung mit hoher Bandbreite ist für diese Option erforderlich.
- **Beide Server (repliziert)**
Repliziert alle Katalogdateien vom verwalteten Backup Exec-Server auf den zentralen Administrationsserver. Wenn ein verwalteter Backup Exec-Server nicht verfügbar ist, können Sie den Katalog vom zentralen Administrationsserver durchsuchen. Sie können allerdings keine Daten wiederherstellen, weil der verwaltete Backup Exec-Server nicht verfügbar ist. Eine Netzwerkverbindung mit hoher Bandbreite ist für diese Option erforderlich.

Siehe ["Mit CAS bereitgestellte, zentralisierte und replizierte Katalogspeicherorte"](#) auf Seite 1476.

Privater Cloud-Server

Ist diese Option aktiviert, kann ein verwalteter Service-Provider einen Backup Exec-Server in seinem Rechenzentrum suchen und ihn dann für eine CAS-Umgebung mit anderen Backup Exec-Servern, die sich über WAN an den Kundenorten des verwalteten Dienstbieters befinden, konfigurieren. Als eine Alternativoption zum Versenden von Bändern zur externen Aufbewahrung können Backups ausgeführt und lokal gespeichert werden und dann auf das Deduplizierungsspeichergerät des Cloud-Servers kopiert werden. Zusätzlich kann diese Funktion von den Kunden mit weit verteilten Netzwerken verwendet werden, die Backup Exec-Server in den standortfernen Niederlassungen für lokale Backups verwenden möchten. Danach können kopiert die Backup-Sätze auf einen Backup Exec-Server, der sich in einem zentralen Rechenzentrum befindet, kopiert werden. Diese Option ist ein Teil der Funktion "Cloud Services für Backup Exec".

4 Klicken Sie auf "Anwenden".

Erreichen der CAS-Kommunikationsschwellenwerte

In einer CAS-Umgebung kann es vorkommen, dass die Verbindung zwischen den verwalteten Backup Exec-Servern und dem zentralen Administrationsserver auch bei normaler Netzwerkverbindung unterbrochen wird. Wenn bei Aufträgen Verbindungsunterbrechungen zwischen einem verwalteten Backup Exec-Server und dem zentralen Administrationsserver auftreten, ändert sich der Kommunikationsstatus des Backup Exec-Servers von "Aktiviert" auf "Verzögert" oder "Keine Verbindung". Die auf ihre Verarbeitung durch den verwalteten Backup Exec-Server wartenden Aufträge werden solange in der Warteschlange des Backup Exec-Servers angehalten, bis die Verbindung wiederhergestellt wird.

Sie können in Backup Exec festlegen, wie lange sich der Status für den verwalteten Backup Exec-Server nicht ändert, wenn der Server nicht mehr reagiert. Wenn der Status eines verwalteten Backup Exec-Servers zu "Verzögert" oder "Keine

Verbindung" wechselt, ändert der zentrale Administrationsserver die Durchführung von Aufträgen, die aktuell oder zukünftig an den verzögerten verwalteten Backup Exec-Server delegiert werden.

Wenn beispielsweise der zentrale Administrationsserver nach Ablauf der festgelegten Zeit keine Verbindung zu einem verwalteten Backup Exec-Server herstellen kann, ändert der zentrale Administrationsserver den Verbindungsstatus des Backup Exec-Servers in "Verzögert". Die Delegierung von Aufträgen an den verwalteten Backup Exec-Server wird unterbrochen, weil darauf gewartet wird, dass der Backup Exec-Server wieder in den Status "Aktiviert" zurückkehrt. Aufträge werden an andere verwaltete Backup Exec-Servern delegiert, die auf dem Zielspeichergerät oder im Backup Exec-Server-Pool aufgeführt sind.

CAS überwacht weiterhin die Zeitspanne, in der keine Verbindung mit dem verwalteten Backup Exec-Server besteht. Nach Verstreichen einer festgelegten Zeitspanne nach dem Auftreten des Status "Verzögert" ändert CAS den Status des verwalteten Backup Exec-Servers in "Keine Verbindung". In diesem Fall markiert CAS den Auftrag als "Fehlgeschlagen" und die Auftragswiederherstellung wird gestartet, indem die benutzerdefinierte Fehlerbehandlungsregel "Wiederhergestellte Aufträge" für sämtliche zum Zeitpunkt des Auftretens des Status "Keine Verbindung" aktiven Aufträge aufgerufen wird.

Siehe ["Ändern der Einstellungen für einen verwalteten Backup Exec-Server"](#) auf Seite 1479.

Aktivieren bzw. Deaktivieren der Kommunikation zwischen dem verwalteten Backup Exec-Server und dem zentralen Administrationsserver

Sie können die Kommunikation zwischen dem verwalteten Backup Exec-Server und dem zentralen Administrationsserver manuell aktivieren bzw. deaktivieren. Wenn Kommunikationen deaktiviert werden, können Aufträge nicht zum verwalteten Backup Exec-Server delegiert werden.

So aktivieren Sie die Kommunikation zwischen dem verwalteten Backup Exec-Server und dem zentralen Administrationsserver

- 1 Klicken Sie mit der rechten Maustaste auf dem zentralen Administrationsserver auf der Registerkarte "Speicher" auf den verwalteten Backup Exec-Server, auf dem Sie Kommunikation aktivieren möchten.
- 2 Wählen Sie "Kommunikation aktiviert".

So deaktivieren Sie Kommunikationen zwischen dem verwalteten Backup Exec-Server und dem zentralen Administrationsserver

- 1 Klicken mit der rechten Maustaste auf dem zentralen Administrationsserver auf der Registerkarte "Speicher" auf den verwalteten Backup Exec-Server, auf dem Sie Kommunikation deaktivieren möchten.
- 2 Wählen Sie "Verbindung aktiviert" aus, um das Häkchen zu entfernen.

Warnmeldungen und Benachrichtigungen in CAS

In einer CAS-Umgebung (Central Admin Server Feature) werden Warnmeldungen, die auf einem verwalteten Backup Exec-Server generiert werden, automatisch auf dem zentralen Administrationsserver kumuliert. Um diese Warnmeldungen auf dem zentralen Administrationsserver anzuzeigen, müssen Sie Warnmeldungskategorien konfigurieren, um Warnmeldungen auf jedem verwalteten Backup Exec-Server und auf dem zentralen Administrationssserver selbst zu aktivieren oder zu deaktivieren.

Wenn auf die aktive Warnmeldung geantwortet und diese auf dem zentralen Administrationssserver gelöscht wurde, wird diese auch auf dem verwalteten Backup Exec-Server gelöscht.

Wenn die Backup Exec-Warnmeldungsfunktion nur auf dem verwalteten Backup Exec-Server, nicht jedoch auf dem zentralen Administrationssserver aktiviert wurde, werden Warnmeldungen nur auf dem verwalteten Backup Exec-Server angezeigt, auf dem sie erstellt wurden. Sie werden nicht auf dem zentralen Administrationssserver angezeigt.

Auf dem zentralen Administrationssserver können Sie Warnmeldungen für alle verwalteten Backup Exec-Server anzeigen oder Sie können die Warnmeldungen filtern, damit nur diejenigen für einen bestimmten verwalteten Backup Exec-Server oder Backup Exec-Server-Pool angezeigt werden.

Sie können eine Benachrichtigung entweder auf dem zentralen Administrationssserver oder dem verwalteten Backup Exec-Server konfigurieren. Unabhängig davon, wo Sie die Benachrichtigung konfigurieren, wird sie, wenn sie für einen delegierten Auftrag konfiguriert wurde, vom zentralen Administrationssserver gesendet. Sie können festlegen, dass der Administrator des verwalteten Backup Exec-Servers, der Administrator des zentralen Administrationssservers oder beide benachrichtigt werden.

Kopieren von Warnmeldungskonfigurationen auf verwaltete Backup Exec-Server

Sie können Warnmeldungen auf dem zentralen Administrationssserver aktivieren bzw. konfigurieren und die Warnmeldungskonfigurationen anschließend auf einen verwalteten Backup Exec-Server kopieren. Nach dem Kopieren der

Warnmeldungskonfigurationen werden die auf einem verwalteten Backup Exec-Server generierten Warnmeldungen auf dem verwalteten Backup Exec-Server und dem zentralen Administrationsserver angezeigt.

So kopieren Sie Warnmeldungskonfigurationen auf verwaltete Backup Exec-Server

- 1 Klicken Sie auf dem zentralen Administrationsserver auf die Backup Exec-Schaltfläche.
- 2 Wählen Sie "Konfiguration und Einstellungen" und anschließend "Einstellungen auf andere Server kopieren".
- 3 Aktivieren Sie unter "Zu kopierende Einstellungen auswählen" die Option "Meldungskonfiguration".
- 4 Klicken Sie auf "Hinzufügen".
- 5 Geben Sie den Namen eines verwalteten Backup Exec-Servers ein, auf den Sie die Warnmeldungskonfiguration kopieren möchten.
- 6 Klicken Sie auf "OK".
- 7 Klicken Sie im Dialogfeld "Einstellungen kopieren" auf "OK".

In einer Meldung auf dem zentralen Administrationsserver wird der erfolgreiche Kopiervorgang bestätigt.

Aktivieren verwalteter Backup Exec-Server für die Verwendung einer verfügbaren Netzwerkkarte

Standardmäßig verwenden Aufträge, die an einen verwalteten Backup Exec-Server delegiert oder vom zentralen Administrationsserver dorthin kopiert werden, die Netzwerk- und Sicherheitseinstellungen des verwalteten Backup Exec-Servers.

Sie können jedoch eine Option auf dem zentralen Administrationsserver auswählen, mit der ein Auftrag, falls die ausgewählte Netzwerkschnittstelle nicht verfügbar sein sollte, jedwede andere Netzwerkschnittstelle verwenden kann, um auf Remote Agents zuzugreifen. Wenn diese Option für einen Backup-Auftrag aktiviert ist, verwendet der verwaltete Backup Exec-Server eine alternative Netzwerkschnittstelle, um wichtige Backup-Aufträge auszuführen, der anderenfalls fehlschlagen würde.

So aktivieren Sie verwaltete Backup Exec-Server für die Verwendung einer verfügbaren Netzwerkkarte

- 1 Auf dem zentralen Administrationsserver erstellen Sie einen Backup-Auftrag.
- 2 Klicken Sie im Dialogfeld "Eigenschaften der Backup-Definition" im Feld "Backup" auf "Bearbeiten".

- 3 Klicken Sie im linken Teilfenster auf "Netzwerk".
- 4 Aktivieren Sie die Option "Zulassen, dass der verwaltete Backup Exec-Server eine beliebige Netzwerkschnittstelle für den Zugriff auf Remote Agents verwendet".
- 5 Konfigurieren Sie alle zusätzlichen Optionen für den Backup-Auftrag.
- 6 Klicken Sie auf "OK".

Info zur Auftragsdelegierung in CAS

Mit Auftragsdelegierung wird die automatische Lastverteilung von Aufträgen zwischen den verschiedenen Speichergeräten der verwalteten Backup Exec-Server bezeichnet. Der Auftrag wird auf dem zentralen Administrationsserver erstellt, kann aber auf einem beliebigen verwalteten Backup Exec-Server ausgeführt werden.

Sofern die Speichergeräte logisch in Geräteserverpools gruppiert sind, können diese, sobald die Speichergeräte verfügbar sind, Aufträge verarbeiten, die vom zentralen Administrationsserver delegiert wurden. Wenn beispielsweise zu einem Speichergerätepool zwei Speichergeräte gehören, von denen das eine gerade einen Auftrag verarbeitet, so delegiert der zentrale Administrationsserver automatisch einen anderen Auftrag an das nicht aktive Speichergerät.

Siehe "[Verwenden von Backup Exec-Server-Pools in CAS](#) " auf Seite 1498.

Kopieren von Aufträgen statt Delegieren von Aufträgen in CAS

Wenn der verwaltete Speicher des Backup Exec-Servers und Mediendaten auf einer lokalen Datenbank auf dem verwalteten Backup Exec-Server aufbewahrt werden, kann der zentrale Administrationsserver keine Aufträge an ihn delegieren. Stattdessen können Sie Auftragsoptionen, Standardzeitpläne, Fehlerbehandlungsregeln und Warnmeldungskonfigurationen vom zentralen Administrationsserver auf den verwalteten Backup Exec-Server kopieren. Eine permanente Netzwerkverbindung zum zentralen Administrationsserver ist nicht erforderlich, wenn die Aufträge lokal auf dem verwalteten Backup Exec-Server ausgeführt werden.

Verwenden Sie für Objekte auf dem zentralen Administrationsserver und allen anderen verwalteten Medienservern, auf die Sie Aufträge kopieren möchten, die gleichen Namen. Beispiel: Verwenden Sie für einen Speicherpool auf dem zentralen Administrationsserver und dem verwalteten Backup Exec-Server denselben Namen. So müssen Sie die Einstellungen oder Namen für jeden verwalteten Backup Exec-Server, auf den Sie Aufträge kopieren, nicht anpassen.

Siehe ["Kopieren von Konfigurationseinstellungen auf einen anderen Backup Exec-Server"](#) auf Seite 782.

Info zum Hinzufügen von Speichergeräten in einer CAS-Umgebung

Vom zentralen Administrationsserver aus können Sie den Assistenten 'Speicher konfigurieren' ausführen, um Geräte für den zentralen Administrationsserver oder für einen der verwalteten Backup Exec-Server einzurichten. Nachdem verwaltete Backup Exec-Server installiert wurden, werden sie auf der Registerkarte "Speicher" des zentralen Administrationsservers angezeigt. Beim Starten des Assistenten 'Speicher konfigurieren' werden Sie aufgefordert, den Server auszuwählen, für den Sie Speicher konfigurieren möchten. Sie können den zentralen Administrationsserver oder jeden verwalteten Backup Exec-Server auswählen, auf dem dieselbe Version von Backup Exec wie auf dem zentralen Administrationsserver ausgeführt wird.

Funktionsweise von Data Lifecycle Management (DLM) in einer CAS-Umgebung

Backup Exec nutzt Data Lifecycle Management (DLM), um abgelaufene Backup-Sätze auf Festplatten, Plattenkassetten, Deduplizierungsspeichern, Speichergruppen und virtuellen Datenträgern automatisch zu löschen. Standardmäßig bewahrt Backup Exec die neuesten Backup-Sätze, die zum Wiederherstellen von gesicherten Komponenten auf einem Server erforderlich sind, selbst dann auf, wenn die Backup-Sätze abgelaufen sind. Wenn Backup-Sätze von anderen Backup-Sätzen abhängen, löscht Backup Exec die Backup-Sätze erst, wenn das Ablaufdatum für alle Backup-Sätze erreicht ist. Selbst wenn der Backup-Satz als abgelaufen angezeigt wird, sind die Daten verfügbar, bis alle abhängigen Backup-Sätze ebenfalls abgelaufen sind.

Soll Backup Exec alle abgelaufenen Backup-Sätze löschen, selbst wenn sie die letzten Backup-Sätze sind, die Sie benötigen, um einen Server wiederherzustellen, können Sie im Dialogfeld "Speicher" die Option "Zulassen, dass Backup-Exec alle abgelaufenen Backup-Sätze löscht" wählen. In einer CAS-Umgebung ist diese Option nur auf dem zentralen Administrationsserver verfügbar. Wenn Sie diese Option auf dem zentralen Administrationsserver aktivieren, löscht DLM alle abgelaufenen Backup-Sätze auf dem zentralen Administrationsserver sowie auf allen verwalteten Backup Exec-Servern. Diese Option löscht alle abgelaufenen Backup-Sätze auf zentral und lokal verwalteten Backup Exec-Servern.

Warnung: Wenn Sie die Option "Zulassen, dass Backup Exec alle abgelaufenen Backup-Sätze löscht" aktivieren, sind möglicherweise die Daten, die Sie benötigen, um einen Server wiederherzustellen, nicht verfügbar.

Wenn Sie einen Backup-Satz über den zentralen Administrationsserver als abgelaufen kennzeichnen, wird DLM sofort auf dem Server ausgeführt, auf dem der Backup-Satz erstellt wurde. Bei diesem Server kann es sich um einen zentralen Administrationsserver oder den verwalteten Backup Exec-Server handeln. DLM wird nur auf dem Speichergerät ausgeführt, auf dem der Backup-Satz manuell als abgelaufen gekennzeichnet wurde. Wenn Sie einen Backup-Satz manuell von einem verwalteten Backup Exec-Server aus als abgelaufen kennzeichnen, wird DLM sofort auf dem Speichergerät ausgeführt, von dem aus der Backup-Satz manuell als abgelaufen gekennzeichnet wurde.

Siehe ["Löschen abgelaufener Backup-Sätze auf plattenbasiertem Speicher durch Data Lifecycle Management \(DLM\)"](#) auf Seite 393.

Abrufen von Medienüberwachungsinformationen für einen verwalteten Backup Exec-Server

Im Bericht "Medienüberwachung" sind die aktuellen Konfigurationsänderungen aufgeführt, die an Ihren Medien vorgenommen wurden. Wenn Sie in einer CAS-Umgebung diesen Bericht auf einem zentralen Administrationsserver ausführen, sind im Bericht nur Daten für die Medien für den zentralen Administrationsserver enthalten. Er enthält keine Daten für die verwalteten Backup Exec-Server. Um die Medienüberwachungsdaten für einen verwalteten Backup Exec-Server abzurufen, müssen Sie sich entweder bei dem lokalen verwalteten Backup Exec Server einloggen oder von der Remote-Administratorkonsole aus auf den verwalteten Backup Exec-Server zugreifen.

So rufen Sie Medienüberwachungsinformationen für einen verwalteten Backup Exec-Server ab

- 1 Sie haben folgende Möglichkeiten:
 - Loggen Sie sich lokal bei dem verwalteten Backup Exec-Server ein.
 - Klicken Sie auf einem Windows-Server oder einer Windows-Workstation an einem Remote-Standort auf "Start", wählen Sie "Backup Exec" und

geben Sie den Namen des Servers ein, mit dem Sie eine Verbindung herstellen möchten, sowie die Anmeldedaten für diesen Server.

- 2 Wählen Sie auf der Registerkarte "Berichte" unter "Berichtgruppen" die Option "Konfiguration" aus.
- 3 Wählen Sie in der Liste der Berichte "Medienüberwachung", und klicken Sie dann auf "Bericht jetzt ausführen", um den Bericht sofort auszuführen, oder auf "Neuer geplanter Bericht", um die Ausführung des Berichts zu einem späteren Zeitpunkt zu planen.

Verwenden von Backup Exec-Server-Pools in CAS

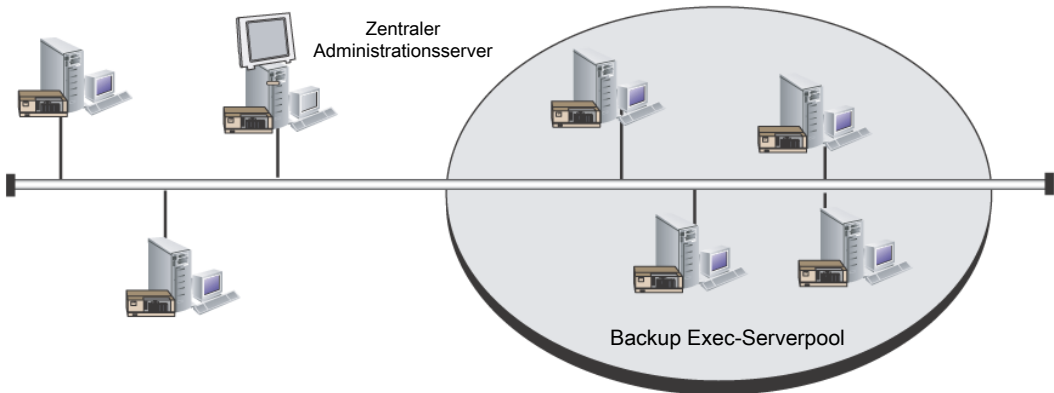
In einer CAS-Umgebung können Sie mehrere verwaltete Backup Exec-Server in Backup Exec-Server-Pools zusammenfassen. Wenn Sie einen Pool verwalteter Backup Exec-Server erstellen, sind alle Gerätepools auf diesen verwalteten Backup Exec-Servern für die Auftragsdelegierung verfügbar. Wenn an die verwalteten Backup Exec-Server im Backup Exec-Server-Pool mehrere Geräte angeschlossen sind, können mehrere kleinere Gerätepools mit weniger Speichergeräten erstellt werden. Dadurch können Sie einige Aufträge an einen bestimmten Gerätepool im Backup Exec-Server-Pool und andere Aufträge an einen anderen Gerätepool im selben Backup Exec-Server-Pool senden.

Backup Exec-Server-Pools können mehrere verwaltete Backup Exec-Server oder nur einen verwalteten Backup Exec-Server enthalten. Ein verwalteter Backup Exec-Server kann zu mehreren Backup Exec-Server-Pools gehören. Der zentrale Administrationsserver kann als verwalteter Backup Exec-Server verwendet und im Backup Exec-Server-Pool mit eingeschlossen werden.

Jeder verwaltete Backup Exec-Server oder Backup Exec-Server in einem Pool muss auf das Zielgerät für das Backup zugreifen können. Wenn es keine Schnittstelle zwischen dem Gerät und den verwalteten Backup Exec-Servern oder Backup Exec-Server-Pools gibt, wird der Auftrag nicht ausgeführt. Die Auftragsliste zeigt den folgenden Status an: Bereit. Im Backup Exec-Serverpool sind keine Backup Exec-Server verfügbar.

In dieser Grafik ist ein Backup Exec-Server-Pool dargestellt.

Abbildung K-3 Ein Beispiel eines mit CAS konfigurierten Backup Exec-Server-Pools innerhalb eines Unternehmensnetzwerks



Siehe ["Erstellen von Backup Exec-Server-Pools"](#) auf Seite 1500.

Siehe ["Auswählen eines Backup Exec-Server-Pools für Backups"](#) auf Seite 1499.

Auswählen eines Backup Exec-Server-Pools für Backups

Sie können einen Auftrag auf Geräten ausführen, die sich auf einem bestimmten verwalteten Backup Exec-Server befinden oder auf Speichergeräten, die Teil einer Gruppe verwalteter Backup Exec-Server sind. Mit diesem Filter können Sie steuern, wohin bestimmte Aufträge delegiert werden. Beispiel: Um Backups von Exchange-Datenbanken immer nur auf den Geräten auszuführen, die an verwaltete Backup Exec-Server in einem Pool mit der Bezeichnung "Exchange-Backups" angeschlossen sind, wählen Sie diese Option und anschließend den Serverpool mit dem Namen "Exchange-Backups" aus.

So wählen Sie einen Backup Exec-Server-Pool für Backups aus

- 1 Erstellen Sie eine Backup-Definition.
- 2 Klicken Sie im Dialogfeld "Backup" auf "Bearbeiten".
- 3 Wählen Sie im Dialogfeld "Backup-Optionen" im linken Teilfenster "Speicher".
- 4 Wählen Sie unter "Backup Exec-Server oder Backup Exec-Server-Pool" den Pool aus, den Sie für alle Backups in der Backup-Definition verwenden möchten.
- 5 Konfigurieren Sie alle zusätzlichen Optionen für die Backup-Definition.

Siehe ["Verwenden von Backup Exec-Server-Pools in CAS"](#) auf Seite 1498.

Erstellen von Backup Exec-Server-Pools

Sie können Backup Exec-Server in einer Gruppe (in einem Pool) zusammenfassen.

Siehe ["Verwenden von Backup Exec-Server-Pools in CAS"](#) auf Seite 1498.

Siehe ["Hinzufügen verwalteter Backup Exec-Server zu einem Backup Exec-Serverpool"](#) auf Seite 1500.

So erstellen Sie einen Backup Exec-Server-Pool

- 1 Wählen Sie auf dem zentralen Administrationsserver auf der Registerkarte "Speicher" in der Gruppe "Konfigurieren" die Option "Speicher konfigurieren".
- 2 Wählen Sie den Server, auf dem Sie den Serverpool erstellen möchten, aus und klicken Sie dann auf "Weiter".
- 3 Wählen Sie "Speicherpools" und klicken Sie anschließend auf "Weiter".
- 4 Wählen Sie "Backup Exec-Serverpool" und klicken auf dann "Weiter".
- 5 Geben Sie einen Namen und eine Beschreibung für den Pool, ein und klicken Sie dann auf "Weiter".
- 6 Aktivieren Sie die Kontrollkästchen neben den Namen der Server, die im Pool enthalten sein sollen, und klicken Sie dann auf "Weiter".
- 7 Klicken Sie auf "Fertigstellen".

Hinzufügen verwalteter Backup Exec-Server zu einem Backup Exec-Serverpool

Sie können verwaltete Backup Exec-Server vorhandenen Backup Exec-Server-Pools hinzufügen.

Siehe ["Erstellen von Backup Exec-Server-Pools"](#) auf Seite 1500.

So fügen Sie verwaltete Backup Exec-Server einem Backup Exec-Server-Pool hinzu

- 1 Wählen Sie auf dem zentralen Administrationsserver die Registerkarte "Speicher" aus.
- 2 Erweitern Sie "Alle Speicherpools" und doppelklicken Sie dann auf einen Backup Exec-Server-Pool, dem Sie verwaltete Backup Exec-Server hinzufügen möchten.
- 3 Klicken Sie unter "Zu dem Pool gehörige Backup Exec-Server" auf "Hinzufügen".
- 4 Aktivieren Sie die Kontrollkästchen für die Backup Exec-Server, die Sie dem Pool hinzufügen möchten, und klicken Sie dann auf "OK".
- 5 Klicken Sie auf "Übernehmen".

Löschen von Backup Exec-Server-Pools

Sie können einen Backup Exec-Server-Pool jederzeit löschen.

So löschen Sie einen Backup Exec-Server-Pool

- 1 Wählen Sie auf dem zentralen Administrationsserver die Registerkarte "Speicher" aus.
- 2 Erweitern Sie "Alle Speicherpools"
- 3 Klicken Sie mit der rechten Maustaste auf den Backup Exec-Server-Pool, den Sie löschen möchten, und klicken Sie dann auf "Löschen".
- 4 Klicken Sie auf "Ja", um zu bestätigen, dass Sie die Backup-Sätze löschen möchten.

Siehe ["Entfernen eines verwalteten Backup Exec-Server aus einem Backup Exec-Server-Pool"](#) auf Seite 1501.

Entfernen eines verwalteten Backup Exec-Server aus einem Backup Exec-Server-Pool

Wenn ein verwalteter Backup Exec-Server entfernt wird, wird dieser Server aus einem Backup Exec Server-Pool gelöscht, aber nicht vom Backup Exec entfernt.

So entfernen Sie einen verwalteten Backup Exec-Server aus einem Backup Exec-Server-Pool

- 1 Wählen Sie auf dem zentralen Administrationsserver die Registerkarte "Speicher" aus.
- 2 Erweitern Sie "Alle Speicherpools" und doppelklicken Sie dann auf den Backup Exec-Server-Pool, der den zu löschenden Server enthält.
- 3 Deaktivieren Sie unter "Zum Pool gehörende Backup Exec-Server" die Kontrollkästchen für die Backup Exec-Server, die Sie aus dem Pool entfernen möchten, und klicken Sie auf "Entfernen".
- 4 Klicken Sie auf "Übernehmen".

Siehe ["Verwenden von Backup Exec-Server-Pools in CAS "](#) auf Seite 1498.

Funktionsweise der zentralisierten Wiederherstellung in CAS

Abhängig davon, ob sich das erforderliche Speichermedium auf Speichergeräten oder an einem externen Ort befindet, kann die Initiierung von

Wiederherstellungsvorgängen vom zentralen Administrationsserver als automatisierter Prozess ausgeführt werden, der kaum Benutzereingriffe erfordert.

Wenn Sie zentrale Wiederherstellung mit online Medien verwenden, führen Sie den Wiederherstellungsassistenten auf dem zentralen Administrationsserver aus. Während der Datenauswahl legt CAS fest, welche Medien erforderlich sind, um die Wiederherstellung abzuschließen, und fragt dann den Backup Exec-Speicher und die Mediendatenbank ab, um die Identität des Speichergeräts festzulegen, in dem sich die Medien befinden. Nachdem Sie den Wiederherstellungsassistenten ausgeführt haben, startet CAS die Wiederherstellung, indem die Aufträge an den zentralen Administrationsserver oder verwalteten Backup Exec-Servern delegiert werden, die die ausgewählten Speichergeräte steuern. Wenn sich die wiederherzustellenden Daten auf verschiedenen Speichermedien befinden, werden Sie aufgefordert, zusätzliche Medien zu laden, damit der Wiederherstellungsvorgang erfolgreich abgeschlossen werden kann.

Wenn Sie zentrale Wiederherstellung mit Offline-Medien verwenden, führen Sie den Wiederherstellungsassistenten auf dem zentralen Administrationsserver aus. Während der Datenauswahl legt CAS fest, welche Medien erforderlich sind, um die Wiederherstellung abzuschließen, und fragt dann den Backup Exec-Speicher und die Mediendatenbank ab, um die Identität des Speichergeräts festzulegen, in dem sich die primären Medien befinden. Wenn das Medium nicht in einem Speichergerät gefunden werden kann, gilt das Medium als offline. CAS zeigt anschließend eine Auswahl von Laufwerkpools und Speichergeräten an, die mit den für die Wiederherstellung verwendeten Medien kompatibel sind. Dadurch haben Sie die Möglichkeit, ein Speichergerät auszuwählen, in das die Medien geladen werden sollen.

Nachdem Identität und Ort des für die Ausführung des Auftrags ausgewählten Speichergeräts bekannt sind, haben Sie folgende Möglichkeiten:

- Senden Sie den angehaltenen Wiederherstellungsauftrag als geplanten Auftrag.
- Rufen Sie das Medium ab, und setzen Sie es in das Speichergerät ein.
- Beenden Sie den Wartestatus für den Auftrag auf dem zentralen Administrationsserver. Damit wird der Wiederherstellungsauftrag ausgeführt.

CAS delegiert den Auftrag nun an den verwalteten Backup Exec-Server, der das ausgewählte Speichergerät steuert. Wenn sich die wiederherzustellenden Daten auf verschiedenen Speichermedien befinden, werden Sie aufgefordert, zusätzliche Medien zu laden, damit der Wiederherstellungsvorgang erfolgreich abgeschlossen werden kann.

Um Wiederherstellungsvorgänge vom zentralen Administrationsserver initiieren zu können, müssen folgende Voraussetzungen erfüllt sein:

- Kommunikationsstatus des verwalteter Backup Exec-Server muss aktiviert werden.
- Verwaltete Backup Exec-Server müssen mit allen Backup Exec-Server-Status online sein, die "Online" anzeigen.

Best Practices für die zentralisierte Wiederherstellung in CAS

Es wird die folgenden Methoden für die zentrale Wiederherstellung empfohlen:

- Wählen Sie für jeden Auftrag nur eine wiederherzustellende Ressource aus.
- Wählen Sie für alle Auswahlen, die sich im selben Wiederherstellungsauftrag befinden, dasselbe Wiederherstellungsgerät oder denselben Backup Exec-Server aus.
- Wählen Sie einen Backup Exec-Server aus, der über kompatible Geräte für alle Medien verfügt, die für den Wiederherstellungsauftrag erforderlich sind.

Funktionsweise der CAS-Wiederherstellung von Daten, die sich auf mehreren Speichergeräten befinden

Wenn sich die für die Wiederherstellung ausgewählten Daten auf einem einzelnen Gerät befinden, das an einen verwalteten Backup Exec-Server angeschlossen ist, wird auf dem zentralen Administrationsserver ein einzelner Wiederherstellungsauftrag erstellt und anschließend von dort delegiert. Wenn jedoch die für die Wiederherstellung ausgewählten Daten sich auf verschiedenen Geräten in der CAS-Umgebung befinden, wird der einzelne Wiederherstellungsauftrag abhängig von der Anzahl der beteiligten Geräte in mehrere separate Wiederherstellungsaufträge aufgeteilt.

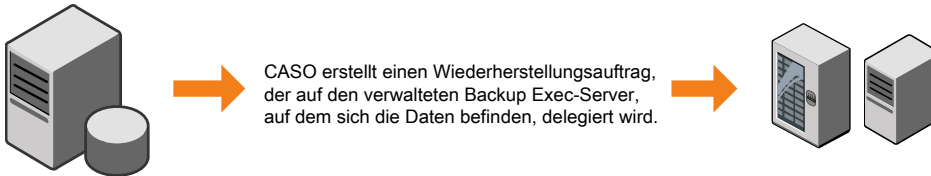
Die aufgeteilten Wiederherstellungsaufträge übernehmen den Namen des ursprünglichen Auftrags, werden jedoch mithilfe einer an den Auftragsnamen angehängten tiefgestellten Ziffer unterschieden und verknüpft.

Wenn Sie beispielsweise einen Wiederherstellungsauftrag erstellen und Daten, die Sie für die Wiederherstellung auswählen, sich in einem einzelnen Gerät auf einem verwalteten Backup Exec-Server befinden, erstellt CAS einen einzelnen Wiederherstellungsauftrag. Wenn Sie jedoch einen Wiederherstellungsauftrag erstellen und die ausgewählten Daten sich auf zwei oder mehreren Geräten, die an den verwalteten Backup Exec-Server angeschlossen sind, befinden, erstellt CAS zwei oder mehrere Wiederherstellungsaufträge.

Die folgende Grafik zeigt an, wie CAS Daten wiederherstellt, die auf nur einem Gerät gespeichert sind.

Abbildung K-4 Für Daten, auf einem einzelnen Speichergerät gespeichert wurden

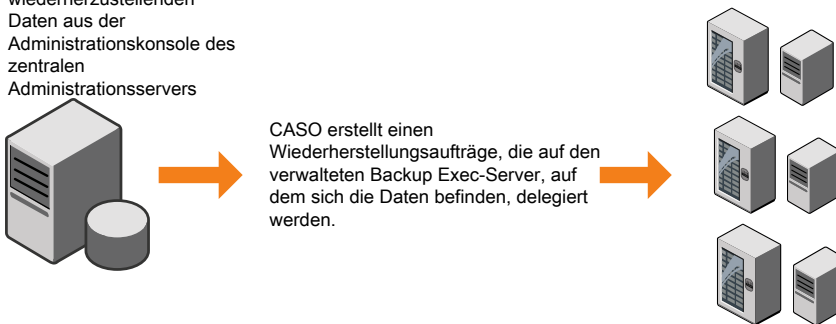
Wählen Sie die wiederherzustellenden Daten aus der Administrationskonsole des zentralen Administrationsservers



Die folgende Grafik zeigt an, wie CAS Daten wiederherstellt, die auf mehreren Geräten gespeichert sind.

Abbildung K-5 Für Daten, die auf mehreren Speichergeräten gespeichert wurden

Wählen Sie die wiederherzustellenden Daten aus der Administrationskonsole des zentralen Administrationsservers



Info zum Wiederherstellen fehlgeschlagener Aufträge in CAS

Die Fehlerbehandlungsregel "Wiederhergestellte Aufträge" ist eine benutzerdefinierte Fehlerbehandlungsregel, die von CAS verwendet wird, um Aufträge wiederherzustellen, die aufgrund von Problemen bei der internen Auftragskommunikation fehlgeschlagen sind. Diese Regel wird bei der Installation von Backup Exec erstellt und ist standardmäßig aktiviert.

Durch die Wiederholungsoptionen für diese Regel wird festgelegt, dass der Auftrag jeweils zweimal mit einem Intervall von fünf Minuten wiederholt wird. Nach dem

ersten Wiederholungsversuch delegiert CAS die Aufträge an einen anderen verfügbaren verwalteten Backup Exec-Server.

Wenn dieser Versuch fehlschlägt, unternimmt CAS einen zweiten Versuch, einen anderen verwalteten Backup Exec-Server für die Auftragsverarbeitung zu finden. Wenn keine verwalteten Backup Exec-Server verfügbar sind, wird als letzte Auftragsbehandlung der Auftrag so lange angehalten, bis der Fehlerbuzustand behoben wurde.

Hinweis: Wenn die Fehlerbehandlungsregel für die Auftragswiederaufnahme aktiviert wird, dann werden wiederhergestellte Aufträge nicht erneut an einen Backup Exec-Server-Pool gesendet, damit sie auf einem anderen Server ausgeführt werden. Die Fehlerbehandlungsregel für die Auftragswiederaufnahme legt den Auftrag erneut fest, damit er auf dem ursprünglichen Server ausgeführt wird, wenn dieser Server online ist. Um einen wiederhergestellten Auftrag zu aktivieren, der erneut an einen Backup Exec-Server-Pool gesendet wird, müssen Sie die Fehlerbehandlungsregel für die Auftragswiederaufnahme deaktivieren.

Hinweis: Wenn Sie einen Auftrag für einen Backup Exec-Server-Pool vorsehen, der mehrere verwaltete Backup Exec-Server enthält und ein Auftragsfehler auftritt, verwendet der Wiederherstellungsvorgang nur die verwalteten Backup Exec-Server im Backup Exec-Server-Pool. Verwaltete Backup Exec-Server, die nicht im Backup Exec-Server-Pool sind, werden nicht für Auftragswiederherstellung verwendet.

Wenn Sie den Auftragsverlaufseintrag für einen wiederhergestellten Auftrag öffnen, werden Auftragsfehler als Fehlerursache sowie eine Erklärung des aufgetretenen internen Kommunikationsfehlers aufgelistet. Im Auftragsverlaufseintrag wird außerdem angezeigt, dass der Auftrag wiederhergestellt wurde.

Hinweis: Für wiederhergestellte Aufträge werden keine Auftragsprotokolle erstellt.

In der folgenden Tabelle finden Sie Informationen zu CAS-Fehlercodes, die in der Standardeinstellung für die benutzerdefinierte Fehlerbehandlungsregel "Wiederhergestellte Aufträge" ausgewählt sind:

Tabelle K-3 Fehlercodes für die benutzerdefinierte Fehlerbehandlungsregel "Wiederhergestellte Aufträge"

Fehlercode	Beschreibung
0xE000881B JOBDISPATCH	Die angezeigte Meldung ist: "Auftrag beim Senden fehlgeschlagen." Der Auftrag wird wiederhergestellt.
0xE000881D JOB_CASO_QUEUE FEHLER	Die angezeigte Meldung ist: "Der Auftrag konnte nicht an den verwalteten Backup Exec-Zielserver delegiert werden. Möglicherweise ist der verwaltete Backup Exec-Server nicht online, oder es ist ein Kommunikationsfehler aufgetreten. Der Auftrag wird wiederhergestellt.
0xE000881E JOB_CASO_REMOTEMMS_STARTFAILURE	Die angezeigte Meldung ist: "Der Auftrag ist am verwalteten Backup Exec-Zielserver fehlgeschlagen, möglicherweise, weil ein Datenbankfehler aufgetreten ist." Der Auftrag wird wiederhergestellt.

Siehe ["Fehlerbehandlungsregeln für fehlgeschlagene oder abgebrochene Aufträge"](#) auf Seite 316.

Siehe ["Benutzerdefinierte Fehlerbehandlungsregel für wiederhergestellte Aufträge"](#) auf Seite 320.

Siehe ["Ändern der Einstellungen für einen verwalteten Backup Exec-Server"](#) auf Seite 1479.

Anhalten oder Wiederaufnehmen eines verwalteten Backup Exec-Servers

Über den zentralen Administrationsserver können verwaltete Backup Exec-Server angehalten und wiederaufgenommen werden.

Wird ein verwalteter Backup Exec-Server angehalten, delegiert der zentrale Administrationsserver keine Aufträge mehr an diesen Server. Wenn der verwaltete Backup Exec-Server angehalten wird, wechselt sein Status von "Online" zu "In Wartestellung".

Vorsicht: Bei der Installation von Backup Exec-Funktionen auf einem verwalteten Backup Exec-Server muss dieser angehalten werden, damit während der Installation keine weiteren Aufträge vom zentralen Administrationsserver an diesen Server delegiert werden. Aktuell ausgeführte Aufträge sollten beendet oder abgebrochen werden, bevor mit der Installation begonnen wird.

Wenn Sie einen angehaltenen verwalteten Backup Exec-Server wiederaufnehmen, treten die folgenden Änderungen ein:

- Aufträge können vom zentralen Administrationsserver zum verwalteten Backup Exec-Server delegiert werden.
- Der Status des verwalteten Backup Exec-Servers ändert sich von "Angehalten" auf "Online" in der Spalte "Status" auf der Registerkarte "Speicher".

So halten Sie einen verwalteten Backup Exec-Server an

- 1 Klicken Sie auf dem zentralen Administrationsserver auf der Registerkarte "Speicher" mit der rechten Maustaste auf den verwalteten Backup Exec-Server, den Sie anhalten möchten.
- 2 Klicken Sie auf "Anhalten".

So nehmen Sie einen angehaltenen verwalteten Backup Exec-Server wieder auf

- 1 Klicken Sie auf dem zentralen Administrationsserver auf der Registerkarte "Speicher" mit der rechten Maustaste auf den verwalteten Backup Exec-Server, den Sie wieder aufnehmen möchten.
- 2 Klicken Sie auf "Anhalten", um das Häkchen neben "Anhalten" zu entfernen.

Beenden oder Starten von Backup Exec-Diensten für einen verwalteten Backup Exec-Server

Sie können die Backup Exec-Dienste auf einem verwalteten Backup Exec-Server vom zentralen Administrationsserver beenden oder starten.

So beenden Sie Backup Exec-Dienste für einen verwalteten Backup Exec-Server

- 1 Klicken mit der rechten Maustaste auf dem zentralen Administrationsserver auf der Registerkarte "Speicher" auf den verwalteten Backup Exec-Server, auf dem Sie Dienste beenden möchten.
- 2 Wählen Sie "Backup Exec-Dienste".
- 3 Klicken Sie im Dialogfeld "Backup Exec-Dienstmanager" auf "Alle Dienste anhalten".
- 4 Klicken Sie auf "Schließen".

So starten Sie Backup Exec-Dienste für einen verwalteten Backup Exec-Server

- 1 Klicken mit der rechten Maustaste auf dem zentralen Administrationsserver auf der Registerkarte "Speicher" auf den verwalteten Backup Exec-Server, auf dem Sie Dienste starten möchten.
- 2 Wählen Sie "Backup Exec-Dienste".
- 3 Klicken Sie im Dialogfeld "Backup Exec-Dienstmanager" auf "Alle Dienste starten".
- 4 Klicken Sie auf "Schließen".

Anzeigen von verwalteten Backup Exec-Servereigenschaften

Auf dem zentralen Administrationsserver können Sie Eigenschaften für verwaltete Backup Exec-Server anzeigen.

So zeigen Sie Eigenschaften für verwaltete Backup Exec-Server an

- 1 Doppelklicken Sie auf der Registerkarte "Speicher" des zentralen Administrationsservers auf den verwalteten Backup Exec-Server, für den Sie Eigenschaften anzeigen möchten.

2 Wählen Sie im linken Teilfenster "Eigenschaften".

Name	Zeigt den Namen des verwalteten Backup Exec-Servers oder des zentralen Administrationsservers an.
Beschreibung	Zeigt an, ob der Server ein verwalteter Backup Exec-Server oder ein zentraler Administrationsserver ist. Sie können diese Beschreibung ändern.
Serverstatus	Zeigt den aktuellen Status des Servers an, z. B. online, angehalten, nicht verfügbar oder offline.
Version	Zeigt die installierte Version von Backup Exec an.
Lizenz	Stellt Informationen über die Backup Exec-Lizenz zur Verfügung, die auf dem Server installiert ist.
Zeitzone	Zeigt die Zeitzone an, die für den Server eingestellt ist.
Startdatum und -uhrzeit	Zeigt an, wann der Server gestartet wurde.
Aktuelles Datum und Uhrzeit	Zeigt das aktuelle Datum und die aktuelle Uhrzeit auf dem Server an.
Betriebssystemtyp	Zeigt den Typ des auf dem Server installierten Betriebssystems an.
Betriebssystemversion	Zeigt die Version des auf dem Server installierten Betriebssystems an.
Build des Betriebssystems	Zeigt die Buildnummer des auf dem Server installierten Betriebssystems an.
Prozessortyp	Zeigt den Typ des Prozessors im Server an.
Anzahl der Prozessoren	Zeigt die Anzahl von Prozessoren im Server an.
Gesamter physischer Speicher	Zeigt den gesamten physischen Speicherplatz auf dem Server an.
Verfügbarer physischer Speicher	Zeigt den verfügbaren physischen Speicherplatz auf dem Server an.

Gesamter virtueller Speicher	Zeigt den gesamten virtuellen Speicherplatz auf dem Server an.
Verfügbarer virtueller Speicher	Zeigt den verfügbaren virtuellen Speicherplatz auf dem Server an.
Gesamtgröße der Seitendatei	Zeigt den gesamten Speicherplatz an, der in der Auslagerungsdatei des Servers zur Verfügung steht.

Anzeigen der Einstellungen für einen zentralen Administrationsserver

Wenn Central Admin Server Feature (CAS) installiert ist, können Sie Informationen zum Speicherort der Datenbanken für Backup Exec anzeigen. Die Datenbanken umfassen die Backup Exec-Datenbank, die Geräte- und Mediendatenbank und die Katalogdatenbank.

Wenn Sie bei der Installation von Backup Exec die Standardoption zur Erstellung einer lokalen Backup Exec-SQL Express-Instanz, in der die Backup Exec-Datenbank gespeichert werden soll, gewählt haben, befinden sich alle Datenbanken auf dem lokalen Backup Exec-Server. Falls Sie eine andere Instanz im Netzwerk auswählen, in der die Backup Exec-Datenbank gespeichert werden soll, befinden sich alle Datenbanken auf dem Microsoft SQL Server, der die Instanz enthält.

So zeigen Sie die Einstellungen für einen zentralen Administrationsserver an

- 1 Sie haben folgende Möglichkeiten:
 - Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Eigenschaften des lokalen Servers".

- Auf der Registerkarte "Speicher" doppelklicken Sie auf den zentralen Administrationsserver.

2 Klicken Sie im linken Teilfenster auf "Einstellungen".

Server	Zeigt den Namen des Microsoft SQL Servers an, der die Backup Exec-Datenbank enthält.
Instanz	Zeigt den Namen der Instanz an, in der die Backup Exec-Datenbank installiert ist.
Name	Zeigt den Microsoft SQL Server-Namen der Backup Exec-Datenbank an.
Pfad	Zeigt den Pfad zur Backup Exec-Datenbank an.
Server	Zeigt den Namen des Microsoft SQL-Servers an, der die ADAMM-Datenbank enthält.
Instanz	Zeigt den Namen der Instanz an, in der die ADAMM-Datenbank installiert ist.
Name	Zeigt den Microsoft SQL Server-Namen der ADAMM-Datenbank an.
Pfad	Zeigt den Pfad der ADAMM-Datenbank an.
Server	Zeigt den Namen des Microsoft SQL-Servers an, der die Backup Exec-Katalogdatenbank enthält.
Instanz	Zeigt die Datenbankinstanz an, die die Katalogdatenbank enthält.
Name	Zeigt den Microsoft SQL Server-Namen der Backup Exec-Katalogdatenbank an.
Pfad	Zeigt den Pfad zur Backup Exec-Katalogdatenbank an.
Privater Cloud-Server	Gibt an, ob die Option "Privater Cloud-Server" aktiviert oder deaktiviert ist.

Notfallwiederherstellung in CAS

Verwenden Sie Backup Exec Simplified Disaster Recovery (SDR), um in einer CAS-Umgebung sowohl verwaltete Backup Exec-Server als auch den zentralen Administrationsserver zu schützen.

Siehe ["Info zu Simplified Disaster Recovery"](#) auf Seite 941.

Beachten Sie vor dem Implementieren von SDR in einer CAS-Umgebung folgende Hinweise:

- Um Wiederherstellungsmedien für alle verwalteten Backup Exec-Server oder zentralen Administrationsserver zu erstellen, muss der Assistent zum Erstellen einer Simplified Disaster Recovery Disk auf dem zentralen Administrationsserver ausgeführt werden. Falls Sie eine Umgebung der standortfernen Verwaltung verwenden, stellen Sie eine Verbindung zum zentralen Administrationsserver her.
- Wenn die verwalteten Backup Exec-Server mithilfe eines bootfähigen Datenträger-Image geschützt werden sollen, müssen Sie den Assistenten zum Erstellen einer Simplified Disaster Recovery Disk auf allen verwalteten Backup Exec-Server ausführen, auf denen ein bootfähiges Speichergerät installiert ist.
- Der zentrale Administrationsserver muss lokal gesichert und wiederhergestellt werden.

Notfallwiederherstellung eines verwalteten Backup Exec-Server, der von einem fehlgeschlagenem, zentralen Administrationsserver verwaltet wird.

Wenn Verbindungen zwischen dem verwalteten Backup Exec-Server und dem zentralen Administrationsserver noch aktiv sind, können Sie einen verwalteten Backup Exec-Server in einen eigenständig Backup Exec-Server ändern, indem Sie ihn von der Registerkarte "Speicher" löschen. Wenn der zentrale Administrationsserver jedoch einen Systemausfall erfährt, gehen die Verbindungen zwischen dem verwalteten Backup Exec-Server und dem zentralen Administrationsserver verloren. Der verwaltete Backup Exec-Server kann nicht von der Registerkarte "Speicher" gelöscht werden. Jedoch können Sie den verwalteten Backup Exec-Server in einen eigenständigen Backup Exec-Server ändern, indem Sie die Windows-Funktion "Programm ändern" verwenden.

So wandeln Sie einen verwalteten Backup Exec-Server in einen eigenständigen Backup Exec-Server um, wenn die Verbindung zwischen den beiden Servern unterbrochen wurde.

- 1** Auf dem verwalteten Backup Exec-Server öffnen Sie die Windows-Systemsteuerung.
- 2** Wählen Sie "Programme hinzufügen/entfernen" oder "Programme und Funktionen", je nachdem, welche Windows-Version Sie verwenden.
- 3** Wählen Sie "Backup Exec" aus der Liste und klicken Sie dann auf "Ändern".
- 4** Klicken Sie im Fenster "Zusätzliche Optionen" auf "Weiter".
- 5** Klicken Sie im Bereich "Lizenzen hinzufügen" auf "Weiter".
- 6** Klicken Sie im Fenster "Konfigurationsoptionen" auf "Weiter".
- 7** Klicken Sie im Bereich "Sprachen auswählen" auf "Weiter".
- 8** Wählen Sie im Bereich "Zentraler Administrationsserver:" "Lokal verwalteter Backup Exec-Server" und klicken Sie dann auf "Weiter".
- 9** Wenn die Fehlermeldung angezeigt wird, dass der verwaltete Backup Exec-Server nicht in der Lage ist, den zentralen Administrationsserver zu kontaktieren, klicken Sie auf "OK".

Hinweis: Wenn keine Fehlermeldung angezeigt wird, dann erkannte Backup Exec einen Server mit dem gleichen Namen wie der zentrale Administrationsserver auf dem Netzwerk. Wenn dieser Server der zentrale Administrationsserver ist und er korrekt ausgeführt wird, sollten Sie in der Lage sein, ihn von der Registerkarte "Speicher" auf dem zentralen Administrationsserver aus in einen verwalteten Backup Exec-Server umzuwandeln.

- 10** Klicken Sie auf "Weiter".

- 11 Klicken Sie im Bereich "Installation - Zusammenfassung" auf "Installieren".
- 12 Fügen Sie nach Abschluss der Installation dem Backup Exec-Server eventuell erforderliche Geräte und Speicher hinzu.

Hinweis: Sie müssen möglicherweise auch das Speichergerät inventarisieren und katalogisieren, abhängig von der verwendeten Katalogmethode, als der verwaltete Backup Exec-Server mit dem zentralen Administrationsserver verbunden wurde.

Wenn der zentrale Administrationsserver wieder online ist, können Sie diesen eigenständigen Backup Exec-Server zurück in einen verwalteten Backup Exec-Server wandeln.

Siehe ["Umwandlung eines Backup Exec-Servers in einen verwalteten Backup Exec-Server"](#) auf Seite 1469.

Fehlerbehebung in CAS

Wenn Probleme mit CAS auftreten, prüfen Sie die folgenden Fragen und Antworten.

Tabelle K-4 Fehlerbehebung in CAS

Frage	Antwort
Die Fehlermeldung 1065 "Die angegebene Datenbank existiert nicht" wird angezeigt. Was verursacht diesen Fehler?	<p>Dieser Fehler kann eine der folgenden Ursachen haben:</p> <ul style="list-style-type: none">■ UDP-Datenverkehr wird im Netzwerk zwischen dem zentralen Administrationsserver und dem verwalteten Backup Exec-Server blockiert.■ Die SQL-Konfiguration auf dem zentralen Administrationsserver wurde nicht richtig festgelegt.■ Wenn der zentrale Administrationsserver auf einer benannten SQL-Instanz installiert ist und der SQL-Browserdienst nicht ausgeführt wird.■ Die benannten Kanäle oder TCP/IP-Protokolle sind nicht aktiviert oder nicht für Remote-Verbindungen eingestellt.

Frage	Antwort
Ich habe die Systemzeit geändert, aber die Änderung wurde nicht auf meinen verwalteten Backup Exec-Server oder zentralen Administrationsservern übernommen. Woran liegt das?	Wenn Sie Änderungen an der Systemzeit des verwalteten Backup Exec-Servers oder des zentralen Administrationsservers vornehmen, müssen Sie die Backup Exec-Dienste neu starten. Backup Exec verarbeitet die Änderung der Systemzeit beim Neustart des Dienstes.
Ich erhielt den Fehler "Bereit. Der Auftragsspeicher enthält keine passenden Geräte". Was verursacht diesen Fehler?	<p>Dieser Fehler kann auftreten, wenn Sie verwaltete Backup Exec-Server aus dem falschen Speicherort entfernen. Um verwaltete Backup Exec-Server aus einem zentralen Administrationsserver zu entfernen, verwenden Sie die Option "Löschen" auf der Registerkarte "Speicher". Wenn Sie einen verwalteten Backup Exec-Server aus der Registerkarte "Speicher" entfernen, wird der Server ein eigenständiger Server, also kann er als eigenständiger Server noch gesichert werden und wiederhergestellt werden, aber er kann durch den zentralen Administrationsserver nicht mehr gesteuert werden. Entfernen Sie den verwalteten Backup Exec-Server nicht aus der Registerkarte "Backup und Wiederherstellung".</p> <p>Siehe "Löschen eines verwalteten Backup Exec-Servers aus einer CAS-Umgebung" auf Seite 1472.</p>

Siehe ["Infos zu Central Admin Server Feature"](#) auf Seite 1450.

Ausführen von Backup Exec Utility für CAS-Vorgänge

Eine separate Anwendung, die als "Backup Exec Utility" bezeichnet wird, steht zum Ausführen folgender CAS-Vorgänge zur Verfügung:

- Verschieben Sie einen verwalteten Backup Exec-Server.
- Deaktivieren oder aktivieren Sie Kommunikation mit einem verwalteten Backup Exec-Server.

Das Backup Exec Utility sollte nur unter Anleitung des technischen Supports verwendet werden. Eine unsachgemäße Verwendung dieses Dienstprogramms kann Konfigurationsänderungen zur Folge haben und dadurch die Ausführung von Backup Exec verhindern.

So starten Sie das Backup Exec-Dienstprogramm:

- 1 Doppelklicken Sie im Backup Exec-Installationsordner in *<Backup Exec-Installationsordner>\Backup Exec* auf "BEUtility".
- 2 Wählen Sie im Menü "Backup Exec Utility" die Option "Hilfe", um Informationen zum Einsatz aufzurufen.

Deinstallieren von Backup Exec vom zentralen Administrationsserver

Bevor Sie Backup Exec vom zentralen Administrationsserver deinstallieren, müssen Sie auf diesem alle verwalteten Backup Exec-Server von der Registerkarte "Speicher" löschen.

Vorsicht: Wenn die Deinstallation nicht in der folgenden Reihenfolge vorgenommen wird, kann es beim Schließen von Backup Exec-Diensten während der Deinstallation von Backup Exec auf den verwalteten Backup Exec-Servern zu langen Wartezeiten kommen.

So deinstallieren Sie Backup Exec vom zentralen Administrationsserver

- 1 Klicken Sie auf dem zentralen Administrationsserver auf der Registerkarte "Speicher" mit der rechten Maustaste auf einen verwalteten Backup Exec-Server.
- 2 Wählen Sie die Option "Löschen".
- 3 Klicken Sie auf "Ja", um den Löschvorgang zu bestätigen.
- 4 Wiederholen Sie die Schritte 1 und 3 für jeden verwalteten Backup Exec-Server, den der zentrale Administrationsserver verwaltet.
- 5 Deinstallieren Sie Backup Exec vom zentralen Administrationsserver.
Siehe ["Deinstallieren von Backup Exec"](#) auf Seite 127.

Deinstallieren von Backup Exec von einem verwalteten Backup Exec-Server

Sie müssen den verwalteten Backup Exec-Server von der Registerkarte "Speicher" auf dem zentralen Administrationsserver löschen, bevor Sie Backup Exec deinstallieren.

So deinstallieren Sie Backup Exec von einem verwalteten Backup Exec-Server

- 1** Klicken Sie auf dem zentralen Administrationsserver auf der Registerkarte "Speicher" mit der rechten Maustaste auf einen verwalteten Backup Exec-Server.
- 2** Wählen Sie die Option "Löschen".
- 3** Klicken Sie auf "Ja", um den Löschvorgang zu bestätigen.
- 4** Deinstallieren Sie Backup Exec vom verwalteten Backup Exec-Server.

Siehe "[Deinstallieren von Backup Exec](#)" auf Seite 127.

Backup Exec Advanced Disk-based Backupfunktion

Dieser Anhang enthält folgende Themen:

- [Info zum Einsatz von Advanced Disk-based Backup Feature](#)
- [So verwenden Sie synthetische Backups anstelle von wiederkehrenden vollständigen Backups](#)
- [Festlegen der Standard-Backup-Optionen für Advanced Disk Based Backup Feature](#)
- [Infos zur True Image-Wiederherstellung für synthetische Backups](#)
- [Verwenden von Offhost-Backups zur Verarbeitung von Remote-Computer-Backups auf dem Backup Exec-Server](#)
- [Konfigurieren von Offhost-Backup-Optionen für einen Backup-Auftrag](#)
- [Bewährte Methoden für Off-Host-Backup](#)
- [Fehlerbehebung bei Off-Host-Backups](#)
- [Off-Host-Backup-Probleme mit Hardwareanbietern](#)

Info zum Einsatz von Advanced Disk-based Backup Feature

Advanced Disk-based Backup Feature enthält die folgenden Funktionen:

So verwenden Sie synthetische Backups anstelle von wiederkehrenden vollständigen Backups■ **Synthetisches Backup**

Diese Funktion aktiviert ein vollständiges Backup von einem vollständigen Basis-Backup und von folgenden inkrementellen Backups.

Ein synthetisches Backup bietet die folgenden Vorteile:

- Reduzierter Backup-Aufwand, da das synthetische Backup außerhalb des Backup-Zeitrahmens geplant werden kann.
- Verringerter Netzwerkverkehr, da das synthetische Backup nicht über das Netzwerk ausgeführt werden muss.
- Bei der True Image-Wiederherstellung kann Backup Exec den Zustand der Inhalte von Verzeichnissen zum Zeitpunkt eines synthetischen vollständigen oder inkrementellen Backups wiederherstellen.

■ **Off-Host-Backup**

Diese Funktion ermöglicht, dass ein Backup-Vorgang anstatt auf dem Remote- oder Hostcomputer auf einem Backup Exec-Server verarbeitet wird. Die Ausführung des Backup auf einem Backup Exec-Server statt auf dem Remote-Computer ermöglicht eine höhere Backup-Leistung und verringert die Last des Remote-Computers.

Advanced Disk Based Backup Feature (ADBO) wird als Teil der Enterprise Server Option installiert, für die Sie eine Lizenz auf dem Backup Exec-Server eingeben müssen.

Siehe ["So verwenden Sie synthetische Backups anstelle von wiederkehrenden vollständigen Backups"](#) auf Seite 1520.

Siehe ["Verwenden von Offhost-Backups zur Verarbeitung von Remote-Computer-Backups auf dem Backup Exec-Server"](#) auf Seite 1527.

Siehe ["Info zum Installieren von und den Lizenzierungsoptionen für Backup Exec"](#) auf Seite 44.

Siehe ["Festlegen der Standard-Backup-Optionen für Advanced Disk Based Backup Feature"](#) auf Seite 1522.

So verwenden Sie synthetische Backups anstelle von wiederkehrenden vollständigen Backups

Mit der Funktion "Synthetisches Backup" müssen keine regelmäßigen vollständigen Backups für unterstützte remote Ressourcen mehr durchgeführt werden. Das synthetische Backup wird von einem vollständigen Backup ("Basis" genannt) und von den folgenden inkrementellen Backups zusammengesetzt.

So verwenden Sie synthetische Backups anstelle von wiederkehrenden vollständigen Backups

Dieses synthetische Backup wird dann zum neuen Basis-Backup, sodass bis zur Erstellung des nächsten synthetischen Backups nur inkrementelle Backups durchgeführt werden müssen. Das synthetische Backup ist auf dem Stand des letzten inkrementellen Backups, das es enthält.

Die Komponenten eines synthetischen Backups sind folgende:

- **Basis-Backup.**
Das Basis-Backup ist das erste vollständige Backup, das ausgeführt wird, das mit dem synthetischen Backup verknüpft ist. Das vollständige Basis-Backup wird nur einmal ausgeführt. Dabei werden alle Dateien auf dem ausgewählten Computer gesichert.
- **Regelmäßige inkrementelle Backups.**
Inkrementelle Backup-Aufträge sichern die Dateien, die sich nach dem Basis-Backup ändern.
- **Regelmäßige synthetische Backups.**
Der synthetische Backup-Prozess kombiniert die Daten vom Basis-Backup und von den inkrementellen Backups, um ein synthetisiertes vollständiges Backup des ausgewählten Computers zu bilden. Dieses synthetisierte vollständige Backup wird ein neues Basis-Backup, das mit folgenden inkrementellen Backup-Sätzen kombiniert wird, um ein neues synthetisiertes vollständiges Backup zu bilden.

Für die Backups in einem synthetischen Backup, können Sie eine Stufe hinzufügen, um die Backup-Daten auf Band zu kopieren.

True Image-Wiederherstellung wird automatisch für synthetische Backups aktiviert. Mit der True Image-Wiederherstellung können Sie Verzeichnisse wiederherstellen, wie sie zu der Zeit des synthetischen Backups existierten. Dateien, die vor dem synthetischen Backup gelöscht wurden, werden nicht wiederhergestellt. Bei der True Image-Wiederherstellung werden nur die korrekten Dateiversionen aus den entsprechenden synthetischen vollständigen oder inkrementellen Backups, in denen sie enthalten sind, wiederhergestellt.

Nur Dateisystemdaten werden für synthetische Backups unterstützt. Unterstützte Daten umfassen gemeinsame Dateisystemobjekte, wie zum Beispiel Datenträger, Laufwerke und Ordner.

Voraussetzungen für synthetische Backups

Beachten Sie vor der Erstellung eines synthetischen Backup folgende Hinweise:

- Wenn Sie einen Verschlüsselungscode verwenden, müssen alle verknüpften Backups den gleichen Verschlüsselungscode verwenden. Ändern Sie nicht den Verschlüsselungscode, nachdem die Backups erstellt wurden. Der in den

zugehörigen Backups ausgewählte Verschlüsselungscode wird automatisch auf das synthetische Backup angewendet.

- Sie müssen Datenträgerspeicher konfigurieren, bevor Sie ein synthetisches Backup erstellen können. Für synthetische Backups müssen inkrementelle Backups Datenträgerspeicher verwenden. Das vollständige Basis-Backup und das vollständiges synthetische Backup können Band- oder Datenträgerspeicher verwenden.

Siehe ["Konfigurieren von Festplattenspeicher"](#) auf Seite 372.

- Wenn Sie den Basis-Backup-Auftrag zum Bandspeicher senden und Sie Bandspeicher für den synthetischen Backup-Auftrag verwenden möchten, müssen Sie zwei Bandlaufwerk haben. Sie müssen ein Bandlaufwerk verwenden, um das Basis-Backup zu installieren und ein Bandlaufwerk, um das synthetische Backup zu installieren.
- Sie können Dateisystemdaten nur für synthetische Backups auswählen.

Siehe ["Konfigurieren von Offhost-Backup-Optionen für einen Backup-Auftrag"](#) auf Seite 1530.

Siehe ["Infos zur True Image-Wiederherstellung für synthetische Backups"](#) auf Seite 1524.

Festlegen der Standard-Backup-Optionen für Advanced Disk Based Backup Feature

Sie können die bei der Installation von Backup Exec für alle Advanced Disk Based Backup Feature-Aufträge festgelegten Standardeinstellungen verwenden oder eigene Standardeinstellungen wählen. Sie können die Standardeinstellungen übergehen, wenn Sie einzelne Aufträge erstellen.

So legen Sie die Standard-Backup-Optionen für Advanced Disk Based Backup Feature fest

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- 2 Wählen Sie "Auftragsstandardeinstellungen" und dann eine Backup-Option.

Beispiel: Wenn Sie die die Standardoptionen für Advanced Disk Based Backup Feature-Backups-to-Disk einrichten möchten, wählen Sie "Backup-to-Disk" aus. Die Optionen, die angezeigt werden, hängen von den konfigurierten Speichergerätetypen ab. Verschiedene Standardoptionen können für Backup-Aufträge auf verschiedenen Speichertypen konfiguriert werden.

3 Wählen Sie im linken Teilfenster "Advanced Disk-based Backup".

4 Wählen Sie die entsprechenden Optionen aus:

Verwenden eines Offhost-Backup, um Backupverarbeitung von einem Remote-Computer auf einen Backup-Exec-Server zu verschieben

Wählen Sie diese Option aus, um ein Offhost-Backup zu aktivieren.

Off-Host-Backup aktiviert Backup Exec, um die Backup-Verarbeitung vom Hostcomputer auf den Backup Exec-Server zu verschieben. Das Off-Host Backup erstellt Snapshots der Datenträger, die für das Backup auf dem Remote-Computer ausgewählt werden. Die Snapshots werden dann auf den Backup Exec-Server importiert und dort gesichert.

Backup-Auftrag fortführen (Off-Host-Backup wird nicht verwendet)

Wählen Sie diese Option aus, um den Backup-Auftrag abzuschließen, ohne dass die Offhost-Funktion verwendet wird, wenn eine der folgenden Bedingungen auftritt:

- Die ausgewählten Datenträger unterstützen Off-Host-Backup nicht.
- Ein Fehler tritt auf, der sich auf den Snapshotimport oder den Datenträgerimport bezieht.

Backup-Auftrag abbrechen (nach einem Fehler werden keine weiteren Auswahlen gesichert)

Wählen Sie diese Option aus, damit der Backup-Auftrag fehl schlägt, wenn eine der folgenden Bedingungen auftritt:

- Die ausgewählten Datenträger unterstützen Off-Host-Backup nicht.
- Ein Fehler tritt auf, der sich auf den Snapshotimport oder den Datenträgerimport bezieht.

Logische Datenträger für das Offhost-Backup nacheinander verarbeiten

Wählen Sie diese Option aus, um das Backup mehrerer Datenträger in einem einzelnen Auftrag zu aktivieren, während Snapshots jeweils nur von einem logischen Datenträger erstellt werden. Von mehreren Datenträgern muss möglicherweise ein einzelner Snapshot erstellt werden, um die Datenintegrität zu gewährleisten oder wenn ein Datenträger Bereitstellungspunkte enthält.

Nachdem ein Snapshot des logischen Datenträgers erstellt und der logische Datenträger gesichert wurde, wird der Snapshot gelöscht, bevor ein weiterer Snapshot vom nächsten logischen Datenträger erstellt wird. Durch diese Option wird das Einhalten der Mindestruhezeit zum Erstellen des Snapshot erhöht.

Ein logischer Datenträger kann aus mehreren physischen Datenträgern bestehen, d. h. ein einzelner logischer Datenträger kann alle Datenträger der Datenbank umfassen.

Siehe ["Info zum Einsatz von Advanced Disk-based Backup Feature"](#) auf Seite 1519.

Siehe ["Sichern von Daten"](#) auf Seite 174.

Infos zur True Image-Wiederherstellung für synthetische Backups

True Image-Wiederherstellung wird automatisch für synthetische Backups aktiviert. Die True Image-Wiederherstellung ermöglicht Backup Exec den Zustand von Inhalten aus zum Zeitpunkt des letzten vollständigen Backups oder inkrementellen Backups wiederherzustellen. Die Wiederherstellungsauswahl in Backup-Sätzen wird von einer Ansicht der Verzeichnisse erstellt, wie sie zur Zeit des synthetischen Backups bestanden. Dateien, die vor dem Backup gelöscht wurden, können nicht wiederhergestellt werden. Bei der True Image-Wiederherstellung werden nur die korrekten Dateiversionen aus den entsprechenden vollständigen oder inkrementellen Backups, in denen sie enthalten sind, wiederhergestellt. Vorherige Versionen werden nicht wiederhergestellt und überschrieben, wenn sie nicht benötigt werden.

Hinweis: Für eine True Image-Wiederherstellung muss die Option "Speicherbasierte Kataloge verwenden" in den Einstellungen "Kataloge" aktiviert werden.

Siehe ["Konfigurieren der Standardoptionen für Kataloge"](#) auf Seite 279.

Backup Exec sammelt die Informationen, die erforderlich sind, um die Dateien und die Verzeichnisse zu erkennen, die von einem Bandarchiv oder von einem komprimierten Archiv verschoben, umbenannt (tar) oder installiert worden sind. Abhängig davon, wie die Dateien verpackt und installiert wurden, werden einige der kürzlich installierten Dateien nicht beim normalen inkrementellen Backup gesichert. Bei Auswahl dieser Option vergleicht Backup Exec die Pfadnamen mit den Pfadnamen vorheriger vollständiger oder inkrementeller Backups. Wenn ein Name neu ist oder geändert wurde, wird die Datei bzw. das Verzeichnis gesichert.

Die folgenden Beispiele zeigen, wie mithilfe der True Image-Wiederherstellung Dateien gesichert werden, die sonst nicht Teil eines Backup wären:

- Eine Datei, die "C:\pub\doc" heißt, wird auf C:\spec\doc verschoben oder installiert. Hier ist das Archivbit für Dateien und Unterverzeichnisse in diesem Verzeichnis unverändert, aber das Verzeichnis "C:\pub\doc" ist neu im C:\spec\Verzeichnis und wird gesichert.
- Ein Verzeichnis mit dem Namen C:\security\dev\ wird umbenannt in C:\security\devices\. Hier ist das Archivbit für Dateien und Unterverzeichnisse im Verzeichnis unverändert, aber C:\security\devices\ ist ein neues Verzeichnis und wird gesichert.

Die folgende Tabelle zeigt die Dateien, die im Zuge von mehreren Backups im Verzeichnis "C:\user\doc" zwischen dem 1. und dem 04. Dezember 2012 gesichert wurden:

Tabelle L-1 Beispieltabelle mit Dateien, die aufgrund der aktivierten True Image-Wiederherstellung gesichert werden

Tag	Art des Backup	Gesicherte Dateien in "C:\user\doc"	Gesicherte Dateien in "C:\user\doc"	Gesicherte Dateien in "C:\user\doc"	Gesicherte Dateien in "C:\user\doc"	Gesicherte Dateien in "C:\user\doc"	Gesicherte Dateien in "C:\user\doc"
1. Dezember 2012	Vollständiges Backup	file1	file2	VerzA\DateiA	VerzB\fileB	file3	
2. Dezember 2012	Inkrementell	file1	file2	VerzA\fileA	-----	-----	
3. Dezember 2012	Inkrementell	file1	file2	VerzA\fileA	-----	-----	
4. Dezember 2012	Inkrementell	file1	file2	-----	-----	-----	file4

Hinweis: Gedankenstriche (-----) weisen darauf hin, dass die Datei vor diesem Backup gelöscht wurde.

Angenommen, Sie wollen die Version des Verzeichnisses "C:\user\doc" vom 4. Dezember 2012 wiederherstellen.

Sie führen eine normale Wiederherstellung des vollständigen Backup-Satzes durch, der von einer normalen Wiederherstellung von folgenden inkrementellen Backup-Sätzen gefolgt wird. Das wiederhergestellte Verzeichnis enthält alle Dateien und Verzeichnisse, die je in "C:\user\doc" ab dem 1. Dezember 2012 (letztes vollständiges Backup) bis zum 4. Dezember 2012 existierten.

Die folgenden Dateien und Verzeichnisse sind beispielsweise enthalten:

- file1
- file2
- VerzA\fileA
- VerzB\fileB
- file3
- file4

Wenn Sie eine True Image-Wiederherstellung des Backups vom 4. Dezember 2012 durchführen, enthält das wiederhergestellte Verzeichnis nur die Dateien und Verzeichnisse, die zum Zeitpunkt des inkrementellen Backups vom 4. Dezember 2012 vorhanden waren.

Die folgende Liste enthält die zu diesem Zeitpunkt vorhandenen Dateien und Verzeichnisse:

- file1
- file2
- file4

Backup Exec stellt keine der vor dem inkrementellen Backup vom 4. Dezember 2012 gelöschten Dateien wieder her.

Das wiederhergestellte Verzeichnis umfasst nicht die "dirA"-Unterverzeichnisse, obwohl sie am 4. Dezember 2012 gesichert wurden. Backup Exec stellt diese Verzeichnisse nicht wiederher, weil sie nicht zu der Zeit des inkrementellen Backups existierten, was der Verweis für die True Image-Wiederherstellung war.

Die zum Zeitpunkt der True Image-Wiederherstellung im Verzeichnis enthaltenen Dateien, die nicht bei dem Backup vorhanden waren, bleiben erhalten.

Angenommen, Sie haben die Datei "file5" nach dem inkrementellen Backup vom 4. Dezember 2012, aber vor der Wiederherstellung, erstellt.

In diesem Fall enthält das Verzeichnis nach der Wiederherstellung folgende Dateien:

- file1

- file2
- file4
- file5

Siehe ["So verwenden Sie synthetische Backups anstelle von wiederkehrenden vollständigen Backups"](#) auf Seite 1520.

Siehe ["Konfigurieren von Offhost-Backup-Optionen für einen Backup-Auftrag"](#) auf Seite 1530.

Verwenden von Offhost-Backups zur Verarbeitung von Remote-Computer-Backups auf dem Backup Exec-Server

Off-Host-Backup aktiviert Backup Exec, um die Backup-Verarbeitung vom Hostcomputer auf den Backup Exec-Server zu verschieben. Das Off-Host Backup erstellt Snapshots der Datenträger, die für das Backup auf dem Remote-Computer ausgewählt werden. Die Snapshots werden dann auf den Backup Exec-Server importiert und dort gesichert.

Nach dem Backup werden die Snapshots vom Backup Exec exportiert und anschließend wieder auf dem Remote-Computer bereitgestellt und erneut mit dem Quelldatenträger synchronisiert. Dieser Prozess erfordert Lösungen von Hardwareanbietern, die übertragbare Snapshots unterstützen können. Transportfähige Snapshots sind Snapshots, die Sie auf den Backup Exec-Server importieren oder von ihm exportieren können. Der ausgewählte Microsoft Volume Shadow Copy Services (VSS)-Provider wird bei dem Off-Host-Backup auf allen Datenträgern verwendet. Ein Off-Host-Backup-Auftrag wird jeweils auf dem Remote-Computer durchgeführt.

Off-Host-Backup unterstützt Folgendes:

- Microsoft Volume Shadow Copy Service (VSS)
- Backups für NTFS-Datenträger mit vollständigen, inkrementellen und Differenzial-Backup-Methoden
- SQL Agent-Backups für Datenbanken Microsoft SQL Server 2000 und höher.
- Exchange Agent-Backups für Microsoft Exchange Server 2010-Instanzen, die unter Windows Server 2008 ausgeführt werden. Die Unterstützung von Backup Exec Granular Recovery Technology für Exchange Agent-Backups ist darin enthalten.

Anforderungen für Off-Host-Backup

Im Folgenden werden die Voraussetzungen für das Off-Host-Backup aufgeführt:

Tabelle L-2 Off-Host-Backup-Anforderungen

Element	Beschreibung
Backup Exec-Server	Advanced Disk Based Backup Feature muss installiert werden.
Remote-Computer	Agent for Windows muss auf dem Remote-Computer installiert sein.
Backup Exec-Server und der Remote-Computer	<p>Folgendes muss sowohl auf dem Backup Exec-Server als auch auf dem Remote-Computer installiert sein:</p> <ul style="list-style-type: none"> ■ Das gleiche Betriebssystem: Microsoft Windows Server 2008 und höher. ■ Die aktuellen Patches der Volume Shadow Copy Services (VSS). ■ Ein beliebiger Hardware-Snapshot-Provider für Microsoft VSS. Andernfalls können die Snapshots der Datenträger nicht auf den Backup Exec-Server exportiert werden. ■ Funktion, auf die SAN Shared Storage Option oder den logischen Datenträger zuzugreifen, die vom Backup Exec-Server und dem Remote-Computer gemeinsam genutzt werden.
Off-Host-Backups von Exchange Server-Ressourcen mit aktivierter GRT-Option	Off-Host-Backup unterstützt Exchange Agent-Backups für Microsoft Exchange Server 2010 unter Windows Server 2008 mit Service Pack 2 und höher. Sowohl de Backup Exec- als auch der Exchange-Server müssen die gleiche Version mit dem gleichen Patch-Level ausführen (inkl. VSS-Patches). Die Geräte müssen ebenfalls in der Hardwarekompatibilitätsliste aufgeführt werden.
Central Admin Server Feature	Wenn Central Admin Server Feature (CAS) installiert ist, achten Sie darauf, dass der Auftrag nicht vom zentralen Administrationsserver delegiert wird. So kann der Auftrag an einen verwalteten Backup Exec-Server delegiert werden, der keine Off-Host-Funktion hat. Bei CAS-Aufträgen, die die Off-Host-Backup-Methode verwenden, müssen Sie das Speichergerät manuell auswählen.

Beim Offhost-Backup mit Advanced Disk Based Backup Feature wird Folgendes nicht unterstützt:

- Option "Auftragswiederaufnahme"

Siehe ["Konfigurieren der Auftragswiederaufnahme"](#) auf Seite 667.

- Datenträger mit Windows-BitLocker-Laufwerksverschlüsselung
- Die Backup-Methode für Dateien Kataloge verwenden.
Siehe ["Ermittlung des Backup-Status von Dateien in Backup Exec"](#) auf Seite 218.

Bewährte Methoden für Off-Host-Backup

Folgende Vorgehensweisen werden empfohlen:

- Stellen Sie sicher, dass die Quelldatenträger und die Snapshot-Datenträger nicht auf die gleichen physischen Datenträger zugreifen. Andernfalls schlägt jeder Versuch, den Snapshotdatenträger vom ursprünglichen Datenträger zu teilen fehl.
- Bei den meisten Hardware- und Software-Providern liegen Beschränkungen in Bezug auf übertragbare Datenträgertypen vor. Deshalb wird empfohlen, dass Sie Off-Host-Backup-Aufträge nur für das Sichern von Daten verwenden, für die alle abhängigen Datenträger importiert und exportiert werden können.
- Stellen Sie sicher, dass der für das Backup ausgewählte Datenträger importiert bzw. exportiert werden kann und dass sich der VSS-Hardwareanbieter auf der Kompatibilitätsliste befindet. Andernfalls schlägt die Fehlerbehebung des Off-Host-Backup fehl. Das Backup kann fortgesetzt werden, wenn das Off-Host-Backup fehlschlägt.
Die unterstützten Speichertypen finden Sie in der Liste der mit Backup Exec kompatiblen Hardware.
- Das Hitachi Raid Manager-Protokoll darf sich nicht auf einem Datenträger befinden, von dem ein Snapshot erstellt wird. Bei Hitachi wird während des Snapshot-Reservierungsvorgangs I/O auf die Raid Manager-Protokolldatei ausgeführt, und der VSS-Koordinator blockiert den Zugang zu jedem Laufwerk, von dem ein Snapshot erstellt wird. Wenn sich also das Protokollverzeichnis für Raid Manager auf dem Datenträger befindet, von dem gerade ein Snapshot erstellt wird, werden I/O-Vorgänge für das Protokoll blockiert und der Snapshot-Vorgang steckt fest.
- Wenn Central Admin Server Feature (CAS) installiert wird, müssen Sie den Speicher für das Offhost-Backup manuell auswählen. Andernfalls wird der Auftrag möglicherweise zu einem Backup Exec-Server delegiert, der keine Off-Host-Funktion hat.
Siehe ["Verwenden von Backup Exec-Server-Pools in CAS "](#) auf Seite 1498.
- Wenn Sie Off-Host-Backup ausführen, das einen VSS-Hardwareanbieter in einer Microsoft Cluster-Umgebung (MSCS) verwendet, dürfen sich der Backup Exec-Server und der Remote-Computer nicht in derselben Clustergruppe befinden. Die Clusteranwendungen können die LUNs (Logical Unit Numbers,

Nummern der logischen Einheit), die doppelte Signaturen und Partitions-Layouts haben, nicht unterstützen. Die Snapshots, die LUNs enthalten, müssen zu einem Hostcomputer transportiert werden, der sich außerhalb des Clusters befindet.

Siehe ["Sichern von Daten"](#) auf Seite 174.

Siehe ["Konfigurieren von Offhost-Backup-Optionen für einen Backup-Auftrag"](#) auf Seite 1530.

Siehe ["Festlegen der Standard-Backup-Optionen für Advanced Disk Based Backup Feature"](#) auf Seite 1522.

Siehe ["Fehlerbehebung bei Off-Host-Backups"](#) auf Seite 1533.

Konfigurieren von Offhost-Backup-Optionen für einen Backup-Auftrag

Mit dem Offhost-Backup kann Backup Exec die Backup-Verarbeitung vom Hostcomputer, d.h. vom Remote-Computer mit den für das Backup ausgewählten Datenträgern, zum Backup Exec-Medienserver verschoben werden. Das Off-Host Backup erstellt Snapshots der Datenträger, die für das Backup auf dem Remote-Computer ausgewählt werden. Die Snapshots werden dann auf den Medienserver importiert und dort gesichert.

So konfigurieren Sie Offhost-Backup-Optionen für einen Backup-Auftrag

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" mit der rechten Maustaste auf den oder die zu sichernden Server oder die Servergruppe.
- 2 Wählen Sie "Backup", und wählen Sie dann den Typ des durchzuführenden Backups aus.
- 3 Klicken Sie im Dialogfeld "Backup-Eigenschaften" im Feld "Auswahl" auf "Bearbeiten".
- 4 Aktivieren Sie im Dialogfeld "Backup-Auswahl" die Kontrollkästchen für die zu sichernden Ressourcen, und heben Sie die Markierung der Kontrollkästchen für die Quellen auf, die nicht gesichert werden sollen.
- 5 Klicken Sie auf "OK".
- 6 Klicken Sie im Dialogfeld "Eigenschaften der Backup-Definition" im Feld "Backup" auf "Bearbeiten".
- 7 Wählen Sie im Dialogfeld "Backup-Optionen" einen Zeitplan für diesen Auftrag.
- 8 Wählen Sie im Dialogfeld "Backup-Optionen" im linken Teilfenster "Advanced Disk-based Backup" aus.

9 Stellen Sie eine der folgenden Optionen für diesen Auftrag ein:

Verwenden eines Offhost-Backup, um Backupverarbeitung von einem Remote-Computer auf einen Backup-Exec-Server zu verschieben	<p>Wählen Sie diese Option aus, um ein Offhost-Backup zu aktivieren.</p> <p>Off-Host-Backup aktiviert Backup Exec, um die Backup-Verarbeitung vom Hostcomputer auf den Backup Exec-Server zu verschieben. Das Off-Host Backup erstellt Snapshots der Datenträger, die für das Backup auf dem Remote-Computer ausgewählt werden. Die Snapshots werden dann auf den Backup Exec-Server importiert und dort gesichert.</p>
Backup-Auftrag fortführen (Off-Host-Backup wird nicht verwendet)	<p>Wählen Sie diese Option aus, um den Backup-Auftrag abzuschließen, ohne dass die Offhost-Funktion verwendet wird, wenn eine der folgenden Bedingungen auftritt:</p> <ul style="list-style-type: none"> ■ Die ausgewählten Datenträger unterstützen Off-Host-Backup nicht. ■ Ein Fehler tritt auf, der sich auf den Snapshotimport oder den Datenträgerimport bezieht.
Backup-Auftrag abbrechen (nach einem Fehler werden keine weiteren Auswahlen gesichert)	<p>Wählen Sie diese Option aus, damit der Backup-Auftrag fehl schlägt, wenn eine der folgenden Bedingungen auftritt:</p> <ul style="list-style-type: none"> ■ Die ausgewählten Datenträger unterstützen Off-Host-Backup nicht. ■ Ein Fehler tritt auf, der sich auf den Snapshotimport oder den Datenträgerimport bezieht.

Logische Datenträger für das Offhost-Backup nacheinander verarbeiten

Wählen Sie diese Option aus, um das Backup mehrerer Datenträger in einem einzelnen Auftrag zu aktivieren, während Snapshots jeweils nur von einem logischen Datenträger erstellt werden. Von mehreren Datenträgern muss möglicherweise ein einzelner Snapshot erstellt werden, um die Datenintegrität zu gewährleisten oder wenn ein Datenträger Bereitstellungspunkte enthält.

Nachdem ein Snapshot des logischen Datenträgers erstellt und der logische Datenträger gesichert wurde, wird der Snapshot gelöscht, bevor ein weiterer Snapshot vom nächsten logischen Datenträger erstellt wird. Durch diese Option wird das Einhalten der Mindestruhezeit zum Erstellen des Snapshot erhöht.

Ein logischer Datenträger kann aus mehreren physischen Datenträgern bestehen, d. h. ein einzelner logischer Datenträger kann alle Datenträger der Datenbank umfassen.

- 10 Klicken Sie im Dialogfeld "Backup-Optionen" auf eine der für diesen Auftrag festzulegenden optionalen Einstellungen.
- 11 Klicken Sie auf "OK".
- 12 Klicken Sie im Dialogfeld "Eigenschaften der Backup-Definition" auf "OK".

Siehe ["Info zum Einsatz von Advanced Disk-based Backup Feature"](#) auf Seite 1519.

Siehe ["Verwenden von Offhost-Backups zur Verarbeitung von Remote-Computer-Backups auf dem Backup Exec-Server"](#) auf Seite 1527.

Bewährte Methoden für Off-Host-Backup

Folgende Vorgehensweisen werden empfohlen:

- Stellen Sie sicher, dass die Quelldatenträger und die Snapshot-Datenträger nicht auf die gleichen physischen Datenträger zugreifen. Andernfalls schlägt jeder Versuch, den Snapshotdatenträger vom ursprünglichen Datenträger zu teilen fehl.
- Bei den meisten Hardware- und Software-Providern liegen Beschränkungen in Bezug auf übertragbare Datenträgertypen vor. Deshalb wird empfohlen, dass Sie Off-Host-Backup-Aufträge nur für das Sichern von Daten verwenden, für die alle abhängigen Datenträger importiert und exportiert werden können.
- Das Off-Host-Backup schlägt fehl, wenn ein Datenträger, den Sie für das Backup auswählen, nicht importiert oder exportiert werden kann. Das Off-Host-Backup

schlägt auch fehl, wenn sich der erforderliche VSS-Hardwareanbieter nicht auf einer Liste der kompatiblen Hardware befindet. Das Backup kann fortgesetzt werden, wenn das Off-Host-Backup fehlschlägt.

Die unterstützten Speichertypen finden Sie in der Liste der mit Backup Exec kompatiblen Hardware.

- Das Hitachi Raid Manager-Protokoll darf sich nicht auf einem Datenträger befinden, von dem ein Snapshot erstellt wird. Bei Hitachi wird während des Snapshot-Reservierungsvorgangs I/O auf die Raid Manager-Protokolldatei ausgeführt, und der VSS-Koordinator blockiert den Zugang zu jedem Laufwerk, von dem ein Snapshot erstellt wird. Wenn sich also das Protokollverzeichnis für Raid Manager auf dem Datenträger befindet, von dem gerade ein Snapshot erstellt wird, werden I/O-Vorgänge für das Protokoll blockiert und der Snapshot-Vorgang steckt fest.
- Wenn Central Admin Server Feature (CAS) installiert wird, müssen Sie den Speicher für das Offhost-Backup manuell auswählen. Andernfalls wird der Auftrag möglicherweise zu einem Backup Exec-Server delegiert, der keine Off-Host-Funktion hat.
Siehe ["Verwenden von Backup Exec-Server-Pools in CAS "](#) auf Seite 1498.
- Wenn Sie Off-Host-Backup ausführen, das einen VSS-Hardwareanbieter in einer Microsoft Cluster-Umgebung (MSCS) verwendet, dürfen sich der Backup Exec-Server und der Remote-Computer nicht in derselben Clustergruppe befinden. Die Clusteranwendungen können die LUNs (Logical Unit Numbers, Nummern der logischen Einheit), die doppelte Signaturen und Partitions-Layouts haben, nicht unterstützen. Die Snapshots, die LUNs enthalten, müssen zu einem Hostcomputer transportiert werden, der sich außerhalb des Clusters befindet.

Siehe ["Fehlerbehebung bei Off-Host-Backups"](#) auf Seite 1533.

Fehlerbehebung bei Off-Host-Backups

Bei Off-Host-Backups muss darauf geachtet werden, dass für die VSS-Anbieter und die zu übertragenden Datenträger jeweils die korrekten Einstellungen ausgewählt wurden. Advanced Disk Based Backup Feature unterstützt nicht alle Speichergruppen.

Die unterstützten Speichertypen finden Sie in der Liste der mit Backup Exec kompatiblen Hardware.

Um eine Problembehebung bei Off-Host-Backup durchzuführen, sollten Sie die Tools verwenden, die beim VSS-Anbieter verfügbar sind, um die erforderliche Installation für Off-Host-Backup zu überprüfen.

Die minimalen Einrichtungsanforderungen sind wie folgt:

- Von Datenträger, die Sie sichern möchten, kann ein Snapshot erstellt werden.
- Datenträger werden vom Remote-Computer und dem Backup Exec-Server gemeinsam genutzt.
- Ein Off-Host-Backup-Auftrag kann nur die Datenträger enthalten, die zum Backup Exec-Server für den Backup transportiert werden können.

Weiterhin müssen die folgenden Faktoren beachtet werden:

- Windows Server 2008 mit Service Pack 2 muss auf dem Backup Exec-Server und auf dem Remote-Computer installiert sein. Beide Computer müssen mit den aktuellen Patches der Volume Shadow Copy Services (VSS) ausgestattet sein.
- Auf dem Backup Exec-Server und dem Remote-Computer muss Microsoft XML Core Services (MSXML 6.0 SP2) installiert und aktiv sein.

Fehlerbehebung bei Off-Host-Backup-Problemen hängt vom VSS-Anbieter ab, der für die Snapshots verwendet wird.

Die folgenden Installationsprobleme, die für alle Anbieter gelten, verursachen möglicherweise Off-Host-Backup-Fehler:

Tabelle L-3 Allgemeine Einstellungsprobleme für Off-Host-Backup

Problem	Lösung
Die Datenträger werden nicht gemeinsam genutzt.	Sie müssen sicherstellen, dass alle Datenträger sich auf den Datenträgern befinden, die vom Remote-Computer und dem Backup Exec-Server gemeinsam genutzt werden. Wenn die Datenträger nicht gemeinsam genutzt werden, schlägt der Importvorgang fehl. Sie müssen möglicherweise die Snapshots bereinigen und die Datenträger erneut manuell synchronisieren.
Der VSS-Anbieter ist nicht auf dem Backup Exec-Server und dem Remote-Computer installiert.	Der Anbieter, der für den Snapshot verwendet wird, muss auf dem Backup Exec-Server und auf dem Remote-Computer installiert sein. Wenn der Anbieter nicht auf dem Backup Exec-Server installiert ist, schlägt der Importvorgang fehl. Sie müssen möglicherweise die Snapshots bereinigen und die Datenträger erneut manuell synchronisieren.
Datenträger sind nicht übertragbar.	Alle Datenträger, die für Backup ausgewählt werden, müssen zum Backup Exec-Server transportfähig sein. Überprüfen Sie bei der Auswahl von Microsoft SQL oder Exchange bzw. anderen Datenbankanwendungen für das Backup, ob die Datenbanken und Protokolldateien auf übertragbaren Datenträgern gespeichert sind.

Problem	Lösung
Der VSS-Anbieter kann keinen Snapshot von ausgewählten Datenträger erstellen.	Alle Datenträger, die für Backup ausgewählt werden, müssen zum Backup Exec-Server transportfähig sein. Auf allen Datenträgern, die Sie für Backup auswählen, muss über denselben Anbieter ein Snapshot erstellt werden können. Sie müssen sicherstellen, dass derselbe VSS-Anbieter alle Datenträger in einem Backup-Auftrag unterstützt.
Speicherort der Protokolle ist falsch.	Wenn der Anbieter oder die unterstützende Anwendung Protokolldateien während des normalen Snapshotvorgangs erstellt, sollten sich die Protokolldateien nicht auf den Datenträgern, auf denen Snapshots erstellt werden können, befinden. VSS kann die Puffer nicht leeren, und der Snapshot überschreitet einen Zeitwert. Speichern Sie die Protokolle auf einem anderen Datenträger.
Der Provider von VSS-Dienstleistungen wurde nicht gestartet.	Der Anbieterdienst muss ausgeführt werden und der Windows-Volumeschattenkopie-Dienst von Windows darf nicht deaktiviert werden.
Die Identifikationsdaten sind falsch.	Die Identifikationsdaten der Computerstufe, die für den Auftrag verwendet werden, müssen auf dem Backup Exec-Server und dem Remote-Computer gleich sein. Nicht übereinstimmende Identifikationsdaten führen zu Fehlern bei den Snapshots oder dem Backup.
Der VSS-Anbieter ist nicht auf allen Backup Exec-Servern in einer Central Admin Server Feature(CAS)-Umgebung installiert.	Wenn Sie einen Backup-Auftrag in einer CAS-Umgebung konfigurieren, müssen Sie den Auftrag zu den verwalteten Backup Exec-Servern senden, auf denen der ausgewählte VSS-Anbieter installiert wird. Der zentrale Administrationsserver darf den Auftrag nicht delegieren. Andernfalls wird der Auftrag möglicherweise zu einem verwalteten Backup Exec-Server delegiert, der keine Off-Host-Funktion hat.

Problem	Lösung
Der Backup Exec-Server und der Remote-Computer befinden sich in derselben Clustergruppe.	<p>Für ein Off-Host-Backup in einer Microsoft Cluster-Umgebung dürfen sich der Backup Exec-Server und der Remote-Computer nicht in derselben Clustergruppe befinden. Die Clusteranwendungen können die LUNs (Logical Unit Numbers, Nummern der logischen Einheit), die doppelte Signaturen und Partitions-Layouts haben, nicht unterstützen. Deshalb müssen Sie die Snapshots transportieren, die die LUNs für einen Backup Exec-Server enthalten, der außerhalb des Cluster ist, in dem sich der Hostcluster befindet.</p> <p>Siehe "Funktionsweise von Backup Exec in einer Microsoft Cluster Server-Umgebung" auf Seite 914.</p> <p>Wenn Sie ein Hitachi 9970 verwenden und versuchen, Microsoft Cluster-Daten mit Advanced Disk Based Backup Feature zu sichern, wird eventuell folgende Fehlermeldung angezeigt:</p> <p>Der Auftrag schlug mit dem folgenden Fehler fehl: Beim Abfragen des Writer-Status ist ein Fehler aufgetreten.</p> <p>Um diesen Fehler zu beheben, stellen Sie sicher, dass der RM Shadow Copy-Anbieter für den Volume-Snapshot-Dienst vorhanden ist und ausgeführt wird. Sollte dieser Dienst nicht ausgeführt werden, führen Sie RMVSSPRV.exe in c:\horcm\tool aus. Wenden Sie sich an Hitachi, wenn der Dienst immer noch nicht ausgeführt werden kann.</p>

Off-Host-Backup-Probleme mit Hardwareanbietern

Hardware-Datenträger-Array-Anbieter unterstützen möglicherweise VSS-Snapshots und die Übertragung von Datenträgern auf den Backup Exec-Server zum Sichern in einer SAN-Umgebung. Die Verwendung von Hardware-Providern erfordert umfassende Kenntnisse darüber, wie Datenträger-Arrays zur Freigabe für den Remote-Computer und den Backup Exec-Server in einer SAN-Umgebung konfiguriert werden.

Informationen zum Einrichten von Datenträger-Arrays für Off-Host-Backup finden Sie in der Dokumentation zu Hardware-Datenträger-Arrays. Beachten Sie dabei insbesondere die Einschränkungen zur Verwendung der Datenträger-Arrays mit VSS-Snapshots sowie die Hinweise zum Überprüfen der Übertragbarkeit von Datenträgern. Es wird empfohlen, dass Sie alle Tools nutzen, die Händler zum Überprüfen der Einstellung und zur Fehlerbehebung zur Verfügung stellen.

Ein mögliches Off-Host-Backup-Problem, das auftreten kann, wenn Sie Hitachi-Hardware verwenden, ist, dass Hitachi nur Basisdatenträger für Off-Host-Backup unterstützt. Die Off-Host-Backup-Funktion wird nicht unterstützt,

wenn ein Computer eine Kombination von dynamischen und von Basisdatenträgern und den Hitachi-Anbieter verwendet.

Siehe ["Info zum Einsatz von Advanced Disk-based Backup Feature"](#) auf Seite 1519.

Siehe ["Verwenden von Offhost-Backups zur Verarbeitung von Remote-Computer-Backups auf dem Backup Exec-Server"](#) auf Seite 1527.

Off-Host-Backup-Probleme mit Hardwareanbietern

Hardware-Datenträger-Array-Anbieter unterstützen möglicherweise VSS-Snapshots und die Übertragung von Datenträgern auf den Backup Exec-Server zum Sichern in einer SAN-Umgebung. Die Verwendung von Hardware-Providern erfordert umfassende Kenntnisse darüber, wie Datenträger-Arrays zur Freigabe für den Remote-Computer und den Backup Exec-Server in einer SAN-Umgebung konfiguriert werden.

Informationen zum Einrichten von Datenträger-Arrays für Off-Host-Backup finden Sie in der Dokumentation zu Hardware-Datenträger-Arrays. Beachten Sie dabei insbesondere die Einschränkungen zur Verwendung der Datenträger-Arrays mit VSS-Snapshots sowie die Hinweise zum Überprüfen der Übertragbarkeit von Datenträgern. Es wird empfohlen, dass Sie alle Tools nutzen, die Händler zum Überprüfen der Einstellung und zur Fehlerbehebung zur Verfügung stellen.

Ein mögliches Off-Host-Backup-Problem, das auftreten kann, wenn Sie Hitachi-Hardware verwenden, ist, dass Hitachi nur Basisdatenträger für Off-Host-Backup unterstützt. Die Off-Host-Backup-Funktion wird nicht unterstützt, wenn ein Computer eine Kombination von dynamischen und von Basisdatenträgern und den Hitachi-Anbieter verwendet.

Siehe ["Fehlerbehebung bei Off-Host-Backups"](#) auf Seite 1533.

Backup Exec NDMP-Funktion

Dieser Anhang enthält folgende Themen:

- Funktionen von NDMP Feature
- Anforderungen für das Verwenden von NDMP Feature
- Info zum Installieren von NDMP Feature
- Hinzufügen von NDMP-Server zu Backup Exec
- Gemeinsames Nutzen des Bandlaufwerks auf NDMP-Servern zwischen mehreren Backup Exec-Servern
- NDMP-Backup-Optionen für NDMP-Server
- Backup-Auswahlen für NDMP-Server
- Verwenden von Mustern zum Ausschließen von Dateien und Verzeichnissen von einem NDMP-Server-Backup
- Unterstützte Konfigurationen für das Duplizieren von Daten aus NDMP-Servern
- Wiederherstellen und Umleiten von Wiederherstellungsdaten für NDMP-Server
- Festlegen der Standard-Backup-Optionen für NDMP Feature
- Anzeigen der Eigenschaften eines NDMP-Servers
- Anzeigen von Speichereigenschaften für einen NDMP-Server

Funktionen von NDMP Feature

Backup Exec NDMP Feature verwendet das Network Data Management Protocol (NDMP), um NAS-NDMP-Server zu sichern und wiederherzustellen.

Sie können die folgenden Konfigurationen verwenden, um die Daten auf einem NDMP-Server zu sichern:

- Eine direkt angehängte Konfiguration, in der ein Bandgerät oder eine virtuelle Bandbibliothek direkt mit dem NDMP-Server verbunden ist.
- Eine Dreizeigekonfiguration, in der ein Bandgerät oder eine virtuelle Bandbibliothek mit einem anderen NDMP-Server verbunden ist.
- Eine Remote-Konfiguration, in der ein Speichergerät am Backup Exec-Server angeschlossen ist.
- Eine Konfiguration, in der ein Speichergerät am selben SAN wie der Backup Exec-Server angeschlossen ist.

Hinweis: Sie können Daten von einem NDMP-Server nicht in eine simulierte Bandbibliothek oder auf einem Bandgerät sichern, das mit Backup Exec Remote Media Agent for Linux verbunden ist.

Sie können Backup-Sätze von einem NDMP-Server nicht an einen Computer umleiten, auf dem Windows- oder Linux ausgeführt wird.

Informationen zu den Best Practices zum Einsatz von Backup Exec NDMP Option finden Sie unter *Best Practices für Backup Exec*.

Siehe ["Anforderungen für das Verwenden von NDMP Feature"](#) auf Seite 1539.

Siehe ["Gemeinsames Nutzen des Bandlaufwerks auf NDMP-Servern zwischen mehreren Backup Exec-Servern"](#) auf Seite 1542.

Anforderungen für das Verwenden von NDMP Feature

Die folgenden Komponenten sind erforderlich:

- Backup Exec muss auf einem Windows-Server installiert werden, auf dem ein unterstütztes Betriebssystem ausgeführt wird.
Die unterstützten Betriebssysteme finden Sie in der Liste der mit Backup Exec kompatiblen Software.
- Der NDMP-Netzwerkspeicherserver muss Version 4 von Network Data Management Protocol ausführen.

Die unterstützten Speichertypen finden Sie in der Liste der mit Backup Exec kompatiblen Hardware.

Siehe ["Info zum Installieren von NDMP Feature"](#) auf Seite 1540.

Siehe ["Hinzufügen von NDMP-Server zu Backup Exec"](#) auf Seite 1540.

Info zum Installieren von NDMP Feature

NDMP Feature wird als separate Add-On-Komponente von Backup Exec lokal auf dem Backup Exec-Server installiert. Auf die NAS-NDMP-Server werden keine Dateien kopiert.

Siehe ["Installieren zusätzlicher Agents und Funktionen auf dem lokalen Backup Exec-Server"](#) auf Seite 66.

Siehe ["Anforderungen für das Verwenden von NDMP Feature"](#) auf Seite 1539.

Hinzufügen von NDMP-Server zu Backup Exec

Sie können Backup Exec einen NAS-NDMP-Server hinzufügen, um ihn zu sichern und die angeschlossenen Speichergeräte zu verwenden.

Wenn Sie einen NDMP-Server in einer Central Admin Server Feature-Umgebung hinzufügen, müssen Sie sie einem der folgenden Elemente hinzufügen:

- Dem zentralen Administrationsserver
- Einem verwalteten Backup Exec-Server, auf dem sich das Gerät und die Mediendatenbank befindet

Tabelle M-1 So fügen Sie Backup Exec einen NDMP-Server hinzu

Aufgabe	Methode
So fügen Sie einen zu sichernden NDMP-Server hinzu	<p>Verwenden Sie den Assistenten "Server hinzufügen" und fügen Sie den NDMP-Server als Dateiserver oder NDMP-Datenserver hinzu. Der NDMP-Server wird der Liste der Servern auf der Registerkarte "Backup und Wiederherstellung" hinzugefügt.</p> <p>Siehe "Serverliste auf der Registerkarte "Backup und Wiederherstellung" auf Seite 166.</p>

Aufgabe	Methode
So fügen Sie einen NDMP-Server zum Sichern und Nutzen seiner angeschlossenen Speichergeräte hinzu	<p>Verwenden Sie den Assistenten "Speicher konfigurieren", um den NDMP-Server der Liste der Server auf der Registerkarte "Backup und Wiederherstellung" hinzuzufügen. Nachdem die Backup Exec-Dienste neu gestartet wurden, erkennt Backup Exec automatisch alle Speichergeräte, die am NDMP-Server angeschlossen sind. Die Speichergeräte werden auf der Registerkarte "Speicher" angezeigt.</p> <p>Siehe "So fügen Sie den NDMP-Server zum Sichern und Nutzen seiner angeschlossenen Speichergeräte hinzu" auf Seite 1541.</p>

So fügen Sie den NDMP-Server zum Sichern und Nutzen seiner angeschlossenen Speichergeräte hinzu

- 1

Klicken Sie auf der Registerkarte "Speicher" in der Gruppe "Konfigurieren" auf "Speicher konfigurieren".
- 2

Sie haben folgende Möglichkeiten:

Wenn Central Admin Server Feature nicht installiert ist

Klicken Sie auf "Netzwerkspeicher" und dann auf "Weiter".

Wenn Central Admin Server Feature installiert ist

Gehen Sie dazu in folgender Reihenfolge vor:

■ Wählen Sie den Backup Exec-Server aus, auf dem Sie Speicher konfigurieren wollen, und klicken Sie dann auf "Weiter".

■ Klicken Sie auf "Netzwerkspeicher" und dann auf "Weiter".

3

Klicken Sie auf "NDMP-Speicher" und dann auf "Weiter".

4

Geben Sie einen Hostnamen oder einen vollständig qualifizierten Domännennamen des NDMP-Servers und eine Beschreibung ein und klicken Sie dann auf "Weiter".

Gemeinsames Nutzen des Bandlaufwerks auf NDMP-Servern zwischen mehreren Backup Exec-Servern**5** Füllen Sie die folgenden Felder aus:

Portnummer

Geben Sie die für die Kommunikation zwischen dem Backup Exec-Server und dem NDMP-Server zu verwendende Portnummer ein.

Login-Konto

Wählen Sie den Namen des Login-Kontos für den NDMP-Server aus. Sie können ein neues Login-Konto hinzufügen oder ein vorhandenes bearbeiten.

Verwenden der ICMP-Pingvorgänge von Backup Exec zum Erkennen des Servers

Wählen Sie diese Option aus, damit Backup Exec den NDMP-Server mit Ping-Vorgängen erkennen kann.

6 Klicken Sie auf "Weiter".**7** Lesen Sie die Übersicht und führen einen der folgenden Schritte aus:

So ändern Sie die Konfiguration

Gehen Sie dazu in folgender Reihenfolge vor:

- Klicken Sie auf die Überschrift, die die Elemente enthält, die Sie ändern möchten.
- Nehmen Sie alle Änderungen, vor und klicken Sie dann auf "Weiter", bis die Übersicht angezeigt wird.
- Klicken Sie auf "Fertigstellen".

So konfigurieren Sie den NDMP-Server

Klicken Sie auf "Fertigstellen".

8 Klicken Sie auf die Registerkarte "Backup und Wiederherstellung" und zeigen Sie den NDMP-Server in der Liste der Server an.

Gemeinsames Nutzen des Bandlaufwerks auf NDMP-Servern zwischen mehreren Backup Exec-Servern

Um die Bandlaufwerke, die an einem NAS-NDMP-Server angeschlossen sind, gemeinsam zu nutzen, muss NDMP Feature und Central Admin Server Feature (CAS) installiert sein. CAS wird im Rahmen von Enterprise Server Feature (ESF) installiert.

Sie können dann auswählen, welche Backup Exec-Server die Bandlaufwerke gemeinsam nutzen können. Der Backup Exec-Server, den Sie verwendeten, um den NDMP-Server hinzuzufügen, wird automatisch für die gemeinsame Nutzung ausgewählt.

Hinweis: Wenn Sie aus einer früheren Version von Backup Exec aktualisiert haben, wird die vorhandene Konfiguration beibehalten. Sie müssen daher die gemeinsame Nutzung für bestehende Konfigurationen nicht einrichten.

So nutzen Sie ein Bandlaufwerk auf NDMP-Servern zwischen mehrere Backup Exec-Servern gemeinsam

- 1 Klicken Sie auf der Registerkarte "Speicher" mit der rechten Maustaste auf das Speichergerät, das Sie freigeben möchten.
- 2 Klicken Sie auf "Freigeben".
- 3 Prüfen Sie die Backup Exec-Server oder die verwalteten Backup Exec-Server, die dieses Speichergerät gemeinsam nutzen sollen.
- 4 Klicken Sie auf "OK".

Siehe ["Infos zu Central Admin Server Feature"](#) auf Seite 1450.

NDMP-Backup-Optionen für NDMP-Server

Wenn Sie einen Backup-Auftrag für einen NAS-NDMP-Server erstellen, können Sie die Optionen verwenden, die für den Auftrag und den Typ des NDMP-Servers angebracht sind.

Die folgenden Backup-Optionen sind für NDMP-Server von NetApp und Fujitsu verfügbar:

Tabelle M-2 NDMP-Backup-Optionen für NetApp/Fujitsu

Element	Beschreibung
Zugriffskontrolllisten sichern	Sichert NetApp-Zugriffskontrolllisten.

Element	Beschreibung
Dateiverlauf aktivieren	<p>Aktiviert die Erstellung von Dateiverlaufsdaten. Der Dateiverlauf wird zum Optimieren der Wiederherstellung ausgewählter Backup-Sätze verwendet. Die Erzeugung und die Verarbeitung des Dateiverlaufs führen jedoch dazu, dass das Backup mehr Zeit in Anspruch nimmt. Das Deaktivieren dieser Option verkürzt die Backup-Zeit.</p> <p>Wenn der Dateiverlauf nicht generiert wird und Sie zu einem späteren Zeitpunkt Daten wiederherstellen müssen, muss der gesamte Datenträger wiederhergestellt werden.</p>
Backup-Methode	<p>Gibt die Backup-Stufe an. Stufe 0 entspricht einem vollständigen Backup. Stufe 1 entspricht einem Differenzial-Backup, das neue oder seit dem letzten Backup der Stufe 0 geänderte Dateien sichert. Bei Backups der Stufen 2 bis 9 werden die seit dem Backup der vorhergehenden Stufe neuen oder geänderten Dateien gesichert. Beispielsweise werden beim Backup der Stufe 2 die seit dem Backup der Stufe 1 neuen oder geänderten Dateien gesichert. Beim Backup der Stufe 3 werden die seit dem Backup der Stufe 2 neuen oder geänderten Dateien gesichert usw.</p>

Die folgenden Backup-Optionen sind für IBM-Server verfügbar:

Tabelle M-3 NDMP-Backup-Optionen für IBM

Element	Beschreibung
Zugriffskontrolllisten sichern	Sichert NetApp-Zugriffskontrolllisten.

Element	Beschreibung
Dateiverlauf aktivieren	<p>Aktiviert die Erstellung von Dateiverlaufsdaten. Der Dateiverlauf wird zum Optimieren der Wiederherstellung ausgewählter Backup-Sätze verwendet. Die Erzeugung und die Verarbeitung des Dateiverlaufs führen jedoch dazu, dass das Backup mehr Zeit in Anspruch nimmt. Das Deaktivieren dieser Option verkürzt die Backup-Zeit.</p> <p>Wenn der Dateiverlauf nicht generiert wird und Sie zu einem späteren Zeitpunkt Daten wiederherstellen müssen, muss der gesamte Datenträger wiederhergestellt werden.</p>
Backup-Methode	<p>Gibt die Backup-Stufe an. Stufe 0 entspricht einem vollständigen Backup. Stufe 1 entspricht einem Differenzial-Backup, das neue oder seit dem letzten Backup der Stufe 0 geänderte Dateien sichert. Bei Backups der Stufen 2 bis 9 werden die seit dem Backup der vorhergehenden Stufe neuen oder geänderten Dateien gesichert. Beispielsweise werden beim Backup der Stufe 2 die seit dem Backup der Stufe 1 neuen oder geänderten Dateien gesichert. Beim Backup der Stufe 3 werden die seit dem Backup der Stufe 2 neuen oder geänderten Dateien gesichert usw.</p>
SENDFILE	<p>Gibt an, ob die Aufträge die Umgebungsvariable SENDFILE verwenden dürfen. Wenn dieses Kontrollkästchen aktiviert ist, steuert Backup Exec SENDFILE und legt den entsprechenden Wert fest. Wenn das Kontrollkästchen nicht aktiviert ist, wird die Variable SENDFILE auf 0 festgelegt und nicht für den Auftrag verwendet.</p>

Die folgenden Backup-Optionen sind für NDMP-Server von EMC verfügbar:

Tabelle M-4 NDMP-Backup-Optionen für EMC

Element	Beschreibung
Backup-Typ	<p>Legt den Backup-Typ für diesen Backup-Auftrag fest.</p> <p>Die folgenden Backup-Typen sind verfügbar:</p> <ul style="list-style-type: none">■ Ausgabe■ VBB
Sichern mit integrierten Wiederaufnahmepunkten (SnapSure)	<p>Ermöglicht Backup Exec die Erstellung eines Backup-Satzes mit EMC SnapSure. Weitere Informationen zu SnapSure finden Sie in der EMC-Dokumentation.</p>
Dateiverlauf aktivieren	<p>Aktiviert die Erstellung von Dateiverlaufsdaten. Der Dateiverlauf wird zum Optimieren der Wiederherstellung ausgewählter Backup-Sätze verwendet. Die Erzeugung und die Verarbeitung des Dateiverlaufs führen dazu, dass das Backup mehr Zeit in Anspruch nimmt. Das Deaktivieren dieser Option verkürzt die Backup-Zeit. Wenn die Dateiverlaufsoption deaktiviert wurde und Sie zu einem späteren Zeitpunkt Daten wiederherstellen möchten, muss der gesamte Datenträger wiederhergestellt werden.</p>
Backup-Methode	<p>Gibt die Backup-Stufe an. Stufe 0 entspricht einem vollständigen Backup. Stufe 1 entspricht einem Differenzial-Backup, das neue oder seit dem letzten Backup der Stufe 0 geänderte Dateien sichert. Bei Backups der Stufen 2 bis 9 werden die seit dem Backup der vorhergehenden Stufe neuen oder geänderten Dateien gesichert. Beispielsweise werden beim Backup der Stufe 2 die seit dem Backup der Stufe 1 neuen oder geänderten Dateien gesichert. Beim Backup der Stufe 3 werden die seit dem Backup der Stufe 2 neuen oder geänderten Dateien gesichert usw.</p>

Bei anderen NDMP-Servern als NetApp, IBM, Fujitsu und EMC zeigt Backup Exec die entsprechenden Optionen an. Die Werte für die meisten Optionen, wie zum Beispiel Backup-Stufe und Dateiverlaufsoption, können geändert werden. Sie

können den Wert mancher Optionen in einen vordefinierten Wert ändern, und manche Optionen können nicht geändert werden.

Die für den jeweiligen NDMP-Server angezeigten Optionen wurden getestet. Während der NDMP-Server jedoch möglicherweise zusätzliche Optionen unterstützt, könnten diese nicht offiziell unterstützt werden. Backup Exec validiert nicht die Werte, die Sie für die Optionen eingeben, stellen Sie deshalb sicher, dass Sie die korrekten Werte eingeben. Weitere Informationen über die angezeigten Optionen finden Sie in der Dokumentation für Ihren NDMP-Server.

Backup-Auswahlen für NDMP-Server

Wenn Sie ein Backup erstellen, können Sie einen NAS-NDMP-Server auswählen. Auf dem NDMP-Server können Sie Datenträger oder Verzeichnisse auswählen oder die ein- oder auszuschließenden Daten festlegen.

Die folgenden Beschränkungen treffen zu, wenn Sie Datenträger oder Verzeichnisse auf NDMP-Servern für Backup auswählen:

- Sie können für jeden NDMP-Server gesamte Datenträger einschließen.
- Unterordner können Sie nur für NDMP-Server von NetApp, IBM oder Fujitsu einschließen.
- Sie können Dateien oder Verzeichnisse nicht ausschließen.

Siehe ["Sichern von Daten"](#) auf Seite 174.

Wenn Sie festlegen möchten, was in dem Backup-Auftrag ein- bzw. ausgeschlossen werden soll, haben Sie folgende Möglichkeiten:

- Auswählen bestimmter Verzeichnisse, um sie in den Backup-Auftrag einzuschließen
- Geben Sie die Namen der ein- bzw. auszuschließenden Verzeichnisse und Dateien im Dialogfeld "Einschließen/Ausschließen" ein.

Tabelle M-5 Was Sie in NDMP-Sever-Backups ein- bzw. ausschließen können

Typ des NDMP-Servers	Einschließen	Ausschließen
NetApp/IBM/Fujitsu	Ein oder mehrere Verzeichnisse	Verzeichnisse und Dateien basierend auf dem Ausschlussmuster.
EMC	Einzelnes Verzeichnis	Verzeichnisse und Dateien, jedoch nur bei Auswahl des Typs Dump-Backup.

Typ des NDMP-Servers	Einschließen	Ausschließen
Sonstiges	Einzelne oder mehrere Verzeichnisse, abhängig vom NDMP-Server.	Verzeichnisse und Dateien. Detaillierte Informationen finden Sie in der NDMP-Server-Dokumentation.

Siehe ["Verwenden von Mustern zum Ausschließen von Dateien und Verzeichnissen von einem NDMP-Server-Backup"](#) auf Seite 1548.

Verwenden von Mustern zum Ausschließen von Dateien und Verzeichnissen von einem NDMP-Server-Backup

Wenn Sie Dateien und Verzeichnisse von einer Backup-Auswahl für eine NetApp/IBM/Fujitsu-Appliance oder einen EMC Celerra-Netzwerkspeicher ausschließen, müssen Sie Muster verwenden. Sie sollten Muster sorgfältig eingeben, um sicherzustellen, dass Sie die richtigen Dateien und Verzeichnisse ausschließen. Backup Exec überprüft nicht die Gültigkeit von Ausschlussmustern. Wenn Sie ein ungültiges Muster eingeben, wird das Muster ignoriert und die Dateien oder Verzeichnisse werden nicht ausgeschlossen.

Weitere Informationen zu Mustern finden Sie in der NDMP-Serverdokumentation.

Das folgende Beispiel zeigt ein Muster, das Dateien und Verzeichnisse von einer Backup-Auswahl für einen NetApp/IBM/Fujitsu-NDMP-Server ausschließt:

Tabelle M-6 Beispielmuster für NetApp/IBM/Fujitsu-NDMP-Server

Muster	Beispiel:
tmp	Schließt alle Dateien und Verzeichnisse aus, die den Namen "tmp" haben.
*.core	Schließt alle Dateien und Verzeichnisse aus, die mit ".core" enden.

Um Verzeichnisse für einen EMC Celerra-NDMP-Server auszuschließen, geben Sie den Namen des EMC Celerra-Servers oder den Namen des Dateisystems nicht in das Muster ein. Die Namen des NDMP-Servers und des Dateisystems sind bereits im Textfeld "Ressourcenname" des Dialogfelds Einschließen/Ausschließen enthalten. Wenn Sie den Namen des NDMP-Servers und des Dateisystems im Muster wiederholen, ignoriert der EMC Celerra-NDMP-Server den Ausschluss.

Geben Sie den Pfad vom Stammverzeichnis zum Verzeichnis ein, das Sie ausschließen möchten. Geben Sie keinen vorangestellten Schrägstrich (/) ein.

Das folgende Beispiel zeigt ein Muster, das Verzeichnisse von einer Backup-Auswahl für einen EMC Celerra NDMP-Server ausschließt:

Tabelle M-7

Beispielmuster zum Ausschluss von Verzeichnissen für einen EMC Celerra NDMP-Server

Muster	Beschreibung
test_exclusion/subdir1	Schließt nur das Verzeichnis "subdir1" aus dem Dateisystem aus, das im Textfeld "Ressourcenname" aufgeführt ist.
test_exclusion/d*	Schließt alle Verzeichnisse aus, die mit dem Buchstaben "d" unter dem Verzeichnis "/test_exclusion" beginnen.

Das folgende Beispiel zeigt ein Muster, das Dateien von einer Backup-Auswahl für einen EMC Celerra NDMP-Server ausschließt:

Tabelle M-8

Beispielmuster zum Ausschluss von Dateien für einen EMC Celerra NDMP-Server

Muster	Beschreibung
*.mp3	Schließt alle Dateien aus, die mit ".mp3" enden.
temp	Schließt alle Dateien aus, die den Namen "temp" haben.

Siehe ["Backup-Auswahlen für NDMP-Server "](#) auf Seite 1547.

Siehe ["Info zum Auswählen von zu sichernden Daten "](#) auf Seite 186.

Unterstützte Konfigurationen für das Duplizieren von Daten aus NDMP-Servern

Mit NDMP Feature können Sie die Backup-Daten von einem NAS-NDMP-Server in den Speicher duplizieren, der mit einem Backup Exec-Server oder an einem anderen NDMP-Server verbunden ist.

Backup Exec unterstützt die folgenden Konfigurationen für das Duplizieren von Backup-Daten aus NDMP-Servern:

- Zwei Speichergeräte, die lokal am Backup Exec-Server angeschlossen sind.
- Zwei Bandlaufwerke, die lokal an einem NDMP-Server angeschlossen sind.
- Ein Bandlaufwerk, das lokal an einem NDMP-Server und ein Bandlaufwerk, das lokal an einem anderen NDMP-Server angeschlossen ist.
- Ein Speichergerät, das lokal an einem Backup Exec-Server und ein Bandlaufwerk, das lokal an einem NDMP-Server angeschlossen ist.

Die Vorgehensweise zum Duplizieren von Backup-Daten aus NDMP-Servern entspricht dem zum Duplizieren anderer Datentypen. Für NDMP-Server des Typs NetApp/IBM/Fujitsu müssen Sie auch die Anmeldedaten für den Quell-NDMP-Server auswählen.

Siehe ["Manuelles Duplizieren von Backup-Sätzen bzw. Auftragsverläufen"](#) auf Seite 246.

Wiederherstellen und Umleiten von Wiederherstellungsdaten für NDMP-Server

Mit NDMP Feature können Sie zum Wiederherstellen von Daten für einen NAS-NDMP-Server den Wiederherstellungsassistenten auf der Registerkarte "Backup und Wiederherstellung" verwenden. Wenn für den Backup-Auftrag der Dateiverlauf nicht deaktiviert war, können Sie während des Wiederherstellungsvorgangs einzelne Dateien zur Wiederherstellung auswählen. Sie können Dateien und Verzeichnisse nicht ausschließen, wenn Sie die Wiederherstellung auf einem NDMP-Server durchführen. Ausgeschlossene Verzeichnisse und Dateien werden wiederhergestellt.

Backup Exec kann nicht genügend Datei- und Verzeichnisinformationen über einen NDMP-Server-Wiederherstellungsauftrag erfassen, um die Abschnitte "Backup-Satz-Übersicht" und "Backup-Satz-Informationen" des Auftragsverlaufs genau auszufüllen. Deshalb wird die Anzahl der Dateien, Verzeichnissen, übersprungenen Dateien, beschädigten Dateien und gerade verwendeten Dateien, mit 0 angegeben.

Hinweis: Stellen Sie sicher, dass die standardmäßige Katalogoption "Speicherbasierte Kataloge verwenden" ausgewählt ist. Andernfalls können NDMP-Server-Backup-Sätze nicht katalogisiert werden.

Umleiten von Wiederherstellungsdaten für NDMP-Server

Sie können NDMP Feature zum Umleiten von Wiederherstellungsdaten von einem NAS-NDMP-Server auf einen anderen NDMP-Server verwenden.

Berücksichtigen Sie beim Umleiten von NDMP-Server-Daten die folgenden Beschränkungen:

- Sie können NDMP-Server-Daten nicht zu einem Computer umleiten, auf dem Windows- oder Linux-Betriebssysteme ausgeführt werden.
- Sie können Nicht-NDMP-Server-Daten wie NTFS- oder SQL-Daten nicht zu einem NDMP-Server umleiten.
- Der NDMP-Server, zu dem Sie die wiederhergestellten Daten umleiten möchten, muss vom gleichen Händler wie der NDMP-Server sein, von dem die Daten gesichert wurden.

Backup Exec kann nicht genügend Datei- und Verzeichnisinformationen über einen NDMP-Server-Wiederherstellungsauftrag erfassen, um die Abschnitte "Auftragszusammenfassung" und "Satz – Detaillierte Informationen" des Auftragsverlaufs genau auszufüllen. Deshalb wird für Wiederherstellungs- und Überprüfungsvorgänge die Anzahl der Dateien, Verzeichnissen, übersprungenen Dateien, beschädigten Dateien und gerade verwendeten Dateien, immer mit 0 angegeben. "Auftragszusammenfassung" und "Satz – Detaillierte Informationen" werden Backup- und Duplizierungsvorgänge angezeigt.

Hinweis: Überprüfungsvorgänge werden nur für NetApp-Server unterstützt.

Siehe ["Konfigurieren der Standardoptionen für Kataloge"](#) auf Seite 279.

Siehe ["Methoden für das Wiederherstellen von Daten in Backup Exec"](#) auf Seite 258.

Siehe ["Wiederherstellungsoptionen für NDMP-Server"](#) auf Seite 1551.

Wiederherstellungsoptionen für NDMP-Server

Mit NDMP Feature können Sie einen Wiederherstellungsauftrag für einen NAS-NDMP-Server erstellen. Die im Wiederherstellungsassistenten angezeigten Optionen variieren je nach Typ des NDMP-Servers.

Siehe ["Wiederherstellen und Umleiten von Wiederherstellungsdaten für NDMP-Server"](#) auf Seite 1550.

Tabelle M-9 NDMP Feature-Wiederherstellungsoptionen für NetApp/IBM/Fujitsu

Element	Beschreibung
Zugriffskontrolllisten wiederherstellen	Stellt NetApp-Zugriffskontrolllisten wieder her.

Element	Beschreibung
Wiederherstellung mit direktem Zugriff aktivieren	<p>Ermöglicht Backup Exec die Verwendung von Direct Access Recovery (DAR) während des Wiederherstellungsauftrags. Bei einer Wiederherstellung mit direktem Zugriff kann Backup Exec die genaue Position einer Datei in einem gesicherten Datenstrom angeben. Anschließend kann der NDMP-Server die für die zu wiederherstellende einzelne Datei geltenden Daten lesen. Durch die Wiederherstellung mit direktem Zugriff müssen weniger Informationen verarbeitet werden und der Zeitaufwand für die Wiederherstellung ist erheblich geringer.</p> <p>Wenn Sie diese Option nicht aktivieren, dauert die Wiederherstellung möglicherweise erheblich länger.</p> <p>Hinweis: Nicht alle Anbieter bieten Direct Access Recovery.</p>
Wiederherstellung ohne Daten auf die Festplatte zu schreiben (Daten überprüfen, ohne eine Wiederherstellung durchzuführen)	<p>Prüft die Gültigkeit der für den Wiederherstellungsauftrag ausgewählten Daten. Backup Exec stellt die Daten nicht wieder her.</p> <p>Bei NDMP-Severn von NetApp oder IBM sollten Sie anstelle der in der Backup-Definition verfügbaren Überprüfungsoption diese Option verwenden.</p>
Ordnerstruktur des Backups neu erstellen, sobald alle Daten wiederhergestellt wurden, da andernfalls alle Daten ohne Ordnerstruktur wiederhergestellt werden	<p>Stellt die Daten mit der ursprünglichen intakten Verzeichnisstruktur wieder her.</p>

Tabelle M-10 NDMP Feature-Wiederherstellungsoptionen für EMC

Element	Beschreibung
Wiederherstellung mit direktem Zugriff aktivieren	<p>Ermöglicht Backup Exec die Verwendung von Direct Access Recovery (DAR) während des Wiederherstellungsauftrags. Bei einer Wiederherstellung mit direktem Zugriff kann Backup Exec die genaue Position einer Datei in einem gesicherten Datenstrom angeben. Anschließend kann der NDMP-Server die für die zu wiederherstellende einzelne Datei geltenden Daten lesen. Durch die Wiederherstellung mit direktem Zugriff müssen weniger Informationen verarbeitet werden und der Zeitaufwand für die Wiederherstellung ist erheblich geringer.</p> <p>Wenn Sie diese Option nicht aktivieren, dauert die Wiederherstellung möglicherweise erheblich länger.</p> <p>Hinweis: Nicht alle Anbieter bieten Direct Access Recovery.</p>
Ordnerstruktur des Backups neu erstellen, sobald alle Daten wiederhergestellt wurden, da andernfalls alle Daten ohne Ordnerstruktur wiederhergestellt werden	Stellt die Daten mit der ursprünglichen intakten Verzeichnisstruktur wieder her.
Vorhandene Dateien überschreiben	Überschreibt die Dateien auf dem Wiederherstellungsziel, die dieselben Namen wie Dateien haben, die wiederhergestellt werden. Verwenden Sie diese Option nur, wenn Sie eine ältere Version einer Datei wiederherstellen möchten.

Bei anderen NDMP-Servern als NetApp, IBM, Fujitsu und EMC zeigt Backup Exec die entsprechenden Variablen und Standardwerte für den spezifischen Typ des NDMP-Servers an. Sie können die Werte bei Bedarf anpassen. Variablen, die mit dem Präfix "@@" beginnen, sind Backup Exec-spezifisch, nicht NDMP-Server-spezifisch. Die für den jeweiligen NDMP-Server angezeigten Optionen wurden getestet. Während der NDMP-Server jedoch möglicherweise zusätzliche Optionen unterstützt, könnten diese nicht offiziell unterstützt werden. Backup Exec validiert nicht die Werte für die Variablen, die Sie eingeben, also sollten Sie sicherstellen, dass Sie die Werte richtig eingeben. Weitere Informationen zu den zu verwendenden Werten finden Sie in der Dokumentation für Ihren NDMP-Server.

Festlegen der Standard-Backup-Optionen für NDMP Feature

Sie können die Standardeinstellungen verwenden, die Backup Exec bei der Installation für NDMP Feature festlegt, oder eigene Standardeinstellungen wählen. Sie können darüber hinaus die Standardeinstellungen für alle spezifischen Backup-Aufträge ändern.

So legen Sie Standard-Backup-Optionen für NDMP Feature fest

- 1 Klicken Sie auf die Backup Exec-Schaltfläche und wählen Sie dann "Konfiguration und Einstellungen".
- 2 Wählen Sie "Auftragsstandardeinstellungen" und dann eine Backup-Option.
- 3 Im linken Teilfenster klicken Sie auf "NDMP".
- 4 Sie haben folgende Möglichkeiten:
 - Wählen Sie die entsprechenden Optionen für NetApp, IBM und Fujitsu-NDMP-Server:

Zugriffskontrolllisten sichern

Sichert NetApp-Zugriffskontrolllisten.

Dateiverlauf aktivieren

Aktiviert die Erstellung von Dateiverlaufsdaten. Der Dateiverlauf wird zum Optimieren der Wiederherstellung ausgewählter Backup-Sätze verwendet. Die Erzeugung und die Verarbeitung des Dateiverlaufs führen jedoch dazu, dass das Backup mehr Zeit in Anspruch nimmt. Das Deaktivieren dieser Option verkürzt die Backup-Zeit.

Wenn der Dateiverlauf nicht generiert wird und Sie zu einem späteren Zeitpunkt Daten wiederherstellen müssen, muss der gesamte Datenträger wiederhergestellt werden.

Backup-Methode	Gibt die Backup-Stufe an. Stufe 0 entspricht einem vollständigen Backup. Die Stufen 1 bis 9 stehen für unterschiedliche Stufen von inkrementellen Backups. Beim Backup der Stufe 1 werden die seit dem Backup der Stufe 0 neuen oder geänderten Dateien gesichert. Beim Backup der Stufe 2 werden die seit dem Backup der Stufe 1 neuen oder geänderten Dateien gesichert usw.
----------------	--

■ Wählen Sie die entsprechenden Optionen für EMC-NDMP-Server aus

Backup-Typ	<p>Legt den Backup-Typ für diesen Backup-Auftrag fest.</p> <p>Die folgenden Backup-Typen sind verfügbar:</p> <ul style="list-style-type: none"> ■ Ausgabe ■ VBB
Sichern mit integrierten Wiederaufnahmepunkten (SnapSure)	Ermöglicht Backup Exec die Erstellung eines Backup-Satzes mit EMC SnapSure. Weitere Informationen zu SnapSure finden Sie in der EMC-Dokumentation.
Dateiverlauf aktivieren	Aktiviert die Erstellung von Dateiverlaufsdaten. Der Dateiverlauf wird zum Optimieren der Wiederherstellung ausgewählter Backup-Sätze verwendet. Die Erzeugung und die Verarbeitung des Dateiverlaufs führen dazu, dass das Backup mehr Zeit in Anspruch nimmt. Das Deaktivieren dieser Option verkürzt die Backup-Zeit. Wenn die Dateiverlaufsoption deaktiviert wurde und Sie zu einem späteren Zeitpunkt Daten wiederherstellen möchten, muss der gesamte Datenträger wiederhergestellt werden.

Backup-Methode	Gibt die Backup-Stufe an. Stufe 0 entspricht einem vollständigen Backup. Die Stufen 1 bis 9 stehen für unterschiedliche Stufen von inkrementellen Backups. Beim Backup der Stufe 1 werden die seit dem Backup der Stufe 0 neuen oder geänderten Dateien gesichert. Beim Backup der Stufe 2 werden die seit dem Backup der Stufe 1 neuen oder geänderten Dateien gesichert usw.
----------------	--

5 Klicken Sie auf "Übernehmen".

Anzeigen der Eigenschaften eines NDMP-Servers

Sie können die Eigenschaften eines zu sichernden am Netzwerk angeschlossenen Speicher-NDMP-Servers anzeigen.

So zeigen Sie die Eigenschaften eines NDMP-Servers an

- 1 Doppelklicken Sie auf der Registerkarte "Backup und Wiederherstellung" auf den NDMP-Server.
- 2 Wählen Sie im linken Teilfenster "Eigenschaften".
- Siehe ["NDMP-Servereigenschaften"](#) auf Seite 1556.

NDMP-Servereigenschaften

Sie können folgende Speichereigenschaften für einen Netzwerk-NDMP-Server anzeigen.

Siehe ["Anzeigen der Eigenschaften eines NDMP-Servers"](#) auf Seite 1556.

Tabelle M-11 NDMP-Server-Eigenschaften

Element	Beschreibung
Name	Gibt den Namen des NDMP-Servers an.
Beschreibung	Zeigt die benutzerdefinierte Beschreibung des NDMP-Servers an.

Element	Beschreibung
Login-Konto	Gibt den Namen des Login-Kontos für den NDMP-Server an. Sie können ein neues Login-Konto hinzufügen oder ein vorhandenes Konto bearbeiten.

Anzeigen von Speichereigenschaften für einen NDMP-Server

Sie können die Eigenschaften eines NDMP-Netzwerkspeicherservers anzeigen.

So zeigen Sie Speichereigenschaften für einen NDMP-Server an

- Auf der Registerkarte "Speicher" doppelklicken Sie auf den NDMP-Server.
- Wählen Sie im linken Teilfenster "Eigenschaften".

Siehe ["Speichereigenschaften für einen NDMP-Server"](#) auf Seite 1557.

Speichereigenschaften für einen NDMP-Server

Sie können folgende Speichereigenschaften für einen NAS-NDMP-Server anzeigen.

Siehe ["Anzeigen von Speichereigenschaften für einen NDMP-Server"](#) auf Seite 1557.

Tabelle M-12 Speichereigenschaften eines NDMP-Servers

Element	Beschreibung
Servename	Gibt den Namen des NDMP-Servers an.
Beschreibung	Zeigt die benutzerdefinierte Beschreibung des Servers an.
Status	Gibt den Status des Speichers des NDMP-Servers an. Siehe "Status von Backup Exec-Servern und Speichergeräten" auf Seite 576.
Port	Zeigt den Port an, der für die Kommunikation zwischen dem Backup Exec-Server und dem NDMP-Server verwendet wird.

Element	Beschreibung
ICMP-Pingvorgänge zur Erkennung des Servers verwenden	Zeigt an, ob ICMP-Ping aktiviert ist. ICMP-Ping ermöglicht es Backup Exec, die Ping-Funktion zum Auffinden des NDMP-Servers zu verwenden.
Login-Konto	Gibt den Namen des Login-Kontos für den NDMP-Server an. Sie können ein neues Login-Konto hinzufügen oder ein vorhandenes Konto bearbeiten.
Host-ID	Zeigt die Kennungsnummer an, die der NDMP-Server generiert.
Systemversion	Zeigt die auf dem NDMP-Server installierte Softwareversion an.

Backup Exec Agent for Linux

Dieser Anhang enthält folgende Themen:

- [Info zu Agent for Linux](#)
- [Info zu geöffneten Dateien und Agent for Linux](#)
- [Anforderungen für Agent for Linux](#)
- [Installieren von Agent for Linux](#)
- [Info zum Festlegen des Vertrauens für einen standortfernen Linux-Computer in der Backup Exec-Liste von Servern](#)
- [Hinzufügen zusätzlicher Backup Exec-Server, auf denen Agent for Linux Informationen bereitstellen kann](#)
- [Info zum Konfigurieren von Agent for Linux](#)
- [Ausschließen der Dateien und Verzeichnisse von allen Backup-Aufträgen für Linux-Computer](#)
- [Bearbeiten von Konfigurationsoptionen für Linux-Computer](#)
- [Info zum Sichern eines Linux-Computers durch Verwendung des Agent for Linux](#)
- [Info zum Wiederherstellen von Daten auf Linux-Computern](#)
- [Bearbeiten der Standardoptionen für Backup-Aufträge für Linux-Computer](#)
- [Deinstallieren von Agent for Linux](#)
- [Starten des Agent for Linux-Daemon](#)
- [Beenden des Agent for Linux-Daemon](#)

- [Fehlerbehebung für den Agent for Linux](#)

Info zu Agent for Linux

Backup Exec Agent for Linux (Linux-Agent) wird als separate Add-On-Komponente installiert. Der Linux-Agent ermöglicht Netzwerkadministratoren, Backup- und Wiederherstellungsvorgänge auf Linux-Servern durchzuführen, die mit dem Netzwerk verbunden sind. Der Linux-Agent muss auf den Linux-Servern installiert werden, bevor Sie Backup- oder Wiederherstellungsvorgänge durchführen können.

Informationen zu den Best Practices zum Einsatz des Backup Exec Agent for Linux (Linux-Agent) finden Sie unter *Best Practices für Backup Exec*.

Siehe ["Info zu geöffneten Dateien und Agent for Linux"](#) auf Seite 1560.

Siehe ["Anforderungen für Agent for Linux"](#) auf Seite 1560.

Siehe ["Installieren von Agent for Linux"](#) auf Seite 1561.

Info zu geöffneten Dateien und Agent for Linux

Agent for Linux nutzt erweiterte Funktionen, die Probleme verhindern sollen, die manchmal bei Backup-Vorgängen auftreten können (z. B. beim Sichern geöffneter Dateien).

Nachdem Sie Dateien und Ordner ausgewählt und den Backup-Auftrag gesendet haben, zeichnet der Linux Agent automatisch einen Snapshot des oder der Datenträger auf. Der Snapshot stellt eine Aufzeichnung der Daten zu einem bestimmten Zeitpunkt dar. Wenn der Linux Agent einen Snapshot erstellt, unterbricht er vorübergehend die Schreibaktivitäten auf einem Datenträger, damit der Snapshot erstellt werden kann. Während des Backup können Dateien geöffnet sein und Daten geändert werden.

Der Linux Agent unterstützt folgende Datenträgerkonfigurationen: Simple, Logical Volume Manager (LVM) und RAID.

Siehe ["Anforderungen für Agent for Linux"](#) auf Seite 1560.

Anforderungen für Agent for Linux

Die folgenden Elemente sind für die Installation von Agent for Linux (Linux-Agent) erforderlich:

- Auf dem Backup Exec-Server muss das TCP/IP installiert sein.
- Auf dem Linux-Server muss Perl 5.8.8 oder höher installiert sein.

- Sie müssen über ein Rootlogin-Konto auf den Linux-Servern verfügen.
- Sie müssen die Backup Exec-Installationsmedien besitzen.
- Sie müssen eine Lizenz für den Linux-Agent auf dem Backup Exec-Server eingeben.

Hinweis: Bei manchen Versionen von Linux kann es erforderlich sein, dass Sie das Paket "libstdc++.so.5" installieren.

Siehe ["Fehlerbehebung für den Agent for Linux"](#) auf Seite 1590.

Es wird empfohlen, dass Sie das Protokoll "Secure Shell" (SSH) verwenden, wenn Sie den Linux-Agent von einem Linux-Server auf einen anderen Linux-Server über eine Push-Installation installieren. Sie müssen SSH aktivieren, bevor Sie den Linux-Agent über eine Push-Installation installieren.

Backup Exec installiert automatisch Remote Media Agent for Linux, wenn es Agent for Linux auf einem Linux-Server installiert. Jedoch müssen Sie eine separate Lizenz für Remote Media Agent for Linux eingeben, bevor es verwendet werden kann.

Siehe ["Info zu Remote Media Agent for Linux "](#) auf Seite 1598.

Die unterstützten Betriebssysteme, Plattformen und Anwendungen finden Sie in der Liste der mit Backup Exec kompatiblen Software.

Siehe ["Installieren von Agent for Linux"](#) auf Seite 1561.

Siehe ["Anforderungen für das Sichern von Novell Open Enterprise Server auf "SUSE Linux Enterprise Server""](#) auf Seite 1581.

Installieren von Agent for Linux

Führen Sie folgende Schritte mithilfe der Backup Exec-Installationsmedien aus:

- Installieren Sie Agent for Linux (Linux-Agent) auf einem lokalen Linux-Server.
- Installieren Sie den Linux-Agent über eine Push-Installation von einem Linux-Server auf andere standortferne Linux-Server.

Wenn Sie den Linux-Agent über eine Push-Installation installieren, wird standardmäßig RSH (Remote Shell) verwendet. Es wird empfohlen, stattdessen SSH (Secure Shell) zu verwenden. Um SSH verwenden zu können, müssen Sie es aktivieren, bevor Sie den Linux Agent installieren. Weitere Informationen zu SSH finden Sie in Ihrer Betriebssystemdokumentation.

Bevor Sie Linux Agent installieren, sollten Sie die Anforderungen überprüfen:

Siehe ["Anforderungen für Agent for Linux"](#) auf Seite 1560.

Wenn Sie den Linux-Agent installieren, erstellt Backup Exec die beoper-Gruppe und fügt Root als Mitglied hinzu. Die beoper-Gruppe enthält die Namen der Benutzer, die eine Berechtigung zum Sichern und Wiederherstellen der Linux-Server haben. Wenn Backup Exec während der Linux-Agent-Installation jedoch einen NIS-Server erkennt, dann wird die beoper-Gruppe nicht erstellt. Sie müssen die beoper-Gruppe auf den Linux-Servern manuell erstellen, auf denen Sie den Linux-Agent installieren möchten.

Wenn die Installation abgeschlossen ist, speichert Backup Exec die Installations-Protokolldatei auf dem folgenden Speicherort auf dem Server, auf dem der Linux-Agent installiert ist:

```
/var/tmp/vxif/installralus<summary file number>/installralus.log
```

Siehe ["Installation von Agent for Linux"](#) auf Seite 1562.

Installation von Agent for Linux

Sie können Agent for Linux (Linux Agent) auf einem lokalen Linux-Server installieren. Sie können dann über eine Push-Installation den Linux Agent vom lokalen Linux-Server auf einen oder mehrere standortferne Linux-Server installieren.

Siehe ["Installieren von Agent for Linux"](#) auf Seite 1561.

Hinweis: Sie müssen die Datei "RALUS_RMALS_<Versionsnummer>.gz" auf einem Linux-Computer entpacken. Die Installation läuft nicht, wenn sie auf einem Computer entzippt wird, auf dem das Windows-Betriebssystem ausgeführt wird.

So installieren Sie Agent for Linux

- 1 Legen Sie die Backup Exec-Installationsmedien in das entsprechende Laufwerk des Linux-Servers ein.
- 2 Loggen Sie als Root auf dem Server ein, auf dem der Linux Agent installiert werden soll.
- 3 Navigieren Sie zum folgenden Verzeichnis auf dem Installationsmedium.
<Linux>
- 4 Kopieren Sie die Datei "RALUS_RMALS_<Versionsnummer>.gz" in dieses Verzeichnis in ein Verzeichnis auf dem lokalen Computer.
- 5 Dekomprimieren Sie die Datei.

Beispiel:

```
gunzip RALUS_RMALS_<Versionsnummer>.gz
```

6 Entzippen Sie die Datei.

Beispiel:

```
tar -xf RALUS_RMALS_<Versionsnummer>.tar
```

7 Sie haben folgende Möglichkeiten:

So installieren Sie den Linux Agent auf dem lokalen Linux-Server

Starten Sie das Skript "installralus".

Beispiel: `./installralus`

So installieren Sie den Linux Agent aus dem lokalen Linux-Server auf einem oder mehreren Remote-Linux-Servern

Gehen Sie dazu in folgender Reihenfolge vor:

- Starten Sie das Skript "installralus" mithilfe des SSH-Switch.
Beispiel: `./installralus -usessh`
- Geben Sie den Namen, die IP-Adresse oder den vollständig qualifizierten Domännennamen eines Linux-Servers ein.

Hinweis: Um den Agent auf mehreren Remote-Linux-Servern zu installieren, lassen Sie ein Leerzeichen zwischen den einzelnen Kennungen.

- 8 Wenn das Installationsprogramm bei der erstmaligen Systemüberprüfung ein gültiges Betriebssystem für den Linux-Server gefunden hat, drücken Sie die **Eingabetaste**.
- 9 Überprüfen Sie die Paketinstallations-Übersicht, und drücken Sie dann die **Eingabetaste**.
- 10 Wenn die Systemanforderungen für die Installation geprüft wurden, drücken Sie die Eingabetaste.
- 11 Beginnen Sie die Voraussetzungsprüfung, indem Sie die **Eingabetaste** drücken.
- 12 Starten Sie den NIS-Server-Scan, indem Sie die **Eingabetaste** drücken.
- 13 Überprüfen Sie die Ergebnisse des NIS-Server-Scans und wählen Sie eine der folgenden Vorgehensweisen:

Wenn ein NIS-Server erkannt wird

Das Linux Agent-Installationsprogramm kann die beoper-Gruppe nicht erstellen. Sie müssen sie manuell erstellen, wenn die Linux Agent-Installation abgeschlossen ist.

Fahren Sie mit dem nächsten Schritt fort.

Wenn kein NIS-Server erkannt wird

Benutzen Sie das Installationsprogramm, um die beoper-Gruppe zu erstellen.

Gehen Sie dazu in folgender Reihenfolge vor:

- Um die Beoper-Gruppe durch das Installationsprogramm erstellen zu lassen, geben Sie **J** ein.
- Um die nächste verfügbare Gruppen-ID auszuwählen, geben Sie **N** ein.
- Um das Root-Benutzerkonto der beoper-Gruppe hinzuzufügen, geben Sie **J** ein.
- Fahren Sie mit dem nächsten Schritt fort.

- 14** Starten Sie die Installation, indem Sie die **Eingabetaste** drücken.
- 15** Drücken Sie nach Abschluss der Installation die Eingabetaste, um die nachfolgenden Konfigurationen sowie die Installation von SymSnap-Treibern zu starten.
- 16** Drücken Sie auf J, um den Beremote-Dienst automatisch zu starten, oder drücken Sie auf N, um den Dienst später zu starten.
- 17** Drücken Sie nach Abschluss des Konfigurationsprozesses die **Eingabetaste**, um das Installationsprotokoll in der folgenden Datei zu speichern:
`/var/tmp/vxif/installralusNummer der Zusammenfassungsdatei/installralus.log`
- 18** Wenn das Linux Agent-Installationsprogramm keine beoper-Gruppe erstellt hat, müssen Sie sie erstellen.

Siehe "[Manuelles Erstellen der Backup Exec-Operatorengruppe \(beoper\)](#)" auf Seite 1565.

19 Konfigurieren Sie den Agent for Linux entsprechend.

Siehe ["Info zum Konfigurieren von Agent for Linux"](#) auf Seite 1568.

20 Wenn der Dienst "Beremote" nicht aufgeführt wird, starten Sie den Agent for Linux Daemon.

Siehe ["Starten des Agent for Linux-Daemon"](#) auf Seite 1589.

Info zur Backup Exec-Operator-Gruppe (beoper) für den Agent for Linux

Die beoper-Gruppe enthält die Namen der Benutzer, die eine Berechtigung zum Sichern und Wiederherstellen der Linux-Server haben.

Wenn Sie Agent for Linux (Linux Agent) installieren, erstellt Backup Exec die beoper-Gruppe und fügt Root als Mitglied hinzu. Jeder Linux-Benutzer, den Sie der beoper-Gruppe hinzufügen, erhält die notwendigen Berechtigungen, die Server zu sichern und wiederherzustellen.

Wenn jedoch ein NIS-Server während der Remote Agent-Installation erkannt wird, kann Backup Exec die beoper-Gruppe nicht erstellen. Sie müssen die beoper-Gruppe auf den Linux-Servern manuell erstellen, auf denen Sie den Linux-Agent installieren möchten. Sie müssen die beoper-Gruppe vor dem Starten von Backup- und Wiederherstellungsvorgängen erstellen. Andernfalls schlagen Verbindungen zwischen den Linux-Servern und dem Backup Exec-Server fehl.

Bevor die Mitglieder der beoper-Gruppe Backup- oder Wiederherstellungsvorgänge durchführen können, müssen sie ein Backup Exec-Login-Konto haben.

Siehe ["Manuelles Erstellen der Backup Exec-Operatorengruppe \(beoper\)"](#) auf Seite 1565.

Siehe ["Backup Exec-Login-Konten"](#) auf Seite 762.

Manuelles Erstellen der Backup Exec-Operatorengruppe (beoper)

Sie müssen eine beoper-Gruppe auf jedem Server erstellen, auf dem Sie Agent for Linux installieren möchten (Linux-Agent).

Siehe ["Info zur Backup Exec-Operator-Gruppe \(beoper\) für den Agent for Linux"](#) auf Seite 1565.

Hinweis: Stellen Sie sicher, dass Sie verstehen, wie Gruppenberechtigungen auf Linux-Servern konfiguriert werden, bevor Sie eine Gruppen-ID für die beoper-Gruppe zuweisen.

Tabelle N-1 Manuelles Erstellen der beoper-Gruppe

Schritt	Aktion	Weitere Informationen
Schritt 1	<p>Navigieren Sie zum Linux-Server, auf dem Sie den Linux-Agent installieren möchten.</p> <p>Wenn sich der Linux-Server in einer NIS-Domäne befindet, navigieren Sie zur Gruppendatei der NIS-Domäne.</p>	<p>Weitere Informationen darüber, wie einer Gruppendatei einer NIS-Domäne eine Gruppe hinzugefügt wird, finden Sie in der NIS-Dokumentation.</p>
Schritt 2	<p>Erstellen Sie eine Gruppe mit dem folgenden Namen (Groß- und Kleinschreibung muss beachtet werden):</p> <p>beoper</p>	<p>Weitere Informationen zum Erstellen einer Gruppe finden Sie in der Dokumentation zum Betriebssystem.</p>
Schritt 3	<p>Fügen Sie in der beoper-Gruppe die Benutzer hinzu, die die Berechtigung zum Sichern und Wiederherstellen des Linux-Servers haben sollen.</p>	<p>Weitere Informationen über das Hinzufügen von Benutzern zu einer Gruppe finden Sie in der Dokumentation zum Betriebssystem.</p>
Schritt 4	<p>Erstellen eines Backup Exec-Login-Konto für jeden Benutzer, den Sie der beoper-Gruppe hinzufügen.</p>	<p>Siehe "Backup Exec-Login-Konten" auf Seite 762.</p>

Info zum Festlegen des Vertrauens für einen standortfernen Linux-Computer in der Backup Exec-Liste von Servern

Wenn Sie vom Backup Exec-Server eine Verbindung zu einem Linux-Computer herstellen, müssen Sie Vertrauenseinstellungen zwischen dem Backup Exec-Server und dem standortfernen Linux-Computer festlegen. Dies ist auch erforderlich, wenn Sie einen standortfernen Linux-Computer konfigurieren möchten, um die clientseitige Deduplizierung durchzuführen.

Siehe ["Erstellen eines Vertrauensverhältnisses zwischen dem Backup Exec-Server und einem Remote-Computer"](#) auf Seite 1031.

Siehe ["Festlegen von Vertrauen und Hinzufügen von standortfernen Linux-Computern zur Backup Exec-Liste von Servern"](#) auf Seite 1567.

Festlegen von Vertrauen und Hinzufügen von standortfernen Linux-Computern zur Backup Exec-Liste von Servern

Sie können einen oder mehrere standortferne Linux-Computer der Liste von Servern auf der Registerkarte "Backup und Wiederherstellung" hinzufügen. Wenn Sie standortferne Linux-Computer hinzufügen, müssen Sie eine vertrauenswürdige Verbindung zwischen dem Backup Exec-Server und den standortfernen Linux-Computern herstellen, um sichere Kommunikation sicherzustellen.

So legen Sie Vertrauen fest und fügen einen standortfernen Linux-Computer der Backup Exec-Liste von Servern hinzu

- 1 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" unter "Server" auf "Hinzufügen".
- 2 Klicken Sie auf "Linux-Computer".
- 3 Befolgen Sie die Anweisungen auf dem Bildschirm.

Siehe ["Hinzufügen zusätzlicher Backup Exec-Server, auf denen Agent for Linux Informationen bereitstellen kann"](#) auf Seite 1567.

Siehe ["Info zum Konfigurieren von Agent for Linux"](#) auf Seite 1568.

Hinzufügen zusätzlicher Backup Exec-Server, auf denen Agent for Linux Informationen bereitstellen kann

Sie können zusätzliche Backup Exec-Server angeben, zu denen Agent for Linux (Linux Agent) Informationen veröffentlichen kann.

Jeder Backup Exec-Server, auf dem der Linux Agent Informationen veröffentlicht, wird in der Liste "Server" von Backup Exec angezeigt.

Um zusätzliche Backup Exec-Server hinzuzufügen, zu denen Agent for Linux Informationen veröffentlichen kann

- 1 Öffnen Sie folgende Datei mit einem Texteditor:

`/etc/VRTSralus/ralus.cfg`

- 2 Fügen Sie die folgende Zeichenfolge hinzu:

Software\Symantec\Backup Exec For Windows\Backup
Exec\Engine\Agents\Agent Directory List *eindeutige ID = IP-Adresse oder
DNS-Name des Backup Exec-Servers*

- 3 Speichern und schließen Sie die Datei.
- 4 Navigieren Sie zum Backup Exec-Server, auf dem sich der Linux Agent veröffentlicht, und fügen Sie der Serverliste den Linux-Server hinzu.

Siehe ["Hinzufügen von zu sichernden Servern zur Serverliste auf der Registerkarte "Backup und Wiederherstellung"](#) auf Seite 167.

Info zum Konfigurieren von Agent for Linux

Backup Exec erstellt auf jedem Linux-Server, auf dem Agent for Linux (Linux Agent) installiert ist, eine Datei mit dem Namen "`ralus.cfg`". Sie können die Zeichenfolgen, Kennungen und Variablen in dieser Datei bearbeiten, um Optionen für den Linux Agent hinzuzufügen.

Optionen, die Sie in der Datei "`ralus.cfg`" bearbeiten können:

- Der Port, an den der Linux Agent Veröffentlichungsmeldungen senden muss.
- Die Protokollierungsstufe für Oracle- und DB-Datenbankvorgänge, die Backup Exec Linux Agent Utility verwenden, und für NDMP-Informationen.
- Die Einstellungen, damit der Linux Agent auf einen oder mehrere Backup Exec-Server veröffentlichen kann.
- Die Dateien und Verzeichnisse auf Linux- und Unix-Servern, die Sie von den Backups ausschließen möchten.
- Die Einstellung für ein Target Service Agent-Dateisystem-Backup für Novell OES.

Das Format der Datei "`ralus.cfg`" enthält drei Komponenten. Die erste Komponente (A) im folgenden Beispiel ist eine obligatorische Zeichenkette.

Die zweite Komponente (B) ist eine eindeutige Kennung, gefolgt von einem Gleichheitszeichen (=). Eindeutige Kennungen können aus laufenden Nummern, Buchstaben oder alphanumerischen Zeichen bestehen. Beispiel: 1, 2, 3 oder A, B, C. Sie können auch AA, BB, CC oder A1, A2, B1, B2 verwenden.

Ausschließen der Dateien und Verzeichnisse von allen Backup-Aufträgen für Linux-Computer

Die dritte Komponente des Formats "`ralus.cfg`" ist der Name "NetBIOS", der vollständig qualifizierte Domänenname oder die IP-Adresse des Backup Exec-Servers.

Die Datei "`ralus.cfg`" enthält einen Registrierungsschlüssel, der für die Technologie "Open File" des Linux Agent erforderlich ist. Der Name des Schlüssels ist "DisableOFO" und wird in der Datei "`ralus.cfg`" in folgender Form angezeigt:

```
Software\Symantec\Backup Exec for Windows\Backup
Exec\Engine\RALUS\DisableOFO=0
```

Standardmäßig wird der "DisableOFO"-Schlüssel auf "0" eingestellt, was bedeutet, dass der Linux Agent aktiv ist und die gefundenen offenen Dateien sichert. Jedoch können Sie die Open File-Technologie deaktivieren, indem Sie den Wert des Schlüssels auf "1" ändern und danach den Linux Agent-Dämon neu starten.

Hinweis: Advanced Open File Feature (AOFO) wird unter Novell OES nicht unterstützt. Sie müssen den AOFO-Schlüssel in der Datei "`ralus.cfg`" auf dem Linux-Server deaktivieren, auf dem Agent for Linux installiert ist.

Abbildung N-1 Beispiel der Datei "`ralus.cfg`"

A	B	C
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\Agents\Agent Directory List 1=	srv.mycompany.com	
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\Agents\Agent Directory List 2=	datasrv	
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\Agents\Agent Directory List 3=	66.35.250.151	

A = Erforderliche Zeichenkette

B = Erforderliche und eindeutige ID (Reihenfolge/Aussehen irrelevant)

C = Auszuschließende Datei bzw. Ordner

Siehe ["Bearbeiten von Konfigurationsoptionen für Linux-Computer"](#) auf Seite 1570.

Siehe ["Konfigurationsoptionen für Linux-Computer"](#) auf Seite 1570.

Siehe ["Beenden des Agent for Linux-Daemon"](#) auf Seite 1590.

Siehe ["Starten des Agent for Linux-Daemon"](#) auf Seite 1589.

Ausschließen der Dateien und Verzeichnisse von allen Backup-Aufträgen für Linux-Computer

Sie können bestimmte Dateien und Verzeichnisse auf Linux-Computern von allen Backup-Aufträgen ausschließen. Bearbeiten Sie die Datei "`ralus.cfg`", um die auszuschließenden Dateien festzulegen.

Im Folgenden sehen Sie ein Beispiel für Zeichenfolgen in der Datei "ralus.cfg", die Dateien und Verzeichnisse von allen Backup-Aufträgen ausschließen.

Abbildung N-2 Beispiel für Ausschluss von Dateien und Verzeichnissen im Format "ralus.cfg"

	A	B	C
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\RALUS\SystemExclude1	1		
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\RALUS\SystemExclude2	2		
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\RALUS\SystemExclude3	3		
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\RALUS\SystemExclude4	4		

A = Erforderliche Zeichenkette
 B = Erforderliche und eindeutige ID (Reihenfolge/Aussehen irrelevant)
 C = Auszuschließende Datei bzw. Ordner

Um Dateien und Verzeichnisse für bestimmte Backup-Aufträge auszuschließen, geben Sie die ausgeschlossenen Dateien und Verzeichnisse in den Backup-Auftragseigenschaften an.

Siehe ["Bearbeiten von Konfigurationsoptionen für Linux-Computer"](#) auf Seite 1570.

Bearbeiten von Konfigurationsoptionen für Linux-Computer

Sie können Konfigurationsoptionen für den Agent for Linux bearbeiten.

Siehe ["Info zum Konfigurieren von Agent for Linux"](#) auf Seite 1568.

So bearbeiten Sie Konfigurationsoptionen für Linux-Computer

- 1 Öffnen Sie folgende Datei mit einem Texteditor:

```
/etc/VRTSralus/ralus.cfg
```

- 2 Ändern Sie die entsprechende Zeichenfolge in der Datei.

Siehe ["Konfigurationsoptionen für Linux-Computer"](#) auf Seite 1570.

Konfigurationsoptionen für Linux-Computer

Sie können Optionen bearbeiten, um Agent for Linux (Linux Agent) zu konfigurieren.

Siehe ["Bearbeiten von Konfigurationsoptionen für Linux-Computer"](#) auf Seite 1570.

Tabelle N-2 Konfigurationsoptionen für Linux-Computer

Zeichenfolge und Standardwerte	Beschreibung
Software\Symantec\Backup Exec For Windows\Agent Browser\TcpIp\AdvertisementPort=6101	Zeigt den Port an, an den der Linux Agent Meldungen senden, veröffentlichen und bereinigen muss.
Software\Symantec\Backup Exec for Windows\Backup Exec\Debug\AgentConfig=0	Aktiviert die Protokollierung für Linux Agent-Dienstprogramm, das bei Oracle-Vorgängen verwendet wird. Es gibt folgende Werte: <ul style="list-style-type: none"> ■ 0 Protokollierung ist nicht aktiviert. ■ 1 Protokollierung ist aktiviert. Backup Exec generiert automatisch die Protokolldatei.
Software\Symantec\Backup Exec for Windows\Backup Exec\Debug\VBBSAlevel=0	Aktiviert die Protokollierung für Linux Agent for Oracle-Vorgänge. Es gibt folgende Werte: <ul style="list-style-type: none"> ■ 0 Protokollierung ist nicht aktiviert. ■ 5 Normale Protokollierung ist aktiviert. ■ 6 Erweiterte Protokollierung ist aktiviert. Große Protokolldateien können erstellt werden.

Zeichenfolge und Standardwerte	Beschreibung
Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\Agents\Advertise All=1	<p>Aktiviert den Linux Agent, sodass dieser Informationen auf allen Backup Exec-Servern veröffentlicht, die in den \Agents\Agent Directory List-Zeichenfolgen aufgelistet sind.</p> <p>Es gibt folgende Werte:</p> <ul style="list-style-type: none"> ■ 1 Der Linux Agent veröffentlicht Informationen auf jedem Backup Exec-Server in der Agent Directory List. ■ 0 Der Linux Agent veröffentlicht Informationen auf dem ersten Backup Exec-Server in der Agent-Verzeichnisliste. Bei erfolgreichem Versuch veröffentlicht der Linux Agent Informationen auf jedem beliebigen Backup Exec-Server. Wenn der Versuch nicht erfolgreich ist, versucht der Linux Agent die Informationen auf dem nächsten Backup Exec-Server in der Liste zu veröffentlichen. Der Linux Agent setzt die Versuche so lange fort, bis er das Ende der Liste erreicht.

Zeichenfolge und Standardwerte	Beschreibung
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\Agents\Advertise Now=0	<p>Aktiviert den Linux Agent, sodass er einen neuen Veröffentlichungszyklus startet, nachdem Sie Einstellungen in der Datei "ralus.cfg" hinzugefügt oder bearbeitet haben.</p> <p>Es gibt folgende Werte:</p> <ul style="list-style-type: none"> ■ 0 The Linux Agent veröffentlicht Informationen in einem Abstand, der unter "Agents\Advertising Interval Minutes" festgelegt ist. Mögliche Änderungen an der Datei "ralus.cfg" treten in Kraft, wenn ein neuer Veröffentlichungszyklus beginnt. ■ 1 Der Linux Agent beginnt einen neuen Veröffentlichungszyklus. Mögliche Änderungen an der Datei "ralus.cfg" treten sofort in Kraft. Wenn der Backup Exec-Server die Veröffentlichungsinformationen nicht erhält, unternimmt der Linux Agent zehn weitere Versuche. Die Versuche zum Veröffentlichen von Informationen auf dem Backup Exec-Server erfolgen im Abstand von einer Minute. Sind die Informationen nach den zehn Versuchen nicht gesendet, überspringt der Linux Agent diesen Backup Exec-Server bis zum nächsten Veröffentlichungszyklus. Der Veröffentlichungszyklus entspricht der Anzahl von Minuten, die in der Zeichenfolge "Agents\Advertising Interval Minutes" festgelegt ist.

Zeichenfolge und Standardwerte	Beschreibung
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\Agents\Advertisement Purge=0	<p>Ermöglicht das Senden einer Löschmeldung an alle Backup Exec-Server in der \Agents\Advertisement Purge-Zeichenfolge. Wenn ein Backup Exec-Server eine Löschmeldung erhält, entfernt er den Linux Agent aus der Backup Exec-Liste verfügbarer Server. Der Linux Agent funktioniert weiterhin.</p> <p>Es gibt folgende Werte:</p> <ul style="list-style-type: none"> ■ 0 Bereinigen Sie den Linux Agent nicht von Backup Exec-Servern, die in der \Agents\Advertisement Purge-Zeichenketten aufgelistet sind. ■ 1 Bereinigen Sie den Linux Agent von einem oder mehreren Backup Exec-Servern in der \Agents\Advertisement Purge-Zeichenkette.
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\Agents\Advertising Disabled=0	<p>Aktiviert den Linux Agent, um auf Backup Exec-Servern zu veröffentlichen.</p> <p>Es gibt folgende Werte:</p> <ul style="list-style-type: none"> ■ 0 Der Linux Agent versucht, Informationen auf den Backup Exec-Servern bereitzustellen, die in der \Agents\Agent Directory List-Zeichenfolge aufgelistet sind. ■ 1 Der Linux Agent veröffentlicht keine Informationen auf den Backup Exec-Servern.
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\Agents\Advertising Interval Minutes=240	<p>Legt die Anzahl von Minuten fest, die der Linux Agent zwischen Veröffentlichungszyklen warten muss. Die Standardanzahl von Minuten ist 240. Der zulässige Bereich hierfür liegt zwischen 1 Minute und 720 Minuten.</p>

Zeichenfolge und Standardwerte	Beschreibung
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\Agents\Agent Directory List_1=<Backup Exec server name>	<p>Zeigt die Liste der NetBIOS-Namen, vollständig qualifizierten Domännennamen oder IP-Adressen an, auf denen der Linux Agent Informationen veröffentlicht.</p> <p>Der Backup Exec-Server, von dem aus der Linux Agent über Push-Installation installiert wird, wird standardmäßig der Agent-Verzeichnisliste hinzugefügt.</p>
Software\Symantec\Backup Exec For Windows\Backup Exec\Engine\Agents\Auto Discovery Enabled=1	<p>Fügt einen Backup Exec-Server der \Agents\Agent Directory List-Zeichenkette hinzu, wenn der Backup Exec-Server einen Backup-Auftrag durchführt, dem der Linux Agent zugeordnet ist.</p> <p>Es gibt folgende Werte:</p> <ul style="list-style-type: none"> ■ 1 Fügt der Agent Directory List den Backup Exec-Server hinzu, der den Backup-Auftrag durchführt. Der Linux Agent kann Informationen auf dem Backup Exec-Server veröffentlichen. ■ 0 Der Backup Exec-Server, der den Backup-Auftrag durchführt, wird der Agent Directory List nicht hinzugefügt.
Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\Logging\RANT NDMP Debug Level=0	<p>Zeigt den Ausführlichkeitsgrad der Protokollierung der NDMP-Informationen für den Linux Agent an.</p> <p>Es gibt folgende Werte:</p> <ul style="list-style-type: none"> ■ 0 Protokolliert nur die NDMP-Fehler. ■ 1 Protokolliert die NDMP-Fehler und -Warnungen. ■ 2 Protokolliert die NDMP-Fehler, Warnungen und Meldungen, die zwischen dem Remote-Computer und dem Backup Exec-Server gesendet werden.

Zeichenfolge und Standardwerte	Beschreibung
Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\RALUS\Encoder=	Zeigt den Kodierer an, den Sie hinzufügen können, wenn der Standardkodierer Zeichen auf der Benutzeroberfläche falsch anzeigt.
Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\RALUS\ShowTSAFS=	<p>Hiermit können Sie ein Backup des Target Service Agent-Dateisystems (TSAFS) für Anwendungen unter Novell Open Enterprise Services durchführen. Diese Option ist standardmäßig nicht aktiviert.</p> <p>Der Linux Agent sichert alle Dateisysteme unter Verwendung des Root-Objekts. Wenn ShowTSAFS aktiviert wird, erscheint die Novell Open Enterprise Services-Ressource in der Backup-Auswahlliste. Wenn Sie für den Backup den ganzen Computer auswählen, dann werden überflüssige Backups durchgeführt. Es wird empfohlen, diese Option nicht zu aktivieren.</p> <p>Es gibt folgende Werte:</p> <ul style="list-style-type: none"> ■ Leer oder 0 Das TSA-Dateisystem erscheint nicht als Backup-Auswahl. ■ 1 Die TSA-Dateisystem-Ressource erscheint als Backup-Auswahl.
Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\RALUS\SystemExclude1=	<p>Listet die Dateien auf, die von allen Linux Agent-Backup-Aufträgen ausgeschlossen werden sollen.</p> <p>Siehe " Ausschließen der Dateien und Verzeichnisse von allen Backup-Aufträgen für Linux-Computer" auf Seite 1569.</p>
Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\RALUS\SystemFSTypeExclude1	Listet den Typ des Dateisystems auf, der vom Linux Agent-Backup ausgeschlossen werden soll.

Zeichenfolge und Standardwerte	Beschreibung
Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\RMAL\DisableRMAL=0	<p>Hier können Sie Remote Media Agent for Linux verwenden, um den Linux-Server zu sichern, auf dem es installiert ist. Diese Option ist standardmäßig nicht aktiviert.</p> <p>Wenn Sie Remote Media Agent for Linux unter einer nicht unterstützten Version von Linux installieren, ist der Agent nicht verfügbar. Sie können die Aufträge, die auf den an den Linux-Server angeschlossenen Geräten ausgeführt werden, nicht erstellen. Jedoch können Sie den Linux-Server sichern, indem Sie die Komponente Agent for Linux-Komponente verwenden. Diese Komponente wird mit Remote Media Agent for Linux installiert. Sie müssen den Wert dieser Zeichenkette auf 1 ändern, um die Agent for Linux-Komponente zu verwenden.</p> <p>Es gibt folgende Werte:</p> <ul style="list-style-type: none"> ■ 0 Sie können Backup-, Wiederherstellungs- und Dienstprogrammaufträge auf dem Backup Exec-Server erstellen, die auf den Speichergeräten des Linux-Servers ausgeführt werden. ■ 1 Sie können die Agent for Linux-Komponenten nur verwenden, um den Linux-Server zu sichern, auf dem er installiert ist. <p>Siehe "Fehlerbehebung für den Agent for Linux" auf Seite 1590.</p>

Zeichenfolge und Standardwerte	Beschreibung
Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\RALUS\DisableOFO=0	<p>Ermöglicht Ihnen das Aktivieren oder Deaktivieren der Open File-Technologie des Linux Agent.</p> <p>Standardmäßig wird der "DisableOFO"-Schlüssel auf "0" eingestellt, was bedeutet, dass der Linux Agent aktiv ist und die gefundenen offenen Dateien sichert. Sie können die Open File-Technologie deaktivieren, indem Sie den Standardwert des Schlüssels in "1" ändern und danach den Linux Agent-Daemon neu starten.</p>
Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\RALUS\AOFOL\CacheFileMountPoint =	<p>Der alternative Cache-Dateispeicherort für Advanced Open File Feature (AOF). Dieser Speicherort sollte der Bereitstellungspunkt sein.</p> <p>Standardmäßig wird die Snapshot-Cache-Datei auf dem Bereitstellungspunkt des Datenträgers erstellt.</p> <p>Wenn Sie den Speicherort angeben, verwendet der Linux-Agent diesen Speicherort, um die Snapshot-Cache-Datei zu erstellen.</p>
Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\RALUS\AOFOL\CacheFileSize =	<p>Die alternative Cache-Dateigröße. Die Größe sollte mindestens 10% der Datenträgergröße sein, die Sie planen, zu sichern und der Größenwert muss Vielfachen von 4 KB-Blöcken entsprechen.</p> <p>Der Linux-Agent akzeptiert den alternativen Cache-Dateispeicherort und die -größe, wenn Werte für beide richtig konfiguriert werden.</p>

Info zum Sichern eines Linux-Computers durch Verwendung des Agent for Linux

Die folgenden Backup-Methoden werden angezeigt, wenn Sie Agent for Linux (Linux-Agent) zum Sichern von Daten verwenden:

- Vollständig - Mit geänderter Uhrzeit
- Differenzial - Mit geänderter Uhrzeit
- Inkrementell - Mit geänderter Uhrzeit

Auf dem Novell OES-Server werden jedoch nur vollständige Backups unterstützt. Wenn Sie eine andere Backup-Methode auswählen, wird stattdessen ein vollständiges Backup ausgeführt. Der Agent for Linux unterstützt auch synthetisches vollständiges Backup, Novell OES jedoch nicht.

Siehe ["Linux-Backup-Optionen"](#) auf Seite 1579.

Siehe ["Hinzufügen einer Stufe zu einer Backup-Definition"](#) auf Seite 244.

Siehe ["Bearbeiten von Stufen"](#) auf Seite 245.

Siehe ["Infos zum Sichern und Wiederherstellen von Novell Open Enterprise Server\(OES\)-Komponenten "](#) auf Seite 1580.

Linux-Backup-Optionen

Der folgenden Optionen für Agent for Linux (Linux Agent) sind verfügbar, wenn Sie Linux-Computer sichern.

Siehe ["Info zum Sichern eines Linux-Computers durch Verwendung des Agent for Linux"](#) auf Seite 1578.

Tabelle N-3 Optionen für Backup-Aufträge für Linux-Computer

Element	Beschreibung
Datei- und Verzeichniszeitstempel während Backups speichern	<p>Hindert den Linux Agent am Ändern der Attribute eines Objekts, wenn ein Backup durchgeführt wird. Ein Objekt ist eine Datei oder ein Verzeichnis.</p> <p>Diese Option ist standardmäßig nicht ausgewählt.</p> <p>Während eines Backup behält Backup Exec den Zeitstempel des letzten Zugriffs auf das Objekt bei, indem der Zeitstempel auf den Wert vor dem Backup zurückgesetzt wird. Wenn Backup Exec den Zeitstempel des letzten Zugriffs auf das Objekt ändert, aktualisiert das Betriebssystem intern die "ctime" des Objekts.</p> <p>Die "ctime" eines Objekts ist der Zeitpunkt, an dem die Attribute eines Objekts, wie etwa Berechtigungen und Zeitstempel, geändert wurden. Wenn der Linux-Agent nach einem Backup die Attribute nicht ändert, ändert sich die "ctime" des Objekts nicht.</p> <p>Diese Option betrifft nicht die Objektattribute, die während der Wiederherstellungsvorgänge festgelegt werden.</p>

Element	Beschreibung
Lokalen Bereitstellungspunkten folgen	<p>Backup Exec folgt beim Sichern von Daten lokalen Bereitstellungspunkten.</p> <p>Diese Option ist standardmäßig aktiviert.</p> <p>Weitere Informationen über lokale Bereitstellungspunkte finden Sie in der Dokumentation zum Betriebssystem.</p>
Standortfernen Bereitstellungspunkten folgen	<p>Backup Exec folgt beim Sichern von Daten standortfernen Bereitstellungspunkten.</p> <p>Diese Option ist standardmäßig nicht ausgewählt.</p> <p>Bei dieser Option treten folgenden Einschränkungen auf:</p> <ul style="list-style-type: none"> ■ Die geladenen Daten müssen sich auf einem Backup Exec-kompatiblen Computer befinden. Die unterstützten Betriebssysteme, Plattformen und Anwendungen finden Sie in der Liste der mit Backup Exec kompatiblen Software. ■ Wenn der Bereitstellungspunkt zu einem Betriebssystem führt, das Backup Exec nicht unterstützt, kontaktieren Sie zur Problembeseitigung den Anbieter des Betriebssystems. <p>Weitere Informationen über standortferne Bereitstellungspunkte finden Sie in der Dokumentation zum Betriebssystem.</p>
Remote-Dateien sperren, damit sie von Anwendungen während Backups nicht geändert werden können	<p>Gewährt dem Linux-Agent exklusiven Zugriff auf die Dateien auf Remote-Servern, die über Network File System (NFS) verbunden sind. Das Sperren der Remote-Dateien hindert andere Anwendungen am Ändern der Daten während des Backups.</p>
Backup-Methode für eDirectory	<p>Löscht eine Backup-Methode zum Sichern von eDirectory-Daten für Novell OES auf SUSE Linux Enterprise Server.</p> <p>Siehe "Informationen zum Wiederherstellen von Novell OES-Komponenten" auf Seite 1582.</p>

Infos zum Sichern und Wiederherstellen von Novell Open Enterprise Server(OES)-Komponenten

Bevor Sie Novell OES-Komponenten sichern können, muss der Agent for Linux auf dem Server installiert werden, auf dem sich die Novell OES-Komponenten befinden.

Backup Exec unterstützt die folgenden Komponenten von Novell Open Enterprise Servers (OES):

- Novell iFolder
- Novell eDirectory
- Novell GroupWise

Hinweis: Backup Exec 2014 und höher unterstützt GroupWise12 nicht.

- Novell Storage Services (NSS)

Hinweis: Beim Sichern von Novell OES-Komponenten wie GroupWise, iFolders oder eDirectories, selbst wenn Sie die Option "Inkrementelles Backup" bzw. "Differentielles Backup" ausgewählt haben, sichert Backup Exec alle Daten, weil diese OES-Komponenten inkrementelle Backups nicht unterstützen. Beim Sichern von NSS-Dateisystemdaten werden jedoch vollständige, inkrementelle und differenzielle Backups als reguläre Dateisysteme unterstützt.

Siehe ["Anforderungen für das Sichern von Novell Open Enterprise Server auf "SUSE Linux Enterprise Server""](#) auf Seite 1581.

Anforderungen für das Sichern von Novell Open Enterprise Server auf "SUSE Linux Enterprise Server"

Backup Exec erfordert Folgendes, um Novell OES zu sichern:

- Um Novell eDirectory, iFolder und GroupWise zu schützen, müssen die notwendigen Target Service Agents (TSA) geladen werden. Beachten Sie die Novell-Dokumentation für Details zum Laden des TSA für diese Novell OES-Komponenten.
- Ein lokaler UNIX-Benutzername, der das Äquivalent des eDirectory-Benutzers auf Administratorebene in der beoper-Gruppe ist. Backup Exec unterstützt keine eDirectory-Benutzer.
Siehe ["Info zur Backup Exec-Operator-Gruppe \(beoper\) für den Agent for Linux"](#) auf Seite 1565.
- Ein Backup Exec-Login-Konto, das die Anmeldedaten für den entsprechenden eDirectory-Benutzer auf Administratorebene enthält, muss zum Durchführen von Backup-Aufträge für eDirectory vorhanden sein.

Siehe ["Sichern von Daten"](#) auf Seite 174.

Siehe ["Info zum Sichern eines Linux-Computers durch Verwendung des Agent for Linux"](#) auf Seite 1578.

Info zum Wiederherstellen von Daten auf Linux-Computern

Sie können Optionen für Wiederherstellungsaufträge angeben, um Linux-Computer wiederherzustellen.

Siehe ["Methoden für das Wiederherstellen von Daten in Backup Exec"](#) auf Seite 258.

Siehe ["Optionen für Wiederherstellungsaufträge für Linux-Computer"](#) auf Seite 1582.

Informationen zum Wiederherstellen von Novell OES-Komponenten

Beim Sichern von Novell OES-Komponenten sichert Backup Exec die vollen Daten, selbst wenn Sie ein inkrementelles oder Differenzial-Backup auswählen. Auch wenn in der Wiederherstellungsansicht die zur Wiederherstellung verfügbare Backup-Instanz als "Inkrementell" oder "Differenzial" angezeigt wird, wird beim Auswählen ein vollständiges Backup ausgeführt.

Backup Exec unterstützt keine umgeleitete Wiederherstellung der Novell OES-Komponenten "iFolder" und "eDirectory" von einer OES-Umgebung in eine nicht-OES-Umgebung.

Siehe ["Methoden für das Wiederherstellen von Daten in Backup Exec"](#) auf Seite 258.

Optionen für Wiederherstellungsaufträge für Linux-Computer

Siehe ["Info zum Wiederherstellen von Daten auf Linux-Computern"](#) auf Seite 1582.

Tabelle N-4 Optionen für Wiederherstellungsaufträge für Linux-Computer

Element	Beschreibung
Remote-Dateien sperren, wenn die Bereitstellungspunkte die nötigen Rechte besitzen	<p>Gewährt Backup Exec exklusiven Zugriff auf die Dateien auf Remote-Computern, die über Network File System (NFS) verbunden sind.</p> <p>Diese Option ist in der Standardeinstellung aktiviert.</p>

Element	Beschreibung
DIB-Satz wiederherstellen	Stellt die DIB (Directory Information Base), auch bekannt als NDS-Datenbank (Novell Directory Services), wieder her.
DIB nach Überprüfung aktivieren	<p>Ermöglicht Backup Exec das Umbenennen der Datenbank von .RST in .NDS nachdem der Prüfvorgang erfolgreich abgeschlossen wurde. Wenn die Überprüfung fehlschlägt, wird die .RST-Datei gelöscht und die ursprüngliche .NDS-Datei bleibt funktionsfähig.</p> <p>Wenn Sie diese Option nicht auswählen, steht die .RST-Datei nach Wiederherstellung der Datenbank zur manuellen Aktivierung oder Notfallwiederherstellung zur Verfügung.</p>
Datenbank nach Abschluss öffnen	<p>Ermöglicht das Öffnen der Datenbank durch Backup Exec, nachdem die Wiederherstellung abgeschlossen wurde.</p> <p>Wenn Sie Wartungsaufgaben durchführen möchten, bevor die Datenbank geöffnet wird, wählen Sie diese Option nicht aus.</p>
Datenbank nach dem Wiederherstellen überprüfen	Ermöglicht das Überprüfen der Datenbank durch Backup Exec, nachdem die Wiederherstellung abgeschlossen wurde.
Roll-Forward-Protokollverzeichnis	Zeigt den Speicherort des Roll-Forward-Protokollverzeichnisses an.
Backup-Datei auf Festplatte belassen	<p>Der Novell DIB-Dateisatz wird auf der Festplatte beibehalten.</p> <p>Siehe "Informationen zum Wiederherstellen von Novell OES-Komponenten" auf Seite 1582.</p>

Bearbeiten der Standardoptionen für Backup-Aufträge für Linux-Computer

Sie können die vorhandenen Standardoptionen für alle Backup- und Wiederherstellungsaufträge für Linux-Systeme bearbeiten.

So bearbeiten Sie Standardoptionen für Backup-Aufträge für Linux-Systeme

- 1 Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und dann "Auftragsstandardeinstellungen".
- 2 Wählen Sie entweder "Auf Festplatte sichern" oder "Auf Band sichern" und anschließend "Linux".
- 3 Stellen Sie die entsprechenden Optionen ein.
Siehe "[Standardoptionen für Backup-Aufträge für Linux-Computer](#)" auf Seite 1584.
- 4 Klicken Sie auf "OK".

Standardoptionen für Backup-Aufträge für Linux-Computer

Sie können Standardeigenschaften von Backup-Aufträgen für alle Aufträge auf Linux-Computern festlegen.

Siehe "[Bearbeiten der Standardoptionen für Backup-Aufträge für Linux-Computer](#)" auf Seite 1584.

Die unterstützten Betriebssysteme, Plattformen und Anwendungen finden Sie in der Liste der mit Backup Exec kompatiblen Software.

Tabelle N-5 Standardoptionen für Backup-Aufträge für Linux-Computer

Element	Beschreibung
Datei- und Verzeichniszeitstempel während Backups speichern	<p>Hindert den Linux Agent am Ändern der Attribute eines Objekts, wenn ein Backup durchgeführt wird. Ein Objekt ist eine Datei oder ein Verzeichnis.</p> <p>Diese Option ist standardmäßig nicht ausgewählt.</p> <p>Während eines Backup behält Backup Exec den Zeitstempel des letzten Zugriffs auf das Objekt bei, indem der Zeitstempel auf den Wert vor dem Backup zurückgesetzt wird. Wenn Backup Exec den Zeitstempel des letzten Zugriffs auf das Objekt ändert, aktualisiert das Betriebssystem intern die "ctime" des Objekts.</p> <p>Die "ctime" eines Objekts ist der Zeitpunkt, an dem die Attribute eines Objekts, wie etwa Berechtigungen und Zeitstempel, geändert wurden. Wenn der Linux-Agent nach einem Backup die Attribute nicht ändert, ändert sich die "ctime" des Objekts nicht.</p> <p>Diese Option betrifft nicht die Objektattribute, die während der Wiederherstellungsvorgänge festgelegt werden.</p>
Lokalen Bereitstellungspunkten folgen	<p>Backup Exec folgt beim Sichern von Daten lokalen Bereitstellungspunkten.</p> <p>Diese Option ist standardmäßig aktiviert.</p> <p>Weitere Informationen über lokale Bereitstellungspunkte finden Sie in der Dokumentation zum Betriebssystem.</p>
Standortfernen Bereitstellungspunkten folgen	<p>Backup Exec folgt beim Sichern von Daten standortfernen Bereitstellungspunkten.</p> <p>Diese Option ist standardmäßig nicht ausgewählt.</p> <p>Bei dieser Option treten folgenden Einschränkungen auf:</p> <ul style="list-style-type: none"> Die bereitgestellten Daten müssen sich auf einem Backup Exec-kompatiblen Betriebssystem befinden. Wenn der Bereitstellungspunkt zu einem Betriebssystem führt, das Backup Exec nicht unterstützt, kontaktieren Sie zur Problembehebung den Anbieter des Betriebssystems. <p>Weitere Informationen über standortferne Bereitstellungspunkte finden Sie in der Dokumentation zum Betriebssystem.</p>

Element	Beschreibung
Backup-Methode für eDirectory	Zeigt eine Backup-Methode für das Sichern von eDirectory-Daten für Novell OES unter SUSE Linux Enterprise Server an. Siehe " Infos zum Sichern und Wiederherstellen von Novell Open Enterprise Server(OES)-Komponenten " auf Seite 1580.
Remote-Dateien sperren, damit sie von Anwendungen während Backups nicht geändert werden können	Gewährt dem Linux-Agent exklusiven Zugriff auf die Dateien auf Remote-Servern, die über Network File System (NFS) verbunden sind. Das Sperren der Remote-Dateien hindert andere Anwendungen am Ändern der Daten während des Backup- oder Wiederherstellungsauftrags.

Deinstallieren von Agent for Linux

Eine automatisierte Deinstallation für Agent for Linux (Linux-Agent) ist auf den Backup Exec-Installationsmedien verfügbar.

`/opt/VRTS/install/logs/uninstallralus<Nummer der Zusammenfassungsdatei>.summary`

So deinstallieren Sie Agent for Linux

- 1 Legen Sie das Backup Exec-Installationsmedium in das entsprechende Gerät am Linux-Server ein.
- 2 Loggen Sie sich als Root auf dem Server ein, von dem der Linux-Agent deinstalliert werden soll.
- 3 Navigieren Sie zum folgenden Verzeichnis auf dem Backup Exec-Installationsmedium:

<Linux>
- 4 Starten Sie das Skript "uninstallralus".

Beispiel:

`./uninstallralus`
- 5 Um Linux Agent von einem oder mehreren Servern zu deinstallieren, geben Sie den Namen, die IP-Adresse oder den vollständig qualifizierten Domännennamen des Linux-Servers ein.

Hinweis: Für mehrere Server trennen Sie die Kennungen durch Leerzeichen voneinander.

- 6 Drücken Sie die **Eingabetaste**.
- 7 Nachdem die Paketüberprüfung für den Linux-Agent erfolgreich abgeschlossen ist, drücken Sie die **Eingabetaste**.
- 8 Wenn Sie aufgefordert werden, die RALUS-Pakete zu deinstallieren, drücken Sie die **Eingabetaste**.
- 9 Wenn Sie aufgefordert werden, den SymSnap-Treiber zu deinstallieren, drücken Sie die Eingabetaste.
- 10 Um die Deinstallationszusammenfassung an folgendem Speicherort auf dem Linux-Server zu speichern, drücken Sie die **Eingabetaste**:

`/opt/VRTS/install/logs/uninstallralus<Nummer der Zusammenfassungsdatei>.summary`

Siehe ["Installation von Agent for Linux"](#) auf Seite 1562.

Manuelles Deinstallieren von Agent for Linux

Sie können Agent for Linux (Linux-Agent) manuell deinstallieren.

So deinstallieren Sie Agent for Linux manuell

- 1 Verwenden Sie eine Terminalsitzung, um eine Verbindung zum Linux-Server als Root-Benutzer herzustellen.
- 2 Wechseln Sie zum folgenden Verzeichnis:

`/opt/VRTSralus/bin`

Beispiel:

`cd /opt/VRTSralus/bin`
- 3 Löschen Sie die folgende Zeile, wenn sie in der Datei `"/etc/inittab"` vorkommt:

`/opt/VRTSralus/bin/VRTSralus.init`

Beispiel:

`rm -r /opt/VRTSralus/bin/VRTSralus.init`
- 4 Kopieren Sie die Datei `"RALUS_RMALS_<Versionsnummer>.gz"` in diesem Verzeichnis in ein Verzeichnis auf dem lokalen Computer.
- 5 Entpacken Sie die Datei mit dem folgenden Befehl:

`gunzip RALUS_RMALS_<Versionsnummer>.gz`
- 6 Entzippen Sie die Datei mit dem folgenden Befehl:

`tar -xf RALUS_RMALS_<Versionsnummer>.tar`

- 7** Beenden Sie den Linux-Agent-Daemon.

Siehe ["Beenden des Agent for Linux-Daemon"](#) auf Seite 1590.

- 8** Entfernen Sie das Linux-Agent-Paket vom Linux-Server.

Beispiel:

Debian GNU/Linux, Ubuntu	<code>dpkg -r VRTSralus</code>
Linux	<code>rpm -e VRTSralus</code>

- 9** Wechseln Sie zurück zum Stammverzeichnis.

Beispiel:

```
cd /
```

- 10** Entfernen Sie die folgenden Dateien:

```
/etc/VRTSralus
```

```
/opt/VRTSralus
```

```
/var/VRTSralus
```

Beispiel:

```
rm -r /etc/VRTSralus /opt/VRTSralus /var/VRTSralus
```

- 11** Geben Sie **y** ein, wenn Sie aufgefordert werden, in Verzeichnisse tieferer Ebene zu wechseln.
- 12** Geben Sie **y** ein, wenn Sie zum Löschen eines Verzeichnisses aufgefordert werden.
- 13** Entfernen Sie Laufzeitskripte, wenn sie vorhanden sind.

Siehe ["Beim manuellen Deinstallieren des Agent for Linux zu entfernende Laufzeitskripte"](#) auf Seite 1588.

Beim manuellen Deinstallieren des Agent for Linux zu entfernende Laufzeitskripte

Wenn Sie Agent for Linux (Linux-Agent) manuell deinstallieren, entfernen Sie die folgenden Laufzeitskripts, wenn sie vorhanden sind.

Tabelle N-6 Beim manuellen Deinstallieren des Linux-Agent zu entfernende Laufzeitskripte

Betriebssystem	Zu entfernende Laufzeitskripte
Debian, Ubuntu	<code>/etc/rc5.d/S95VRTSralus.init</code> <code>/etc/rc3.d/S95VRTSralus.init</code> <code>/etc/rc2.d/S95VRTSralus.init</code> <code>/etc/init.d/VRTSralus.init</code> Beispiel: <code>rm /etc/rc5.d/S95VRTSralus.init</code>
Red Hat Linux, Asianux	<code>/etc/rc.d/rc5.d/S95VRTSralus.init</code> <code>/etc/rc.d/rc3.d/S95VRTSralus.init</code> <code>/etc/rc.d/rc2.d/S95VRTSralus.init</code> <code>/etc/rc.d/init.d/VRTSralus.init</code> Beispiel: <code>rm /etc/rc.d/rc5.d/S95VRTSralus.init</code>
Novell Open Enterprise Server 1.0/ SUSE Linux Enterprise Server 9 (nur 32 Bit)	<code>/etc/init.d/rc5.d/SxxVRTSralus.init</code> <code>/etc/init.d/rc3.d/SxxVRTSralus.init</code> <code>/etc/init.d/rc2.d/SxxVRTSralus.init</code> <code>/etc/init.d/VRTSralus.init</code> Beispiel: <code>rm /etc/init.d/rc5.d/SxxVRTSralus.init</code>
Novell Open Enterprise Server 2.0/ SUSE Linux Enterprise Server 10 (32 Bit und 64 Bit)	<code>/etc/init.d/VRTSralus.init,start=2,3,5</code> <code>/etc/init.d/VRTSralus.init</code> Beispiel: <code>rm /etc/init.d/VRTSralus.init</code>

Siehe ["Manuelles Deinstallieren von Agent for Linux "](#) auf Seite 1587.

Starten des Agent for Linux-Daemon

Falls erforderlich, können Sie den Agent for Linux-(Linux-Agent-)Daemon starten, nachdem das Betriebssystem startet.

Siehe ["Beenden des Agent for Linux-Daemon"](#) auf Seite 1590.

So starten Sie den Agent for Linux-Daemon

- 1 Verwenden Sie eine Terminalsitzung, um eine Verbindung zum Linux-Server als Root-Benutzer herzustellen.

- 2 Navigieren Sie zum folgenden Verzeichnis:

`/etc/init.d/`

Beispiel:

```
cd /etc/init.d/
```

- 3 Starten Sie den Linux-Agent-Daemon.

Beispiel:

```
/etc/init.d/VRTSralus.init start
```

Beenden des Agent for Linux-Daemon

Sie können den Agent for Linux-(Linux-Agent-)Daemon beenden.

Siehe ["Starten des Agent for Linux-Daemon"](#) auf Seite 1589.

So beenden Sie den Agent for Linux-Daemon

- 1 Verwenden Sie eine Terminalsitzung, um eine Verbindung zum Linux-Server als Root-Benutzer herzustellen.

- 2 Navigieren Sie zum folgenden Verzeichnis:

`/etc/init.d/`

Beispiel:

```
cd /etc/init.d/
```

- 3 Beenden Sie den Linux-Agent-Daemon:

Beispiel:

```
/etc/init.d/VRTSralus.init stop
```

- 4 Starten Sie den Daemon erforderlichenfalls neu.

Fehlerbehebung für den Agent for Linux

Wenn Probleme mit Agent for Linux (Linux-Agent) auftreten, lesen Sie die folgenden Fragen und Antworten.

Siehe ["Info zu Agent for Linux"](#) auf Seite 1560.

Tabelle N-7 Fehlerbehebung für den Linux-Agent

Frage	Antwort
Einige Zeichen werden in der Terminalsitzung während der Installation nicht richtig angezeigt. Was kann ich tun?	Dieser Fehler tritt auf, wenn auf dem Computer, auf dem Sie den Linux-Agent installieren, ein Gebietsschema mit einer anderen Sprache als Englisch verwendet wird. Sie können versuchen, zu einem anderen Gebietsschema derselben Sprache zu wechseln, um das Problem zu beheben.
Das Linux-Agent-Installationsprogramm ist nicht in der Lage, den Linux-Agent zu installieren. Der folgende Fehler wird in der Protokolldatei "installralus" gemeldet: Was kann ich tun? VxIF::Fehler:: Dateien können nicht komprimiert werden. Hash(0x8711e8)->{{GUNZIP} nicht auf <Hostname> gefunden	Zur Unterstützung der Dekomprimierung der plattformspezifischen Linux-Agent-Pakete können Sie das GNU-Dienstprogramm zur Datenkomprimierung installieren. Installieren Sie dieses Dienstprogramm auf dem Computer, auf dem Sie den Linux-Agent installieren möchten. Das Dienstprogramm ist unter folgender URL verfügbar: http://www.gzip.org .
Agent for Linux ist auf einem Unix- oder Linux-Server in einer NIS-Domäne installiert. Backup Exec ist nicht in der Lage, die Ressourcen auf dem Server zu durchsuchen. Was kann ich tun?	Überprüfen Sie, ob die Gruppenzeile und die Kennwortzeile in der Datei "nsswitch.conf" auf den Kompatibilitätsmodus eingestellt sind. Wenn das der Fall ist, müssen die Dateien "/etc/passwd" und "/etc/group" konfiguriert werden. Weitere Informationen dazu, wie man "nsswitch.conf" zur Verwendung des Kompatibilitätsmodus konfiguriert, finden Sie auf den nsswitch.conf-Man-Seiten. Alternativ dazu können Sie die Kennwortzeile und die Gruppenzeile in den NIS-Dateien so ändern, dass der Linux-Server den Benutzer über NIS validiert. Wenn der NIS-Server nicht verfügbar ist oder der Benutzer nicht gefunden wird, werden die lokalen Dateien zur Validierung verwendet.

Frage	Antwort
<p>Ich kann den Linux-Agent nicht laden. Wenn ich versuche, den Linux-Agent im console-Modus zu laden, zeigt "/beremote --log-console" die folgende Meldung an:</p> <p>ACE_SV_Semaphore_Complex: Kein Speicherplatz mehr auf dem Gerät.</p> <p>Was kann ich tun?</p>	<p>Dieses Problem tritt auf, wenn der Computer die maximal zulässige Anzahl Semaphore erreicht hat. Es kann nach einer unerwarteten Beendigung des Linux-Agent auftreten. Wenn der Linux-Agent unerwartet beendet wird, kann er einige der verwendeten Semaphore-Ressourcen nicht bereinigen. Andere Prozesse können dazu geführt haben, dass bei der Verwendung von Semaphore die Grenze erreicht wurde. Sie müssen den Computer neu starten, um den Computer sicher wiederherzustellen.</p> <p>Wenn andere Prozesse ausgeführt werden, können Sie den Computer eventuell nicht neu zu starten. Stattdessen können Sie die Befehle verwenden, um alle vom Betriebssystem verwendeten Semaphore aufzulisten und zu entfernen. Seien Sie vorsichtig bei der Auswahl der zu entfernenden Semaphore. Semaphore, die durch den Linux-Agent verwendet werden, können nicht identifiziert werden. Wenn Sie die Semaphore anderer gerade verwendeter Programme entfernen, können diese Programme instabil werden.</p> <p>Zum Auflisten von Semaphore können Sie folgenden Befehl eingeben:</p> <pre>ipcs -a</pre> <p>Zum Entfernen von Semaphore für jede aufgelistete Kennung können Sie folgenden Befehl eingeben:</p> <pre>ipcrm -s <id></pre>

Frage	Antwort
<p>Ich kann den Linux-Agent nicht laden. Wenn ich versuche, den Linux-Agent im console-Modus zu laden, zeigt "/beremote --log-console" die folgende Meldung an: Fehler beim Laden gemeinsam genutzter Bibliotheken: libstdc++.so.5: Gemeinsam genutzte Objektdatei kann nicht geöffnet werden: Datei oder Verzeichnis nicht vorhanden.</p> <p>Was kann ich tun?</p>	<p>Dieser Fehler wird angezeigt, wenn sich die Bibliothek "libstdc++.so.5" nicht im /usr/lib-Verzeichnis befindet. Diese Bibliothek ist notwendig, um den Linux-Agent starten und ausführen zu können. Um dieses Problem zu lösen, installieren Sie das Paket "libstdc++5".</p> <p>Sie können dieses Paket von dem Datenträger installieren, auf dem Ihre Linux-Kopie Ihnen zur Verfügung gestellt wurde. Alternativ können Sie den folgenden Befehl von einem Computer mit Internetzugang aus ausführen:</p> <pre>apt-get install libstdc++5</pre> <p>Führen Sie bei SUSE Linux Enterprise Server 11 den folgenden Befehl aus:</p> <pre>zypper install libstdc++5</pre>
<p>Unter Asianux meldet Backup Exec, dass das Backup Exec-Login-Konto für Backup und Wiederherstellungsoptionen nicht Teil der Gruppe "beoper" ist.</p> <p>Was kann ich tun?</p>	<p>Manchmal wird möglicherweise die Datei "/etc/group" nicht korrekt aktualisiert, wenn ein Benutzer der Gruppe "beoper" hinzugefügt wird. Dies führt zum Fehlschlagen der Linux-API getgrnam(). Zur Umgehung dieses Problems sollten Sie die /etc/group-Datei manuell bearbeiten und der beoper-Gruppe den spezifischen POSIX-Benutzernamen für das betreffende Login-Konto hinzufügen.</p> <p>Weitere Informationen über die /etc/group-Datei finden Sie in der Dokumentation zum Betriebssystem Asianux.</p>

Frage	Antwort
<p>Auf einem Linux-Computer, auf dem GNOME Virtual File System (GVFS) installiert und bereitgestellt ist, kann GVFS nicht durchsucht, gesichert oder wiederhergestellt werden.</p> <p>Was kann ich tun?</p>	

Frage	Antwort
	<p>Auf Computern, auf denen GVFS installiert ist, wird der .gvfs-Bereitstellungspunkt für jeden Benutzer erstellt, der sich über die GNOME-Benutzeroberfläche einloggt. Der Bereitstellungspunkt wird im Stammverzeichnis des Benutzers erstellt. Wenn beispielsweise der Login-Name des Benutzers "John" ist, wird das Verzeichnis wie folgt angezeigt:</p> <pre>Echo \$>ls -la /home/John</pre> <pre>dr-x----- 2 John John 0 2009-06-16 18:16 .gvfs</pre> <p>Die Ausgabe des Bereitstellungsbefehls wird wie folgt angezeigt:</p> <pre>"gvfs-fuse-daemon on /home/John/.gvfs type fuse.gvfs-fuse-daemon (rw,nosuid,nodev,user=John)".</pre> <p>Dieser Bereitstellungspunkt wird erstellt, wenn sich der Benutzer über die grafische Benutzeroberfläche von GNOME einloggt. Der Bereitstellungspunkt wird gelöscht, wenn sich der Benutzer ausloggt.</p> <p>Hinweis: Beim Einloggen über SSH oder Telnet wird der Bereitstellungspunkt nicht angezeigt.</p> <p>In einem Fehler für GVFS wurde gemeldet, dass sogar der Superuser (Root) keinen Zugriff auf das Dateisystem hat. Weitere Informationen finden Sie unter folgender URL:</p> <p>http://bugzilla.gnome.org/show_bug.cgi?id=560658</p> <p>Dieser Defekt hindert den Agent for Linux am Ausführen auf GVFS. Daher kann GVFS nicht durchsucht, gesichert oder wiederhergestellt werden. Außerdem ist auch kein Zugriff auf andere Dateisysteme auf Linux-Computern möglich, auf denen GVFS installiert ist.</p> <p>Darüber hinaus können auf Linux-Computern, auf denen GVFS im Stammorder eines bestimmten Benutzers installiert und bereitgestellt ist, Fehler bei Such-, Backup- und Wiederherstellungsvorgängen auf bzw. in den folgenden Dateisystemen auftreten:</p> <ul style="list-style-type: none">■ SMBFS (auch als Samba bezeichnet)■ Common Internet File System (CIFS)■ Network File System (NFS)■ ReiserFS

Frage	Antwort
	<p>Versuchen Sie den Fehler zu beheben, indem Sie die Bereitstellung von GVFS aufheben und den Vorgang erneut ausführen.</p>
<p>Das Installationsprogramm für Agent for Linux installiert das Perl-Modul "Switch.pm" nicht unter der 64-Bit-Version von Ubuntu 14.04.</p> <p>Was kann ich tun?</p>	<p>Sie müssen "Switch.pm" anhand der folgenden Anweisungen manuell installieren, bevor Sie Backup Exec Agent for Windows installieren.</p> <ul style="list-style-type: none"> ■ Öffnen Sie ein Terminal. ■ Geben Sie "cpan" ein. ■ Geben Sie "install Switch" ein. ■ Geben Sie "exit" ein. <p>Für Ubuntu 14.04 müssen Sie manuelle Logins aktivieren und einen Root-Benutzer hinzufügen:</p> <ul style="list-style-type: none"> ■ Bearbeiten Sie unter "/usr/share/lightdm/lightdm.conf.d" die Datei "50-ubuntu.conf". ■ Fügen Sie folgende Zeile hinzu: greeter-show-manual-login=true ■ Starten Sie den Computer neu und fügen Sie den Root-Benutzer auf der Anmeldeseite hinzu.

Backup Exec Remote Media Agent for Linux

Dieser Anhang enthält folgende Themen:

- [Info zu Remote Media Agent for Linux](#)
- [Funktionsweise von Remote Media Agent for Linux](#)
- [Anforderungen an Remote Media Agent for Linux](#)
- [Infos zu geöffneten Dateien und Remote Media Agent for Linux](#)
- [Info zum Installieren von Remote Media Agent for Linux](#)
- [Deinstallieren von Remote Media Agent for Linux](#)
- [Starten des Remote Media Agent für Linux-Daemon](#)
- [Beenden des Remote Media Agent for Linux-Daemon](#)
- [Info zum Festlegen des Vertrauens für einen Remote Media Agent for Linux-Computer in der Backup Exec-Liste von Servern](#)
- [Hinzufügen zusätzlicher Backup Exec-Server, für die Remote Media Agent for Linux veröffentlichen kann](#)
- [Suchen der Dateien der simulierten Bandbibliothek](#)
- [Info zur Backup Exec-Operator-Gruppe \(beoper\) für Remote Media Agent for Linux](#)
- [Info zum Hinzufügen eines Linux-Servers als Remote Media Agent for Linux](#)
- [Ändern des Ports für die Kommunikation zwischen Backup Exec-Server und Remote Media Agent for Linux](#)

- Info zum Erstellen von Speichergerätepools für mit Remote Media Agent for Linux verbundene Geräte
- Bearbeiten der Eigenschaften von Remote Media Agent for Linux
- Löschen eines Remote Media Agent for Linux aus der Backup Exec-Liste von Servern
- Gemeinsames Nutzen eines Remote Media Agent for Linux von mehreren Backup Exec-Servern
- Info zum Speichern von Daten durch Verwendung des Remote Media Agent for Linux
- Info zum Wiederherstellen von Daten mit Remote Media Agent for Linux
- Tape Library Simulator Utility
- Erstellen einer simulierten Bandbibliothek
- Anzeigen der Eigenschaften von simulierten Bandbibliotheken
- Löschen einer simulierten Bandbibliothek
- Verwalten simulierter Bandbibliotheken über die Befehlszeile
- Befehlszeilen-Switches für das Tape Library Simulator-Dienstprogramm
- Fehlerbehebung in Remote Media Agent for Linux

Info zu Remote Media Agent for Linux

Mit Remote Media Agent for Linux können Sie die Daten von Remote-Computern auf den folgenden Geräten sichern:

- Speichergeräte, die direkt an einen Linux-Server angeschlossen sind
- eine simulierte Bandbibliothek auf einem Linux-Server

Sie können einen Linux-Server einem Backup Exec-Server als Remote Media Agent for Linux hinzufügen. Anschließend können Sie Daten, die sich auf dem Linux-Server oder auf den unterstützten Remote-Computern befinden, auf Geräten sichern, die mit dem Linux-Server verbunden sind. Sie können auch ein virtuelles Gerät auf einem Server erstellen, auf dem Remote Media Agent for Linux installiert ist. Dieses virtuelle Gerät emuliert eine SCSI-Bandbibliothek.

Sie können Daten aus den Remote-Computern sichern, auf denen die folgenden Agents installiert sind:

- Agent for Windows

- Agent for Linux
- Agent for Oracle auf Linux- oder Windows-Servern

Remote Media Agent for Linux unterstützt das Sichern der folgenden Datenbank- und Anwendungs-Agents nicht:

- Agent for Microsoft SQL Server
- Agent for Microsoft Exchange Server
- Agent for Microsoft SharePoint
- Agent for Microsoft Active Directory
- Agent for Microsoft Hyper-V
- Agent for VMware
- Agent for Enterprise Vault

Hinweis: Darüber hinaus werden die folgenden Elemente nicht unterstützt:

Backups, die für Granular Recovery Technology (GRT) aktiviert sind.

NAS-NDMP-Server.

Informationen zu den Best Practices zum Einsatz des Backup Exec Remote Media Agent for Linux (RMAL) finden Sie unter *Best Practices für Backup Exec*.

Siehe ["Funktionsweise von Remote Media Agent for Linux"](#) auf Seite 1599.

Siehe ["Tape Library Simulator Utility"](#) auf Seite 1619.

Funktionsweise von Remote Media Agent for Linux

Sie können vom Backup Exec-Server einen Linux-Server als einen Remote Media Agent for Linux hinzufügen. Sie können Backup-, Wiederherstellungs- und Dienstprogrammaufträge auf dem Backup Exec-Server erstellen, die auf den Speichergeräten des Linux-Servers ausgeführt werden.

Wenn Sie Daten von einem Windows-Server sichern, auf dem Backup Exec Agent for Windows auf einem Speichergerät installiert ist, das an Remote Media Agent for Linux angehängt wird, wird die Datenverbindung direkt zwischen den zwei Computern hergestellt. In diesem Fall spielt der Backup Exec-Server keine Rolle in der Datenübertragung.

Wenn das Speichergerät, das an Remote Media Agent for Linux angehängt ist, ein OpenStorage-Gerät ist, ist eine Direktverbindung zwischen den Daten und dem Gerät erforderlich, um die clientseitige Deduplizierung zu ermöglichen. Wenn keine Direktverbindung verfügbar ist, werden die Daten über den Backup Exec-Server geleitet, um die serverseitige Deduplizierung durchzuführen.

Wenn Sie Backup Exec Central Admin Server Feature verwenden, können mehrere Backup Exec-Server einen Remote Media Agent for Linux-Computer gemeinsam nutzen. Das gemeinsame Nutzen kann aktiviert werden, wenn Sie Remote Media Agent for Linux hinzufügen. Sie können neue Backup Exec-Server auswählen, um Remote Media Agent for Linux gemeinsam zu nutzen oder diese Funktion jederzeit aus den Backup Exec-Servern entfernen.

Siehe ["Freigeben von Speichergeräten"](#) auf Seite 544.

Die Arbeitsleistung erhöht sich, da Daten von den Remote-Computern an die Geräte übertragen werden, die mit dem Linux-Server verbunden sind. Diese Zunahme ist besonders offensichtlich, wenn sich der Backup Exec-Server an einem anderen Standort als der Remote Media Agent for Linux-Computer und der Remote-Computer befindet.

Remote Media Agent for Linux hat keine Benutzeroberfläche. Sie verwenden die Administratorkonsole auf dem Backup Exec-Server, um die Aufträge und die Geräte auf Remote Media Agent for Linux zu verwalten. Der Backup Exec-Server behält Auftragsprotokolle, Kataloge, Auftragsverläufe, Meldungen und Benachrichtigungen bei.

Siehe ["Anforderungen an Remote Media Agent for Linux"](#) auf Seite 1600.

Siehe ["Info zum Installieren von Remote Media Agent for Linux"](#) auf Seite 1601.

Siehe ["Info zum Hinzufügen eines Linux-Servers als Remote Media Agent for Linux"](#) auf Seite 1612.

Siehe ["Tape Library Simulator Utility"](#) auf Seite 1619.

Anforderungen an Remote Media Agent for Linux

Die folgenden Elemente sind erforderlich, um Remote Media Agent for Linux zu installieren:

- Sie benötigen Superuser-Rechte auf dem Linux-Server.
- Auf dem Linux-Server muss Perl 5.8.8 oder höher installiert sein.

Die unterstützten Betriebssysteme, Plattformen und Anwendungen finden Sie in der Liste der mit Backup Exec kompatiblen Hardware und Software.

Es wird empfohlen, dass Sie das Protokoll "Secure Shell" (SSH) verwenden, wenn Sie Remote Media Agent for Linux über eine Push-Installation auf Remote-Servern installieren. Sie müssen SSH aktivieren, bevor Sie Remote Media Agent for Linux installieren.

Hinweis: Bei manchen Versionen von Linux kann es erforderlich sein, dass Sie das Paket "libstdc++.so.5" installieren.

Siehe ["Info zum Installieren von Remote Media Agent for Linux"](#) auf Seite 1601.

Infos zu geöffneten Dateien und Remote Media Agent for Linux

Remote Media Agent for Linux nutzt erweiterte Funktionen für die Verarbeitung öffentlicher Dateien und zum Erstellen von Images, um die manchmal bei Backup-Vorgängen auftretenden Probleme zu bewältigen. Hierzu gehört z. B. das Sichern öffentlicher Dateien.

Nachdem Sie Dateien und Ordner ausgewählt und den Backup-Auftrag gesendet haben, zeichnet der Linux Agent automatisch einen Snapshot der Datenträger auf. Der Snapshot stellt eine Aufzeichnung der Daten zu einem bestimmten Zeitpunkt dar. Wenn Remote Media Agent for Linux einen Snapshot erstellt, verwendet er Snapshot-Technologien, um Schreibvorgänge auf einen Datenträger kurzzeitig zu unterbrechen, damit ein Snapshot des Datenträgers erstellt werden kann. Während des Backup können Dateien geöffnet sein und Daten geändert werden.

Remote Media Agent for Linux unterstützt folgende Datenträgerkonfigurationen: Simple, Logical Volume Manager (LVM) und RAID.

Siehe ["Anforderungen an Remote Media Agent for Linux"](#) auf Seite 1600.

Info zum Installieren von Remote Media Agent for Linux

Führen Sie folgende Schritte mithilfe der Backup Exec-Installationsmedien aus:

- Installieren des Remote Media Agent for Linux auf einem lokalen Linux-Server
- Installieren des Remote Media Agent for Linux über eine Push-Installation auf einem oder mehreren Remote-Linux-Servern.

Wenn Sie den Remote Media Agent for Linux über eine Push-Installation installieren, wird standardmäßig RSH (Remote Shell) verwendet. Es wird empfohlen, stattdessen SSH (Secure Shell) zu verwenden. Um SSH zu

verwenden, müssen Sie es aktivieren, bevor Sie den Remote Media Agent for Linux installieren. Weitere Informationen zu SSH finden Sie in Ihrer Betriebssystemdokumentation.

Bevor Sie Remote Media Agent for Linux installieren, sollten Sie die Anforderungen überprüfen:

Siehe ["Anforderungen an Remote Media Agent for Linux"](#) auf Seite 1600.

Wenn Sie den Remote Media Agent for Linux installieren, erstellt Backup Exec die Gruppe "beoper" und fügt "root" als Mitglied hinzu. Jeder Linux-Benutzer, den Sie der beoper-Gruppe hinzufügen, erhält die erforderlichen Berechtigungen für die Sicherung und Wiederherstellung der Linux-Server.

Wenn Backup Exec jedoch während der Installation des Remote Media Agent for Linux einen NIS-Server erkennt, wird die Gruppe "beoper" nicht erstellt. Sie müssen die beoper-Gruppe auf den Linux-Servern manuell erstellen.

Wenn die Installation abgeschlossen ist, müssen Sie den Linux-Server als Remote Media Agent auf dem Backup Exec-Server hinzufügen. Anschließend können Sie Aufträge an die Geräte senden, die mit dem Linux-Server verbunden sind.

Siehe ["Installieren von Remote Media Agent for Linux"](#) auf Seite 1602.

Siehe ["Manuelles Erstellen der Backup Exec-Operatorengruppe \(beoper\) für Remote Media Agent for Linux"](#) auf Seite 1611.

Siehe ["Info zum Hinzufügen eines Linux-Servers als Remote Media Agent for Linux"](#) auf Seite 1612.

Siehe ["Info zur Backup Exec-Operator-Gruppe \(beoper\) für Remote Media Agent for Linux"](#) auf Seite 1610.

Installieren von Remote Media Agent for Linux

Sie können Remote Media Agent for Linux auf einem lokalen Linux-Server oder über eine Push-Installation auf einem oder mehreren Remote-Linux-Servern installieren.

Siehe ["Info zum Installieren von Remote Media Agent for Linux"](#) auf Seite 1601.

Hinweis: Sie müssen die Datei "RALUS_RMALS_<Versionsnummer>.gz" auf einem Linux-Server entpacken. Die Installation läuft nicht, wenn sie auf einem Computer entzippt wird, auf dem das Windows-Betriebssystem ausgeführt wird.

So installieren Sie Remote Media Agent for Linux

- 1 Legen Sie die Backup Exec-Installationsmedien in das entsprechende Laufwerk des Linux-Servers ein.
- 2 Loggen Sie sich als root auf dem Server ein, auf dem Sie den Remote Media Agent for Linux installieren möchten.
- 3 Öffnen Sie folgenden Ordner auf dem Installationsdatenträger:

<Linux>

- 4 Kopieren Sie die Datei "RALUS_RMALS_<Versionsnummer>.gz" in diesem Verzeichnis in ein Verzeichnis auf dem lokalen Server.
- 5 Dekomprimieren Sie die Datei.

Beispiel:

```
gunzip RALUS_RMALS_<Versionsnummer>.gz
```

- 6 Entzippen Sie die Datei.

Beispiel:

```
tar -xf RALUS_RMALS_<Versionsnummer>.tar
```

- 7 Starten Sie das Skript installrmal.

Beispiel:

```
./installrmal
```

- 8 Sie haben folgende Möglichkeiten:

So installieren Sie auf einem lokalen Server

Drücken Sie die **Eingabetaste**.

So installieren Sie auf einem Remote-Server

Geben Sie den Namen, die IP-Adresse oder den vollständig qualifizierten Domännennamen eines Linux-Servers ein.

So installieren Sie auf mehreren Remote-Servern

Geben Sie die Namen, IP-Adressen oder vollständig qualifizierten Domännennamen der Linux-Server ein. Lassen Sie ein Leerzeichen zwischen jeder Kennung.

- 9 Wenn das Installationsprogramm bei der erstmaligen Systemüberprüfung ein gültiges Betriebssystem für den Linux-Server gefunden hat, drücken Sie die **Eingabetaste**.
- 10 Überprüfen Sie die Paketinstallations-Übersicht, und drücken Sie dann die **Eingabetaste**.

- 11 Wenn die Systemanforderungen für die Installation geprüft wurden, drücken Sie die **Eingabetaste**.
- 12 Beginnen Sie die Voraussetzungsprüfung, indem Sie die **Eingabetaste** drücken.
- 13 Geben Sie den Namen, die IP-Adresse oder den vollständig qualifizierten Domänenname des Backup Exec-Servers (Verzeichnishost) ein, der Remote Media Agent verwenden soll.
- 14 Geben Sie die Namen, IP-Adressen oder vollständig qualifizierten Domännennamen der Backup Exec-Server ein, die diesen Remote Media Agent verwenden sollen.
- 15 Sie haben folgende Möglichkeiten:

Wenn der Servername, die IP-Adresse oder der vollständig qualifizierter Domännename korrekt ist	Drücken Sie die Eingabetaste , um die Installation fortzusetzen.
---	---

Wenn Sie einen Namen, eine IP-Adresse oder einen vollständig qualifizierten Domännennamen ändern möchten	Geben Sie N ein, drücken Sie die Eingabetaste , und ändern Sie dann die Informationen.
--	--

- 16 Starten Sie den NIS-Server-Scan, indem Sie die **Eingabetaste** drücken.
- 17 Überprüfen Sie die Ergebnisse des NIS-Server-Scans und wählen Sie eine der folgenden Vorgehensweisen:

Wenn ein NIS-Server erkannt wird	Das Installationsprogramm für Remote Media Agent for Linux kann die Gruppe "beoper" nicht erstellen. Sie müssen sie manuell erstellen, wenn die Installation des Remote Media Agent for Linux abgeschlossen ist. Fahren Sie mit dem nächsten Schritt fort.
----------------------------------	---

Wenn kein NIS-Server erkannt wird

Benutzen Sie das Installationsprogramm, um die beoper-Gruppe zu erstellen.

Gehen Sie dazu in folgender Reihenfolge vor:

- Um die Beoper-Gruppe durch das Installationsprogramm erstellen zu lassen, geben Sie **J** ein.
- Um die nächste verfügbare Gruppen-ID auszuwählen, geben Sie **N** ein.
- Um das Root-Benutzerkonto der beoper-Gruppe hinzuzufügen, geben Sie **J** ein.
- Fahren Sie mit dem nächsten Schritt fort.

- 18** Starten Sie die Installation, indem Sie die **Eingabetaste** drücken.
- 19** Drücken Sie nach Abschluss der Installation die Eingabetaste, um die nachfolgenden Konfigurationen sowie die Installation von SymSnap-Treibern zu starten.
- 20** Drücken Sie auf J, um den Beremote-Dienst automatisch zu starten, oder drücken Sie auf N, um den Dienst später zu starten.
- 21** Drücken Sie nach Abschluss des Konfigurationsprozesses die **Eingabetaste**, um das Installationsprotokoll in der folgenden Datei zu speichern:

`/var/tmp/vxif/installrmalNummer der Übersichtsdatei/installrmal.log`
- 22** Hat das RMAL-Installationsprogramm keine beoper-Gruppe erstellt, müssen Sie diese erstellen.

Siehe "[Manuelles Erstellen der Backup Exec-Operatorengruppe \(beoper\) für Remote Media Agent for Linux](#)" auf Seite 1611.
- 23** Starten Sie Agent für Linux-Daemon.

Siehe "[Starten des Agent for Linux-Daemon](#)" auf Seite 1589.
- 24** Fügen Sie den Linux-Server als Remote Media Agent hinzu.

Siehe "[Info zum Hinzufügen eines Linux-Servers als Remote Media Agent for Linux](#)" auf Seite 1612.

Deinstallieren von Remote Media Agent for Linux

Sie benötigen das Backup Exec-Installationsmedium, um Remote Media Agent for Linux zu deinstallieren.

Vor dem Deinstallieren von Remote Media Agent for Linux sollten Sie den Speicherort der Dateien der simulierten Bandbibliothek notieren. Dann können Sie nach der Deinstallation alle simulierten Bandbibliotheksdateien löschen. Wenn Sie diese Dateien löschen, löschen Sie die Backup-Daten, die Sie auf dem Linux-Server gespeichert haben.

Siehe ["Suchen der Dateien der simulierten Bandbibliothek"](#) auf Seite 1609.

So deinstallieren Sie Remote Media Agent for Linux

- 1 Legen Sie das Backup Exec-Installationsmedium in das entsprechende Gerät am Linux-Server ein.
- 2 Loggen Sie sich als Systemadministrator (Root) beim Server ein, auf dem Sie Remote Media Agent for Linux deinstallieren möchten.
- 3 Öffnen Sie folgenden Ordner auf dem Installationsdatenträger:

<Linux>

- 4 Starten Sie das Skript `uninstallrmal`.

Beispiel:

```
./uninstallrmal
```

- 5 Sie haben folgende Möglichkeiten:

So deinstallieren Sie Remote Media Agent for Linux von einem Server	Geben Sie den Namen, die IP-Adresse oder den vollständig qualifizierten Domännennamen des Linux-Servers ein.
---	--

So deinstallieren Sie Remote Media Agent for Linux von mehreren Servern	Geben Sie die Namen, die IP-Adressen oder die vollständig qualifizierten Domännennamen der Linux-Server ein. Lassen Sie ein Leerzeichen zwischen jeder Kennung.
---	---

- 6 Drücken Sie die **Eingabetaste**.
- 7 Nachdem die Remote Media Agent for Linux-Paketprüfung erfolgreich abgeschlossen ist, drücken Sie die **Eingabetaste**.
- 8 Wenn Sie aufgefordert werden, die Remote Media Agent-Pakete zu deinstallieren, können Sie durch Drücken der **Eingabetaste** eine Übersicht des Deinstallationsvorgangs speichern und an folgendem Speicherort protokollieren:

`/var/tmp/vxif/uninstallrmalNummer der Zusammenfassungsdatei.log`

- 9 Löschen Sie die simulierten Bandbibliothek-Dateien manuell.

Starten des Remote Media Agent für Linux-Daemon

Bei Bedarf starten den Remote Media Agent for Linux-Daemon, nachdem das Betriebssystem gestartet wurde.

Siehe ["Beenden des Remote Media Agent for Linux-Daemon"](#) auf Seite 1607.

So starten Sie den Remote Media Agent for Linux-Daemon

- 1 Verwenden Sie eine Terminalsitzung, um eine Verbindung zum Linux-Server als Root-Benutzer herzustellen.

- 2 Navigieren Sie zum folgenden Verzeichnis:

/etc/init.d/

Beispiel:

```
cd /etc/init.d/
```

- 3 So starten Sie den Remote Media Agent for Linux-Daemon

Beispiel:

```
/etc/init.d/VRTSralus.init start
```

Beenden des Remote Media Agent for Linux-Daemon

Sie können den Remote Media Agent for Linux-Daemon beenden.

Siehe ["Starten des Remote Media Agent für Linux-Daemon"](#) auf Seite 1607.

So beenden Sie den Remote Media Agent for Linux-Daemon

- 1 Verwenden Sie eine Terminalsitzung, um eine Verbindung zum Linux-Server als Root-Benutzer herzustellen.

- 2 Navigieren Sie zum folgenden Verzeichnis:

/etc/init.d/

Beispiel:

```
cd /etc/init.d/
```

- 3 Beenden Sie den Remote Media Agent for Linux-Daemon.

Beispiel:

```
/etc/init.d/VRTSralus.init stop
```

- 4 Starten Sie den Remote Media Agent for Linux-Daemon bei Bedarf neu.

Info zum Festlegen des Vertrauens für einen Remote Media Agent for Linux-Computer in der Backup Exec-Liste von Servern

Wenn Sie zu einem Remote Media Agent for Linux-Computer vom Backup Exec-Server eine Verbindung herstellen, müssen Sie Vertrauen zwischen dem Backup Exec-Server und dem Remote Media Agent for Linux-Computer herstellen. Sie müssen ein Vertrauen auch herstellen, wenn Sie einen Remote-Remote Media Agent for Linux-Computer zum Ausführen der clientseitigen Deduplizierung konfigurieren möchten.

Siehe ["Erstellen eines Vertrauensverhältnisses zwischen dem Backup Exec-Server und einem Remote-Computer"](#) auf Seite 1031.

Siehe ["Festlegen von Vertrauen und Hinzufügen eines Remote Media Agent for Linux-Computer zur Backup Exec-Liste von Servern"](#) auf Seite 1608.

Festlegen von Vertrauen und Hinzufügen eines Remote Media Agent for Linux-Computer zur Backup Exec-Liste von Servern

Sie können einen oder mehrere Remote Media Agent for Linux-Computer der Serverliste von Backup Exec hinzufügen. Wenn Sie Remote Media Agent for Linux hinzufügen, müssen Sie ein Vertrauen zwischen dem Backup Exec-Server und den Remote-Linux-Computern herstellen, um eine sichere Kommunikation sicherzustellen.

So richten Sie eine vertrauenswürdige Verbindung ein und fügen der Liste der Backup Exec-Server einen Remote Media Agent for Linux-Computer hinzu

- 1 Klicken Sie auf der Registerkarte "Speicher" auf "Speicher konfigurieren", und wählen Sie dann "Netzwerkspeicher" aus.
- 2 Klicken Sie auf "Weiter".
- 3 Wählen Sie Backup Exec Remote Media Agent for Linux aus, und klicken Sie dann auf "Weiter".
- 4 Befolgen Sie die Anweisungen auf dem Bildschirm.

Siehe ["Info zum Festlegen des Vertrauens für einen Remote Media Agent for Linux-Computer in der Backup Exec-Liste von Servern "](#) auf Seite 1608.

Hinzufügen zusätzlicher Backup Exec-Server, für die Remote Media Agent for Linux veröffentlichen kann

Sie können zusätzliche Backup Exec-Server angeben, für die Remote Media Agent for Linux Informationen veröffentlichen kann.

Jeder Backup Exec-Server, zu dem Remote Media Agent for Linux Informationen veröffentlicht, wird in der Backup Exec-Liste von Servern angezeigt.

So fügen Sie zusätzliche Backup Exec-Server hinzu, für die Remote Media Agent for Linux Informationen veröffentlichen kann

- 1 Öffnen Sie folgende Datei mit einem Texteditor:

`/etc/VRTSralus/ralus.cfg`

- 2 Fügen Sie die folgenden Zeichenfolge hinzu:

`Software\Symantec\Backup Exec For Windows\Backup
Exec\Engine\Agents\Agent Directory List eindeutige ID = IP-Adresse oder
DNS-Name des Backup Exec-Servers`

- 3 Speichern und schließen Sie die Datei.
- 4 Fügen Sie auf dem Backup Exec-Server, auf dem sich der Remote Media Agent for Linux veröffentlicht, und fügen Sie den Remote Media Agent for Linux-Server der Liste "Server" hinzu.

Siehe ["Serverliste auf der Registerkarte "Backup und Wiederherstellung"](#) auf Seite 166.

Suchen der Dateien der simulierten Bandbibliothek

Vor dem Deinstallieren von Remote Media Agent for Linux sollten Sie den Speicherort der Dateien der simulierten Bandbibliothek notieren. Nachdem Sie Remote Media Agent for Linux deinstalliert haben, können Sie alle Dateien der simulierten Bandbibliothek löschen. Wenn Sie diese Dateien löschen, löschen Sie die Backup-Daten, die Sie auf dem Linux-Server gespeichert haben.

Siehe ["Deinstallieren von Remote Media Agent for Linux "](#) auf Seite 1605.

Siehe ["Tape Library Simulator Utility"](#) auf Seite 1619.

So finden Sie simulierte Bandbibliothek-Dateien

- 1** Loggen als Sie sich als Root auf dem Server ein, auf dem Sie die simulierten Bandbibliothek-Dateien suchen möchten.
- 2** Navigieren Sie zu dem folgenden Verzeichnis, das den Tape Library Simulator enthält:

`/opt/VRTSralus/bin`

Beispiel:

```
cd /opt/VRTSRalus/bin
```

- 3** Starten Sie das mktls -Dienstprogramm, um die simulierten Bandbibliothek-Dateien und -Ordner aufzulisten.

Beispiel:

```
/opt/VRTSralus/bin/mktls -l
```

- 4** Notieren Sie die Speicherorte der simulierten Bandbibliothek-Dateien.

Info zur Backup Exec-Operator-Gruppe (beoper) für Remote Media Agent for Linux

Die Backup Exec-Operatoren (beoper)-Gruppe enthält die Namen der Benutzer, die berechtigt sind, Linux-Server zu sichern und wiederherzustellen.

Wenn Sie den Remote Media Agent for Linux installieren, erstellt Backup Exec die Gruppe "beoper" und fügt "root" als Mitglied hinzu. Jeder Linux-Benutzer, den Sie der beoper-Gruppe hinzufügen, erhält die erforderliche Berechtigung zum Sichern und Wiederherstellen der Linux-Server.

Wenn jedoch ein NIS-Server während der Remote Media Agent-Installation erkannt wird, kann Backup Exec die Gruppe nicht erstellen. Sie müssen die Gruppe auf den Linux-Servern manuell erstellen, auf denen Sie den Remote Media Agent installieren möchten. Sie müssen die Gruppe "beoper" vor dem Starten von Backup- und Wiederherstellungsvorgängen erstellen. Andernfalls schlagen Verbindungen zwischen den Linux-Servern und dem Backup Exec-Server fehl.

Bevor die Mitglieder der Gruppe "beoper" Backup- oder Wiederherstellungsvorgänge durchführen können, müssen sie ein Backup Exec-Login-Konto haben.

Siehe ["Manuelles Erstellen der Backup Exec-Operatorengruppe \(beoper\) für Remote Media Agent for Linux"](#) auf Seite 1611.

Siehe ["Backup Exec-Login-Konten"](#) auf Seite 762.

Manuelles Erstellen der Backup Exec-Operatorengruppe (beoper) für Remote Media Agent for Linux

Wenn die Remote Media Agent for Linux-Installation einen NIS-Server erkennt, müssen Sie auf jedem Linux-Server, auf dem Sie Remote Media Agent for Linux installieren, die Gruppe "beoper" erstellen.

Siehe ["Info zur Backup Exec-Operator-Gruppe \(beoper\) für Remote Media Agent for Linux"](#) auf Seite 1610.

Hinweis: Stellen Sie sicher, dass Sie verstehen, wie Gruppenberechtigungen auf Linux-Servern konfiguriert werden, bevor Sie eine Gruppen-ID für die beoper-Gruppe zuweisen.

Tabelle O-1 Manuelles Erstellen der beoper-Gruppe

Schritt	Aktion	Weitere Informationen
Schritt 1	<p>Navigieren Sie zum Linux-Server, auf dem Sie den Remote Media Agent for Linux installieren möchten.</p> <p>Wenn sich der Linux-Server in einer NIS-Domäne befindet, navigieren Sie zur Gruppendatei der NIS-Domäne.</p>	Weitere Informationen zum Hinfügen einer Gruppe zu einer Gruppendatei einer NIS-Domäne finden Sie in der NIS-Dokumentation.
Schritt 2	<p>Erstellen Sie eine Gruppe mit dem folgenden Namen (Groß- und Kleinschreibung muss beachtet werden):</p> <p>beoper</p>	Weitere Informationen zum Erstellen einer Gruppe finden Sie in der Betriebssystemdokumentation.
Schritt 3	Fügen Sie in der beoper-Gruppe die Benutzer hinzu, die die Berechtigung zum Sichern und Wiederherstellen des Linux-Servers haben sollen.	Weitere Informationen über das Hinzufügen von Benutzern zu einer Gruppe finden Sie in der Dokumentation zum Betriebssystem.
Schritt 4	Erstellen eines Backup Exec-Login-Konto für jeden Benutzer, den Sie der beoper-Gruppe hinzufügen.	Siehe "Erstellen von Backup Exec-Login-Konten" auf Seite 766.

Info zum Hinzufügen eines Linux-Servers als Remote Media Agent for Linux

Nachdem Sie den Linux-Server als einen Remote Media Agent for Linux hinzugefügt haben, und wenn Sie Central Admin Server Feature erworben und installiert haben, können Sie die Speichergeräte, die über den RMAL-Computer mit anderen Backup Exec-Servern verbunden sind, gemeinsam nutzen.

Siehe ["Hinzufügen eines Linux-Servers als Remote Media Agent for Linux"](#) auf Seite 1612.

Siehe ["Freigeben von Speichergeräten"](#) auf Seite 544.

Siehe ["Infos zu Central Admin Server Feature"](#) auf Seite 1450.

Hinzufügen eines Linux-Servers als Remote Media Agent for Linux

Verwenden Sie die folgenden Schritte, um einen Linux-Server als Remote Media Agent for Linux hinzuzufügen.

Siehe ["Info zum Hinzufügen eines Linux-Servers als Remote Media Agent for Linux"](#) auf Seite 1612.

So fügen Sie einen Linux-Server als Remote Media Agent for Linux hinzu

- 1 Klicken Sie auf der Registerkarte "Speicher" auf "Speicher konfigurieren".
- 2 Wählen Sie "Netzwerkspeicher" aus, und klicken auf dann "Weiter".
- 3 Wählen Sie "Backup Exec Remote Media Agent for Linux" aus, und klicken Sie dann auf "Weiter".
- 4 Folgen Sie den Bildschirmanweisungen, um Remote Media Agent for Linux zu vertrauen und die Dienste neu zu starten.

Siehe ["Freigeben von Speichergeräten"](#) auf Seite 544.

Optionen für den Remote Media Agent for Linux

Sie müssen Informationen zur Verfügung stellen, wenn Sie einem Backup Exec-Server einen Linux-Server als Remote Media Agent for Linux hinzufügen.

Siehe ["Info zum Hinzufügen eines Linux-Servers als Remote Media Agent for Linux"](#) auf Seite 1612.

Tabelle O-2 Optionen zum Hinzufügen von Remote Media Agent for Linux

Element	Beschreibung
Servename	<p>Gibt den Namen des Linux-Servers an, der als Remote Media Agent for Linux hinzugefügt werden soll.</p> <p>Ist Backup Exec Central Admin Server Feature in Ihrer Umgebung installiert, müssen Sie den Hostnamen oder den vollständig qualifizierten Domännennamen des Linux-Servers verwenden. D. h.: Verwenden Sie den Namen des Linux-Computers, der angezeigt wird, wenn Sie Backup-Auswahlen suchen. Falls Sie die IP-Adresse verwenden, kann Backup Exec nicht entscheiden, welcher Gerätepfad für die Aufträge zu verwenden ist.</p>
Portnummer	<p>Enthält den Port für Kommunikationen zwischen dem Backup Exec-Server und dem Remote Media Agent for Linux. Falls Sie die Port-Nummer ändern, müssen Sie die services-Datei im Verzeichnis '/etc' auf dem Linux-Server bearbeiten und den NDMP-Eintrag aktualisieren.</p> <p>Siehe "Ändern des Ports für die Kommunikation zwischen Backup Exec-Server und Remote Media Agent for Linux" auf Seite 1614.</p> <p>Stellen Sie sicher, dass dieser Port in allen Firewalls geöffnet ist, die zwischen dem Remote Media Agent for Linux und dem Backup Exec-Server existieren. Verwenden Sie eine Port-Nummer, die von keiner anderen Anwendung und keinem anderen Dienst verwendet wird.</p> <p>Der Standardport ist 10000.</p>
Beschreibung	<p>Zeigt eine Beschreibung an, die Sie auswählen.</p>

Ändern des Ports für die Kommunikation zwischen Backup Exec-Server und Remote Media Agent for Linux

Element	Beschreibung
Login-Konto	<p>Das Login-Login-Konto für den Remote Media Agent for Linux.</p> <p>Standardmäßig wird das System-Login-Konto für den Backup Exec-Server verwendet.</p>
Verwenden der ICMP-Pingvorgänge von Backup Exec zum Erkennen des Servers	<p>Ermöglicht, dass der Backup Exec-Server ICMP-Ping-Vorgänge zum Suchen des Linux-Servers verwendet. In Umgebungen, in denen Ping-Anfragen gesperrt sind, können Sie diese Option deaktivieren.</p> <p>Diese Option ist in der Standardeinstellung aktiviert.</p>
Login-Konto	<p>Gibt das Backup Exec-Login-Konto an, das Sie für die Anmeldung an diesem Server verwenden.</p> <p>Siehe "Backup Exec-Login-Konten" auf Seite 762.</p>

Siehe ["Info zum Erstellen von Speichergerätepools für mit Remote Media Agent for Linux verbundene Geräte"](#) auf Seite 1615.

Siehe ["Info zum Speichern von Daten durch Verwendung des Remote Media Agent for Linux"](#) auf Seite 1618.

Ändern des Ports für die Kommunikation zwischen Backup Exec-Server und Remote Media Agent for Linux

Sie können den Port ändern, den Backup Exec verwendet, um mit dem Remote Media Agent for Linux zu kommunizieren.

So ändern Sie den Port für die Kommunikation zwischen Backup Exec-Server und Remote Media Agent for Linux

- 1 Verwenden Sie auf dem Computer, auf dem der Remote Media Agent for Linux installiert ist, einen Texteditor, um die Datei "services" im Verzeichnis "/etc" zu öffnen.

Beispiel:

```
vi /etc/services
```

- 2 Durchsuchen Sie die Datei nach einem Eintrag, der dem folgenden ähnlich ist:
ndmp 10000/tcp
- 3 Sie haben folgende Möglichkeiten:

Wenn dieser Eintrag existiert:

Ersetzen Sie die Port-Nummer durch die Port-Nummer, die Sie verwenden möchten.

Wenn dieser Eintrag nicht existiert:

Gehen Sie dazu wie folgt vor:

- Geben Sie am Ende der Datei `ndmp` ein und drücken Sie danach die "Tabulator" -Taste.
- Geben Sie die Port-Nummer, die NDMP verwenden soll, ein, und geben Sie dann `/tcp` ein.
- Drücken Sie die Eingabetaste.

- 4 Speichern Sie die Datei und schließen Sie dann den Editor.
- 5 Starten Sie Agent für Linux-Daemon neu.

Siehe ["Starten des Remote Media Agent für Linux-Daemon"](#) auf Seite 1607.

Info zum Erstellen von Speichergerätepools für mit Remote Media Agent for Linux verbundene Geräte

Remote Media Agents können sich an verschiedenen physischen Standorten befinden. Um den Netzwerkverkehr zu reduzieren und die Arbeitsleistung zu erhöhen, erstellen Sie separate Speichergerätepools für Remote Media Agents an verschiedenen Standorten.

Siehe ["Erstellen von Speichergerätepools"](#) auf Seite 512.

Siehe ["Tape Library Simulator Utility"](#) auf Seite 1619.

Bearbeiten der Eigenschaften von Remote Media Agent for Linux

Sie können die Eigenschaften eines Remote Media Agent for Linux bearbeiten.

So bearbeiten Sie die Eigenschaften von Remote Media Agent for Linux

- 1 Auf der Registerkarte "Speicher" klicken Sie mit der rechten Maustaste auf einen Remote Media Agent for Linux-Server.
- 2 Klicken Sie auf "Details".

Siehe ["Eigenschaften von Remote Media Agent for Linux"](#) auf Seite 1616.

Eigenschaften von Remote Media Agent for Linux

Sie können die Eigenschaften für einen Remote Media Agent for Linux-Server anzeigen und bearbeiten.

Siehe ["Bearbeiten der Eigenschaften von Remote Media Agent for Linux "](#) auf Seite 1616.

In der folgenden Tabelle sind die Eigenschaften von Remote Media Agent for Linux-Servern aufgeführt:

Tabelle O-3 Eigenschaften von Remote Media Agent for Linux

Element	Beschreibung
Name	Der Name, die IP-Adresse oder der vollständig qualifizierte Domänenname des Remote Media Agent for Linux.
Port	Der Port, der für Kommunikationen zwischen dem Backup Exec-Server und Remote Media Agent for Linux verwendet wird.
Backup Exec-Serverstatus	Zeigt den Status des Backup Exec-Servers an. Backup Exec-Serverstatus sind u.a. "Online", "Anhalten", "Nicht verfügbar" und "Offline".
Beschreibung	Eine Beschreibung des Remote Media Agent for Linuxs. Sie können diese Beschreibung bearbeiten.

Element	Beschreibung
ICMP-Pingoperationen zum Erkennen des Remote Media Agent durch Backup Exec aktivieren	<p>Ermöglicht, dass Backup Exec mit dem Remote Media Agent for Linux kommuniziert. In Umgebungen, in denen Ping-Anfragen gesperrt sind, können Sie diese Option deaktivieren.</p> <p>Diese Option ist in der Standardeinstellung aktiviert.</p>
Host-ID	Die Kennnummer, die Remote Media Agent for Linux generiert.
Systemversion	Die Version des Betriebssystems, das auf dem Remote Media Agent ausgeführt wird.
Login-Konto	Das Login-Konto für den Remote Media Agent for Linux. Klicken Sie auf "Ändern", um ein anderes Einlogkonto auszuwählen oder zu erstellen.

Löschen eines Remote Media Agent for Linux aus der Backup Exec-Liste von Servern

So löschen Sie einen Remote Media Agent for Linux aus der Backup Exec-Liste der Server

So löschen Sie einen Remote Media Agent for Linux aus Backup Exec

- 1 Auf der Registerkarte "Speicher" klicken Sie mit der rechten Maustaste auf einen Remote Media Agent for Linux.
- 2 Klicken Sie auf "Löschen".
- 3 Klicken Sie auf Ja.

Siehe ["Festlegen von Vertrauen und Hinzufügen eines Remote Media Agent for Linux-Computer zur Backup Exec-Liste von Servern"](#) auf Seite 1608.

Gemeinsames Nutzen eines Remote Media Agent for Linux von mehreren Backup Exec-Servern

Wenn das Central Admin Server Feature installiert ist, können Sie Backup Exec-Server auswählen, die einen Remote Media Agent for Linux-Server gemeinsam nutzen sollen. Wenn Sie einen Remote Media Agent for Linux-Server hinzufügen,

wird der Backup Exec-Server, dem Sie verwendeten, um das Gerät hinzuzufügen, automatisch für das gemeinsame Nutzen ausgewählt.

Siehe ["Freigeben von Speichergeräten"](#) auf Seite 544.

So nutzen mehrere Backup Exec-Server einen Remote Media Agent for Linux gemeinsam

- 1 Auf der Registerkarte "Speicher" unter "Gesamter Speicher" klicken Sie mit der rechten Maustaste auf einen Remote Media Agent for Linux-Server, auf den der Backup Exec-Server zugreifen soll.
- 2 Wählen Sie "Freigabe" aus.
- 3 Unter "Server" wählen Sie die Backup Exec-Server aus, die Sie mit Remote Media Agent for Linux verwenden möchten.
- 4 Klicken Sie auf "OK".
- 5 Starten Sie die Backup Exec-Dienste auf den in Schritt 3 gewählten Backup Exec-Servern neu.

Siehe ["Starten und Anhalten von Backup Exec-Diensten"](#) auf Seite 776.

Info zum Speichern von Daten durch Verwendung des Remote Media Agent for Linux

Erstellen Sie einen Backup-Auftrag für Remote Media Agent for Linux auf dem Backup Exec-Server.

Siehe ["Sichern von Daten"](#) auf Seite 174.

Siehe ["Bearbeiten von Backup-Definitionen"](#) auf Seite 226.

Siehe ["Hinzufügen einer Stufe zu einer Backup-Definition"](#) auf Seite 244.

Info zum Wiederherstellen von Daten mit Remote Media Agent for Linux

Erstellen Sie einen Wiederherstellungsaufträge für Remote Media Agent for Linux auf dem Backup Exec-Server.

Hinweis: Verwenden Sie Geräte, die mit dem Backup Exec-Server verbunden sind, um Daten wiederherzustellen, die sich auf den durch andere Anwendungen erstellten Bändern befinden. Remote Media Agent for Linux unterstützt nur das Microsoft-Bandformat (MTF).

Siehe ["Methoden für das Wiederherstellen von Daten in Backup Exec"](#) auf Seite 258.

Tape Library Simulator Utility

Durch Tape Library Simulator Utility können Sie ein virtuelles Gerät auf einer Festplatte oder auf einem bereitgestellten Datenträger auf einem Linux-Server erstellen. Dieses virtuelle Gerät emuliert eine SCSI-Bandbibliothek. Remote Media Agent for Linux muss auf dem Server installiert sein.

Wenn Sie Tape Library Simulator Utility ausführen, werden Sie zur Angabe folgender Information aufgefordert:

- Die Anzahl der Schächte, die Sie dieser Bibliothek zuordnen möchten.
- Den Speicherort oder Pfad für die Bibliothek.

Tape Library Simulator Utility erstellt dann die Medien für die simulierte Bandbibliothek. Um sicherzustellen, dass jedes Medien einen eindeutigen Namen aufweist, erstellt Tape Library Simulator Utility eine Barcode-Bezeichnung für jedes Medium. Sie können diese Barcode-Kennungen nicht umbenennen. Jedoch können Sie eine eindeutige Medienbeschreibung hinzufügen.

Die simulierte Bandbibliothek emuliert einen Advanced Intelligent Tape (AIT)-Medientyp. Dieser Medientyp wird selten verwendet, sodass Sie einfach zwischen einem physischen Wechsler und einer simulierten Bandbibliothek unterscheiden können. Die simulierten Medien verfügen auch über eine AIT-Medienkennung.

Das Format der Dateien, die auf die simulierte Bandbibliothek geschrieben werden, ist dem Dateiformat von Backup-to-Disk-Dateien ähnlich. Jedoch können Sie Dateien nicht zwischen simulierten Bandbibliotheken und Backup-to-Disk-Ordern kopieren oder verschieben.

Sie können die simulierte Bandbibliothek Backup Exec-Gerätepools hinzufügen.

Siehe ["Erstellen von Speichergerätepools"](#) auf Seite 512.

Um Tape Library Simulator Utility zu verwenden, müssen Sie über mindestens 500 MB verfügbaren Speicherplatz auf dem Linux-Server verfügen. Der verfügbare Speicherplatz umfasst Festplattenspeicher, Flash-Laufwerke und USB-Laufwerke. Wenn nicht ausreichend Speicherplatz vorhanden ist, schlagen die Aufträge mit einem Fehler zum Ende der Medien fehl. Stellen Sie entweder ausreichend Speicherplatz zur Verfügung oder leiten Sie die Aufträge an einen anderen Datenträger weiter und starten Sie die Aufträge anschließend erneut.

Eine simulierte Bandbibliothek unterstützt nicht alle Aufgaben, die für physische Wechsler verfügbar sind.

Hinweis: Ein schnelles Katalogisieren von Bändern, die untrennbar geworden sind, ist nicht möglich. Backup Exec kehrt automatisch wieder zur langsamen Katalogisierung zurück. Sinngemäß wird folgende Meldung in das Auftragsprotokoll des Katalogs geschrieben:

"Beim Versuch, die Satzzuordnungsdaten des mediengestützten Katalogs zu lesen ist ein Fehler aufgetreten. Es wird versucht, die Medien durch Lesen des Datenbereichs jedes Backup-Satzes zu katalogisieren."

Dieses Problem tritt auf, da am Ende eines Backup-Auftrags ein unvollständiger Bandkatalog auf das Band geschrieben wird. Dies führt dazu, dass darauf folgende Backup-Aufträge die Satzzuordnung des Bands nicht finden können und das Band als nicht lesbar ausweisen.

Siehe ["Info zu Speicheraufträgen"](#) auf Seite 519.

Siehe ["Erstellen einer simulierten Bandbibliothek"](#) auf Seite 1620.

Erstellen einer simulierten Bandbibliothek

Erstellen Sie eine simulierte Bandbibliothek auf einem Server, auf dem Remote Media Agent for Linux installiert ist. Sie müssen die simulierte Bandbibliothek auf einer Festplatte oder einem bereitgestellten Datenträger erstellen.

Siehe ["Tape Library Simulator Utility"](#) auf Seite 1619.

So erstellen Sie eine simulierte Bandbibliothek

- 1 Beenden Sie auf dem Remote Media Agent for Linux-Computer den Agent for Linux-Dämon.

Siehe ["Beenden des Agent for Linux-Daemon"](#) auf Seite 1590.

- 2 Navigieren Sie zum folgenden Pfad, der Tape Library Simulator Utility enthält:

</opt/VRTSralus/bin>

Beispiel:

```
cd /opt/VRTSralus/bin
```

- 3 Starten Sie das mktls -Dienstprogramm.

Beispiel:

```
./mktls
```

- 4 Wählen Sie "Eine neue simulierte Bandbibliothek erstellen" und drücken Sie die Eingabetaste.

- 5 Geben Sie die betreffenden Informationen ein.
 Siehe ["Optionen für simulierte Bandbibliotheken"](#) auf Seite 1621.
- 6 Schließen Sie das Dienstprogramm.
- 7 Starten Sie den Agent for Linux-Daemon neu.
 Siehe ["Starten des Agent for Linux-Daemon"](#) auf Seite 1589.
- 8 Auf dem Backup Exec-Server starten Sie die Backup Exec-Dienste neu.
 Siehe ["Starten und Anhalten von Backup Exec-Diensten"](#) auf Seite 776.

Optionen für simulierte Bandbibliotheken

Wenn Sie eine simulierte Bandbibliothek erstellen, müssen Sie einen Verzeichnispfad und die Anzahl der Schächte angeben.

Siehe ["Erstellen einer simulierten Bandbibliothek"](#) auf Seite 1620.

Tabelle O-4 Optionen für simulierte Bandbibliotheken

Element	Beschreibung
Verzeichnispfad	Geben Sie den Pfad des Verzeichnisses für die simulierte Bandbibliothek ein. Sie können bis zu 512 Zeichen eingeben. Wenn der Pfad nicht existiert, stellt Tape Library Simulator Utility ihn her.
Anzahl der Schächte	Wählen Sie die Anzahl der Schächte für diese simulierte Bandbibliothek aus. Die Anzahl der Schächte kann von 1 bis 50 reichen. Die Standardanzahl ist 20.

Siehe ["Anzeigen der Eigenschaften von simulierten Bandbibliotheken"](#) auf Seite 1621.

Anzeigen der Eigenschaften von simulierten Bandbibliotheken

Sie können Veritas Tape Library Simulator Utility verwenden, um Informationen über die simulierte Bandbibliothek und ihren Inhalt anzuzeigen.

So zeigen Sie Eigenschaften von simulierten Bandbibliotheken an

- 1 Beenden Sie auf dem Remote Media Agent for Linux-Computer den Agent for Linux-Dämon.

Siehe ["Beenden des Agent for Linux-Daemon"](#) auf Seite 1590.
- 2 Navigieren Sie zu dem folgenden Verzeichnis, das Tape Library Simulator Utility enthält:

/opt/VRTSralus/bin

Beispiel:


```
cd /opt/VRTSralus/bin
```
- 3 Starten Sie das mktls -Dienstprogramm.

Beispiel:


```
./mktls
```
- 4 Wählen Sie "Eine existierende simulierte Bandbibliothek anzeigen".
- 5 Bewegen Sie den Mauszeiger auf die simulierte Bandbibliothek, die Sie anzeigen möchten, und drücken Sie die Eingabetaste.
- 6 Drücken Sie die Eingabetaste erneut, um die Eigenschaften der simulierten Bandbibliothek anzuzeigen.

Siehe ["Eigenschaften von simulierten Bandbibliotheken"](#) auf Seite 1622.
- 7 Geben Sie Q ein, um das Dienstprogramm zu schließen.
- 8 Starten Sie den Agent for Linux-Daemon neu.

Siehe ["Starten des Agent for Linux-Daemon"](#) auf Seite 1589.

Eigenschaften von simulierten Bandbibliotheken

Sie können die Eigenschaften einer simulierten Bandbibliothek anzeigen.

Tabelle O-5 Simulierte Bandbibliothek-Eigenschaften

Element	Beschreibung
Anzahl der Laufwerke	Zeigt die Anzahl der Laufwerke für diese simulierte Bandbibliothek an. Eine simulierte Bandbibliothek kann nur ein Laufwerk haben. Dieses Laufwerk ist nicht konfigurierbar.

Element	Beschreibung
Anzahl der Schächte	Gibt die Anzahl der Schächte für diese simulierte Bandbibliothek an. Die Anzahl der Schächte kann von 1 bis 50 reichen. Die Standardanzahl ist 20.
Bandkapazität	Zeigt die Bandkapazität an. Die Standardkapazität ist 100 Gigabyte.
Verzeichnispfad	Zeigt den Verzeichnispfad der simulierten Bandbibliothek an.

Löschen einer simulierten Bandbibliothek

Sie können Tape Library Simulator Utility verwenden, um eine simulierte Bandbibliothek zu löschen. Sie müssen den Inhalt der simulierten Bandbibliothek-Dateien und die Verzeichnisse, die diese Dateien enthalten, manuell löschen.

So löschen Sie eine simulierte Bandbibliothek:

- 1 Beenden Sie auf dem Remote Media Agent for Linux-Computer den Agent for Linux-Dämon.

Siehe ["Beenden des Agent for Linux-Daemon"](#) auf Seite 1590.

- 2 Navigieren Sie zu dem folgenden Verzeichnis, das den Tape Library Simulator enthält:

`/opt/VRTSralus/bin/`

Beispiel:

```
cd /opt/VRTSralus/bin/
```

- 3 Starten Sie das mktls -Dienstprogramm.

Beispiel:

```
./mktls
```

- 4 Wählen Sie "Eine existierende simulierte Bandbibliothek anzeigen".
- 5 Wählen Sie die simulierte Bandbibliothek aus, die Sie löschen möchten.
- 6 Wenn Sie gefragt werden, löschen Sie die simulierte Bandbibliothek.
- 7 Schließen Sie das Dienstprogramm.
- 8 Starten Sie den Agent for Linux-Daemon neu.

Siehe ["Starten des Agent for Linux-Daemon"](#) auf Seite 1589.

- 9 Suchen Sie die Dateien der simulierten Bandbibliothek und löschen Sie sie manuell.

Siehe ["Tape Library Simulator Utility"](#) auf Seite 1619.

- 10 Starten Sie gegebenenfalls auf dem Backup Exec-Server die Backup Exec-Dienste erneut.

Siehe ["Starten und Anhalten von Backup Exec-Diensten"](#) auf Seite 776.

Verwalten simulierter Bandbibliotheken über die Befehlszeile

Sie können mithilfe der Befehlszeile eine simulierte Bandbibliothek erstellen. Erstellen Sie eine simulierte Bandbibliothek auf einer Festplatte oder auf einem beliebigen bereitgestellten Datenträger auf dem Remote Media Agent for Linux-Computer. Mithilfe der Befehlszeile können Sie simulierte Bandbibliotheken auch löschen.

So verwalten Sie simulierte Bandbibliotheken über die Befehlszeile

- 1 Beenden Sie auf dem Remote Media Agent for Linux-Computer den Agent for Linux-Dämon.

Siehe ["Beenden des Agent for Linux-Daemon"](#) auf Seite 1590.

- 2 Navigieren Sie zu dem folgenden Verzeichnis, das Tape Library Simulator Utility enthält:

`/opt/VRTSralus/bin`

Beispiel:

```
cd /opt/VRTSralus/bin
```

- 3 Starten Sie das mktls -Dienstprogramm mit den geeigneten Parametern.

Siehe ["Befehlszeilen-Switches für das Tape Library Simulator-Dienstprogramm"](#) auf Seite 1625.

- 4 Starten Sie den Agent for Linux-Daemon.

Siehe ["Starten des Agent for Linux-Daemon"](#) auf Seite 1589.

Befehlszeilen-Switches für das Tape Library Simulator-Dienstprogramm

Sie können Befehlszeilenparameter benutzen, um simulierte Bandbibliotheken zu verwalten. Beispielsweise stellt die folgende Befehlszeile eine simulierte Bandbibliothek mit 10 Schächten her, die sich bei /TLS2/Testing befindet.

```
./mktls -s10 -p/TLS2/Testing
```

Siehe ["Verwalten simulierter Bandbibliotheken über die Befehlszeile"](#) auf Seite 1624.

Tabelle O-6 Befehlszeilenparameter für Tape Library Simulator Utility

Parameter	Beschreibung
-p<Pfad>	Gibt den Verzeichnispfad für die simulierte Bandbibliothek an. Wenn der Pfad nicht existiert, erstellt ihn das Dienstprogramm. Die maximale Pfadgröße beträgt 512 Zeichen.
-s<Anzahl Schächte>	Gibt die Anzahl der Schächte für diese simulierte Bandbibliothek an. Die Anzahl der Schächte kann von 1 bis 50 reichen. Die Standardanzahl ist 20.
-r	Verhindert das Anzeigen der Informationen.
-l	Enthält die simulierten Bandbibliotheken für Remote Media Agent for Linux
-d -p<Pfad>	Gibt den Pfad der simulierten Bandbibliothek an, die Sie löschen möchten.
-h	Zeigt die Online-Hilfe an.

Fehlerbehebung in Remote Media Agent for Linux

Wenn Probleme mit Remote Media Agent for Linux auftreten, lesen Sie die folgenden Fragen und Antworten.

Tabelle O-7 Fehlerbehebung für den RMAL

Frage	Antwort
Remote Media Agent for Linux erkennt das angeschlossene Gerät nicht. Was kann ich tun?	<p>Stellen Sie zunächst sicher, dass die Backup Exec und Remote Media Agent for Linux das Gerät unterstützen.</p> <p>Die unterstützten Geräte finden Sie in der Liste der mit Backup Exec kompatiblen Hardware.</p> <p>Stellen Sie für auf der Hardware-Kompatibilitätsliste aufgeführte Geräte Folgendes sicher:</p> <ul style="list-style-type: none"> ■ Das Betriebssystem erkennt das Gerät. ■ Das Gerät wird in <code>"/proc/scsi/scsi"</code> aufgeführt. <p>Wenn das Betriebssystem das Gerät erkennen kann, müssen Sie sicherstellen, dass das Gerät in <code>"/etc/VRTSralus/TILDBG.TXT"</code> aufgeführt ist.</p>
Mein Backup Exec-Server zeigt die Geräte nicht an, die mit Remote Media Agent verbunden sind. Was kann ich tun?	<p>Führen Sie die folgenden Verfahren durch:</p> <ul style="list-style-type: none"> ■ Stellen Sie sicher, dass der Agent for Linux-Daemon läuft. Wenn er nicht ausgeführt wird, müssen Sie den Daemon starten, die Stromversorgung des Servers sicherstellen und den korrekten Anschluss aller Kabel überprüfen. ■ Stellen Sie sicher, dass in den Eigenschaften von Remote Media Agent der korrekte Port eingestellt ist und dass ICMP-Ping-Vorgänge aktiviert sind. ■ Stellen Sie sicher, dass die Backup Exec-Dienste nach dem Hinzufügen eines Remote Media Agent zum Backup Exec-Server neu gestartet werden. Die verfügbaren Geräte sollten unter dem Knoten "Remote Media Agent for Linux" angezeigt werden. <p>Siehe "Bearbeiten der Eigenschaften von Remote Media Agent for Linux" auf Seite 1616.</p> <p>Siehe "Starten des Agent for Linux-Daemon" auf Seite 1589.</p>
Warum werden meine standortfernen Geräte in den Speichergerätepools, die von Backup Exec erstellt wurden, nicht angezeigt?	<p>Standardmäßig schließt Backup Exec standortferne Geräte nicht in die Speichergerätepools ein, die es erstellt. Es wird empfohlen, einen separaten Speichergerätepool für Geräte zu erstellen, die mit jedem Remote Media Agent verbunden sind.</p> <p>Siehe "Info zum Erstellen von Speichergerätepools für mit Remote Media Agent for Linux verbundene Geräte" auf Seite 1615.</p>

Frage	Antwort
<p>Remote Media Agent for Linux wird nicht auf dem Remote-Computer ausgeführt. Was kann ich tun?</p>	<p>Stellen Sie sicher, dass der Remote Media Agent for Linux unter einer unterstützten Version von Linux installiert wird.</p> <p>Die unterstützten Betriebssysteme, Plattformen und Anwendungen finden Sie in der Liste der mit Backup Exec kompatiblen Software.</p> <p>Wenn Sie Remote Media Agent for Linux unter einer nicht unterstützten Version von Linux installieren, ist der Agent nicht verfügbar. Sie können die Aufträge, die auf den an den Linux-Server angeschlossenen Geräten ausgeführt werden, nicht erstellen. Jedoch können Sie den Linux-Server sichern, indem Sie die Komponente Agent for Linux-Komponente verwenden. Diese Komponente wird mit Remote Media Agent for Linux installiert.</p> <p>Gehen Sie wie folgt vor, um den Linux-Server mithilfe der Agent for Linux-Komponente zu sichern:</p> <ul style="list-style-type: none"> ■ Bearbeiten Sie die Datei "ralus.cfg". ■ Ändern Sie den Wert in der folgenden Zeichenfolge von 0 in 1: Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\RMAL\DisableRMAL=0. Siehe "Bearbeiten von Konfigurationsoptionen für Linux-Computer" auf Seite 1570. <p>Siehe "Ausführen des begather-Dienstprogramms, um Fehler bei Backup Exec-Komponenten auf Linux-Servern zu beheben" auf Seite 909.</p>
<p>Ich kann Remote Media Agent for Linux nicht laden. Wenn ich versuche, den Remote Media Agent for Linux im Konsolenmodus zu laden, zeigt "beremote --log-console" die folgende Meldung an:</p> <p>Fehler beim Laden gemeinsam genutzter Bibliotheken: libstdc++.so.5: Gemeinsam genutzte Objektdatei kann nicht geöffnet werden: Datei oder Verzeichnis nicht vorhanden.</p> <p>Was kann ich tun?</p>	<p>Dieser Fehler wird angezeigt, wenn sich die Bibliothek "libstdc++.so.5" nicht im /usr/lib-Verzeichnis befindet. Diese Bibliothek ist erforderlich, um den Remote Media Agent for Linux starten und ausführen zu können. Um dieses Problem zu lösen, installieren Sie das Paket "libstdc++.so.5". Sie können dieses Paket von dem Datenträger installieren, auf dem Ihre Linux-Kopie Ihnen zur Verfügung gestellt wurde. Alternativ können Sie den folgenden Befehl von einem Computer mit Internetzugang aus ausführen:</p> <pre>apt-get install libstdc++5</pre> <p>Führen Sie bei SUSE Linux Enterprise Server 11 den folgenden Befehl aus:</p> <pre>zypper install libstdc++5</pre>

Eingabehilfen und Backup Exec

Dieser Anhang enthält folgende Themen:

- [Info zu Eingabehilfen und Backup Exec](#)
- [Informationen zu Tastaturkurzbefehlen in Backup Exec](#)
- [Listenfeldnavigation in Backup Exec](#)
- [Navigation in Dialogfeldern mit Registerkarten in Backup Exec](#)
- [Festlegen der Optionen zur Eingabehilfe](#)

Info zu Eingabehilfen und Backup Exec

Backup Exec erfüllen die Anforderungen in Bezug auf Eingabehilfen für Software, die in Abschnitt 508 des Rehabilitation Act (USA) definiert werden:

<http://www.access-board.gov/508.htm>

Backup Exec mit den Einstellungen für Eingabehilfen des Betriebssystems und einer Reihe von unterstützenden Programmen kompatibel. Alle Handbücher stehen als PDF-Dateien zur Verfügung. Die Online-Hilfe kann als HTML in einem entsprechenden Browser angezeigt werden.

Tastaturnavigation ist für alle Vorgänge und Menüelemente der grafischen Benutzeroberfläche verfügbar. Backup Exec verwendet Standardnavigationsschlüssel von Betriebssystemen.

Auf Elemente der Taskleiste, denen keine Tastaturkurzbefehle zugewiesen sind, kann mithilfe der "Maustasten" des Betriebssystems zugegriffen werden. Diese Tastenkombinationen ermöglichen die Steuerung der Maus über die Tastatur.

Um eine Tabelle der Standardnavigationstasten und Tastaturkurzbefehle von Microsoft anzuzeigen, wählen Sie Ihre Version von Microsoft Windows aus der Tabelle auf der folgenden Seite aus:

<http://www.microsoft.com/enable/products/keyboard.aspx>

Informationen zu Tastaturkurzbefehlen in Backup Exec

Alle Menüelemente können über Zugriffstasten oder Tastaturkurzbefehle ausgewählt werden. Eine Zugriffstaste ist eine Tastenkombination, die einen Schnellaufgriff auf eine Funktion der Benutzeroberfläche bietet. Eine Zugriffstaste (auch als "Hotkey" bezeichnet) ist eine Taste, die zusammen mit der Alt -Taste zur Auswahl von Komponenten der Benutzeroberfläche wie beispielsweise Menüeinträgen verwendet wird. Der Buchstabe für den Hotkey ist am Element in der Benutzeroberfläche markiert.

Zur Auswahl sekundärer Menüelemente öffnen Sie das Hauptmenü und verwenden die Nach-oben- oder die Nach-unten-Taste, bis das gewünschte Element markiert ist. Drücken Sie die Nach-rechts-Taste, um ein Untermenü zu öffnen, und danach die Eingabetaste, um eine Auswahl zu treffen.

Groß- und Kleinschreibung spielt bei Tastaturkurzbefehlen keine Rolle. Hotkey-Tastenkombinationen können entweder nacheinander oder gleichzeitig gedrückt werden. Jedes Menüelement hat einen Hotkey, es stehen jedoch nicht für alle Menüelemente Zugriffstasten zur Verfügung.

Routinefunktionen, wie beispielsweise das Öffnen, Speichern und Drucken von Dateien, können mithilfe der standardmäßigen Tastaturkurzbefehle von Windows durchgeführt werden. Andere Menüelemente sind spezifisch für Backup Exec.

Die folgende Tabelle zeigt die Tastaturkurzbefehle für die Anzeige der Bezeichnungen und des Inhalts der Backup Exec-Schaltfläche:

Tabelle P-1 Tastaturkurzbefehle in Backup Exec

Zugriffstasten	Hotkey	Ergebnis
Alt	F10	Zeigt die Bezeichnung für eine Registerkarte an. Verwenden Sie dies in Verbindung mit der jeweiligen Zugriffstaste, um die Registerkarte zu öffnen.

Zugriffstasten	Hotkey	Ergebnis
Alt	A	Erweitert die Backup Exec-Schaltfläche. Verwenden Sie die Backup Exec-Schaltfläche, um eine Verbindung zum Backup Exec-Server herzustellen, Einstellungen zu konfigurieren und auf Informationen zu Installation und Lizenzierung zuzugreifen. Sie können außerdem auf Backup Exec-Dokumentation und den technischen Support zugreifen.

Siehe ["Tastaturkurzbefehle der Registerkarte "Startseite" auf Seite 1630.](#)

Siehe ["Tastaturkurzbefehle für die Registerkarte "Backup und Wiederherstellung" auf Seite 1631.](#)

Siehe ["Tastenkombinationen auf der Registerkarte "Auftragsüberwachung" auf Seite 1640.](#)

Siehe ["Tastaturkurzbefehle der Registerkarte "Speicher" auf Seite 1644.](#)

Siehe ["Tastaturkurzbefehle der Registerkarte "Berichte" auf Seite 1653.](#)

Tastaturkurzbefehle der Registerkarte "Startseite"

Die folgende Tabelle enthält die Tastaturkurzbefehle für die Registerkarte "Startseite".

Siehe ["Informationen zu Tastaturkurzbefehlen in Backup Exec" auf Seite 1629.](#)

Tabelle P-2 Tastaturkurzbefehle der Registerkarte "Startseite"

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	H	Registerkarte "Startseite"	Öffnet die Registerkarte "Startseite".
Alt	1	Eine Spalte	Zeigt die Elemente der Registerkarte "Startseite" in einer Spalte an.
Alt	2	Zwei Spalten	Zeigt die Elemente der Registerkarte "Startseite" in zwei Spalten an.
Alt	NW	Schmal/Breit	Zeigt die Elemente der Registerkarte "Startseite" in zwei Spalten mit einem schmalen und einem breiten Bereich an.

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	3	Drei Spalten	Zeigt die Elemente der Registerkarte "Startseite" in drei Spalten an.
Alt	D	Rücksetzen der Registerkarte "Startseite"	Stellt die Standardkonfiguration für die Inhalte der Registerkarte "Startseite" wieder her.

Tastaturkurzbefehle für die Registerkarte "Backup und Wiederherstellung"

In der folgenden Tabelle sind die Tastaturkurzbefehle für die Registerkarte "Backup und Wiederherstellung" aufgeführt.

Siehe ["Informationen zu Tastaturkurzbefehlen in Backup Exec"](#) auf Seite 1629.

Siehe ["Tastaturkurzbefehle der Registerkarte "Backup und Wiederherstellung" für die Auftragsansicht"](#) auf Seite 1634.

Siehe ["Tastaturkurzbefehle der Registerkarte "Backup und Wiederherstellung" für die Auftragsverlaufsansicht "](#) auf Seite 1635.

Siehe ["Tastaturkurzbefehle der Registerkarte "Backup und Wiederherstellung" für die Backup-Satz-Ansicht "](#) auf Seite 1637.

Siehe ["Tastaturkurzbefehle der Registerkarte "Backup und Wiederherstellung" für die Ansicht der aktiven Warnmeldungen "](#) auf Seite 1638.

Siehe ["Tastaturkurzbefehle der Registerkarte "Backup und Wiederherstellung" für die Anmeldedatenansicht "](#) auf Seite 1639.

Tabelle P-3 Tastaturkurzbefehle für die Registerkarte "Backup und Wiederherstellung"

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	B	Registerkarte "Backup und Wiederherstellung"	Öffnet die Registerkarte "Backup und Wiederherstellung".
Alt	ST	Standard	Zeigt Backup Exec in einer Ansicht an, die beschreibenden Text bereitstellt.
Alt	CO	Kompakt	Zeigt Backup Exec in einer platzsparenden Ansicht an.

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	F	Sortieren und Filtern	Zeigt Informationen in einer benutzerspezifischen Ansicht an oder ermöglicht Ihnen das Erstellen und Sichern einer benutzerspezifischen Ansicht.
Alt	V	Verzeichnisstruktur	Zeigt Elemente in einer hierarchischen Ansicht an. Dieser Befehl ist auf der Registerkarte "Backup und Wiederherstellung" für die Liste von Servern deaktiviert.
Alt	L	Liste	Zeigt Elemente in einer Liste an, die Sie nach Spalten sortieren können. Dieser Befehl ist auf der Registerkarte "Backup und Wiederherstellung" für die Liste von Servern deaktiviert.
Alt	G	Gruppen	Ermöglicht die Anzeige von Informationen nach Servergruppen. Sie können Servergruppen hinzufügen, entfernen oder bearbeiten.
Alt	B	Backup	Definiert Backup-Aufträge und Einstellungen für die Sicherung Ihrer Daten. Sie können Daten sofort sichern oder einen Zeitpunkt planen.
Alt	E	Einmaliges Backup	Definiert Backup-Aufträge und Einstellungen für eine einmalige Ausführung.
Alt	EB	Backups bearbeiten	Ermöglicht das Bearbeiten eines oder mehrerer vorhandener Backup-Aufträge. Sie können keine synthetischen oder einmalige Backups bearbeiten.

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	CA	Backup-Kalender	Ermöglicht die Anzeige aller Aufträge des geplanten Backup auf einem Kalender.
Alt	RE	Wiederherstellung	Durchsucht die Backup-Sätze von einem einzelnen Server und stellt dann die Daten wieder her.
Alt	SE	Suchen	Sucht nach Backup-Sätzen und stellt dann die Daten wieder her oder kopiert und speichert die Suchkriterien.
Alt	DR	SDR-Datenträger erstellen	Starten Sie den Assistenten zum Erstellen von SDR-Datenträgern, der Ihnen bei der Erstellung eines Wiederherstellungsdatenträgers hilft.
Alt	G	In virtuell konvertieren	Konvertiert Backup-Daten auf einem virtuellen Computer. Sie müssen ein vollständiges Backup ausführen, das alle kritischen Systemkomponenten umfasst, bevor Sie Backup-Daten auf einem virtuellen Computer konvertieren können.
Alt	AS	Hinzufügen	Fügt der Liste von Servern einen oder mehrere Server hinzu. Sie müssen Server hinzufügen, um sie sichern und überwachen zu können.
Alt	RS	Entfernen	Entfernt eine oder mehrere Server von der Liste von Servern. Sie können Server von der Liste entfernen, wenn Sie diese nicht mehr unterstützen möchten.

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	US	Aktualisieren	Aktualisiert die ausgewählten Backup Exec-Server mit den neuesten Hotfixes und Wartungs-Packs.
Alt	HA	Auftragswarteschlange anhalten	Hält die Auftragswarteschlange an. Aktive Aufträge werden weiter ausgeführt, neue Aufträge werden aber erst wieder gestartet, wenn die Pause für die Warteschlange aufgehoben wird.
Alt	RN	Nächstes Backup jetzt ausführen	Führt das nächste geplante Backup für die ausgewählten Server aus.

Tastaturkurzbefehle der Registerkarte "Backup und Wiederherstellung" für die Auftragsansicht

Die folgende Tabelle listet die Tastaturkurzbefehle der Registerkarte "Backup und Wiederherstellung" für die Auftragsansicht auf.

Siehe ["Tastaturkurzbefehle für die Registerkarte "Backup und Wiederherstellung""](#) auf Seite 1631.

Tabelle P-4 Tastaturkurzbefehle der Registerkarte "Backup und Wiederherstellung" für die Auftragsansicht

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	JE	Bearbeiten	Ermöglicht die Bearbeitung einer Backup-Definition. Sie können die Backup-Auswahlen, die Backup-Einstellungen und die Zustände einer Backup-Definition bearbeiten.
Alt	JD	Löschen	Löscht eine Backup-Definition, wenn Sie diese nicht mehr benötigen.
Alt	JC	Abbrechen	Bricht einen aktiven Auftrag während der Ausführung ab.

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	JP	Priorität	Erhöht oder senkt die Priorität eines Auftrags in der Auftragswarteschlange.
Alt	JR	Jetzt ausführen	Führt einen Auftrag sofort aus. Wenn ein Auftrag geplant ist, wird er trotzdem zum geplanten Zeitpunkt ausgeführt.
Alt	JH	Anhalten	Hält einen Auftrag oder die gesamte Auftragswarteschlange an. Der Auftrag oder die Auftragswarteschlange nimmt den normalen Zeitplan wieder auf, sobald Sie diese Option deaktivieren.
Alt	JT	Probelauf	Führt sofort einen Test des ausgewählten Backup-Auftrags aus.
Alt	JA	Auftragsaktivität	Ermöglicht die Anzeige von statistischen und Systeminformationen über einen laufenden Auftrag. Sie können einen aktiven Auftrag auch abbrechen.
Alt	HH	Auftragsverlauf anzeigen	Zeigt ausführliche Information zum Auftragsverlauf an, einschließlich Statistiken zu einzelnen Aufträgen und Auftragszusammenfassungen.

Tastaturkurzbefehle der Registerkarte "Backup und Wiederherstellung" für die Auftragsverlaufsansicht

Die folgende Tabelle listet die Tastaturkurzbefehle der Registerkarte "Backup und Wiederherstellung" für die Auftragsverlaufsansicht auf.

Siehe ["Tastaturkurzbefehle für die Registerkarte "Backup und Wiederherstellung""](#) auf Seite 1631.

Tabelle P-5 Tastaturkurzbefehle der Registerkarte "Backup und Wiederherstellung" für die Auftragsverlaufsansicht

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	HR	Jetzt ausführen	Führt einen Auftrag sofort aus. Wenn ein Auftrag geplant ist, wird er trotzdem zum geplanten Zeitpunkt ausgeführt.
Alt	HL	Auftragsprotokoll anzeigen	Zeigt das Auftragsprotokoll für den ausgewählten Auftragsverlauf an. Das Auftragsprotokoll enthält ausführliche Informationen zum Auftrag, zu Speicher und Medien sowie Auftragsoptionen, Dateistatistiken und Auftragsabschlussstatus (bei abgeschlossenen Aufträgen).
Alt	HD	Löschen	Löscht den ausgewählten Auftragsverlauf und das zugehörige Auftragsprotokoll, wenn diese nicht mehr benötigt werden.
Alt	HH	Auftragsverlauf anzeigen	Zeigt ausführliche Information zum Auftragsverlauf an, einschließlich Statistiken zu einzelnen Aufträgen und Auftragszusammenfassungen.
Alt	EH	Fehlerverarbeitung	Definiert Regeln zum Verarbeiten fehlgeschlagener Aufträge.
Alt	HC	Kopie	Erstellt eine Kopie des Auftragsverlaufs, der alle abhängigen Backup-Sätze eines Auftrags umfasst. Sie können den Auftragsverlauf jetzt kopieren oder einen Zeitpunkt dafür festlegen.

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	HV	Überprüfen	Überprüft für diesen Auftragsverlauf die Integrität der Datensammlung und der Medien, auf denen sich die Daten befinden. Wenn Sie einen Auftragsverlauf überprüfen, prüfen Sie alle abhängigen Backup-Sätze eines Auftrags. Sie können den Auftragsverlauf jetzt überprüfen oder einen Zeitpunkt dafür festlegen.
Alt	EB	Backup bearbeiten	Bearbeiten des Backup für den ausgewählten Auftragsverlauf. Sie können keine synthetischen oder einmaligen Backup-Aufträge bearbeiten.

Tastaturkurzbefehle der Registerkarte "Backup und Wiederherstellung" für die Backup-Satz-Ansicht

Die folgende Tabelle listet die Tastaturkurzbefehle der Registerkarte "Backup und Wiederherstellung" für die Backup-Satz-Ansicht auf.

Siehe "[Tastaturkurzbefehle für die Registerkarte "Backup und Wiederherstellung"](#)" auf Seite 1631.

Tabelle P-6 Tastaturkurzbefehle der Registerkarte "Backup und Wiederherstellung" für die Backup-Satz-Ansicht

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	SQ	Ablauf	Kennzeichnet den ausgewählten Backup-Satz als abgelaufen, wenn Sie ihn nicht mehr benötigen.
Alt	SH	Aufbewahren	Bewahrt den ausgewählten Backup-Satz auf. Sie können verhindern, dass Backup-Sätze ablaufen, indem Sie diese aufbewahren.

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	SC	Katalog	Katalogisiert den ausgewählten Backup-Satz. Durch das Katalogisieren von Backup-Sätzen können Sie die Daten anzeigen, die in diesen Sätzen enthalten sind, und nach Dateien zur Wiederherstellung suchen.
Alt	SU	Kopie	Erstellt eine Kopie des ausgewählten Backup-Satzes. Sie können den Backup-Satz jetzt kopieren oder einen Zeitpunkt dafür festlegen.
Alt	SV	Überprüfen	Überprüft für diesen Backup-Satz die Integrität der Datensammlung und der Medien, auf denen sich die Daten befinden. Sie können den Backup-Satz jetzt überprüfen oder einen Zeitpunkt dafür festlegen.
Alt	SL	Ablaufdatum	Hier können Sie Ablaufdatum und -zeit bearbeiten.
Alt	SK	Abhängige Backup-Sätze anzeigen	Zeigt die vom ausgewählten abhängigen Backup-Sätze an.
Alt	SW	Wiederherstellen	Durchsucht die Backup-Sätze und stellt dann die Daten wiederher.

Tastaturkurzbefehle der Registerkarte "Backup und Wiederherstellung" für die Ansicht der aktiven Warnmeldungen

Die folgende Tabelle listet die Tastaturkurzbefehle der Registerkarte "Backup und Wiederherstellung" für die Ansicht der aktiven Warnmeldungen auf.

Siehe ["Tastaturkurzbefehle für die Registerkarte "Backup und Wiederherstellung""](#) auf Seite 1631.

Tabelle P-7 Tastaturkurzbefehle der Registerkarte "Backup und Wiederherstellung" für die Ansicht der aktiven Warnmeldungen

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	AR	Antworten	Zeigt die Warnmeldung und alle zusätzlichen Informationen an. Sie müssen "Mit 'OK' beantworten" auswählen, um die Warnmeldung zu bereinigen.
Alt	AO	Mit 'OK' beantworten	Bereinigt die Warnmeldung, ohne Informationen über sie anzuzeigen. Verwenden Sie "Mit 'OK' beantworten" nur, wenn Sie die Warnmeldung nicht mehr benötigen.
Alt	AL	Auftragsprotokoll anzeigen	Zeigt das Auftragsprotokoll an, das für diesen Auftrag generiert wurde. Das Auftragsprotokoll enthält ausführliche Informationen zum Auftrag, zu Speicher und Medien sowie Auftragsoptionen, Dateistatistiken und Auftragsabschlussstatus (bei abgeschlossenen Aufträgen).
Alt	AH	Meldungsprotokoll anzeigen	Zeigt Warnmeldungen an, auf die Sie reagiert haben oder die Sie automatisch bereinigt haben.

Tastaturkurzbefehle der Registerkarte "Backup und Wiederherstellung" für die Anmeldedatenansicht

Die folgende Tabelle listet die Tastaturkurzbefehle der Registerkarte "Backup und Wiederherstellung" für die Anmeldedatenansicht auf.

Siehe "[Tastaturkurzbefehle für die Registerkarte "Backup und Wiederherstellung"](#)" auf Seite 1631.

Tabelle P-8 Tastaturkurzbefehle der Registerkarte "Backup und Wiederherstellung" für die Anmeldedatenansicht

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	CT	Anmeldedaten testen	Ermöglicht Ihnen das Prüfen der Kontoanmeldedaten für die ausgewählte Backup-Quelle.
Alt	CD	Ausgewählte Ressource löschen	Löscht die ausgewählte Ressource.
Alt	CC	Aktiven Test abbrechen	Bricht einen aktiven Test der Anmeldedaten ab.

Tastenkombinationen auf der Registerkarte "Auftragsüberwachung"

Die folgende Tabelle enthält die Tastenkombinationen für die Registerkarte "Auftragsüberwachung".

Siehe ["Informationen zu Tastaturkurzbefehlen in Backup Exec"](#) auf Seite 1629.

Siehe ["Tastaturkurzbefehle der Registerkarte "Speicher" für die Auftragsansicht "](#) auf Seite 1648.

Siehe ["Tastaturkurzbefehle der Registerkarte "Speicher" für die Auftragsverlaufsansicht "](#) auf Seite 1650.

Siehe ["Tastaturkurzbefehle der Registerkarte "Speicher" für die Backup-Satz-Ansicht "](#) auf Seite 1651.

Siehe ["Tastaturkurzbefehle der Registerkarte "Speicher" für die Ansicht der aktiven Warnmeldungen "](#) auf Seite 1653.

Tabelle P-9 Tastenkombinationen für die Registerkarte "Auftragsüberwachung"

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	J	Registerkarte "Auftragsüberwachung"	Öffnet die Registerkarte "Auftragsüberwachung".
Alt	ST	Standard	Zeigt Backup Exec in einer Ansicht an, die beschreibenden Text bereitstellt.
Alt	CO	Kompakt	Zeigt Backup Exec in einer platzsparenden Ansicht an.

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	F	Sortieren und Filtern	Zeigt Informationen in einer benutzerspezifischen Ansicht an oder ermöglicht Ihnen das Erstellen und Sichern einer benutzerspezifischen Ansicht.
Alt	V	Verzeichnisstruktur	Zeigt Elemente in einer hierarchischen Ansicht an.
Alt	L	Liste	Zeigt Elemente in einer Liste an, die Sie nach Spalten sortieren können.
Alt	CA	Backup-Kalender	Ermöglicht die Anzeige aller Aufträge des geplanten Backup auf einem Kalender.
Alt	RE	Wiederherstellung	Durchsucht die Backup-Sätze von einem einzelnen Server und stellt dann die Daten wieder her.
Alt	JE	Bearbeiten	Ermöglicht die Bearbeitung einer Backup-Definition. Sie können die Backup-Auswahlen, die Backup-Einstellungen und die Zustände einer Backup-Definition bearbeiten.
Alt	JD	Löschen	Löscht eine Backup-Definition, wenn Sie diese nicht mehr benötigen.
Alt	JC	Abbrechen	Bricht einen aktiven Auftrag während der Ausführung ab.
Alt	JP	Priorität	Erhöht oder senkt die Priorität eines Auftrags in der Auftragswarteschlange.
Alt	JR	Jetzt ausführen	Führt einen Auftrag sofort aus. Wenn ein Auftrag geplant ist, wird er trotzdem zum geplanten Zeitpunkt ausgeführt.

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	JH	Anhalten	Hält einen Auftrag oder die gesamte Auftragswarteschlange an. Der Auftrag oder die Auftragswarteschlange nimmt den normalen Zeitplan wieder auf, sobald Sie diese Option deaktivieren.
Alt	JT	Probelauf	Führt sofort einen Test des ausgewählten Backup-Auftrags aus.
Alt	JA	Auftragsaktivität	Ermöglicht die Anzeige von statistischen und Systeminformationen über einen laufenden Auftrag. Sie können einen aktiven Auftrag auch abbrechen.
Alt	JJ	Auftragsverlauf anzeigen	Zeigt ausführliche Information zum Auftragsverlauf an, einschließlich Statistiken zu einzelnen Aufträgen und Auftragszusammenfassungen.
Alt	HR	Jetzt ausführen	Führt einen Auftrag sofort aus. Wenn ein Auftrag geplant ist, wird er trotzdem zum geplanten Zeitpunkt ausgeführt.
Alt	HL	Auftragsprotokoll anzeigen	Zeigt das Auftragsprotokoll für den ausgewählten Auftragsverlauf an. Das Auftragsprotokoll enthält ausführliche Informationen zum Auftrag, zu Speicher und Medien sowie Auftragsoptionen, Dateistatistiken und Auftragsabschlussstatus (bei abgeschlossenen Aufträgen).

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	HD	Löschen	Löscht den ausgewählten Auftragsverlauf und das zugehörige Auftragsprotokoll, wenn diese nicht mehr benötigt werden.
Alt	HH	Auftragsverlauf anzeigen	Zeigt ausführliche Information zum Auftragsverlauf an, einschließlich Statistiken zu einzelnen Aufträgen und Auftragszusammenfassungen.
Alt	EH	Fehlerverarbeitung	Definiert Regeln zum Verarbeiten fehlgeschlagener Aufträge.
Alt	HC	Kopie	Erstellt eine Kopie des Auftragsverlaufs, der alle abhängigen Backup-Sätze eines Auftrags umfasst. Sie können den Auftragsverlauf jetzt kopieren oder einen Zeitpunkt dafür festlegen.
Alt	HV	Überprüfen	Überprüft für diesen Auftragsverlauf die Integrität der Datensammlung und der Medien, auf denen sich die Daten befinden. Wenn Sie einen Auftragsverlauf überprüfen, prüfen Sie alle abhängigen Backup-Sätze eines Auftrags. Sie können den Auftragsverlauf jetzt überprüfen oder einen Zeitpunkt dafür festlegen.
Alt	EB	Backup bearbeiten	Bearbeiten des Backup für den ausgewählten Auftragsverlauf. Sie können die Backup-Auswahl, die Backup-Einstellungen und die Stufen einer Backup-Definition bearbeiten.

Tastaturkurzbefehle der Registerkarte "Speicher"

Die folgende Tabelle zeigt die Tastaturkurzbefehle für die Registerkarte "Speicher".

Siehe ["Informationen zu Tastaturkurzbefehlen in Backup Exec"](#) auf Seite 1629.

Siehe ["Tastaturkurzbefehle der Registerkarte "Speicher" für die Auftragsansicht "](#) auf Seite 1648.

Siehe ["Tastaturkurzbefehle der Registerkarte "Speicher" für die Auftragsverlaufsansicht "](#) auf Seite 1650.

Siehe ["Tastaturkurzbefehle der Registerkarte "Speicher" für die Backup-Satz-Ansicht "](#) auf Seite 1651.

Siehe ["Tastaturkurzbefehle der Registerkarte "Speicher" für die Ansicht der aktiven Warnmeldungen "](#) auf Seite 1653.

Tabelle P-10 Tastaturkurzbefehle der Registerkarte "Speicher"

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	S	Registerkarte "Speicher"	Öffnet die Registerkarte Speicher.
Alt	ST	Standard	Zeigt Backup Exec in einer Ansicht an, die beschreibenden Text bereitstellt.
Alt	CO	Kompakt	Zeigt Backup Exec in einer platzsparenden Ansicht an.
Alt	F	Sortieren und Filtern	Zeigt Informationen in einer benutzerspezifischen Ansicht an oder ermöglicht Ihnen das Erstellen und Sichern einer benutzerspezifischen Ansicht.
Alt	V	Verzeichnisstruktur	Zeigt Elemente in einer hierarchischen Ansicht an.
Alt	L	Liste	Zeigt Elemente in einer Liste an, die Sie nach Spalten sortieren können.
Alt	SP	Anhalten	Hält ein Gerät an, um die Ausführung von geplanten und neuen Aufträgen darauf zu verhindern.

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	SD	Deaktivieren	Deaktiviert ein Gerät, damit es für andere Anwendungen verfügbar ist.
Alt	SO	Offline	Behebt Fehler des Geräts, um es online zu stellen. Es können erst wieder Vorgänge auf diesem Gerät ausgeführt werden, wenn es online ist.
Alt	CC	Speicher konfigurieren	Startet den Assistenten "Speicher konfigurieren", um verschiedene Arten von Speicher einzurichten, in denen Sie Daten sichern können.
Alt	CT	Fehlerbehebung	Lässt Backup Exec Lösungsvorschläge für Probleme auf dem Gerät bereitstellen.
Alt	CD	Löschen	Entfernt ein Element aus der Backup Exec-Datenbank.
Alt	CS	Freigabe	Stellt ein Gerät zur gemeinsamen Nutzung durch Backup Exec-Server bereit.
Alt	SS	Einlesen	Ruft Informationen über die Medien in den Schächten ab und aktualisiert dann die Backup Exec-Datenbank.
Alt	SI	Inventarisierung	Installiert die Medien im Bandlaufwerk, liest die Medienkennung und aktualisiert die Backup Exec-Datenbank. Sie können Medien jetzt inventarisieren oder einen Zeitpunkt dafür festlegen.
Alt	SC	Katalog	Protokolliert Informationen über die Backup-Sätze und das Speichergerät, auf denen die Backup-Sätze gespeichert sind.

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	SG	Jetzt inventarisieren und katalogisieren	<p>Installiert die Medien in Bandlaufwerken, liest die Medienkennung und aktualisiert die Backup Exec-Datenbank.</p> <p>Außerdem werden Informationen über die Backup-Sätze und das Speichergerät protokolliert, auf denen die Backup-Sätze gespeichert sind.</p>
Alt	SZ	Jetzt initialisieren	Sendet einen Startbefehl an den Wechsler.
Alt	SB	Bezeichnung	<p>Schreibt eine neue Medienkennung auf das Medium im Laufwerk.</p> <p>Beim Schreiben der Kennung werden auf dem Medium vorhandene Daten zerstört.</p>
Alt	SE	Löschen	<p>Fügt ein Kennzeichen am Beginn der Medien ein, das den Zugriff auf die Daten auf dem Medium sperrt.</p> <p>Beim langsamen Löschen werden sämtliche Medien physisch gelöscht.</p>
Alt	VB	Blinken	Aktiviert das Blinksignal der Status-LEDs auf dem physischen Datenträger, um das Identifizieren in einem virtuellen Datenträger zu erleichtern.
Alt	VU	Blinken beenden	Deaktiviert die blinkenden Status-LEDs auf dem physischen Datenträger.
Alt	VC	Virtuellen Datenträger konfigurieren	Konfiguriert einen virtuellen Datenträger auf einer Speichergruppe für den Einsatz mit Backup Exec.

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	JR	Jetzt ausführen	Führt einen Auftrag sofort aus. Wenn ein Auftrag geplant ist, wird er trotzdem zum geplanten Zeitpunkt ausgeführt.
Alt	MA	Mit Mediensatz verknüpfen	Gibt den Anhängezeitraum und den Überschreibschutzzeitraum eines Mediensatzes an, die für ein Medium gelten. Sie können Speicher auswählen und die Eingabetaste drücken, um ausführliche Informationen zu Mediensatzvorgängen und Medienspeichervorgängen anzuzeigen.
Alt	MS	Temporäre Medien	Verknüpft die Medien mit dem Satz temporärer Medien, damit Backup Exec ihn in einem Überschreibungs-Backup-Auftrag verwenden kann. Sie können Speicher auswählen und die Eingabetaste drücken, um ausführliche Informationen zu Mediensatzvorgängen und Medienspeichervorgängen anzuzeigen.
Alt	MT	Zurückziehen	Verknüpft Medien mit dem Satz ausrangierter Medien, damit Backup Exec ihn für Backup-Aufträge verwenden kann. Sie können Speicher auswählen und die Eingabetaste drücken, um ausführliche Informationen zu Mediensatzvorgängen und Medienspeichervorgängen anzuzeigen.

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	MV	Medien zum Speicher verschieben	<p>Ermöglicht die Eingabe der Kennung oder das Scannen des Barcodes, um die Medien in einen Medienspeicher zu verschieben.</p> <p>Sie können Speicher auswählen und die Eingabetaste drücken, um ausführliche Informationen zu Mediensatzvorgängen und Medienspeichervorgängen anzuzeigen.</p>
Alt	RE	Wiederherstellung	Durchsucht die Backup-Sätze von einem einzelnen Server und stellt dann die Daten wieder her.

Tastaturkurzbefehle der Registerkarte "Speicher" für die Auftragsansicht

Die folgende Tabelle listet die Tastaturkurzbefehle der Registerkarte "Speicher" für die Auftragsansicht auf.

Siehe "[Tastaturkurzbefehle der Registerkarte "Speicher"](#)" auf Seite 1644.

Tabelle P-11 Tastaturkurzbefehle der Registerkarte "Speicher" für die Auftragsansicht

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	JE	Backups bearbeiten	<p>Bearbeitet einen oder mehrere vorhandene Backup-Aufträge.</p> <p>Sie können keine synthetischen oder einmalige Backups bearbeiten.</p>
Alt	JE	Bearbeiten	<p>Ermöglicht die Bearbeitung einer Backup-Definition.</p> <p>Sie können die Backup-Auswahlen, die Backup-Einstellungen und die Zustände einer Backup-Definition bearbeiten.</p>

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	JD	Löschen	Löscht eine Backup-Definition, wenn Sie diese nicht mehr benötigen.
Alt	JC	Abbrechen	Bricht einen aktiven Auftrag während der Ausführung ab.
Alt	JP	Priorität	Erhöht oder senkt die Priorität eines Auftrags in der Auftragswarteschlange.
Alt	JR	Jetzt ausführen	Führt einen Auftrag sofort aus. Wenn ein Auftrag geplant ist, wird er trotzdem zum geplanten Zeitpunkt ausgeführt.
Alt	JH	Anhalten	Hält einen Auftrag oder die gesamte Auftragswarteschlange an. Der Auftrag oder die Auftragswarteschlange nimmt den normalen Zeitplan wieder auf, sobald Sie diese Option deaktivieren.
Alt	JT	Probelauf	Führt sofort einen Test des ausgewählten Backup-Auftrags aus.
Alt	JA	Auftragsaktivität	Ermöglicht die Anzeige von statistischen und Systeminformationen über einen laufenden Auftrag. Sie können einen aktiven Auftrag auch abbrechen.
Alt	HH	Auftragsverlauf anzeigen	Zeigt ausführliche Information zum Auftragsverlauf an, einschließlich Statistiken zu einzelnen Aufträgen und Auftragszusammenfassungen.

Tastaturkurzbefehle der Registerkarte "Speicher" für die Auftragsverlaufsansicht

Die folgende Tabelle listet die Tastaturkurzbefehle der Registerkarte "Speicher" für die Auftragsverlaufsansicht auf.

Siehe "[Tastaturkurzbefehle der Registerkarte "Speicher"](#)" auf Seite 1644.

Tabelle P-12 Tastaturkurzbefehle der Registerkarte "Speicher" für die Auftragsverlaufsansicht

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	HR	Jetzt ausführen	Führt einen Auftrag sofort aus. Wenn ein Auftrag geplant ist, wird er trotzdem zum geplanten Zeitpunkt ausgeführt.
Alt	HL	Auftragsprotokoll anzeigen	Zeigt das Auftragsprotokoll für den ausgewählten Auftragsverlauf an. Das Auftragsprotokoll enthält ausführliche Informationen zum Auftrag, zu Speicher und Medien sowie Auftragsoptionen, Dateistatistiken und Auftragsabschlussstatus (bei abgeschlossenen Aufträgen).
Alt	HD	Löschen	Löscht den ausgewählten Auftragsverlauf und das zugehörige Auftragsprotokoll, wenn diese nicht mehr benötigt werden.
Alt	HH	Auftragsverlauf anzeigen	Zeigt ausführliche Information zum Auftragsverlauf an, einschließlich Statistiken zu einzelnen Aufträgen und Auftragszusammenfassungen.
Alt	EH	Fehlerverarbeitung	Definiert Regeln zum Verarbeiten fehlgeschlagener Aufträge.

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	HC	Kopie	Erstellt eine Kopie des Auftragsverlaufs, der alle abhängigen Backup-Sätze eines Auftrags umfasst. Sie können den Auftragsverlauf jetzt kopieren oder einen Zeitpunkt dafür festlegen.
Alt	HV	Überprüfen	Überprüft für diesen Auftragsverlauf die Integrität der Datensammlung und der Medien, auf denen sich die Daten befinden. Wenn Sie einen Auftragsverlauf überprüfen, prüfen Sie alle abhängigen Backup-Sätze eines Auftrags. Sie können den Auftragsverlauf jetzt überprüfen oder einen Zeitpunkt dafür festlegen.
Alt	EB	Backup bearbeiten	Bearbeiten des Backup für den ausgewählten Auftragsverlauf. Sie können keine synthetischen oder einmaligen Backup-Aufträge bearbeiten.

Tastaturkurzbefehle der Registerkarte "Speicher" für die Backup-Satz-Ansicht

Die folgende Tabelle listet die Tastaturkurzbefehle der Registerkarte "Speicher" für die Backup-Satz-Ansicht auf.

Siehe ["Tastaturkurzbefehle der Registerkarte "Speicher""](#) auf Seite 1644.

Tabelle P-13 Tastaturkurzbefehle der Registerkarte "Speicher" für die Backup-Satz-Ansicht

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	SQ	Ablauf	Kennzeichnet den ausgewählten Backup-Satz als abgelaufen, wenn Sie ihn nicht mehr benötigen.

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	SH	Aufbewahren	Bewahrt den ausgewählten Backup-Satz auf. Sie können verhindern, dass Backup-Sätze ablaufen, indem Sie diese aufbewahren.
Alt	SC	Katalog	Katalogisiert den ausgewählten Backup-Satz. Durch das Katalogisieren von Backup-Sätzen können Sie die Daten anzeigen, die in diesen Sätzen enthalten sind, und nach Dateien zur Wiederherstellung suchen.
Alt	SU	Kopie	Erstellt eine Kopie des ausgewählten Backup-Satzes. Sie können den Backup-Satz jetzt kopieren oder einen Zeitpunkt dafür festlegen.
Alt	SV	Überprüfen	Überprüft für diesen Backup-Satz die Integrität der Datensammlung und der Medien, auf denen sich die Daten befinden. Sie können den Backup-Satz jetzt überprüfen oder einen Zeitpunkt dafür festlegen.
Alt	SL	Ablaufdatum	Hier können Sie Ablaufdatum und -zeit bearbeiten.
Alt	SK	Abhängige Backup-Sätze anzeigen	Zeigt die vom ausgewählten abhängigen Backup-Sätze an.
Alt	SW	Wiederherstellen	Durchsucht die Backup-Sätze und stellt dann die Daten wiederher.

Tastaturkurzbefehle der Registerkarte "Speicher" für die Ansicht der aktiven Warnmeldungen

Die folgende Tabelle listet die Tastaturkurzbefehle der Registerkarte "Speicher" für die Ansicht der aktiven Warnmeldungen auf.

Siehe "[Tastaturkurzbefehle der Registerkarte "Speicher"](#)" auf Seite 1644.

Tabelle P-14 Tastaturkurzbefehle der Registerkarte "Speicher" für die Ansicht der aktiven Warnmeldungen

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	AR	Antworten	Zeigt die Warnmeldung und alle zusätzlichen Informationen an. Sie müssen "Mit 'OK' beantworten" auswählen, um die Warnmeldung zu bereinigen.
Alt	AO	Mit 'OK' beantworten	Bereinigt die Warnmeldung, ohne Informationen über sie anzuzeigen. Verwenden Sie "Mit 'OK' beantworten" nur, wenn Sie die Warnmeldung nicht mehr benötigen.
Alt	AL	Auftragsprotokoll anzeigen	Zeigt das Auftragsprotokoll an, das für diesen Auftrag generiert wurde. Das Auftragsprotokoll enthält ausführliche Informationen zum Auftrag, zu Speicher und Medien sowie Auftragsoptionen, Dateistatistiken und Auftragsabschlussstatus (bei abgeschlossenen Aufträgen).
Alt	AH	Meldungsprotokoll anzeigen	Zeigt Warnmeldungen an, auf die Sie reagiert haben oder die Sie automatisch bereinigt haben.

Tastaturkurzbefehle der Registerkarte "Berichte"

Die folgende Tabelle enthält die Tastaturkurzbefehle für die Registerkarte "Berichte".

Siehe ["Informationen zu Tastaturkurzbefehlen in Backup Exec"](#) auf Seite 1629.

Tabelle P-15 Tastaturkurzbefehle der Registerkarte "Berichte"

Zugriffstasten	Hotkey	Befehl	Ergebnis
Alt	R	Bericht jetzt ausführen	Führt einen ausgewählten Bericht sofort aus.
Alt	C	Neuer benutzerdefinierter Bericht	Erstellt einen neuen Bericht mit den von Ihnen ausgewählten Berichtsoptionen.
Alt	N	Neuer geplanter Bericht	Plant einen Bericht, der zu einem bestimmten Datum/Uhrzeit auszuführen ist.
Alt	E	Bearbeiten	Bearbeitet einen geplanten Bericht oder Berichtsoptionen für einen benutzerdefinierten Bericht.
Alt	P	Kopieren	Ermöglicht Ihnen das Kopieren eines benutzerdefinierten Berichts. Backup Exec speichert eine Kopie des Berichts zusammen mit dem ursprünglichen Bericht in der Gruppe 'Benutzerdefinierter Bericht'.
Alt	D	Löschen	Löscht einen benutzerdefinierten, geplanten oder abgeschlossenen Bericht.

Allgemeine Tastaturnavigation innerhalb der Backup Exec-Benutzeroberfläche

Sie können Backup Exec ausschließlich mit der Tastatur verwenden und darin navigieren. Auf der grafischen Benutzeroberfläche hat die aktuelle Verzeichnisstruktur oder Tabelle eine dunkelblaue Markierung, und die aktuell aktive Registerkarte, das Optionsfeld oder das Kontrollkästchen ist mit einer rechteckigen, gestrichelten Linie eingefasst. Diese Bereiche haben einen sogenannten Fokus und reagieren auf Befehle.

Backup Exec verwendet die folgenden Standards für die Tastaturnavigation:

- Mit der Tabulatortaste wechseln Sie den Fokus auf das nächsten aktive Element, sei es ein Bereich, ein Feld oder ein Steuerelement, wobei eine voreingestellte Reihenfolge eingehalten wird. Mit Umschalttaste + Tabulatortaste wechseln Sie den Fokus in die entgegengesetzte Richtung der Reihenfolge.
- Mit Strg + Tabulatortaste verlassen Sie den Konsolenbereich, in dem Sie intern mit der Tabulatortaste navigiert haben.
- Mit der Nach-oben- und der Nach-unten-Taste wechseln Sie den Fokus in einer Liste von Elementen nach oben oder unten.
- Durch Drücken der Alt -Taste zusammen mit dem unterstrichenen Buchstaben eines Felds oder einer Schaltfläche wechseln Sie den Fokus auf dieses Feld oder diese Schaltfläche.
- Mit der Eingabetaste aktivieren Sie Ihre Auswahl. Drücken Sie beispielsweise die Tabulatortaste, um in einem Assistentenfenster die Schaltfläche "Weiter" auszuwählen, wird durch anschließendes Drücken der Entertaste das nächste Fenster angezeigt.
- Mit Umschalttaste + F10 werden Kontextmenüs geöffnet.

Tastaturnavigation innerhalb der Dialogfelder in Backup Exec

Dialogfelder enthalten Gruppen von Steuerelementen, die zum Einstellen von Optionen oder Einstellungen für Programme benötigt werden.

Im Folgenden finden Sie einige allgemeine Regeln zur Navigation in Dialogfeldern:

- Mit der Tabulatortaste wechseln Sie den Fokus zwischen Steuerelementen in einem Dialogfeld anhand einer voreingestellten Reihenfolge.
- Ein dunkler Rand zeigt die Standardbefehlsschaltfläche an. Drücken Sie jederzeit Eingabetaste, um die Schaltfläche mit einem dunklen Rand auszuwählen.
- Mit der Esc -Taste wählen Sie die Schaltfläche "Abbrechen", wenn diese vorhanden ist.
- Mit der Leertaste aktivieren Sie ein Steuerelement, das mit der Tabulatortaste ausgewählt wurde.
- Mit der Leertaste ändern Sie den Status eines Kontrollkästchens oder Optionsfelds, auf dem ein Fokus liegt. Durch Eingabe des unterstrichenen Buchstabens (wenn vorhanden) wechseln Sie den Fokus zu diesem Kontrollkästchen und ändern dessen Status.
- Mit den Pfeiltasten wechseln Sie den Fokus zwischen Optionsfeldern, Listenfeldern, Schiebereglern, Gruppen von Steuerelementen oder Gruppen von Registerkarten.

- Elemente, die nicht geändert werden können, werden von der Reihenfolge der Tabulatortaste ausgenommen. Nicht verfügbare Optionen sind grau hinterlegt und können weder ausgewählt noch fokussiert werden.

Obwohl die hier beschriebenen Steuerelemente in der Regel in Dialogfeldern auftreten, können sie auch in anderen Zusammenhängen vorkommen. Dabei werden dieselben Navigationsstandards angewendet.

Listenfeldnavigation in Backup Exec

In Listenfeldern wird eine Spalte verfügbarer Auswahlmöglichkeiten angezeigt.

Es gibt verschiedene Arten von Listenfeldern mit weiteren Navigationskonventionen:

- Dropdown-Listenfelder zeigen in der Standardeinstellung nur das ausgewählte Element an. Auf einer kleinen Schaltfläche rechts vom Steuerelement wird ein Pfeil nach unten angezeigt. Klicken Sie auf den Pfeil, um weitere Elemente aus dem Listenfeld anzuzeigen. Wenn mehr Auswahlmöglichkeiten bestehen, als im voreingestellten Listenfeldbereich Platz finden, wird an der Seite des Listenfelds ein Schieberegler angezeigt. Drücken Sie die Alt +Nach-unten-Taste, Alt +Nach-oben-Taste oder F4, um die Liste ein- oder auszublenden. Mit der Tabulatortaste wird ein Element ausgewählt.
- Listenfelder mit erweiterter Auswahl unterstützen das Auswählen von einzelnen Elementen, Elementblöcken oder einer Kombination von beiden. Halten Sie nach der Auswahl eines Elements die Strg +Navigationstasten gedrückt, um zusätzliche Elemente oder Elementblöcke zu aktivieren oder zu deaktivieren.

Navigation in Dialogfeldern mit Registerkarten in Backup Exec

In einigen Dialogfeldern werden Registerkarten verwendet, um die vielen Optionen in Gruppen zu unterteilen. Jede Registerkarte enthält verschiedene Gruppen von Steuerelementen. Verwenden Sie die Tabulatortaste, um den Fokus zwischen den Registerkarten in einem Dialogfeld zu wechseln. Durch Eingabe des unterstrichenen Buchstabens verschieben Sie den Fokus ebenfalls auf die Registerkarte, und die Seite mit den dortigen Steuerelementen wird angezeigt.

In der folgenden Tabelle finden Sie die Regeln der Tastaturnavigation in Dialogfeldern mit Registerkarten.

Tabelle P-16 Tastaturnavigation in Dialogfeldern mit Registerkarten

Tastatureingabe	Ergebnis
Strg + Bild-ab-Taste oder Strg + Tabulatortaste	Wechselt zur nächsten Registerkarte und zeigt die Seite an.
Strg + Bild-auf-Taste	Wechselt zur vorherigen Registerkarte und zeigt die Seite an.
Nach-rechts-Taste oder Nach-links-Taste	Wenn sich der Fokus auf einer Registerkartenauswahl befindet, wird die nächste oder die vorherige Registerkarte der aktuellen Zeile ausgewählt und die Seite angezeigt.

Festlegen der Optionen zur Eingabehilfe

Backup Exec reagiert auf die Eingabehilfeeinstellungen des Betriebssystems.

Backup Exec ist mit den Eingabehilfe-Dienstprogrammen von Microsoft kompatibel. In Windows-Betriebssystemen können Eingabehilfeoptionen wie Tastaturverhalten, Kontrasteinstellungen, Warntöne und Mauseinstellungen über die Systemsteuerung eingestellt werden.

Die Eingabehilfefunktionen sind hauptsächlich für die englischsprachige Version vorgesehen. Die lokalisierten Versionen dieses Produkts bieten Unterstützung für die Tastaturnavigation (ohne Maus) mithilfe von Zugriffstasten und Hotkeys.

Weitere Informationen zu den Einstellungen der Eingabehilfe erhalten Sie in der Microsoft-Dokumentation.

Glossar

ADAMM (Advanced Device and Media Management)	Eine Backup Exec-Datenbank, die das Verfolgen von Bandkassettenmedien automatisiert. ADAMM lässt die Backup-Sätze, die auf Bandkassettenmedien gespeichert sind, entsprechend dem verknüpften Mediensatz ablaufen.
Administratorkonsole	Die Benutzeroberfläche, in der Sie Backup Exec-Vorgänge ausführen können. Die Benutzeroberfläche kann vom Backup Exec-Server oder einem Remote-Computer ausgeführt werden.
Agent	Eine Komponente, die Computern (z. B. einem Microsoft SQL Server) ermöglicht, mit dem Backup Exec-Server zu kommunizieren.
Agent for Windows	Ein Backup Exec-Systemdienst, der auf Microsoft Windows-Computer ausgeführt wird und Remote-Backup und -Wiederherstellung auf diesen Computern ermöglicht.
Anhängezeitraum	Der Zeitraum, in dem Daten Band- oder Plattenkassettenmedien hinzugefügt werden können. Der Anhangzeitraum beginnt, wenn der erste Backup-Auftrag auf das Medium geschrieben wird.
Auftrag	Ein Vorgang, der für die Verarbeitung durch den Backup Exec-Server geplant wurde. Aufträge enthalten Quell- oder Zielinformationen, Einstellungen und einen Zeitplan. Es gibt Aufträge zu Backup, Wiederherstellung, Datenerkennung, Berichterstellung, Testlauf und Speichervorgängen.
Auftragsdelegierung	Ein Vorgang, bei dem Aufträge durch einen zentralen Administrationsserver auf verfügbare Speichergeräte auf verwalteten Backup Exec-Servern verteilt werden. Auftragsdelegierung ist nur mit Central Admin Server Option verfügbar.
Auftragsprotokoll	Ein Protokoll, das die Ergebnisse eines Auftrags enthält. Es wird erstellt, wenn der Auftrag ausgeführt wird. Sie können das Auftragsprotokoll auf Auftragsfehler und Auftragsdetails überprüfen.
Auftragsverlauf	Eine Liste der abgeschlossenen und fehlgeschlagenen Backup-, Wiederherstellungs- und Speichervorgangsaufträge.
Auftragsvorlage	Eine Sammlung von Einstellungen, mit denen Backup Exec Aufträge erstellt. Beispiele für Einstellungen: Verschlüsselung, Zeitplan und Benachrichtigungen. Wird ein Backup-Auftrag ausgeführt, kombiniert Backup Exec die Auftragsvorlage mit der Backup-Auswahl, um einen Backup-Auftrag zu erstellen.
Ausrangierte Medien	Band- oder Kassettenmedien, die normalerweise aufgrund einer übermäßigen Anzahl von Fehlern aus dem Betrieb genommen wurden. Ausrangierte Medien sind für Wiederherstellungsaufträge, aber nicht für Backup-Aufträge verfügbar. Medien

müssen ausrangiert werden, bevor sie gelöscht werden können. Wenn Sie gelöschte Medien verwenden möchten, erkennt Backup Exec diese als importierte Medien. Sie müssen ausrangierte Medien katalogisieren, bevor Sie Daten daraus wiederherstellen können.

Backup-Definition	Ein Container für Backup-Auswahl, Auftragsvorlagen und Stadien. Backup Exec kombiniert die Auftragsvorlagen mit der Backup-Auswahl, um Backup-Aufträge zu erstellen. Wenn Sie ein Stadium angeben, wird diese zusätzliche Aufgabe ebenfalls ausgeführt.
Backup-Methode	Eine Option, die Sie beim Ausführen eines Backup-Auftrags auswählen, um ein vollständiges, Differenzial- oder inkrementelles Backup anzugeben.
Backup-Satz	Eine Sammlung von Daten, die aus nur einer Inhaltsquelle gesichert wird. Ein Beispiel für eine Inhaltsquelle kann ein Server oder ein Microsoft Exchange-Datensatz sein. Wenn Sie mehrere Inhaltsquellen auswählen, erstellt Backup Exec mehrere Backup-Sätze.
Backup-Strategie	Die Verfahren, die Sie für das Sichern Ihres Netzwerks implementieren. Die Backup-Strategie gibt an, welche Backup-Methoden verwendet und wann Backups ausgeführt werden.
Backup Exec-Dienstkonto	Ein Benutzerkonto, das für die Backup Exec-Systemdienste konfiguriert ist. Es enthält einen Benutzernamen und ein Kennwort und stellt Rechte zum Einloggen als Dienst und Agieren als Backup Exec-Administrator zur Verfügung.
Backup Exec-Server	Der Computer, auf dem Backup Exec installiert ist und auf dem die Backup Exec Services ausgeführt werden.
Backup Exec-Serverpool	Eine Funktion von Backup Exec Central Admin Server Option, mit der Sie Backup Exec-Server in einem Pool, auf den Sie Backup-Aufträge einschränken können, zusammenfassen können.
Basis	Der erste Backup-Auftrag, der in einem synthetischen Backup ausgeführt wird. Das Basis-Backup wird nur einmal ausgeführt und sichert alle Dateien auf dem ausgewählten Computer. Ein vollständiges Backup wird aus einem Basis-Backup und den folgenden inkrementellen Backups zusammengesetzt bzw. synthetisiert.
benutzerdefinierte Fehlerbehandlungsregel	Eine Fehlerbehandlungsregel, die Sie für einen bestimmten Fehlercode in einer Fehlerkategorie definieren können. Wenn ein Auftrag mit dem Fehlercode fehlschlägt, der mit der benutzerdefinierten Fehlerbehandlungsregel verknüpft ist, werden die Wiederholungsoptionen und die endgültige Auftragsbehandlung auf den Auftrag angewendet.
bevorzugte Serverkonfiguration	Eine Sammlung von Servern und Standorten, die als bevorzugte Backup-Quellen ausgewählt werden. Bevorzugte Serverkonfigurationen haben als Backup-Quellen in den Instanzen Vorrang, in denen Daten zwischen mehreren Servern repliziert werden.

Cloud-Speicher	Ein Online-Speicherort auf mehreren virtuellen Servern, an dem Sie Daten sichern können.
Data Lifecycle Management (DLM)	Ein automatisierter Vorgang zum Freigeben von Speicherplatz, mit dem Backup Exec abgelaufene Backup-Sätze auf plattenbasierten Speichergeräten löscht. Dieser Speicherplatz kann dann von neuen Backup-Sätzen genutzt werden. DLM löscht Backup-Sätze aus plattenbasierten Speichergeräten, wenn der angegebene Aufbewahrungszeitraum abgelaufen ist. Standardmäßig bewahrt Backup Exec die neuesten Backup-Sätze, die zum Wiederherstellen von gesicherten Komponenten auf einem Server erforderlich sind, selbst dann auf, wenn die Backup-Sätze abgelaufen sind.
Datenerkennung	Eine Funktion von Backup Exec, die das Erkennen neuer Backup-Inhalte in einer Windows-Domäne ermöglicht.
Datenträgerspeicher	Ein Speicherort auf einer lokal verbundenen internen Festplatte, einem USB-Gerät, einem FireWire-Gerät oder einem über ein Netzwerk angehängten Speichergerät, auf dem Sie Daten sichern können.
Differenzial	Eine Backup-Methode, die alle Dateien umfasst, die seit dem letzten vollständigen Backup geändert wurden.
eingeschränkter Verschlüsselungscode	Ein Verschlüsselungscode, den jedermann verwenden kann, um Daten unter Verwendung der Verschlüsselung zu sichern. Nur der Schlüsselbesitzer oder ein Benutzer, der die Passphrase kennt, kann Daten wiederherstellen, die mit einem eingeschränkten Verschlüsselungscode verschlüsselt wurden.
Ereignis	Eine Aktion, die während eines Backup Exec-Vorgangs auftritt, zum Beispiel eine Auftragsannullierung.
Fehlerbehandlungsregel	Eine Standard- oder benutzerdefinierte Regel, die Wiederholungsoptionen und die endgültige Auftragsbehandlung für fehlerhafte oder abgebrochene Aufträge festlegt. Über die Wiederholungsoptionen können Sie angeben, wie oft ein fehlgeschlagener Auftrag wiederholt wird und nach welchem Zeitraum die einzelnen Wiederholungen durchgeführt werden. Die endgültige Auftragsbehandlung ermöglicht es, den Auftrag anzuhalten, bis Sie den Fehler beheben können.
gemeinsamer Verschlüsselungscode	Ein Typ Verschlüsselungscode, den jeder verwenden kann, um Daten unter Verwendung der Verschlüsselung zu sichern und verschlüsselte Daten wiederherzustellen.
Gemischtes Backup	Eine Backup-Definition, die mehr als eine Backup-Methode für mehrere Datentypen enthält.
granulare Wiederherstellung	Eine Wiederherstellung von einzelnen Elementen aus einem Backup, für das die Option "Granular Recovery Technology" aktiviert wurde.
GRT (Granular Recovery Technology)	Eine Backup-Option, die in einigen Backup Exec-Agents verfügbar ist. Mit Granular Recovery Technology können Sie einzelne Elemente aus Datenbank-Backups

	wiederherstellen. Ein separates Backup der einzelnen Elemente ist nicht erforderlich, um ein Element wiederherzustellen.
Importierte Medien	Die Medien, die von einem anderen als dieser Installation von Backup Exec erstellt werden, aber sich in den Speichergeräten in der Backup Exec-Umgebung befinden.
inkrementell	Eine Backup-Methode, die nur die Dateien sichert, die seit dem letzten vollständigen oder inkrementellem Backup geändert wurden.
Katalog	Eine Datenbank, die Backup Exec während eines Backup-Vorgangs erstellt. Wenn Sie die wiederherzustellenden Daten auswählen, verwendet Backup Exec die Kataloginformationen für die Suche nach den ausgewählten Elementen für die Wiederherstellung und den Speichergeräte, auf denen diese sich befinden.
Lastenausgleich	<p>Eine Funktion in Backup Exec, die automatisch Aufträge unter allen verfügbaren Speichergeräten in einem Speichergerätepool verteilt.</p> <p>Ebenfalls eine Funktion von Backup Exec Central Admin Server Option, mit der Aufträge automatisch von einem zentralen Administrationsserver auf mehrere Backup Exec-Server für die Verarbeitung auf den einzelnen Speichergeräten verteilt werden.</p>
Login-Konto	Ein Konto, das die Anmeldedaten eines Windows-Benutzerkonten speichert und mit dem Backup um Benutzernamen und Kennwörter verwalten kann. Es kann verwendet werden, um Datenquellen zu durchsuchen oder Aufträge zu verarbeiten.
Medien-ID	Die eindeutige interne Bezeichnung, die Backup Exec jedem in Backup Exec verwendeten Medium zuweist. Die ID enthält Statistiken für jedes Medium. Die Medien-ID kann nicht gelöscht oder geändert werden.
Medienkennung	Eine Bezeichnung zum Identifizieren von Medien. Backup Exec weist die Kennung automatisch zu, aber Sie können sie ändern. Wenn das Medium vorher in einer Bibliothek mit einem Barcode-Leser genutzt wurde, hat die Medienkennung bereits einen Barcode.
Medienrotation	Eine Strategie, die festlegt, wann Bandkassettenmedien von Backup Exec wiederverwendet werden können. Gängige Beispiele für Medienrotationsstrategien sind "Sohn", "Vater/Sohn" und "Großvater/Vater/Sohn".
Mediensatz	Ein Satz von Regeln, die für Band- und Plattenkassettenmedien gelten, die mit einem Mediensatz verknüpft sind. Diese Regeln geben Anhänge-, Überschreibschutz- und Speicherzeiträume an.
Medienspeicher	Eine logische Darstellung des tatsächlichen physischen Speicherorts von Band- bzw. Plattenkassettenmedien, zum Beispiel ein spezieller Medienraum, ein temporärer Behälter oder ein Offsite-Speicherort.
Medienüberschreibschutzzeit	Eine globale Einstellung in Backup Exec, mit der Sie angeben können, ob temporäre, importierte oder zugeordnete Bandlaufwerkmedien unabhängig vom Überschreibschutzzeitraum überschrieben werden sollen.

Offhost-Backup	Eine Funktion von Backup Exec Advanced Disk-based Backup Option, mit der das Backup auf einem Backup Exec-Server anstelle auf dem Remote- oder Hostcomputer verarbeitet werden kann. Das Ausführen des Backup auf einen Backup Exec-Server anstatt auf einem Remote-Computer ermöglicht eine höhere Backup-Leistung und verringert die Last des Remote-Computers.
Offline-Bandkassettenspeicher	Ein Speicherort auf der Registerkarte "Speicher", auf der Band- und Plattenkassettenmedien angezeigt werden, die sich zwar vor Ort aber nicht in Bandlaufwerken, Wechslern oder Medienspeichern befinden. Medien werden automatisch in den Offline-Speicher verschoben, wenn Sie Backup Exec verwenden, um Medien aus einem Bandlaufwerk oder einem Wechsler zu entfernen.
Online-Bandkassettenspeicher	Ein Speicherort auf der Registerkarte "Speicher", auf der Band- und Plattenkassettenmedien angezeigt werden, die in Bandlaufwerken oder Wechslern verfügbar sind. Sie können keine Medien in Online-Medienpeicher verschieben oder dort hinzufügen. Dies erfolgt in Backup Exec automatisch.
Remote-Administrator	Die Benutzeroberfläche von Backup Exec (Administratorkonsole) auf dem Remote-Computer.
replizierter Katalog	Ein Katalogspeicherort in Central Admin Server Option. Alle Dateien im Katalog werden vom verwalteten Backup Exec-Server auf den zentralen Administrationsserver repliziert.
simulierte Bandbibliothek	Eine Bandbibliothek, die den Medientyp "Advanced Intelligent Tape (AIT)" emuliert, und die Bezeichnung "AIT" hat. Eine simulierte Bandbibliothek wird vom Tape Library Simulator erstellt.
Speichergerät	Festplattenspeicher-Gerät, Festplattenkassette, Wechslerlaufwerk, unabhängiges Laufwerk, virtuelles Laufwerk, Wechselspeicher-Laufwerk, Cloud-basiertes Speichergerät und andere von Backup Exec unterstützte Datenspeicher.
Speichergerätepool	Eine Gruppe ähnliche Typen von Speichergeräten, die die Lastverteilung von Backup Exec-Aufträgen ermöglichen.
Stufe	Eine zusätzliche Aufgabe, die Sie für einen Backup-Auftrag ausführen können, z. B. das Erstellen einer zusätzlichen Kopie der Backup-Daten auf einem Festplattenspeicher.
Synthetisches Backup	Eine Funktion der Advanced Disk-based Backup Option, die das Erstellen oder Synthetisieren eines vollständigen Backup aus einer Basis und folgenden inkrementellen Backups ermöglicht.
Tape Library Simulator	Ein Dienstprogramm, mit dem Sie ein virtuelles Gerät auf einer Festplatte oder einem bereitgestellten Datenträger auf einem Computer erstellen können, auf dem Backup Exec Remote Media Agent for Linux installiert ist. Das virtuelle Gerät ist eine "simulierte Bandbibliothek".

temporäre Medien	Bandkassettenmedien, die nicht mit einem Mediensatz verknüpft sind und überschrieben werden können. Zu temporärem Medien gehören neue und gelöschte Medien sowie solche, die aus einer anderen Gruppe verschoben wurden.
True Image-Wiederherstellung	Eine Funktion der Advanced Disk-based Backup Option, die es Backup Exec ermöglicht, den Inhalt von Verzeichnissen in den Zustand zum Zeitpunkt des vollständigen oder inkrementellen Backups wiederherzustellen. Die Wiederherstellungsauswahl wird in den Ansichten der Verzeichnisse getroffen, wie sie zur Zeit eines bestimmten Backup bestanden. Dateien, die vor dem Backup gelöscht wurden, können nicht wiederhergestellt werden. Bei der True Image-Wiederherstellung werden nur die korrekten Dateiversionen aus den entsprechenden vollständigen oder inkrementellen Backups, in denen sie enthalten sind, wiederhergestellt. Vorherige Versionen werden nicht wiederhergestellt und überschrieben, wenn sie nicht benötigt werden.
UMI (Unique Message Identifier)	Ein eindeutiger Code, der mit einem im Auftragsprotokoll gemeldeten Fehler oder bestimmten Warnmeldungen verknüpft ist. Diese Codes enthalten Hyperlinks, über die Sie die Website des technischen Supports aufrufen können. Dort finden Sie technische Hinweise und Tipps zur Fehlerbehebung, die mit einem bestimmten Fehler verknüpft sind.
Veralteter Backup-to-Disk-Ordner	Ein Speichergerät, das in Versionen vor Backup Exec 2012 zum Sichern von Daten auf einer Festplatte erstellt werden konnte. Unter höheren Versionen sind diese veralteten Backup-to-Disk-Ordner schreibgeschützt. Es wird empfohlen, dass Sie stattdessen Festplattenspeichergeräte verwenden.
verteilter Katalog	Ein Katalogspeicherort in Central Admin Server Option. Image-Dateien im Katalog werden aus jedem verwalteten Backup Exec-Server auf den zentralen Administrationsserver verteilt. Diese verteilten Dateien sind klein, weil sie nicht den gesamten Katalog enthalten. Sie enthalten nur Informationen über den Backup-Satz. Protokolldateien, die detaillierte Informationen zum Backup-Satz enthalten, verbleiben auf dem verwalteten Backup Exec-Server.
verwalteter Backup Exec-Server	Ein Backup Exec-Server, der von einem zentralen Administrationsserver verwaltet wird. Verwaltete Backup Exec-Server sind für die eigentliche Verarbeitung von Backup- und -Restore-Aufträgen in einer Central Admin Server Option-Umgebung verantwortlich. Verwaltete Backup Exec-Server sind nur mit Backup Exec Central Admin Server Option verfügbar.
Virtueller Datenträger	Ein logischer Datenträger, den Sie in einer Speichergruppe konfigurieren, um Speicher für den Backup Exec-Server zur Verfügung zu stellen.
vollständig	Eine Backup-Methode, die alle zum Sichern ausgewählten Dateien einschließt.
Warnmeldung	Ein Ereignis in Backup Exec, das normalerweise ein Eingreifen oder eine Bestätigung durch den Benutzer erfordert.

Warnmeldungskategorie	Eine Gruppe von Ereignissen, die in Backup Exec auftreten und die eine Warnmeldung generieren können. Beispiele für Warnmeldungskategorien: Auftragserfolg, Installationswarnung und Datenbankwartungsfehler.
Warnmeldungsquelle	Eine Quelle, die eine Warnmeldung erzeugen kann. Warnmeldungsquellen sind z. B. Aufträge, Medien, Speichergeräte und Computer.
Warnmeldungstyp	Die Klassifikation einer Warnmeldung, die den Schweregrad der Warnmeldung angibt. Warnmeldungstypen umfassen Fehler, Warnung, Informationen und "Eingreifen erforderlich".
wiederverwendbare Medien	Band- oder Plattenkassettenmedien, die einem Mediensatz zugewiesen sind, aber dessen Datenüberschreibschutzzeitraum abgelaufen ist.
Zentraler Administrationsserver	Ein Backup Exec-Server, auf dem Central Admin Server Option (CASO) installiert ist. In einer CASO-Umgebung dient der zentrale Administrationsserver der zentralen Verwaltung, der delegierten Auftragsverarbeitung und der Lastverteilung für verwaltete Backup Exec-Server.
zentralisierter Katalog	Ein Katalogspeicherort in Central Admin Server Option. Alle Dateien im Katalog sind auf dem zentralen Administrationsserver gespeichert.
Zugewiesene Medien	Die Bandkassettenmedien, die mit einem Mediensatz verknüpft sind und die aktuelle Anhänge- und Überschreibschutz-Zeiträume haben.
Überschreibschutzzeitraum	Gibt an, wie lange Daten auf einem bestimmten Bandmedium beibehalten werden, bevor sie überschrieben werden (es sei denn, das Medium wird gelöscht, formatiert, auf ein temporäres Medium verschoben oder wenn die Medienüberschreibschutzstufe auf "Keine" eingestellt ist). Der Überschreibschutzzeitraum wird von dem Datum an gemessen, an dem zuletzt Daten auf dem Medium gespeichert wurden.
Überwachungsprotokoll	Ein laufender Verlauf aller Aktionen, die in Backup Exec ausgeführt werden. Ein Eintrag im Protokoll wird erstellt, wenn eine Aktion auftritt, die entsprechend konfiguriert ist.

Index

Symbole

48, 1159

"Agent for Hyper-V"
Sichern 1167

A

Abgeschlossene Aufträge
Status 322

Abschnitt 508 des Rehabilitation Act
Compliance 1628

Active Directory
Backup in Exchange 1286

Administratorkonsole
Rolle im Backup-Prozess 41
Überblick 130

Advanced Disk Based Backup Feature
Basis
Einrichten 1520
Best Practices für Offhost-Backups 1529, 1532
Host-Computer
Definiert 1527
Offhost-Backup - Überblick 1527
Optionen für Offhost-Backups 1524, 1532
Standardoptionen einstellen 1522
True Image-Wiederherstellung
Überblick 1524
Übertragbare Snapshots
Definiert 1527

Advanced Disk-based Backup Feature
Info 1519

Advanced Open File
Optionen für Backup-Aufträge konfigurieren 664

Agent for Hyper-V
Agent for Windows installieren 1165
Anforderungen 1156
Byteanzahl für vollständige Katalogisierung
berechnen 1186
Hinzufügen eines Hyper-V-Hosts 1163
Infos zum Entfernen eines sofort
wiederhergestellten virtuellen Computers 1203
Installationsübersicht 1159

Instant GRT 1185
mit GRT- und VHDX-Dateien 1159
Push-Installation von Agent for Windows 1166
Schutz von Microsoft-Anwendungsdaten 1180
Standard-Backup-Optionen festlegen 1175
Überblick 1154
und GRT 1180
Virtuelle Computer mit hoher Verfügbarkeit 1184
Vollständige Katalogisierung 1185
Wiederherstellen 1187

Agent for Linux

Agent for Linux-Daemon beenden 1590
Agent for Linux-Daemon starten 1589
Anforderungen 1560
Ausschluss vom Backup 1569
beoper-Gruppe erstellen 1565
beoper-Gruppe, definiert 1565
Bereitstellen von Informationen auf Backup
Exec-Servern 1567
Datei "ralus.cfg" konfigurieren 1568
Deinstallieren 1586
Fehlerbehebung 1590
Festlegen von Vertrauen 1566
Info zu Vertrauenseinstellungen 1031
Info zum Sichern 1578
Installationsprotokoll speichern 1562
installieren 1562
Konfigurationsoptionen in der Datei
"ralus.cfg" 1570
Konfigurationsoptionen in der Datei "ralus.cfg"
bearbeiten 1570
Laufzeitskripte 1588
Manuell deinstallieren 1587
Novell OES, Anforderungen für Backup 1581
Optionen für Backup-Aufträge 1579
Optionen für Wiederherstellungsaufträge 1582
Push-Installation 1561
Sichern von Novell OES-Komponenten 1580
Standardoptionen 1584
Standardoptionen bearbeiten 1584
Unter Verwendung von SSH 1561
Wiederherstellen 1582

- Agent for Microsoft Active Directory
 - Anforderungen 1440
 - Bereinigte Objekte neu erstellen 1446
 - Granular Recovery Technology (GRT)
 - Überblick 1441
 - Info zu 1439
 - Infos zum Wiederherstellen von einzelnen Objekten 1446
 - Kennwörter 1447
 - Tombstones 1446
- Agent for Microsoft SharePoint
 - Anforderungen 1319
 - Einsatz mit SharePoint Server 2010/2013/2016 und SharePoint Foundation 2010/2013/2016 1320
 - Info 1318
 - Installieren 1319
 - Kommunikation zwischen Webservern und Backup Exec deaktivieren oder aktivieren 1332
 - Notfallwiederherstellung für SharePoint 2010/2013/2016 1334
 - Serverfarm hinzufügen 1321
 - Systemanforderungen 1319
 - Überblick 1318
 - Wiederherstellen von SharePoint -Ressourcen 1329
- Agent for VMware
 - Agent for Windows installieren 1094
 - Anforderungen 1090
 - Auswahl der Transportmethode für VMDK-Datei 1107, 1113
 - Backup-Standardeinstellungen 1109
 - Dynamische Einbeziehung 1115
 - Granular Recovery Technology
 - Info 1115
 - GRT-Anforderungen 1115
 - Installieren 1092
 - Microsoft-Anwendungsdaten sichern 1115
 - nicht unterstützte GRT-Konfigurationen 1115
 - nicht unterstützte Zeichen 1090
 - Ressourcen wiederherstellen 1121
 - Sichern 1100
 - Überblick 1089
 - Überblick über die Sofortwiederherstellung 1131
 - VMware vCenter- und ESX-/ESXi-Hosts hinzufügen 1092
- Agent for Windows
 - 1096
 - Anforderungen 1029
 - Anhalten und starten 1030
 - Auf virtuellen Computern installieren 1094
 - Auf virtuellen Hyper-V-Computern installieren 1165
 - Backup Exec Agent Utility 1031
 - Deinstallation mit Befehlsskript 96
 - Hardwarevoraussetzungen 1029
 - In einem Active Directory-Netzwerk installieren 87
 - In einem Microsoft-Cluster installieren 917
 - Info 1028
 - Info zu Vertrauenseinstellungen 1031
 - Informationen auf Backup Exec-Servern bereitstellen 1035
 - Installation mit Befehlsskript 95
 - Installationsmethoden 77
 - Lizenzen 1029
 - Push-Installation auf Remote-Computern 78
 - Push-Installation auf virtuellen Hyper-V-Computern 1166
 - Über Eingabeaufforderung deinstallieren 94
 - Über Eingabeaufforderung installieren 92
 - Updates installieren 84
- Agent für Hyper-V
 - Details zu Ressourcen anzeigen 1164
- Agent für Microsoft SharePoint
 - sichert SharePoint-Daten 1322
- Agents
 - Upgrade durchführen 121
- Aktive Aufträge
 - Abbrechen 291
 - Anhalten 292
 - Anhalten aufheben 294
 - Anzeigen der Eigenschaften 290
 - Auftragsaktivität anzeigen 290
 - Info zum Verwalten und Überwachen 286
 - Status 322
- Aktive Meldungen
 - Reagieren auf 343
- Aktuelle Backup Exec-Gerätetreiber 449
- Alternativer Speicherort
 - SDR einrichten 954
- Amazon-Cloud-Speicher
 - Konfigurieren 412
- Anforderungen
 - Agent for Hyper-V 1156
 - Backup Exec 51
 - Benutzerrechte für Backup-Aufträge 165
 - Central Admin Server Feature 1452

- Exchange Agent 1268
- Konvertierung in virtuelle Computer 590
- NDMP Feature 1539
- Off-Host-Backup 1528
- Remote Media Agent for Linux 1600
- Synthetisches Backup 1521
- Anforderungen für Granular Recovery Technology
 - Anforderungen für VMware 1115
- Anhängezeitraum
 - Ändern 485
 - Bearbeiten 483
 - Definiert 476
- Anzeigen von Informationen in der
 - Administratorkonsole 139
- Archivbit
 - Zur Ermittlung des Backup-Status verwenden 219
- Assistent "Computer wiederherstellen"
 - Anforderungen 987
 - ausführen 987
- Assistent für die Installation der Gerätetreiber 449
- Aufträge
 - Abbrechen 291
 - Ändern der Priorität für geplante 297
 - Anhalten 292
 - Anhalten aufheben 294
 - Anhalten der Auftragswarteschlange aufheben 296
 - Auftragsprotokoll anzeigen 308
 - Auftragswarteschlange anhalten 295
 - Aus Auftragsverlauf löschen 304
 - Ausführen eines geplanten Auftrags 297
 - Fehlerbehandlungsregeln konfigurieren 317
 - Feiertage planen 688, 691
 - Löschen von geplanten 299
 - Nur fehlgeschlagene wiederholen 300
 - Senden einer Benachrichtigung, wenn abgeschlossen 357
 - Status- und Wiederherstellungsoptionen festlegen 330
 - über Auftragsverlauf ausführen 305
 - Verwalten und Überwachen 286
- Auftragsaktivität 290
- Auftragsfortschrittsanzeigen
 - anzeigen 693
- Auftragsprotokoll 308
 - Anzeigen aus einer Warnmeldung 343
 - drucken 311
 - Konfigurieren von Standardoptionen 314
 - Mit vertikalen Anwendungen 314
 - Speichern 312
 - Text suchen 309
 - Verknüpfung zur Website des technischen Supports erstellen 313
- Auftragsstandardeinstellungen
 - Ändern 630
 - mehrere Server oder Anwendungen sichern 693
- Auftragsstandards
 - Auswählen ausschließen 195
 - Backup-Aufträge 630
 - Tage ausschließen 688
 - Zeitplan für richtliniengesteuerte und für Aufträge zum sofortigen Ausführen 685
- Auftragsstatus 322
- Auftragsstatus und -wiederherstellung 330
- Auftragsüberwachung 286, 289
- Auftragsverlauf 289
 - Anzeigen 303
 - Auftrag ausführen 305
 - Aufträge löschen 304
 - duplizieren 249
 - Info zum Überprüfen 252
 - Infos zur Duplizierung 246
 - Nur fehlgeschlagene Aufträge wiederholen 306
 - Überblick 302
 - überprüfen 253
- Auftragsvorlage
 - Definiert 174
- Auftragswarteschlange
 - anhalten 295
 - Anhalten aufheben 296
- Auftragswiederaufnahme
 - Erwägungen 669
 - Info 667
 - Konfigurieren 667
 - Standardeinstellungen konfigurieren 669
 - Unterstützte Funktionen 668
- Ausführen eines Befehls
 - Nach dem Backup 673
 - Vor dem Backup 673
- Ausrangierte Medien
 - Definiert 474
 - Verschieben beschädigter Medien 501
- Ausschließen aktiver Dateien 1290
- Auswerfen von Medien 555
 - Nach Auftragsabschluss 650

- Auszuschließende Tage
 - Auswählen von Tagen für einzelne Backup-Aufträge 242
 - Tage auf anderen Server exportieren 691
 - Tage löschen 690
- Automatischer Ausschluss von SQL-Daten bei Backups auf Datenträgerebene 1228
- Automatisches Zurückfordern von Speicherplatz 393

B

- Backup
 - erstellen 174
 - Überblick 174
 - Verwenden des Remote Media Agent for Linux 1618
 - Virtuelle VMware-Computer 1100
- Backup auf einem anderen Host
 - Empfohlene Verfahren 1529, 1532
 - Übertragbare Snapshots
 - Definiert 1527
- Backup Exec
 - Konsole sperren 134
 - Konsole sperren und freigeben 134
 - Überblick
 - Funktionsweise 40
- Backup Exec Agent Utility
 - Aktivitätsstatus
 - Anzeigen 1033
 - Aktualisierungsintervall
 - Festlegen 1034
 - Anmeldedaten für Linux-Instanzen
 - aktualisieren 1354
 - Auftragsvorlagenname für DBA-initiierte Aufträge 1355
 - Automatisch starten 1034
 - Befehlszeilen-Applet 1041
 - Parameter 1042
 - Verwenden 1041
 - Datenbankzugriff
 - Konfiguration 1038
 - Dienste
 - Öffnen 1031
 - Ereignisanzeige
 - Öffnen 1031
 - Informationen auf Backup Exec-Servern bereitstellen 1035
 - Informationen bereitstellen
 - Backup Exec-Server entfernen 1038

- Backup Exec-Serverinformationen
 - bearbeiten 1037
- Linux
 - Oracle-Instanz konfigurieren 1358
- Port
 - Für Oracle-Vorgänge konfigurieren 1359
- Real Application Cluster (RAC)
 - Auf Backup Exec-Server bereitstellen 1353
- Registrierungseditor
 - Öffnen 1031
- Sicherheit
 - Zertifikat entfernen 1040
- Starten 1032
- Status anzeigen 1033
- Veröffentlichen
 - Backup Exec-Server hinzufügen 1036
- Windows
 - Oracle-Instanz konfigurieren 1351
- Backup Exec Migrator
 - Abrufen von Enterprise Vault-Daten 1433
 - Anforderungen 1413
 - Backup Exec-Server
 - Funktionieren mit 1425
 - Best Practices 1436
 - Datenmigrationsvorgang 1414
 - Enterprise Vault-Aufbewahrungszeiträume 1422
 - Ereignisse
 - Info 1418
 - Fehlerbehebung 1437
 - Funktionsweise 1414
 - Info 1413
 - Info zu gestaffelten Migrationen 1417
 - Info zum Abrufen von Enterprise Vault-Daten 1432
 - Info zur Backup Exec-Ansicht
 - "Backup-Sätze" 1431
 - Konfiguration 1423
 - Migrierte Dateien
 - Informationen zum Löschen 1422
 - mit Enterprise Vault kommunizieren 1428
 - Optionen von Migrator for Enterprise Vault 1427
 - Protokolle
 - Informationen 1418
 - Speicherort der Protokolldatei 1419
- Backup Exec Services
 - Anhalten und starten 776
- Backup Exec-Diagnoseanwendung
 - generieren 904

- Backup Exec-Dienste
 - Dienstkonto-Identifikationsdaten ändern 777
 - Startoptionen ändern 778
- Backup Exec-Einstellungen
 - Daten für Backup suchen 708
 - Datenbankverwaltung und -sicherheit 694
 - DBA-initiierte Aufträge 746
 - Einstellungen ändern 692
 - Konfigurieren der Einstellungen für Veritas™ Information Map 759
 - Netzwerk und Sicherheit 713
 - Optionen für Granular Recovery Technology (GRT) 744
- Backup Exec-Server 41
 - Eigenschaften anzeigen 783
- Backup mit Agent 1098
- Backup- oder Wiederherstellungsauftrag
 - Debugging aktiviert 301, 307
- Backup-Auftrag
 - Aus vorhandener Backup-Definition erstellen 177
 - Auswahl einschließen 198
 - Auswahlen ausschließen 195
 - Auswahlen global ausschließen 195
 - Bearbeiten 226
 - Befehle vor/nach dem Auftrag 670
 - Daten auswählen 186
 - Deduplizierung 1079
 - einmalig 174
 - erforderliche Benutzerrechte 165
 - erstellen 174, 177
 - Nächste geplante Instanz ausführen 225
 - Vorbereiten 155
- Backup-Auswahl
 - Info 186
 - Mehrfache Server oder Anwendungen 190
 - Reihenfolge ändern 192
 - Vollständig qualifizierte Domännennamen verwenden 192
 - Wichtige Systemkomponenten 190
- Backup-Definition
 - Aus vorhandener Backup-Definition erstellen 177
 - Auswahl einschließen 198
 - Auswahlen ausschließen 195
 - Bearbeiten 226
 - Daten auswählen 186
 - definiert 174
 - einmalig 174
 - erstellen 174, 177
- Backup-Methoden
 - Ausgewählte Dateien und Ordner nach erfolgreichem Backup löschen 222
 - Bestimmte Datentypen 212
 - Differenziell 207
 - Duplizieren 206
 - Info zu 205
 - Inkrementell 208
 - Konfigurieren 215
 - Vollständig 206
 - Vorteile und Nachteile 208
- Backup-Netzwerk
 - Überblick 711
- Backup-Sätze
 - Ablaufdatum 404
 - Ablaufdatum ändern 404
 - Ablaufen verhindern 406
 - Aufbewahrenen 406
 - automatisch abgelaufene löschen 393
 - duplizieren 247
 - Eigenschaften anzeigen 408
 - Info 401
 - Info zum Duplizieren 246
 - Info zum Überprüfen 252
 - Inhalt anzeigen 408
 - katalogisieren 284
 - Nach Aufbewahrung freigeben 407
 - überprüfen 253
- Backup-Strategien
 - Erhöhen der Leistungswerte mit Agent for Windows 1029
- Backup-to-Disk-Ordner
 - Als schreibgeschützter veralteter Speicher 439
 - Importieren 443
 - Mit Simplified Disaster Recovery wiederherstellen 439
 - Neu erstellen 442
 - Speicherort ändern 441
- Backups auf Datenträgerebene
 - Automatischer Ausschluss von SQL-Daten 1228
- Bänder
 - DLT-Bandlaufwerk 883
- Bandlaufwerke
 - Puffergröße 454
 - Pufferzahl 454
 - Schwellenwert 455
 - Standardeinstellungen 455
 - Statistiken 457

- Bandmedien
 - beschädigt 501
 - löschen 502
 - Mit außergewöhnlich vielen Fehlern 501
 - Scannen von Barcode-Kennungen 501
 - Verknüpfen mit einem Mediensatz oder einem Speicher 505
- Bandmedien kennzeichnen
 - Umbenennen 495
- Bandmedienkennung
 - Barcodes 494
 - importiert 494
 - Überblick 492
 - Umbenennen 495
- Bandmedienvorgänge
 - Verknüpfen von Medien mit Mediensätzen 505
- Barcode-Kennungen
 - Überblick 494
- Barcode-Medien, Suchen in Laufwerken und Portalen 549
- Barcodekennungen
 - Standard 494
 - Wechsler-support 494
- Basis-Backup
 - Einstellung für synthetisches Backup 1520
- Befehl nach dem Auftrag
 - Backup-Aufträge 670
 - Für Backup-Auftrag festlegen 673
 - Konfigurieren 672
- Befehl vor dem Auftrag
 - Backup-Aufträge 670
 - Für Backup-Auftrag festlegen 673
 - Konfigurieren 672
- Befehlszeile
 - Backup Exec installieren 103
 - Remote Administrator installieren 98
 - Switches für Installation 104
- Benachrichtigung
 - aktivieren 348
 - Beenden 358
 - Einrichten 344
 - Empfänger aus Gruppe entfernen 351
 - Empfängereigenschaften bearbeiten 353
 - Für abgeschlossene Aufträge senden 357
 - Gruppenempfänger konfigurieren 351
 - konfigurieren 345
- Benachrichtigung per SMS
 - Konfigurieren 345
- Benachrichtigungen
 - Überblick 334
- Benutzerdefinierte Fehlerbehandlungsregel für wiederhergestellte Aufträge 317
- beoper-Gruppe
 - Agent forLinux, Info 1565
 - erstellen 1565
- Bericht "Auftragszusammenfassung" 832
- Bericht "Backup-Empfehlungen" 822
- Bericht "Backup-Sätze nach Mediensatz" 823
- Bericht "Backup-Umfang nach Ressourcen geordnet" 824
- Bericht "Cloud-Speicherübersicht" 824
- Bericht "Ereignisempfänger" 830
- Bericht "Erfolgsrate des Backups von Ressourcen" 822
- Bericht "Erfolgsrate von Backup-Aufträgen" 821
- Bericht "Fehlerbehandlungsregeln" 829
- Bericht "Fehlgeschlagene Backup-Aufträge" 831
- Bericht "Für Wiederherstellung erforderliche Medien" 836
- Bericht "Geplante Serverarbeitslast" 848
- Bericht "Gerätezusammenfassung" 827
- Bericht "Kürzlich geschützte Ressourcen" 844
- Bericht "Medien zum Speicher verschieben" 838
- Bericht "Medienfehler" 835
- Bericht "Medienspeicherinhalt" 837
- Bericht "Medienüberwachung" 834
- Bericht "Medienzusammenfassung" 836
- Bericht "Medium aus Speicher abrufen" 846
- Bericht "Meldungsverlauf" 819
- Bericht "Nächtliche Zusammenfassung" 841
- Bericht "Probelaufergebnisse" 849
- Bericht "Problemdateien" 842
- Bericht "Ressourcenrisikoanalyse" 845
- Bericht "Täglicher Geräteinsatz" 825
- Bericht "Überwachungsprotokoll" 821
- Bericht "Verfügbarkeit temporärer Medien" 849
- Bericht "Verwaltete Backup Exec-Server" 833
- Bericht "Vorgangsübersicht" 839
- Bericht "Warnmeldungsverlauf nach Backup Exec-Server" 820
- Bericht "Wechslerinventar" 847
- Bericht "Wiederherstellungssatz-Details nach Ressource" 845
- Bericht "Zusammenfassung zu Deduplizierungsgeräten" 826
- Bericht "Zusammenfassung zum Datenträgerspeicher" 828

- Bericht "Zusammenfassung zur Deduplizierung" 827
 - Bericht zum Migrationsabschluss 125
 - Berichte
 - Abgeschlossenen Bericht erneut ausführen 810
 - Anzeigen abgeschlossener 810
 - Anzeigen der Eigenschaften 813
 - Auftragszusammenfassung 832
 - Ausführung 794
 - Backup-Sätze nach Mediensatz 823
 - Backup-Umfang nach Ressourcen geordnet 824
 - Bearbeiten 810
 - Benutzerdefiniert
 - Diagrammoptionen ändern 806
 - Vorschauansicht 807
 - benutzerdefiniert
 - Gruppierung oder Sortierung ändern 805
 - Benutzerdefiniert erstellen 796
 - Benutzerdefiniert, Ändern der Filter 802
 - Benutzerdefinierte Berichte kopieren 807
 - Cloud-Speicherübersicht 824
 - drucken 809
 - Ereignisempfänger 830
 - Erfolgsrate des Backups von Ressourcen 822
 - Erfolgsrate von Backup-Aufträgen 821
 - Fehlerbehandlungsregeln 829
 - Fehlgeschlagene Backup-Aufträge 831
 - Für Wiederherstellung erforderliche Medien 836
 - Geplante Serverarbeitslast 848
 - Gerätezusammenfassung 827
 - Kürzlich beschriebene Medien 842
 - Kürzlich geschützte Ressourcen 844
 - Liste von Standardberichten 814
 - löschen 811
 - Medien zum Speicher verschieben 838
 - Medienfehler 835
 - Medienspeicherinhalt 837
 - Medienübersicht 836
 - Medienüberwachung 834
 - Medium aus Speicher abrufen 846
 - Nächtliche Zusammenfassung 841
 - Planen 794
 - Probelaufergebnisse 849
 - Problemdateien 842
 - Ressourcenrisikoanalyse 845
 - Speichern 808
 - Standards festlegen 811
 - Täglicher Geräteeinsatz 825
 - Überblick 792
 - Übersicht zu Deduplizierungsgeräten 826
 - Überwachungsprotokoll 821
 - Verfügbarkeit temporärer Medien 849
 - Verwaltete Backup Exec-Server 833
 - Vorgangsübersicht 839
 - Warnmeldungsverlauf 819
 - Warnmeldungsverlauf nach Backup Exec-Server 820
 - Wechslerinventar 847
 - Wiederherstellung bereit (Validierungsübersicht) 843
 - Wiederherstellungssatz-Details nach Ressource 845
 - Zusammenfassung zum Datenträgerspeicher 828
 - Zusammenfassung zur Deduplizierung 827
 - berichte
 - Backup-Empfehlungen 822
 - beschädigte Bandmedien
 - ausrangieren 501
 - Bevorzugte Konfigurationseinstellungen des Standards für Bandlaufwerke 455
 - Bevorzugte Serverkonfigurationen für Austausch DAGs
 - Als Standard entfernen 1281
 - Als Standard festlegen 1280
 - Info 1279–1280
 - Boot-Manager
 - Wiederherstellen in SDR 987
 - Byteanzahl
 - Falsch 891
 - Für Katalogisierung berechnen 1186
- ## C
- ### CAS
- Aktualisieren 1466
 - Anforderungen 1452
 - Angehaltenen verwalteten Backup Exec-Server wiederaufnehmen 1507
 - Auftragsdelegierung 1495
 - Backup Exec Utility
 - Ausführen 1516
 - Backup Exec vom verwalteten Backup Exec-Server deinstallieren 1518
 - Backup Exec vom zentralen Administrationsserver deinstallieren 1517
 - Backup Exec-Dienste beenden 1508
 - Backup Exec-Dienste starten 1508
 - Backup Exec-Server
 - In einen verwalteten Backup Exec-Server umwandeln 1469

- Backup Exec-Server-Pool
 - Auswahl für Backup 1499
 - Erstellen 1500
 - Löschen 1501
 - Überblick 1498
 - Verwaltete Backup Exec-Server entfernen 1501
 - Verwaltete Backup Exec-Server hinzufügen 1500
- Benachrichtigungen 1493
- Daten aus mehreren Geräten wiederherstellen 1503
- Einstellungen für verwaltete Backup Exec-Server 1479
- Fehlerbehebung 1515
- In zentralen Administrationsserver umwandeln 1468
- Installieren 1455
- Installieren des verwalteten Backup Exec-Servers 1456
- Installieren über eine Firewall 1463
- Katalogspeicherorte 1476
- Löschen eines verwalteten Backup Exec-Servers 1472
- Netzwerkkarten
 - Verfügbare verwenden 1494
- Netzwerkverkehr
 - Reduzieren 1475
- Notfallwiederherstellung 1513
- Schwellenwerte für die Kommunikation 1491
- Speicher- und Mediendaten 1453
- Status 1491
- Überblick 1450
- Verbindungen aktivieren 1492
- Verbindungen deaktivieren 1492
- Verwalteten Backup Exec-Server anhalten 1507
- Verwalteter Backup Exec-Server
 - Eigenschaften anzeigen 1508
 - Konfigurationsoptionen 1461
- Warnmeldungen 1493
- Wiederherstellen fehlgeschlagener Aufträge 1504
- Zentraler Administrationsserver
 - Für einen verwalteten Backup Exec-Server festlegen 1469
- Zentralisierte Wiederherstellung
 - Mehrere Speichergeräte 1502
 - Überblick 1501
- CHECKCATALOG-Dienstprogramm 1224
- CHECKDB-Dienstprogramm 1224

- Checkliste vor dem Upgrade 124
- Checkliste vor der Installation 46
- Client-seitige Deduplizierung
 - Überblick 1078
- CloudConnect Optimizer
 - Auftrag bearbeiten 436
 - Auftrag konfigurieren 435
 - Auftrag löschen 437
 - Info 434
- Cluster
 - Fehlerbehebung 940
 - Microsoft 922
 - Alle Laufwerkpools 920
 - Ändern der Failover-Reihenfolge der Knoten 920
 - BEUtility 922
 - Deinstallieren von Backup Exec 919
 - Failover-Neustart 914
 - Hinzufügen oder Entfernen eines Failover-Knotens 920
 - Installation 916, 918
 - Konfigurationen 923–925, 927, 929
 - Notfallwiederherstellung 938
 - Notfallwiederherstellung von Backup Exec in einem Cluster mithilfe von SDR 936
 - Überblick 932
 - Notfallwiederherstellung 933
 - Gesamter Cluster manuell 937
 - Knoten mithilfe von SDR 935
 - SDR zur Vorbereitung verwenden 934
 - Verwendung mit Backup Exec 912

D

- Data Lifecycle Management, Übersicht 393
- Datei- und Ordneroptionen
 - für Backup-Aufträge konfigurieren 676
- Dateien
 - Ein- und Ausschließen für NDMP-Server 1547
- Dateien der virtuellen Festplatte von Microsoft
 - Verwalten 185
- Dateiverlauf
 - Für NDMP Feature aktivieren 1554
- Daten ausschließen
 - Importieren einer Liste von Daten 688
- Daten für Backup suchen
 - Info 708
 - Konfigurieren 708
 - Server hinzufügen 708

- Datenbank-Snapshots
 - SQL 1241, 1254
- Datenbankserver
 - In Microsoft-Clustern 922
- Datenbankverwaltung und -sicherheit
 - Info 694
- Datenbankwartung und -Sicherheit
 - Konfigurieren 694
- Datenträgerspeicher
 - Eigenschaften bearbeiten 376
- Datenverbindung zu Remote-Computern 1599
- DBA gestartete Aufträge
 - Erstellen einer Vorlage 746
 - Vorlage löschen 748
- DBA-initiierte Aufträge
 - allgemeine Optionen 753
 - Duplizierungs-Auftrags-Einstellungen 755
 - Netzwerkoptionen 753
 - Speicheroptionen 748
 - Vorlagen 746
- Debug-Monitor 910
- Debugging aktiviert
 - Backup- oder Wiederherstellungsauftrag 301, 307
- Deduplication Feature
 - Anforderungen 1051
 - Clientseitige Deduplizierung (Überblick) 1078
 - Daten zwischen OpenStorage- oder Deduplizierungsspeichergeräten kopieren 1080
 - Deduplizierungsmethoden für Agents 1049
 - Deduplizierungsspeichereigenschaften 1067
 - Direktzugriff
 - Eigenschaften bearbeiten 1074
 - Speichergeräte wählen 1073
 - Geräte gemeinsam nutzen 1077
 - Info zum Kopieren von deduplizierten Daten auf Bänder 1084
 - Info zum Sichern 1079
 - Installieren 1056
 - Login-Kontokennwort für Deduplizierungsspeicher ändern 1072
 - Mit Verschlüsselung 1084
 - Notfallwiederherstellung des Deduplizierungsspeichers 1085
 - Notfallwiederherstellung von OpenStorage-Geräten 1087
 - OpenStorage-Gerät, Überblick 1058
 - OpenStorage-Geräteeigenschaften 1061
 - Überblick 1047
 - Überblick über Deduplizierungsspeicher 1064
 - Wiederherstellen eines Deduplizierungs-Plattenspeichergeräts 1085
- Deduplizierung
 - Windows 184
- Deduplizierungdatenträgerspeicher
 - Überblick 1064
- Deduplizierungdatenträgerspeichergeräte
 - Eigenschaften bearbeiten 1067
- Deduplizierungs-Plattenspeichergeräte
 - Wiederherstellen 1085
- Deduplizierungsspeicher
 - Ändern des Login-Konto-Kennwort 1072
- Deduplizierungsspeichergeräte
 - Anforderungen 1051
 - Notfallwiederherstellung 1085
- Deinstallation
 - Backup Exec 127
 - Backup Exec-Funktionen vom lokalen Backup Exec-Server 128
 - Befehlszeile 128
- Deinstallieren
 - Backup Exec von einem Microsoft-Cluster 919
- Diagnosedatei
 - Befehlszeilenparameter 906
- Dialogfelder mit Registerkarten
 - Navigation 1656
- Dienste
 - Dienstkonto-Identifikationsdaten ändern 777
 - Starten und anhalten 776
 - Startoptionen ändern 778
- Dienstkonto
 - Identifikationsdaten ändern 777
- Dienstprogramm zum Wiederherstellen von Partitionen
 - Anforderungen 1434
 - Archiv-ID suchen 1434
 - Ausführen 1435
 - Fehlerbehebung 1437
 - Info 1433
 - Protokolle
 - Informationen 1418
 - Speicherort der Protokolldatei 1419
- Dienstprogrammpartitionen
 - Wiederherstellen 275
- Differenzielle Backups
 - Info 207
 - Vorteile und Nachteile 210

- DirectCopy auf Band
 - Kopieren von Daten 255
 - Überblick 255
- Direktzugriff
 - Eigenschaften bearbeiten 1074
 - Speichergeräte wählen 1073
- DLT-Band
 - Laufwerk blockiert bei Katalogisierung 883
- Domänencontroller
 - Installation durch umgeleitete
 - Wiederherstellung 272
 - Systemstatus wiederherstellen 270
- Duplizierung zwischen OpenStorage-Geräten oder
 - Deduplizierungdatenträgerspeichergeräten 1080
- dynamische Einbeziehung
 - für Hyper-V 1179

E

- E-Mail-Benachrichtigung
 - konfigurieren 345
- egisterkarte "Startseite"
 - Konfigurieren 139
- Eigenschaften
 - Aktiver Auftrag 290
- Eigenschaften des lokalen Servers
 - Anzeigen, Info 783
 - Eigenschaften anzeigen 783
- Eingabeaufforderung
 - Agent for Windows deinstallieren 94
- Eingabehilfe
 - Tastaturkurzbefehle
 - Registerkarte "Berichte" 1653
 - Registerkarte "Speicher" 1644
 - Registerkarte "Startseite" 1630
- Eingabehilfen
 - Dialogfelder 1655
 - Einstellungen 1657
 - Tastaturkurzbefehle 1629
 - Registerkarte "Backup und
 - Wiederherstellung" 1631
 - Registerkarte "Backup und
 - Wiederherstellung" für die
 - Anmeldedatenansicht 1639
 - Registerkarte "Backup und
 - Wiederherstellung" für die Ansicht der
 - aktiven Warnmeldungen 1638
 - Registerkarte "Backup und
 - Wiederherstellung" für die
 - Auftragsansicht 1634

- Registerkarte "Backup und
 - Wiederherstellung" für die
 - Auftragsverlaufsansicht 1635
- Registerkarte "Backup und
 - Wiederherstellung" für die
 - Backup-Satz-Ansicht 1637
- Registerkarte "Speicher" für die Ansicht der
 - aktiven Warnmeldungen 1653
- Registerkarte "Speicher" für die
 - Auftragsansicht 1648
- Registerkarte "Speicher" für die
 - Auftragsverlaufsansicht 1650
- Registerkarte "Speicher" für die
 - Backup-Satz-Ansicht 1651
- Tastaturnavigation 1654
- Tastenkombinationen
 - Auftragsüberwachung 1640
- Überblick 1628
- Eingeschränkte Login-Konten
 - Info 765
- Eingeschränkte Verschlüsselungscodes
 - Definiert 730
- Einmalige Konvertierung in virtuellen Computer 616
- Einschließen von Tagen
 - Erstellen 240
- Einzelblockmodus
 - Einstellung für Bandlaufwerke 455
- Empfänger
 - aus Gruppe entfernen 351
 - Bearbeiten 353
 - Benachrichtigung beenden 358
 - E-Mails und Textmeldungen aktivieren 348
 - Gruppen konfigurieren 351
 - Löschen 353
- Enterprise Vault Agent
 - Anforderungen 1392
 - Auswählen einer Backup-Methode 1393
 - Automatische Umleitung von Enterprise
 - Vault-Komponenten 1407
 - Backup Exec Migrator
 - Abrufen von Enterprise Vault-Daten 1433
 - Anforderungen 1413
 - Best Practices 1436
 - Datenmigrationsvorgang 1414
 - Enterprise
 - Vault-Aufbewahrungszeiträume 1422
 - Fehlerbehebung 1437
 - Funktionieren mit einem Backup
 - Exec-Server 1425

- Funktionsweise 1414
- Info 1413
- Info zu gestaffelten Migrationen 1417
- Info zum Abrufen von Enterprise
 - Vault-Daten 1432
- Info zur Backup Exec-Ansicht
 - "Backup-Sätze" 1431
- Informationen zu Ereignissen 1418
- Konfiguration 1423
- Löschen der migrierten Dateien 1422
- Mit Enterprise Vault kommunizieren 1428
- Optionen von Migrator for Enterprise
 - Vault 1427
- Protokolle, Informationen 1418
- Speicherort der Protokolldatei 1419
- VxBSA-Protokolle 1418
- Backup Exec-Server
 - Protokolle 1418
 - Speicherort der Protokolldatei 1419
- Best Practices 1412
- Betriebsbereiter Zustand 1400
- Dienstprogramm zum Wiederherstellen von Partitionen
 - Anforderungen 1434
 - Ausführen 1435
 - Fehlerbehebung 1437
 - Info 1433
 - Protokolle 1418
 - Speicherort der Protokolldatei 1419
 - Suchen einer Archiv-ID 1434
- Info zum Wiederherstellen einzelner Dateien und Ordner 1406
- Informationen zum Umleiten eines Wiederherstellungsjobs 1408
- Informationen zum Wiederherstellen 1400
- Installieren 1392
- Migration
 - Eigenschaften der Speicherpartition 1430
- Nicht betriebsbereiter Zustand 1400
- Sammlungen
 - Eigenschaften der Speicherpartition 1424
 - Konfiguration 1424
- Umleitungsoptionen 1409
- Verfügbare Backup-Methoden 1395
- Wiederherstellungsoptionen 1402
- Eröffnungsbildschirm
 - Beim Starten anzeigen 693
- ESX-/ESXi-Host hinzufügen 1092
- Exchange Agent
 - Active Directory
 - sichern 1286
 - Anforderungen 1268
 - Ausschließlich Dateien bei Backups auf Datenträgerebene 1290
 - Automatischer Ausschluss von Dateien bei Backups auf Datenträgerebene 1290
 - Backup auf einem anderen Host
 - Mit Granular Recovery Technology (GRT) 1287
 - Backup-Methoden 1297, 1300, 1306, 1308
 - Backup-Strategien 1284
 - Backups auf Datenträgerebene
 - Automatisches Ausschließen von Dateien 1290
 - Daten umleiten 1309
 - Datenbanken
 - Konfiguration 1309
 - Datenbankverfügbarkeitsgruppe 1294
 - Dienstkonto 1268
 - einzelne Meldungen aus dem öffentlichen Ordner vom Band wiederherstellen 1309
 - Empfohlene Verfahren 1281
 - Exchange in einer Datenbankverfügbarkeitsgruppe 1304
 - Exchange-Web-Dienste
 - Überblick 1287
 - Fehlerbehebung für Snapshot-Aufträge und Aufträge auf einem anderen Host 1290
 - Granular Recovery Technology (GRT)
 - Für Backup festlegen 1301, 1309
 - Überblick 1287
 - Voraussetzungen für 1269
 - Installation 1277
 - Internet Information Service (IIS) Metabase
 - sichern 1286
 - Notfallwiederherstellung 1316
 - Postfach-Zugriffsanforderungen 1283
 - Schützen von Exchange mit VSS 1288
 - Sichern
 - Exchange 1290
 - sichern
 - Empfohlene Auswahlen 1286
 - Snapshot-Backup
 - konfigurieren 1288
 - Snapshot-Technologie 1288
 - Systemstatus
 - sichern 1286

- Überblick 1267
- Wiederherstellen von Daten auf dem Server 1309
- Wiederherstellen von Daten von
 - Snapshot-Backups 1309
- Wiederherstellung einzelner Objekte
 - Voraussetzungen 1269
- Wiederherstellungsanforderungen 1309
- Exchange-Web-Dienste
 - Verwenden mit Exchange Agent 1287
- Exportieren abgelaufener Medien 566
- Exportieren von Medien 566
- Externe Aufbewahrung der gesicherten Daten 150

F

- Failback
 - Definiert 915
- Failover
 - Ändern der Failover-Reihenfolge der Knoten 920
 - Definiert 912
 - Hinzufügen oder Entfernen eines
 - Failover-Knotens 920
 - Neustart 914
- FAT
 - Partition 891
- Fehlerbehandlungsregel für Cluster-Failover 321
- Fehlerbehandlungsregeln
 - aktivieren oder deaktivieren 318
 - Benutzerdefinierte Regel für wiederhergestellte
 - Aufträge 317
 - Benutzerdefinierte Regel löschen 319
 - Benutzerdefinierte Regeln
 - Definiert 316–317
 - Benutzerdefinierte Regeln für wiederhergestellte
 - Aufträge 320
 - Cluster-Failover-Regel 321
 - Erstellen 317
 - Für fehlgeschlagenen Auftrag aktivieren 319
 - Standardregeln
 - Definiert 316
 - Überblick 316
- Fehlerbehebung
 - Backupprobleme 889
 - Cluster 940
 - Fehlermeldungen 889
 - Hardware-bezogene Probleme 880
 - Installation 897
 - Leistung von Backup Exec
 - Verbessern 900
 - Remote Media Agent for Linux 1625

- Sofortwiederherstellung in der Cloud 900
- Fehlercodes
 - Unique Message Identifier
 - Anzeigen 313
- Fehlgeschlagene Aufträge
 - Wiederholen 300
- Festplattenspeicher
 - Erstellen 372
- Filter
 - Für Warnmeldungen 342
- Firewall
 - Aktivieren einer SQL-Instanz 727
 - Backup Exec-Ports 724
 - Durchsuchen von Systemen 723
 - Verwendung mit Backup Exec 722
- Formatieren von Medien 555
- Fortsetzen des Exchange-Backups, wenn
 - Konsistenzprüfung fehlschlägt 1293, 1303

G

- GDPR Guard
 - BEMCLI-Befehle 871
 - Best Practices 876
 - Blockieren 874
 - Blockierte Elemente wiederherstellen 875
 - Fehlerbehebung 897
 - Info 869
 - Unterstützte Datentypen 873
- Geänderte Uhrzeit
 - Zur Ermittlung des Backup-Status
 - verwenden 219
- Gemeinsame Verschlüsselungscodes 730
- Genannte Transaktion
 - Wiederherstellen in 1256
- Geöffnete Dateien
 - Sichern nicht möglich 890
- Geplante Aufträge
 - Ändern der Priorität 297
 - Anhalten 292
 - Anhalten aufheben 294
 - Info zum Verwalten und Überwachen 286
 - Löschen 299
 - sofortiges Ausführen 297
 - Status 322
- Geräte
 - OpenStorage, Überblick 1058
 - Über iSCSI angeschlossene Gerät
 - hinzufügen 447
 - USB-Bandgeräte wieder verbinden 447

- Google Cloud
 - Anforderungen 411, 414
- Google Cloud Storage
 - Konfigurieren 415
- Granular Recovery Technology
 - Anwendung mit VMware 1115
 - mit Agent for Hyper-V 1180
 - nicht unterstützte Konfigurationen für VMware 1115
- Granular Recovery Technology (GRT)
 - Anforderungen 742
 - Empfohlene Geräte 743
 - Exchange-Daten 1287
 - Backup auf einem anderen Host 1287
 - Staging 740
 - Standardoptionen festlegen 744
 - Unter Verwendung der
 - Exchange-Web-Dienste 1287
 - Wiederherstellen einzelner Elemente 737
- GRT
 - Anforderungen für VMware 1115
 - Anwendung mit VMware 1115
 - nicht unterstützte Konfigurationen für VMware 1115
- Gruppe "Alle Server"
 - Info 168
- Gruppe "Ausrangierte Server"
 - Info 168
 - Server hinzufügen 172
- Gruppen
 - Für Empfang von Benachrichtigungen konfigurieren 351
- Gruppenrichtlinienobjekt, konfigurieren 90

H

- Hardware
 - Fehlerbehebung 880
 - Schutz im Falle eines Systemausfalls 149
- Hauptknoten in einem Cluster 915
- Hinzufügen
 - Remote Media Agent for Linux 1612
- Hinzufügen von Bändern durch das Importieren von Medien 558
- Hotkey
 - Definiert 1629
- Hyper-V
 - Sofortwiederherstellung 1193, 1201
- Hyper-V-Host
 - Hinzufügen einer Liste von Servern 1163

I

- IBM-Computer
 - Mit Simplified Disaster Recovery wiederherstellen 986
- Identifikationsdaten
 - Für Aufträge ersetzen 235
 - Für Aufträge erstellen 236
 - Für Aufträge prüfen 234
 - Für Backup-Quellen erstellen 236
 - Für Backup-Quellen prüfen 234
 - Für eine Backup-Quelle ersetzen 235
- Identifikationsdaten (Teilfenster)
 - Backup-Quellen löschen 238
 - Info 234, 238
- Importieren von Medien 558
- Importierte Bandmedien
 - Gekennzeichnet durch Backup Exec 494
- Importierte Medien
 - Überschreiben 488
- Initialisieren eines Wechslers 553
- Inkrementelle Backups
 - Info 208
 - Vorteile und Nachteile 211
- Installation
 - Agent for Windows 77
 - Agent for Windows mit Befehlsskript 95
 - Agent for Windows mit Befehlsskript deinstallieren 96
 - Agent for Windows über Eingabeaufforderung 92
 - Agent for Windows über Eingabeaufforderung deinstallieren 94
 - Aufgaben nach der Installation 126
 - Backup Exec deinstallieren 127
 - Befehlszeilen-Switches 104
 - Checkliste 46
 - Checkliste vor dem Upgrade 124
 - Environment Check
 - Überblick 48
 - Funktionen vom lokalen Backup Exec-Server deinstallieren 128
 - Gruppenrichtlinienobjekt konfigurieren 90
 - Microsoft SQL Server 2014 Express 50
 - Migrationsbericht 125
 - NDMP Feature 1540
 - Parameterdateien
 - Erstellen 111
 - Push-Installation auf Remote-Computern 68
 - Push-Installation von Agent for Windows 78
 - Remote Administrator 96

- Remote Administrator über die Befehlszeile 98
- Systemanforderungen 51
- typisch 55
- Über die Befehlszeile 103
- Überblick 44
- Umformung erstellen 87
- Updates für den Agent for Windows 84
- WMI-Leistungszähler 365
- WMI-SNMP-Provider 365
- Zusätzliche Funktionen 66
- Installationsparameterdatei
 - erstellen 112
- Installationsprotokoll 113
 - Agent for Linux 1562
- Installationsübersicht
 - Agent for Hyper-V 1159
- Installationsübersichtsbericht 113
 - Anzeigen 113
- Installieren
 - Auf einer vorhandenen Microsoft SQL Server 2008-Instanz 50
 - Media Agent for Linux 1602
 - SharePoint Agent 1319
 - Zusätzliche Backup Exec-Optionen in einem Microsoft-Cluster installieren 918
- installieren
 - Backup Exec in einem Microsoft Cluster 916
- Installierte Aktualisierungen
 - Anzeigen 117
- Instant GRT
 - für GRT-Aufträge 737
 - Konfigurieren 656
- Internet Information Services (IIS) Metabase
 - sichern 1286
- Inventarisieren
 - Wechsler beim Starten der Backup Exec-Dienste 459
- IPv4 712
- IPv6 712

K

- Kalender
 - Alle geplanten Backup-Aufträge anzeigen 243
 - Datum ausschließen 688
- Katalog
 - Ebenen 283
 - Medien mit verschlüsselten Backup-Sätzen 505
 - Standardoptionen bearbeiten 279

- Kataloge
 - Zur Ermittlung des Backup-Status verwenden 220
- Katalogfehler
 - DLT-Bandlaufwerk blockiert 883
- Katalogisieren
 - Definiert 277
 - Instant GRT 277
 - Konfigurieren der Optionen für Vollständige Katalogisierung 656
 - Medien 548
 - Vollständige Katalogisierung 277
- Kennwort
 - Ändern für ein Login-Konto 770
- Kennzeichnen von Bandmedien
 - Kennzeichnung importierter Bandmedien 494
 - Mithilfe von Barcode-Kennungen 494
- Kennzeichnen von Medien 492
- Knoten
 - Definiert 912
 - Konfigurationen in einem Microsoft Cluster 923
 - Microsoft
 - Ändern der Failover-Reihenfolge der Knoten 920
 - Hinzufügen oder Entfernen eines Failover-Knotens 920
 - Notfallwiederherstellung mithilfe von SDR 935
- Kompakte Ansicht 139
- Konfiguration
 - Feiertage 688, 691
- Konfigurationseinstellungen
 - Kopieren auf einen anderen Server 782
- Konfigurieren des Speicherassistenten
 - Überblick 523
- Konsistenzprüfungsoptionen
 - Exchange Agent 1293, 1303
 - SQL Agent 1222
- Konvertieren auf virtuellen Computer
 - von Zeitpunkt 614
- Konvertierung auf virtuellen Computern
 - von Zeitpunkt 614
- Konvertierung des virtuellen Computers
 - Einstellungsstandardoptionen 623
 - Hinzufügen einer Phase 607
- Konvertierung für virtuelle Computer
 - Einstellungsstandardoptionen 623
- Konvertierung in virtuelle Computer
 - Anforderungen 590
 - Backup-Methoden 581

- Gleichzeitig mit Backup-Auftrag 592
- Hinzufügen einer Phase zur 607
- Konvertieren von Datenträgern größer als 2 TB 581
- Nach einem Backup-Auftrag 599
- Optionen 581
- Überblick 581
- Verarbeitung der Backup-Auswahl 581
- Windows Server 2012 Hyper-V-Host 581
- Konvertierung in virtuellen Computer
 - Einmalig 616
- Kürzlich beschriebene Medien (Bericht) 842

L

- Laufwerkpools
 - Erstellen in einem Microsoft-Cluster 920
- Laufzeitskripte, für Agent for Linux 1588
- Leistung
 - Erhöhen während Backups der
 - Windows-Remote-Computer 1029
- Library Expansion Feature
 - Einrichten der Hardware 458
 - SCSI-Adressen für Hardware 458
- Liste von Servern
 - Info 166
 - Servergruppen 168
- Listenansicht 139
- Listenfelder
 - Navigation 1656
- Lizenzen 44
 - Agent for Windows 1029
- Lizenzinformationen
 - Anzeigen 118
 - Veritas Smart Meter 118
- Lizenzvertragsinformationen
 - Info 119
 - Kundennummern verwalten 120
- Login-Informationen
 - Kopieren auf einen anderen Server 774
- Login-Konten
 - Ändern des Kennworts 770
 - Auf einen anderen Server kopieren 774
 - Bearbeiten 768
 - eingeschränkt 765
 - Ersetzen 770
 - Erstellen 766
 - Info 762
 - Löschen 771
 - prüfen 706

- Prüfung planen 706
- SQL-Datenbanken 1220
- Standard
 - Info 763
- Standard ändern 772
- System-Login-Konto 764
- Testen 775
- Lokaler Backup Exec-Server
 - Verbindung trennen 101
- löschen
 - Bandmedien 502

M

- Master-Datenbank (SQL)
 - Backup 1223
- Media Agent for Linux
 - beoper-Gruppe 1602
 - Installieren 1602
- Medien
 - Ausrangiert
 - Definiert 474
 - löschen 502
 - Temporär
 - Definiert 474
 - Überschreiben zugewiesener oder importierter 488
 - Überschreiboptionen 488
- Medien-ID
 - Definiert 492
- Medienrotation
 - Strategien
 - Großvater 508
 - Sohn 508
 - Vater/Sohn 508
- Medienrotationsstrategie Großvater 508
- Medienrotationsstrategie Vater/Sohn 508
- Mediensatz
 - Erstellen 480
 - Löschen 486
 - Speicherregel-Eigenschaften 499
 - Standard 473
 - Umbenennen 487
- Medienspeicher, Info zu 496
- Medienüberschreibschutzstufe
 - Definiert 487
- Meldungen
 - Fehler 889
- Methode zum Sichern und Löschen von Dateien
 - Speicherplatz freigeben 222

- Microsoft Cluster Server
 - Verwendung mit Backup Exec 914
- Microsoft SharePoint-Daten
 - sichern 1322
 - wiederherstellen 1329
- Microsoft SQL Server 2014
 - Installieren 50
- Migrationsbericht 125
- MSCS
 - Verwendung mit Backup Exec 914
- MSDE
 - 2014-Komponenten
 - Installiert mit Backup Exec 50
- Muster für Ausschlüssen in NDMP Feature 1548

N

- NAS-NDMP-Server
 - Sichern 1539
- Navigation
 - Listenfelder 1656
 - Registerkarten 1656
- NDMP Feature
 - Anforderungen 1539
 - Daten wiederherstellen 1550
 - Eigenschaften des Speichergeräts anzeigen 1557
 - Gesicherte Daten duplizieren 1549
 - Installieren 1540
 - Muster verwenden 1548
 - NDMP-Server hinzufügen 1540
 - Serveereigenschaften anzeigen 1556
 - Sichern von NDMP-Servern 1543
 - Speicher auf NDMP-Servern gemeinsam nutzen 1542
 - Standardoptionen festlegen 1554
 - Überblick 1539
 - Wiederhergestellte Daten umleiten 1550
- Netzwerk
 - Optionen für Backup-Aufträge konfigurieren 223
 - Überblick über Backup-Netzwerke 711
- Netzwerk und Sicherheit
 - Konfigurieren 713
- Netzwerkverkehr
 - Reduzieren in CAS 1475
- Nicht erkanntes Medium 473
- Notfallvorbereitung
 - Exchange-Server 1316
 - Externe Aufbewahrung 150
 - Hardwareschutz 149

- Plan für die Notfallwiederherstellung (DPP) 148
- Überblick 148
- Notfallwiederherstellung
 - Alternativer Pfad in SDR 957
- Cluster
 - Backup Exec in einem Microsoft-Cluster mithilfe von SDR 936
 - Gesamter Cluster manuell 937
 - Knoten mithilfe von SDR 935
 - SDR zur Vorbereitung verwenden 934
 - Überblick 933
- Deduplizierungsspeichergerät 1085
- Einstellen der Speicherpfade
 - Notfallwiederherstellungs-Informationsdatei 955
- Exchange-Server 1316
- Microsoft SharePoint 2010/2013/2016 1334
- Microsoft-Cluster
 - Backup Exec 938
 - Datendateien 938
 - OpenStorage-Geräte 1087
- Novell OES
 - Anforderungen für Backup 1581
 - Unterstützte Komponenten 1580
 - Wiederherstellen 1582
- NTFS
 - Partition 891

O

- Off-Host-Backup
 - Fehlerbehebung 1533
 - Probleme mit Hardware-Anbietern 1536
- Offhost-Backup
 - Host-Computer
 - Definiert 1527
 - Konfigurieren 1530
 - Snapshot eines einzelnen Datenträgers 1524, 1532
 - Standardoptionen einstellen 1522
 - Überblick 1527
- OpenStorag-Geräte
 - Notfallwiederherstellung 1087
- OpenStorage-Geräte
 - Anforderungen 1051
 - Eigenschaften bearbeiten 1061
 - Überblick 1058
- Optimierte Duplizierung 1080
- Option zur Wiederherstellung des Point-In-Time-Protokolls
 - SQL Agent 1256

Oracle Agent

- Aktualisieren der Login-Daten für Instanzen 1346, 1354
- Authentifizierung für Oracle-Vorgänge 1359
- Authentifizierungsdaten 1359
 - Festlegen 1360
 - Löschen 1362
- Backup-Optionen 1367
- DBA gestartete Aufträge
 - Auftragsvorlagenname 1356
- Einstellungen für von DBA gestartete Aufträge
 - Vorlage erstellen 746
- erweiterte Wiederherstellungsoptionen 1373
- Funktionen 1340
- Identifikationsdaten für Instanzen
 - aktualisieren 1362
- Installieren 1342
- Konfiguration 1342
- Linux-Server
 - Anzeigen einer Oracle-Instanz 1356
 - Bearbeiten einer Oracle-Instanz 1356
 - Datenbankzugriff aktivieren 1358
 - Konfigurieren einer Oracle-Instanz 1353
 - Löschen einer Oracle-Instanz 1357
- Mehrere Datenströme
 - Angaben 1367, 1374
- Optionen für Authentifizierungsdaten 1361
- Optionen für Backup Exec Agent Utility 1349
- Oracle Net Service-Name 1348
- Oracle-Datenbanken auf Linux
 - veröffentlichen 1355
- Port
 - Für Oracle-Vorgänge konfigurieren 1359
- Real Application Cluster (RAC) 1353, 1364
- Sichern 1362
- Standardoptionen 1345
- Umgeleitete Wiederherstellung 1372
- von DBA gestartete Wiederherstellung 1371
- von DBA gestartetes Backup 1366
- Wiederherstellen 1368
- Wiederherstellungskatalog 1348, 1355
- Wiederherstellungsoptionen 1372
- Windows-Computer
 - Anzeigen einer Oracle-Instanz 1349
 - Bearbeiten einer Oracle-Instanz 1350
 - Datenbankzugriff aktivieren 1351
 - Konfigurieren einer Oracle-Instanz 1345
 - Löschen einer Oracle-Instanz 1350

P

- Parameterdateien
 - Erstellen 111
- Partition
 - Erstellen für Wechsler 466
 - FAT 891
 - NTFS 891
- Partitionen
 - Entfernen oder neu konfigurieren 470
- Passphrasen 730
- Phasen
 - Arten 244
- PHYSICAL_ONLY-Dienstprogramm 1224
- Plattenbasierter Speicher
 - Info 367
- Plattenkassettenspeicher
 - Info 384
- Popup-Warmmeldungen
 - Aktivieren oder deaktivieren 361
- Portnummer
 - Ändern für Remote Media Agent for Linux 1612
- Postfach-Zugriffsanforderungen für Exchange 1283
- Priorität
 - Ändern für geplanten Auftrag 297
 - Info zu 297
- Private Cloud
 - Cloud-Instanz anzeigen 424
 - Cloud-Instanz bearbeiten 424
 - Cloud-Instanz erstellen 422
 - Cloud-Instanz löschen 425
- Private Cloud-basierte Speichergeräte
 - Anforderungen 420
- Privates Cloud-basiertes Speichergerät
 - Konfigurieren 423
- Probelaufauftrag
 - ausführen 252
 - Info zu 251
- Prüfung
 - Für Aufträge konfigurieren 655
- Puffergröße
 - Einstellung für Bandlaufwerke 454
 - für Plattenkassettengeräte festlegen 389
- Pufferzahl
 - Einstellung für Bandlaufwerke 454

R

- ralus.cfg
 - Bearbeiten von Konfigurationsoptionen 1570
 - Info, Agent for Linux 1568

- Info, für Remote Media Agent for Linux-Computer 1608
- Konfigurationsoptionen 1570
- Registerkarte "Backup und Wiederherstellung"
 - Serverliste 166
- Registerkarte "Startseite"
 - Info zu 139
 - Layoutelemente 139
 - Standardkonfiguration wiederherstellen 139
 - Supportelemente 139
 - Systemzustandelemente 139
- Registerkarten 132
- Reinigen eines Laufwerks 556
- Reinigungsslots
 - Festlegen für Wechsler 465
- Remote Administrator
 - Ausführung 100
 - Installieren 96
 - Installieren über die Befehlszeile 98
- Remote Media Agent for Linux
 - Änderung der Anschlussnummer 1612
 - Anforderungen 1600
 - Anzeigen der Eigenschaften 1616
 - Backup von Daten 1618
 - Deinstallieren 1605
 - Eigenschaften von simulierten Bandbibliotheken 1622
 - Eigenschaften von simulierten Bandbibliotheken anzeigen 1621
 - Fehlerbehebung 1625
 - Festlegen des Serverstatus 1616
 - Funktionsweise 1599
 - ICMP-Ping 1612
 - Optionen für simulierte Bandbibliotheken 1621
 - simulierte Bandbibliothek erstellen 1620
 - simulierte Bandbibliothek löschen 1623
 - simulierte Bandbibliotheken über die Befehlszeile verwalten 1624
 - Tape Library Simulator Utility 1619
 - Tape Library Simulator-Dienstprogramm
 - Befehlszeilen-Switches 1625
 - Wiederherstellen von Daten 1618
 - zur Backup Exec-Datenbank hinzufügen 1612
- Remote-Computer
 - Push-Installation 68
- Reparieren (Funktion) 114
- Replizierte Kataloge in CAS 1476
- RSS Reader
 - Anpassen 147

- Artikel anzeigen 147
- Optionen 147
- Standard-RSS-Feed entfernen 147
- Überblick 147

S

SAN

- Fehlerbehebung 892
- Fehlerbehebung bei Offline-Speichergeräten 892
- Hardwarefehler 894
- SAN zurücksetzen 895

Schattenkopiekomponenten

- Dateisystem 204

Schwellenwert

- Einstellung für Bandlaufwerke 455

SCSI

- Durchgangmodus für Bandlaufwerke 456
- Festlegen der Adresse für Wechslerlaufwerke 458

SCSI-Bus

- Konfigurieren für Bandgeräte in einem Microsoft Cluster 927

Seeding eines Deduplizierungsspeichergeräts 1080

Servereigenschaften

- anzeigen 784
- Anzeigen, Info 783
- Remote Media Agent for Linux 1616

Servergruppen

- Ausblenden 170
- Bearbeiten 171
- Einblenden 170
- Entfernen 173
- Erstellen 169
- Info 168
- Server ausrangieren 172
- Server entfernen 171
- Server hinzufügen 170
- Sichern 174

Serverliste

- Gefundene Server hinzufügen 710
- Server entfernen 168
- Server hinzufügen 167

SGMon 910

Shadow Copy-Komponenten wiederherstellen 274

SharePoint Agent

- Anforderungen 1319

- Einsatz mit SharePoint Server 2010/2013/2016 und SharePoint Foundation 2010/2013/2016 1320
- Info 1318
- Installieren 1319
- Kommunikation zwischen Webservern und Backup Exec deaktivieren oder aktivieren 1332
- Notfallwiederherstellung für SharePoint 2010/2013/2016 1334
- Serverfarm hinzufügen 1321
- SharePoint-Daten wiederherstellen 1329
- sichert SharePoint-Daten 1322
- Systemanforderungen 1319
- Überblick 1318
- SharePoint-Farmen
 - Anzeigen der Eigenschaften 1333
 - Hinzufügen 1321
- Silent-Mode-Installation 103
- Simplified Disaster Recovery
 - Alternativen Speicherort festlegen 954
 - Anforderungen 943
 - Assistent "Computer wiederherstellen"
 - Verschlüsselte Backup-Sätze 987
 - Wiederherstellen von einem externen Backup Exec-Server 987
 - Bearbeiten des Standardpfads 955
 - Boot-Manager 987
 - Cluster
 - Backup Exec in einem Microsoft-Cluster wiederherstellen 936
 - Knoten wiederherstellen 935
 - Erweiterte Datenträgerkonfiguration
 - Info 1001
 - Für Backups aktivieren 950
 - Inhalt des Simplified Disaster Recovery-Datenträger-Image 980
 - Installieren 941
 - Keine Internetverbindung
 - ADK 1809 974
 - ADK 8.1 oder ADK 10 977
 - Microsoft Exchange Server
 - Wiederherstellen 999
 - Microsoft Hyper-V-Hosts 999
 - Microsoft SQL Server
 - Wiederherstellen 999
 - OS/2-Boot-Manager
 - Wiederherstellen 987
 - SharePoint Portal Server
 - Wiederherstellen 999
 - Speicherpools und Speicherplätze
 - Wiederherstellung 995
 - Überblick 941
 - Wiederherstellen von IBM-Computern 986
 - Wiederherstellungsanforderungen in SDR 987
 - Windows Server 2008 R2 bis Windows Server 2016 963
 - Windows Server 2008 R2 bis Windows Server 2019 959
 - Windows Server 2008 SP2 966
- Simplified Disaster Recovery-Datenträger-Image
 - Inhalt 980
- Simulierte Bandbibliothek
 - Anzeigen der Eigenschaften 1621
 - Erstellen 1620
 - Löschen 1623
- Snapshot-Technologie
 - Verwenden mit Exchange Agent 1288
- SNMP
 - Traps für Warnmeldungen 361
 - Konfigurieren des Systemdiensts für Windows 364
 - Präfix für Objekt-ID 361
 - Traps
 - Definiert 361
 - WMI-Provider installieren 365
- Sofortwiederherstellung
 - Entfernen eines virtuellen VMware-Computers 1140
 - Erstellen eines Auftrags für die Sofortwiederherstellung eines virtuellen VMware-Computers 1137
 - Hyper-V 1193
 - VMware-Anforderungen 1134
 - VMware-Hinweise 1135
 - VMware-Überblick 1131
- Sofortwiederherstellung in der Cloud
 - Abonnement oder Tresor ändern 865
 - Anforderungen in Backup Exec 856
 - Ansicht manuell aktualisieren 861
 - Azure-Ressourcen konfigurieren 857
 - Details zum virtuellen Computer anzeigen 861
 - Failover verwalten 865
 - Fehlerbehebung 900
 - Fehlerdetails anzeigen 860
 - Info 852
 - Infrastruktur vorbereiten 866
 - Konfigurationsdetails anzeigen 860
 - Konfigurierte Azure-Ressource entfernen 866

- Registerkarte 853
- Replikation aktivieren 862
- Replikation verwalten 864
- Vorkonfiguration im Azure-Portal
 - VMware- bzw. Hyper-V-Infrastruktur 857
- Vorkonfigurationen im Azure-Portal 856
- Zertifikat prüfen 867
- Sofortwiederherstellung von Hyper-V
 - Anforderungen 1199
 - Best Practices 1207
 - Einschränkungen 1200
 - Entfernen 1203–1204
- Sohn, Medienrotationsstrategie 508
- Sortieren, Filter und Kopieren 135
- Spannen eines Bands 554
- Speicher
 - Aktivieren 553
 - Ändern in online 547
 - anhalten 552
 - Assistent für die Installation der Gerätetreiber 449
 - Assistent für Hot Swap-Geräte 447
 - Backup-Satz-Aufbewahrung nach Speichertyp 403
 - Barcode zum Verschieben von Medien scannen 501
 - Deaktivieren 553
 - Deduplizierungsgeräte gemeinsam nutzen 1077
 - Globale Einstellungen bearbeiten 535
 - Info zu Bandlaufwerken und Wechslern 447
 - Info zum gemeinsamen Nutzen 544
 - Löschen 546
 - starten 552
 - umbenennen 547
- Speicher- und Mediendaten
 - Speicherort in CAS 1453
- Speicher-Trends 369
- Speichergeräte
 - installieren 47
- Speichergerätepools
 - Ändern der Standardwerte 515
 - Erstellen 512
 - Geräte hinzufügen oder entfernen 517
 - Info 512
 - Vom System definiert 512
 - Zuerst Gerät mit dem geringsten freien Speicherplatz 515
 - Zuerst Gerät mit dem meisten freien Speicherplatz 515
- Speicherpools und Speicherplätze, Wiederherstellung mit SDR 995
- Speicherregeln für Mediensätze 499
- Speicherung
 - Für Backup-Jobs konfigurieren 645
- Speichervorgänge
 - Abgelaufene Medien exportieren 566
 - Inventarisieren und katalogisieren 552
 - Inventarisierung 550
 - Katalogisieren 548
 - Laufwerk reinigen 556
 - Medien auswerfen 555
 - Medien exportieren 566
 - Medien importieren 558
 - Scannen 549
 - Spannen 554
 - Überblick 519
 - Vorderen Ladeschacht freigeben 569
 - Vorderen Ladeschacht sperren 569
 - Wechsler initialisieren 553
 - WORM (Format) 553
- SQL
 - Wiederherstellung in eine genannte Transaktion 1256
- SQL Agent
 - Anforderungen 1220
 - Database Consistency Checking (DBCC) Empfehlungen 1222
 - Datenbank-Snapshots Überblick 1226
 - Funktionen 1219
 - Installation 1221
 - Konsistenzprüfung 1224 Empfehlungen 1222
 - Login-Konten 1220
 - Notfallwiederherstellung 1262 Manuell 1264
 - Sichern
 - Datenbanken 1228
 - Konsistenzprüfungsempfehlungen 1222
 - Strategien 1221
 - Windows-Registrierung 1222
 - sichern
 - Backup-Methoden 1241, 1254
 - Konsistenzprüfung nach dem Backup 1238, 1251
 - Snapshot-Technologie Verwenden 1225
 - Strategieempfehlungen 1221

- Überblick 1218
- Wiederherstellen
 - Master-Datenbank 1259
 - Option zur Wiederherstellung des Point-In-Time-Protokolls 1256
 - Sehr große Datenbanken 1256
 - TDE-verschlüsselte Datenbank-Backups 1256
 - Umleiten von Wiederherstellungen 1256
- Standard-Backup-Optionen
 - Hyper-V 1175
- Standardansicht 139
- Standardoptionen
 - Agent for VMware 1109
 - Konvertierung in virtuelle Computer 623
 - NDMP Feature 1554
 - Simplified Disaster Recovery
 - Einstellungen 955
- steuern Sie Verbindung mit dem Remote Media Agent for Linux 1599
- Strukturansicht 139
- Stufen
 - Bearbeiten 245
 - Definiert 174
 - Hinzufügen 244
 - Info 244
- Suchassistent 260
- Suchen 260
- Synthetisches Backup
 - Anforderungen 1521
 - Basis-Backup 1520
 - Verschlüsselung
 - Voraussetzungen für 1522
- System-Login-Konto
 - erstellen 773
 - Info 764
- Systemanforderungen
 - Backup Exec 51
- Systemstatus
 - auf Domänencontroller wiederherstellen 270
 - Wiederherstellen 268

T

- Tape Library Simulator Utility
 - Anzeigen der Eigenschaften 1621
 - Ausführung über die Befehlszeile 1624
 - simulierte Bandbibliothek erstellen 1620
 - Überblick 1619

- Tape Library Simulator-Dienstprogramm
 - Löschen der Bibliothek 1623
- tapeinst.exe 449
- Tastaturkurzbefehle
 - Registerkarte "Backup und Wiederherstellung" 1631
 - Registerkarte "Backup und Wiederherstellung" für die Anmeldedatenansicht 1639
 - Registerkarte "Backup und Wiederherstellung" für die Ansicht der aktiven Warnmeldungen 1638
 - Registerkarte "Backup und Wiederherstellung" für die Auftragsansicht 1634
 - Registerkarte "Backup und Wiederherstellung" für die Auftragsverlaufsansicht 1635
 - Registerkarte "Backup und Wiederherstellung" für die Backup-Satz-Ansicht 1637
 - Registerkarte "Berichte" 1653
 - Registerkarte "Speicher" 1644
 - Registerkarte "Speicher" für die Ansicht der aktiven Warnmeldungen 1653
 - Registerkarte "Speicher" für die Auftragsansicht 1648
 - Registerkarte "Speicher" für die Auftragsverlaufsansicht 1650
 - Registerkarte "Speicher" für die Backup-Satz-Ansicht 1651
 - Registerkarte "Startseite" 1630
- Tastaturnavigation
 - Dialogfelder 1655
 - Standard 1654
- Tastenkombinationen
 - Auftragsüberwachung (Registerkarte) 1640
- Technischer Support
 - Kontaktieren 902
- Teilfenster "Details"
 - Hyper-V 1164
- Temporäre Medien
 - Definiert 474
 - Erstellen 488
- Testlaufauftrag
 - Konfigurieren 653
- Text kopieren 135
- Transparent Database Encryption
 - SQL Agent 1256
- True Image-Wiederherstellung
 - Überblick 1524
- Typische Installation 55

U

- Über iSCSI angeschlossene Geräte
 - Hinzufügen 447
- Überschreibschutzzeitraum
 - Ändern 484
 - Bearbeiten 482
 - Definiert 477
- Überwachungsprotokoll
 - Anzeigen 780
 - Entfernen von Einträgen 781
 - In Datei speichern 781
 - Info zu 779
 - Konfiguration 779
- Umbenennen
 - Bandmedienkennungen 495
- Umformung, erstellen 87
- Umgebungsprüfung
 - Vor Installation oder Upgrade ausführen 48
- Umgeleitete Wiederherstellung
 - Exchange-Daten 1309
- UMI-Fehlercode (Unique Message Identifier)
 - Anzeigen 313
- Updates
 - für Agent for Windows installieren 84
 - Installierte anzeigen 117
- Upgrades
 - Checkliste 124
 - Überblick 121
- USB-Bandgeräte
 - Wieder verbinden 447

V

- Veritas QuickAssist 904
- Veritas SaaS-Backup
 - Verbindung herstellen 134
- Veritas Update
 - Info 115
 - Manuelles Ausführen 117
 - Planen von automatischen Updates 116
- Veritas-Supportdatenbank
 - suchen 901
- Veritas™ Information Map
 - Anforderungen 1018
 - Backup Exec 1018
 - Best Practices 1022
 - Einschränkung 1027
 - Fehlerbehebung 1023
 - Info 1017
 - Integration 1019
 - Unterstützte Datenquellen 1022
- Veröffentlichen
 - Auf Backup Exec-Servern
 - Mit Agent for Windows 1035
 - Linux-Computern auf Backup Exec-Servern 1567
- Verschlüsselte Dateien
 - Informationen zum Katalogisieren von Medien 505
- verschlüsselte SQL-Datenbankwiederherstellung 1256
- Verschlüsselung
 - Hardware 729
 - Info 727
 - Mit Deduplizierung 1084
 - Software 728
 - Typen 727
 - Wiederherstellen verschlüsselter SQL-Datenbanken 1256
- Verschlüsselungscodes
 - 128-Bit AES 727
 - 256-Bit AES 727
 - Eingeschränkt 730
 - Ersetzen 733
 - erstellen 732
 - Gemeinsame 730
 - Sicherheitsfragen 730
 - Überblick 729
 - Verschlüsselungstypen 727
 - Verwalten 731
- Verschlüsselungsschlüssel
 - Informationen zum Löschen 736
 - Löschen 736
 - Wiederherstellen verschlüsselter Daten 276
- Version von Backup Exec, Anzeigen 134
- Versionen von Backup Exec
 - Auflistung und Beschreibung 40
- Verteilte Kataloge in CAS 1476
- Vertrauen
 - Erstellen 1031
 - Festlegen für einen Remote Media Agent for Linux-Computer 1608
 - Festlegen für einen standortfernen Linux-Computer 1566
- Verwalteter Backup Exec-Server
 - Aktualisieren 1466
 - Einstellungen ändern 1479
 - Installieren 1456
 - Netzwerkkarte
 - verfügbare verwenden 1494
 - Pools 1498

- verwalteter Backup Exec-Server
 - Aufträge kopieren zu 1495
 - Verzeichnisse
 - Ein- und Ausschließen für NDMP-Server 1547
 - Verzögerte Aufträge
 - Schwellenwerte festlegen 330
 - VHD-Dateien
 - Verwalten 185
 - VHDX-Dateien
 - mit GRT 1159
 - virtuelle Bibliothek
 - DirectCopy auf physische Geräte 255
 - Virtuelle Computer
 - automatischer Schutz für Hyper-V 1179
 - Virtuelle Computer mit hoher Verfügbarkeit
 - Sichern und Wiederherstellen 1184
 - Virtuelles Backup 1098
 - Virtueller Computer
 - Sichern 1100
 - VMware vCenter-Server hinzufügen 1092
 - VMware-virtuelle Computer
 - Agent for Windows über eine Push-Installation installieren 1096
 - Vollständige Backups
 - Info 206
 - Vorteile und Nachteile 209
 - Vollständige Katalogisierung
 - Byteanzahl für Hyper-V berechnen 1186
 - für GRT-Aufträge 737
 - Konfigurieren 656
 - und Sichern eines virtuellen Hyper-V-Computers 1185
 - Von Backup Exec verwendete Anschlüsse
 - Listener 726
 - Standard 724
 - Von DBA gestartete Aufträge
 - Vorlage bearbeiten 747
 - VSS
 - Konsistenzprüfung vor Exchange-Backup durchführen 1293, 1303
 - Verwenden zum Schützen von Exchange-Daten 1288
- W**
- Warnmeldung
 - Löschen aus Warnmeldungsverlauf 340
 - Warnmeldungen
 - Anzeigeort 336
 - Auf der Registerkarte "Startseite" anzeigen 338
 - Auftragsprotokoll anzeigen 343
 - Benachrichtigung 345
 - Benachrichtigung bei Abschluss des Auftrags senden 357
 - Benachrichtigung für Empfänger beenden 358
 - Benachrichtigungen einrichten 344
 - Definition 334
 - E-Mails und Textmeldungen aktivieren 348
 - Empfänger löschen 353
 - Filter 342
 - Gruppen für Benachrichtigung konfigurieren 351
 - Informationsmeldungen löschen 344
 - Kategorien 334
 - Kategorien konfigurieren 354
 - Konfigurieren von Standardeinstellungen 359
 - Popups aktivieren 361
 - Popups deaktivieren 361
 - Reagieren auf 343
 - Schweregrad 334
 - SNMP-Traps 361
 - Text kopieren 341
 - Wechsler
 - Beim Starten von Backup Exec-Diensten initialisieren 464
 - Beispielkonfiguration 459
 - Einrichten der Hardware 458
 - Erstellen von Partitionen 466
 - Inventarisieren beim Starten der Backup Exec-Dienste 459
 - Partitionen entfernen 470
 - Partitionen neu konfigurieren 470
 - Reinigungsschacht 465
 - Verwendung mit Backup Exec 457
 - Wichtige Systemkomponenten
 - Auswählen 190
 - Info 200
 - Wiederherstellungsszenarien 202
 - Wiederhergestellte Aufträge
 - Schwellenwerte festlegen 330
 - Wiederherstellen
 - 262
 - Aus einem Backup-Satz 263
 - Aus einem Server 262
 - Aus Speichergerätmedien 263
 - Dateisystemdaten 265
 - Dienstprogramm-Partitionen 275
 - Domänencontroller in einer vorhandenen Domäne 272

- Erstellen von Wiederherstellungsaufträgen für den Remote Media Agent for Linux 1618
- Exchange-Daten 1309
- Mit anderer Backup-Software erstellte Medien 277
- Nach Daten zum Wiederherstellen suchen 260
- Online-Wiederherstellung eines Windows-Computers 267
- Schattenkopiekomponenten 274
- SQL-Master-Datenbank 1259
- Starten des Wiederherstellungsassistenten 258
- Systemstatus auf einem Domänencontroller 270
- Systemstatusdaten 268
- UEFI-Systempartitionen 275
- Verschlüsselte Daten 276
- Wiederherstellen von Daten 258
- Wiederherstellungsauftrag abbrechen 277
- Wiederherstellung bereit (Validierungsübersicht) 843
- Wiederherstellungsassistent 258
- Windows Server 2008
 - Read Only Domain Controller 52
 - Server Core 52
- Windows Server 2012
 - Mit Agent für Hyper-V 1159
- Windows-Änderungsjournal
 - Fehler auflösen 221
 - Von Backup Exec festgelegte Standardeinstellungen 221
 - Zur Ermittlung des Backup-Status verwenden 220
- Windows-Benutzerrechte 165
- Windows-Deduplizierungsdatenträger
 - Sichern 184
- Windows-Registrierung
 - Sichern mit SQL Agent 1222
- Windows-Verwaltungsinstrumentation (WMI)
 - WMI-Funktion hinzufügen 365
- WMI
 - Installieren des Leistungszähler-Anbieters 365
 - Leistungszähler-Provider deinstallieren 366
 - SNMP-Provider deinstallieren 366
 - SNMP-Provider installieren 365
- WORM-Medien 495
- Auszuschließende Tage für einzelne Backup-Aufträge 242
- Auszuschließende Tage löschen 690
- Daten einschließen 240
- Daten einschließen und ausschließen 240
- Exportieren der auszuschließenden Tage 691
- für Backup-Jobs konfigurieren 635
- Importieren einer Liste von Daten zum Ausschließen aus dem Backup-Zeitplan 688
- Konflikte 240
 - über 239
 - Verfügbarkeitsfenster 239
- Zeitpunkt
 - Konvertierung auf virtuellen Computern 614
- Zentrale Kataloge in CAS 1476
- zentralisierte Wiederherstellung
 - bewährte Methoden 1503
- Ziel-Backup Exec-Server
 - Hinzufügen 782
 - Liste importieren 782
- Zuerst Speichergerät im Pool mit dem geringsten freien Speicherplatz 515
- Zuerst Speichergerät im Pool mit dem meisten freien Speicherplatz 515
- Zugewiesene Medien
 - Überschreiben 488
- Zugriffstasten
 - Definiert 1629

Z

- Zeitplan
 - Auswählen von Tagen für alle Backups 688
 - Auszuschließende Tage für alle Backups 688