

NetBackup™ Web UI Administrator's Guide

Release 10.1



NetBackup™ Web UI Administrator's Guide

Last updated: 2022-09-08

Legal Notice

Copyright © 2022 Veritas Technologies LLC. All rights reserved.

Veritas, the Veritas Logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Veritas is required to provide attribution to the third party ("Third-party Programs"). Some of the Third-party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the Third-party Legal Notices document accompanying this Veritas product or available at:

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

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. Veritas Technologies LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

<http://www.veritas.com>

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

<https://www.veritas.com/support>

You can manage your Veritas account information at the following URL:

<https://my.veritas.com>

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

<https://sort.veritas.com/documents>

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

NB.docs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

<http://www.veritas.com/community/>

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1	Introducing the NetBackup web user interface	
	12
	About the NetBackup web UI	12
	Terminology	15
	First-time sign in to the NetBackup web UI	17
	Sign in to the NetBackup web UI	18
	Sign out of the NetBackup web UI	20
	Documentation for Catalog Recovery Wizard, disk array hosts, disk pools, and Host Properties in the NetBackup web UI	20
Chapter 2	Monitoring and notifications	23
	The NetBackup dashboard	23
	About the Activity monitor	24
	Job monitoring	25
	Workloads that require a custom RBAC role for specific job permissions	26
	View a job	27
	View the jobs in the List view	28
	View the jobs in the Hierarchy view	28
	Jobs: cancel, suspend, restart, resume, delete	28
	Search for or filter jobs in the jobs list	29
	Create a jobs filter	30
	Edit or delete a jobs filter	32
	Troubleshooting the viewing of jobs	32
	Job notifications	33
	Send email notifications for job failures	33
	Send notifications to the backup administrator about failed backups	36
	Send notifications to a host administrator about backups	37
	Configure the nbmail.cmd script on the Windows hosts	37
	NetBackup event notifications	39
	View notifications	40
	Modify or disable NetBackup event notifications in the web UI	40
	About configuring automatic notification cleanup tasks	46

Section 1	Managing hosts	48
Chapter 3	Managing host properties	49
	Edit the host properties of a server or client	49
	Reset a host's attributes	50
Chapter 4	Managing credentials for workloads and systems that NetBackup accesses	52
	Overview of credential management in NetBackup	52
	Add a credential in NetBackup	53
	Add a credential for an external KMS	54
	Add a credential for NetBackup Callhome Proxy	55
	Edit or delete a named credential	55
	Add a credential for Network Data Management Protocol (NDMP)	56
	Edit or delete Network Data Management Protocol (NDMP) credentials in NetBackup	57
Chapter 5	Managing deployment	58
	Managing the NetBackup Package repository	58
	Update host	59
	Deployment policies	60
Section 2	Configuring storage and backups	61
Chapter 6	Configuring storage	62
	About storage configuration	62
	Create a Media Server Deduplication Pool (MSDP) storage server	63
	Create a Cloud storage, OpenStorage, or AdvancedDisk storage server	65
	Create a disk pool	67
	Create a storage unit	68
	Create a universal share	69
	Create a Media Server Deduplication Pool (MSDP) storage server for image sharing	71
	Using image sharing from the NetBackup web UI	72
	Troubleshooting storage configuration	73
	Troubleshooting universal share configuration issues	74

	Using instant access for MS-Windows and Standard policies	77
Chapter 7	Overview of backups in the web UI	78
	Backups methods supported in the NetBackup web UI	78
	Protection plan vs. policy FAQs	78
	Support for NetBackup classic policies	79
Chapter 8	Managing protection plans	81
	Create a protection plan	81
	Customizing protection plans	87
	Edit or delete a protection plan	88
	Subscribe an asset or an asset group to a protection plan	89
	Unsubscribe an asset from a protection plan	90
	View protection plan overrides	90
	About Backup Now	91
Chapter 9	Managing classic policies	93
	Add a policy	93
	Example policy - Exchange Server DAG backup	94
	Example policy - Sharded MongoDB cluster	95
Chapter 10	Managing backup images	97
	About the NetBackup catalog	97
	Search for backup images	97
Chapter 11	Pausing data protection activity	99
	Pause backups and other activity	99
	Allow NetBackup and authorized users to pause data protection activity	100
	Pause backups and other activity on a client	100
	View paused backups and other paused activities	100
	Resume data protection activity	101
Section 3	Managing security	102
Chapter 12	Security events and audit logs	103
	View security events and audit logs	103
	About NetBackup auditing	103
	User identity in the audit report	107

	Audit retention period and catalog backups of audit records	107
	Viewing the detailed NetBackup audit report	108
	Send audit events to system logs	110
Chapter 13	Managing security certificates	112
	About security management and certificates in NetBackup	112
	NetBackup host IDs and host ID-based certificates	113
	Managing NetBackup security certificates	114
	Reissue a NetBackup certificate	115
	Managing NetBackup certificate authorization tokens	117
	Using external security certificates with NetBackup	118
	Configure an external certificate for the NetBackup web server	119
	Remove the external certificate configured for the web server	120
	Update or renew the external certificate for the web server	120
	View external certificate information for the NetBackup hosts in the domain	121
Chapter 14	Managing host mappings	123
	View host security and mapping information	123
	Approve or add mappings for a host that has multiple host names	124
	Remove mappings for a host that has multiple host names	128
Chapter 15	Managing user sessions	129
	Sign out a NetBackup user session	129
	Unlock a NetBackup user	130
	Configure when idle sessions should time out	130
	Configure the maximum of concurrent user sessions	131
	Configure the maximum of failed sign-in attempts	131
	Display a banner to users when they sign in	132
Chapter 16	Managing the security settings for the primary server	133
	Certificate authority for secure communication	133
	Disable communication with NetBackup 8.0 and earlier hosts	134
	Disable automatic mapping of NetBackup host names	134
	Configure the global data-in-transit encryption setting	135
	About NetBackup certificate deployment security levels	136

Select a security level for NetBackup certificate deployment	138
About TLS session resumption	139
Set a passphrase for disaster recovery	139
About trusted primary servers	140
Add a trusted primary server	141
Remove a trusted primary server	142

Chapter 17 Using access keys, API keys, and access codes

.....	143
Access keys	143
API keys	143
Add an API key or view API key details (Administrators)	144
Edit, reissue, or delete an API key (Administrators)	145
Add an API key or view your API key details	146
Edit, reissue, or delete your API key	147
Use an API key with NetBackup REST APIs	148
Access codes	148
Get CLI access through web UI authentication	149
Approve your CLI access request	149
Approve CLI access requests of other users	149
Edit access settings	150

Chapter 18 Configuring authentication options

Sign-in options for the NetBackup web UI	151
Configure user authentication with smart cards or digital certificates	152
Configure smart card authentication with domain	152
Configure smart card authentication without domain	153
Edit the configuration for smart card authentication	154
Add or delete a CA certificate that is used for smart card authentication	155
Disable or temporarily disable smart card authentication	156
About Single Sign-On (SSO) configuration	156
Configure NetBackup for Single Sign-On (SSO)	158
Configure the SAML KeyStore	159
Configure the SAML keystore and add and enable the IDP configuration	162
Enroll the NetBackup primary server with the IDP	164
Manage an IDP configuration	165
Video: Configure Single Sign-On in NetBackup	167
Troubleshooting SSO	168
Redirection issues	168

	Unable to sign in due to authorization-related issues	170
Chapter 19	Managing role-based access control	172
	RBAC features	172
	Authorized users	173
	Configuring RBAC	174
	Notes for using NetBackup RBAC	174
	Add AD or LDAP domains	175
	View users in RBAC	175
	Add a user to a role (non-SAML)	175
	Add a smart card user to a role (non-SAML, without AD/LDAP)	176
	Add a user to a role (SAML)	177
	Remove a user from a role	178
	Disable web UI access for operating system (OS) administrators	178
	Disable command-line (CLI) access for operating system (OS) administrators	178
	Default RBAC roles	179
	Add a custom RBAC role	181
	Edit or remove a role a custom role	182
	Add a custom RBAC role to restore Azure-managed instances	183
	Add a custom RBAC role for a PaaS administrator	184
	Role permissions	185
	Manage access permission	186
	View access definitions	188
Section 4	Detection and reporting	189
Chapter 20	Detecting malware	190
	About malware detection	190
	Configure a new scan host pool	194
	Add an existing scan host	194
	Manage credentials	194
	Remove the scan host	196
	Deactivate the scan host	196
	Scan a policy client backup images for malware	196
	Perform malware scanning	198
	Scan a VMware asset for malware	200
	View the malware scan status	201

	Actions for malware scanned images	202
	Recover from malware-affected images (clients protected by policies)	203
	Recover a VMware asset affected by malware	204
	Troubleshooting	205
Chapter 21	Detecting anomalies	206
	About backup anomaly detection	206
	How a backup anomaly is detected	207
	View anomalies	208
	Configure anomaly detection settings	209
Chapter 22	Usage reporting and capacity licensing	211
	Track protected data size on your primary servers	211
	Add a local primary server	212
	Select license types to display in usage reporting	213
	Scheduling reports for capacity licensing	213
	Other configuration for incremental reporting	216
	Troubleshooting failures for usage reporting and incremental reporting	218
Section 5	NetBackup workloads and NetBackup Flex Scale	219
Chapter 23	NetBackup SaaS Protection	220
	Overview of NetBackup for SaaS	220
	Adding NetBackup SaaS Protection Hubs	222
	Configuring the autodiscovery frequency	223
	Proxy configuration for autodiscovery	223
	Viewing asset details	224
	Configuring permissions	225
	Troubleshooting SaaS workload issues	226
Chapter 24	NetBackup Flex Scale	228
	Managing NetBackup Flex Scale	228
	Access NetBackup Flex Scale from the NetBackup web UI	229
	Access NetBackup from the Flex Scale infrastructure management console	230
	Manage NetBackup and the Flex Scale cluster infrastructure from the Flex Scale UI	231

Chapter 25	NetBackup workloads	233
	Protection of other asset types and clients	233
Section 6	Disaster recovery and troubleshooting	234
Chapter 26	Managing Resiliency Platforms	235
	About Resiliency Platform in NetBackup	235
	Understanding the terms	236
	Configuring a Resiliency Platform	237
	Add a Resiliency Platform	237
	Configure a third-party CA certificate	238
	Edit or delete a Resiliency Platform	238
	View the automated or not-automated VMs	239
	Troubleshooting NetBackup and Resiliency Platform issues	241
Chapter 27	Managing Bare Metal Restore (BMR)	243
	About Bare Metal Restore (BMR)	243
	Add a custom role for a Bare Metal Restore (BMR) administrator	244
Chapter 28	Troubleshooting the NetBackup Web UI	246
	Tips for accessing the NetBackup web UI	246
	If a user doesn't have the correct permissions or access in the NetBackup web UI	248
	Unable to validate the user or group when configuring LDAP server	248

Introducing the NetBackup web user interface

This chapter includes the following topics:

- [About the NetBackup web UI](#)
- [Terminology](#)
- [First-time sign in to the NetBackup web UI](#)
- [Sign in to the NetBackup web UI](#)
- [Sign out of the NetBackup web UI](#)
- [Documentation for Catalog Recovery Wizard, disk array hosts, disk pools, and Host Properties in the NetBackup web UI](#)

About the NetBackup web UI

Note: The NetBackup web UI is best viewed at a 1280x1024 or higher screen resolution.

The NetBackup web user interface provides the following features:

- Ability to access the primary server from a web browser, including Chrome and Firefox. For details on supported browsers for the web UI, see the [NetBackup Software Compatibility List](#).

Note that the NetBackup web UI may behave differently for different browsers. Some functionality, for example a date picker, may not be available on all browsers. These inconsistencies are due to the capabilities of the browser and not because of a limitation with NetBackup.

- A dashboard that displays a quick overview of the information that is important to you.
- Role-based access control (RBAC) that lets the administrator configure user access to NetBackup and to delegate the tasks such as security, storage management, or workload protection.
- Management of NetBackup security settings, certificates, API keys, and user sessions.
- Management of NetBackup host properties.
- Data protection is achieved through protection plans or policies. (Policy support is limited at this time. Additional policy types will be added in future releases.)
- Detection and reporting features provide for the detection of malware and anomalies and provide usage reporting to track the size of backup data on your primary servers. You can also easily connect to Veritas Net Insights Console to view and manage NetBackup licensing.

Access control in the NetBackup web UI

NetBackup uses role-based access control to grant access to the web UI. Access control is accomplished through roles.

- A role defines the operations that a user can perform and the access that the user has to any workload assets, protection plans, or credentials. A user can have multiple roles, which allows for full and for flexible customization of user access.
- RBAC is only available for the web UI and the APIs.
Other access control methods for NetBackup are not supported for the web UI and APIs, with the exception of Enhanced Auditing (EA).

Monitor NetBackup jobs and events

The NetBackup web UI lets administrators more easily monitor NetBackup operations and events and identify any issues that need attention.

- The dashboard displays an overview of NetBackup operations and security information. This information includes jobs, certificates, tokens, security events, malware and anomaly detection, and usage reporting.
The dashboard widgets that display depend on a user's RBAC role and permissions.
- Email notifications can be configured so administrators receive notifications when job failures occur. NetBackup supports any ticketing system that can receive inbound email.

Protection plans: One place to configure schedules and storage

Data protection with protection plans is fully managed with role-based access control (RBAC). The NetBackup administrator can manage which users can view and manage assets and can perform backups and restores. Each default workload administrator role (for example, Default VMware Administrator) allows a user access to protection plans, jobs, and credentials.

Protection plans offer the following benefits:

- A workload administrator can create and manage protection plans, including the backup schedules and storage that is used. This administrator selects the protection plans that protect assets.
See [“Role permissions”](#) on page 185.
- In addition to schedules for backups, a protection plan can also include a schedule for replication and long-term retention.
- When you select from your available storage, you can see any additional features available for that storage.
- Users with a workload administrator role can create protection plans, manage credentials, subscribe assets to the protection plans that meet the SLO, and monitor protection status.

The web UI supports protection plans for the following workloads.

- Apache Cassandra
- Cloud
- Cloud object store
- Kubernetes
- Microsoft SQL Server
- MySQL
- Nutanix AHV
- OpenStack
- Oracle
- PostgreSQL
- Red Hat Virtualization (RHV)
- SaaS
- VMware

Backup policies

NetBackup classic policies are available for the Administrator that wants to continue to use policies for data protection.

See [“Support for NetBackup classic policies”](#) on page 79.

Server-directed and self-service recovery

Administrators can perform server-directed restores from the web UI. This type of restore is available for all policy types.

The workload administrator can perform self-service recovery of VMs, databases, or other asset types. This type of recovery is available for the assets that are protected with recovery points.

For the workloads that support the instant access feature, users can mount a snapshot for immediate access to a VM's files or to a database.

Terminology

The following table describes the concepts and terms in web user interface.

Table 1-1 Web user interface terminology and concepts

Term	Definition
Administrator	A user that has complete access and permissions to NetBackup and all of the interfaces, including the NetBackup web UI. The root, administrator, and Enhanced Auditing user all have complete access to NetBackup. In the <i>NetBackup Web UI</i> guides, the term <i>NetBackup administrator</i> also refers to a user that has full permissions for NetBackup. Also see <i>role</i> .
Asset group	See <i>intelligent group</i> .
Asset	The data to be protected, such as physical clients, virtual machines, and database applications.
Backup now	An immediate backup of an asset. NetBackup performs a one-time, full backup of an asset using the selected protection plan. This backup does not affect any scheduled backups.
Classic policy	In the NetBackup web UI, indicates that a legacy policy protects the asset.
External certificate	A security certificate that is issued from any CA other than NetBackup.

Table 1-1 Web user interface terminology and concepts (*continued*)

Term	Definition
Intelligent group	<p>Allows NetBackup to automatically select assets for protection based on the criteria (queries) that you specify. An intelligent group automatically stays up-to-date with changes in the production environment. These groups are also referred to as asset groups.</p> <p>These groups appear under the tab Intelligent VM groups or Intelligent groups.</p>
NetBackup certificate	A security certificate that is issued from the NetBackup CA.
Protection plan	A protection plan defines when backups are performed, how long the backups are retained, and the type of storage to use. Once a protection plan is set up, assets can be subscribed to the protection plan.
RBAC	<p>Role-based access control. The role administrator can delegate or limit access to the NetBackup web UI through the roles that are configured in RBAC.</p> <p>Note: The roles that you configure in RBAC do not control access to the NetBackup Administration Console.</p>
Role	For RBAC, defines the operations that a user can perform and the assets or objects that they can access. For example, you can configure a role to manage recovery of specific databases and the credentials that are needed for backups and restores.
Storage	The storage to which the data is backed up, replicated, or duplicated (for long-term retention).
Subscribe, to a protection plan	The action of selecting an asset or an asset group to subscribe to a protection plan. The asset is then protected according to the schedule in the plan. The web UI also refers to <i>Subscribe</i> as <i>Add protection</i> .
Unsubscribe, from a protection plan	<i>Unsubscribe</i> refers to the action of removing protection or removing an asset or asset group from a plan.
Workload	The type of asset. For example: VMware, Microsoft SQL Server, or Cloud.

First-time sign in to the NetBackup web UI

After the installation of NetBackup, an administrator must sign into the NetBackup web UI from a web browser and create RBAC roles for users. A role gives a user permissions and access to the NetBackup environment through the web UI, based on the user’s role in your organization. Some users have access to the web UI by default.

See [“Authorized users”](#) on page 173.

If you do not have access to root or to administrator credentials you can use the `bpbaz -AddRBACPrincipal` command to add an administrator user.

To sign in to a NetBackup primary server using the NetBackup web UI

- 1 Open a web browser and go to the following URL.

`https://primaryserver/webui/login`

The *primaryserver* is the host name or IP address of the NetBackup primary server that you want to sign in to.

If you are not able to access the web UI, refer to [Support and additional configuration](#).

- 2 Enter the administrator credentials and click **Sign in**.

For this type of user	Use this format	Example
Local user	<i>username</i>	jane_doe
Windows user	<i>DOMAINusername</i>	WINDOWS\jane_doe
UNIX user	<i>username@domain</i>	john_doe@unix

- 3 On the left, select **Security > RBAC**.

- 4 You can give users access to the NetBackup web UI in one of the following ways:
- Create roles for all users that require access to NetBackup.
 - Delegate the task of creating roles to another user.
Create a role that has permissions to add RBAC roles. This user can then create roles for all users that require access to the NetBackup web UI.

See [“Configuring RBAC ”](#) on page 174.

Root or administrator access is no longer needed for the web UI once you have delegated one or more users with permissions to create RBAC roles.

Support and additional configuration

Refer to the following information for help with accessing the web UI.

- Ensure that you are an authorized user.
See [“Authorized users”](#) on page 173.
- For details on supported browsers for the web UI, see the [NetBackup Software Compatibility List](#).
- If port 443 is blocked or in use, you can [configure and use a custom port](#).
- If you want to use an external certificate with the web browser, see the instructions for [configuring an external certificate](#) for the web server.
- See [other tips](#) for accessing the web UI.

Sign in to the NetBackup web UI

Authorized users can sign in to a NetBackup primary server from a web browser, using the NetBackup web UI.

For more information, refer to the *Authorized users* section in the *NetBackup™ Web UI Administrator's Guide*.

The following sign-in options are available:

- [Sign in with a username and password](#)
- [Sign in with a certificate or smart card](#)
- [Sign in with single sign-on \(SSO\)](#)

Sign in with a username and password

Only authorized users can sign in to NetBackup web UI. Contact your NetBackup security administrator for more information.

To sign in to a NetBackup primary server using a username and password

- 1 Open a web browser and go to the following URL.

`https://primaryserver/webui/login`

The *primaryserver* is the host name or IP address of the NetBackup primary server that you want to sign in to.

- 2 Depending on the sign-in options that are available, choose from the following:
 - Enter your credentials and click **Sign in**.
 - If the default method is not username and password, click **Sign in with username and password**. Then enter your credentials.

The following are example credentials:

For this type of user	Use this format	Example
Local user	<i>username</i>	jane_doe
Windows user	<i>DOMAINusername</i>	WINDOWS\jane_doe
UNIX user	<i>username</i>	john_doe

Sign in with a certificate or smart card

You can sign in to NetBackup web UI with a smart card or digital certificate if you are an authorized user. Contact your NetBackup security administrator for more information.

To use a digital certificate that is not on a smart card, you must first upload the certificate to the browser's certificate manager. See the browser documentation for instructions or contact your certificate administrator for more information.

To sign in with a certificate or smart card

- 1 Open a web browser and go to the following URL.
`https://primaryserver/webui/login`
The *primaryserver* is the host name or IP address of the NetBackup primary server that you want to sign in to.
- 2 Click **Sign in with certificate or smart card**.
- 3 When your browser prompts you, select the certificate.

Sign in with single sign-on (SSO)

You can sign in to NetBackup web UI with the single sign-on (SSO) option if SAML is configured as an identity provider in your NetBackup environment. Contact your NetBackup security administrator for more information.

To sign in to a NetBackup primary server using SSO

- 1 Open a web browser and go to the following URL.
`https://primaryserver/webui/login`
 The *primaryserver* is the host name or IP address of the NetBackup primary server that you want to sign in to.
- 2 Click **Sign in with single sign-on**.
- 3 Follow the steps as provided by your administrator.
 On subsequent logons, NetBackup signs you in automatically to the primary server.

Sign out of the NetBackup web UI

Note that NetBackup automatically signs you out of the web UI after 24 hours, which is the maximum time that is allowed for a user session. After that time NetBackup requires that you sign in again. You can also sign out if you want to change the sign-in option that you want to use (username and password, smart card, or single sign-on (SSO)).

To sign out of the NetBackup web UI

- ◆ On the top right, click the profile icon and click **Sign out**.

Documentation for Catalog Recovery Wizard, disk array hosts, disk pools, and Host Properties in the NetBackup web UI

The NetBackup web UI includes some functions that are not documented in this guide. Unless noted otherwise, refer to the [NetBackup Administrator's Guide, Volume I](#) for details about these functions:

Catalog Recovery

- Catalog Recovery Wizard

Disk array Hosts

- Disk array hosts

Disk pools

- Update Disk Volume option
- OpenStorage disk pool state

Host Properties:

- Access Control
- Active Directory
- Backup host pools (see the *NetBackup Snapshot Administrator's Guide*)
- Client Attributes
- Client Name
- Client Settings for UNIX clients
- Client Settings for Windows clients
- Credential Access
- Data Classification
- Default Job Priorities
- Distributed application restore mapping
- Encryption
- Enterprise Vault
- Enterprise Vault Hosts
- Exclude Lists
- General Server
- Global Attributes
- Logging
- Lotus Notes
- NDMP Global Credentials
- Network
- Network Settings
- Nutanix AHV access hosts (see the *NetBackup Nutanix Administrator's Guide*)
- Port Ranges
- Restore Failover
- Retention Periods
- RHV Access Hosts
- Servers
- SLP settings

- Universal Settings
- User Account Settings
- VMware Access Hosts

Monitoring and notifications

This chapter includes the following topics:

- [The NetBackup dashboard](#)
- [About the Activity monitor](#)
- [Job monitoring](#)
- [Job notifications](#)
- [NetBackup event notifications](#)

The NetBackup dashboard

Table 2-1 The NetBackup dashboard

Dashboard widget	Description
Jobs	Lists job information, including the number of active and queued jobs and the status of attempted and completed jobs.
Malware detection	Displays the malware scan result status for the images including Impacted, Not impacted, Failed, In progress, and Pending.
Anomaly detection	<p>Displays the total anomalies that are reported so far.</p> <p>See “View anomalies” on page 208.</p> <p>Note: An anomalies count of 0 indicates there are no anomalies generated or that the anomaly detection services are not running.</p>

Table 2-1 The NetBackup dashboard (*continued*)

Dashboard widget	Description
Paused protection activities	<p>Lists any paused protection activities for clients. These activities include new backups, duplication, and image expiration. NetBackup pauses protection if it detects malware in backup images.</p> <p>Automatic indicates the activities that are automatically paused by NetBackup. User-initiated indicates an activity that was paused manually by a user.</p> <p>See “Pause backups and other activity” on page 99.</p>
Tokens	<p>Displays the information about the authorization tokens in your environment.</p>
Certificates	<p>Displays the information about the NetBackup host ID-based security certificates or the external certificates in your environment.</p> <p>For external certificates, the following information is shown for NetBackup 8.2 and later hosts:</p> <ul style="list-style-type: none">■ Total hosts. The total number of hosts. The hosts must be online and able to communicate with NetBackup primary server.■ Missing. The number of hosts that do not have an external certificate enrolled.■ Valid. The number of hosts that have an external certificate enrolled.■ Expired. The number of hosts with expired external certificates. <p>More details are available in Certificates > External certificates.</p> <p>See “About security management and certificates in NetBackup” on page 112.</p>
Security events	<p>The Access history view includes a record of logon events. The Audit events view includes the events that users initiate on the NetBackup primary server.</p>
Usage reporting	<p>Lists the size of the backup data for the NetBackup primary servers in your organization. This reporting is useful to track capacity licensing. Use the drop-down lists in the top right to select the time period and the view that you want to display. Click on a server name to see specific details for that server.</p> <p>Additional details are available for how to configure NetBackup to display primary server information in this widget.</p> <p>See “Track protected data size on your primary servers” on page 211.</p>

About the Activity monitor







Use the Activity monitor to monitor and control the following aspects of NetBackup. Updates to the Activity monitor occur as jobs are initiated, updated, and completed.

Jobs	Displays all of the jobs that are in process or that have completed for the primary server that is currently selected. The Jobs tab also displays details about the jobs. See “ Job monitoring ” on page 25.
Daemons	Displays the status of NetBackup daemons on the primary server. Click Change server to select a different server.
Processes	Displays the NetBackup processes that run on on the primary server. Click Change server to select a different server.











Job monitoring

Use the **Jobs** node in the Activity monitor to monitor the jobs in your NetBackup environment. The default view for jobs is the **List view** that contains the non-hierarchical list of all the jobs. You can also use the **Hierarchical view** to see the hierarchy of parent and child jobs.

List view

<input type="checkbox"/>	Job ID ↑	Type	Client or display name	Job state
<input type="checkbox"/>	 22322314	Backup	pe...10	Done
<input type="checkbox"/>	 22322315	Backup	pe...10	Done
<input type="checkbox"/>	 22322316	Backup	pe...10	Done
<input type="checkbox"/>	 22322317	Backup	pe...10	Done
<input type="checkbox"/>	 22322318	Backup	pe...10	Done
<input type="checkbox"/>	 22322319	Backup	pe...08	Done

Hierarchy view

<input type="checkbox"/>	Job ID ↑	Type	Client or display name	Job state
▼ <input type="checkbox"/>	 22322314	Backup	pe...10	Done
<input type="checkbox"/>	 22322315	Backup	pe...10	Done
<input type="checkbox"/>	 22322316	Backup	pe...10	Done
<input type="checkbox"/>	 22322317	Backup	pe...10	Done
<input type="checkbox"/>	 22322318	Backup	pe...10	Done
▼ <input type="checkbox"/>	 22322319	Backup	pe...08	Done
<input type="checkbox"/>	 22322320	Backup	pe...08	Done
<input type="checkbox"/>	 22322321	Backup	pe...08	Done
<input type="checkbox"/>	 22322322	Backup	pe...08	Done
<input type="checkbox"/>	 22322323	Backup	pe...08	Done

RBAC permissions for jobs

The type of jobs that you can view and manage depend on the RBAC role that you have. For example, a workload administrator (such as the Default VMware Administrator role) can view and manage only jobs for that workload. In contrast, the Administrator role lets you view and manage all NetBackup jobs.

See “[Workloads that require a custom RBAC role for specific job permissions](#)” on page 26.

Job hierarchy view

If you have an RBAC role that allows access to jobs, you can see the jobs list in the job hierarchy view. For example, the Default VMware Administrator role lets you see VMware jobs in the hierarchy view. However, if you only have access to one or more VMs (asset-level access), no jobs display in the job hierarchy view.

See “[Default RBAC roles](#)” on page 179.

Workloads that require a custom RBAC role for specific job permissions

The 10.1 release now offers granular job access for certain workloads. This functionality lets you create a custom RBAC role with job permissions for a particular workload.

Note that these workloads do not have a corresponding default RBAC role. When you configure the custom role, the permissions in the **Workloads** card do not apply for these workloads. You can configure job permissions for the following workload types:

BackTrack	Hyper-V	NDMP
DataStore	Informix	PureDisk Export
DB2	Lotus Notes	SAP
Enterprise Vault	SharePoint	Standard
Exchange	MS-Windows	Sybase
FlashBackup	NAS Data Protection	Vault
FlashBackup Windows	NBU Catalog	

To create a custom role with job permissions

- 1 Create a custom RBAC role.
- 2 On the **Assets** tab, locate the workload name and select the job permissions for the workload.

For example, consider that you want to create a custom role so a Hyper-V administrator can view Hyper-V jobs. Locate **Hyper-V** and select the wanted job permissions.

- 3 Select any additional permissions that you want for the role.

For example:

- Other global permissions
- Permissions for protection plans and for credentials

- 4 Add the users you want to assign to the role.

RBAC job permissions for BigData workloads

In the 10.1 release, you cannot configure job permissions specifically for BigData workloads (Hadoop, HBase or MongoDB). To view and manage jobs for BigData, create a role that has the RBAC permissions for all NetBackup jobs.

To configure job permissions

- 1 Create a custom RBAC role.
- 2 Under **Permissions**, click **Assign**.
- 3 On the **Global** tab, expand NetBackup management.
- 4 Locate **Jobs** and select the job permissions you want for the role.
- 5 Add the wanted users to the role.

View a job

For each job that NetBackup runs you can see the following details: the file list and the status of the job, the logged details for the job, and the job hierarchy.

The jobs that you can view depend on the type of RBAC role that you have.

See [“Job monitoring”](#) on page 25.

To view a job and the job details

- 1 On the left, click **Activity monitor > Jobs**.
- 2 Click the job name that you want to view.
- 3 On the **Overview** tab you can view information about a job.
 - The **File List** contains the files that are included in the backup image.
 - The **Status** section shows the status and the status codes that are related to the job. Click the status code number to view information about this status code in the Veritas Knowledge Base.
See the [NetBackup Status Codes Reference Guide](#).

- 4 Click the **Details** tab to view the logged details about a job. You can filter the logs by error type using the drop-down menu.
See [“Search for or filter jobs in the jobs list”](#) on page 29.
- 5 Click the **Job hierarchy** tab to view the complete hierarchy for the job, including any ancestor and any child jobs.
See [“View the jobs in the Hierarchy view”](#) on page 28.

View the jobs in the List view

In the **Jobs** node in the Activity monitor, the list view displays the jobs, without showing the relationship of parent and child jobs.

To view the jobs in the List view

- 1 On the left, click **Activity monitor > Jobs**.
- 2 Click the **List view** button.



View the jobs in the Hierarchy view

In the **Jobs** node in the Activity monitor, the hierarchy view displays the jobs so you can see the complete hierarchy of the jobs. This view includes the top-level job (or root job) and its child jobs (if applicable). A child job can, in turn, be a parent of its own child jobs.

To view the jobs in the Hierarchy view

- 1 On the left, click **Activity monitor > Jobs**.
- 2 Click the **Hierarchy view** button.



- 3 Locate the top-level job and expand it to see the child jobs.

Jobs: cancel, suspend, restart, resume, delete

Depending on the state of a job, you can perform certain actions on that job.

To manage a job

- 1 Click **Activity monitor > Jobs**.
- 2 Select one or more jobs.
- 3 The top menu shows the actions that you can perform for the selected jobs.

Cancel	<p>You can cancel the jobs that have not yet completed. They can be in one of the following states: queued, re-queued, active, incomplete, or suspended.</p> <p>When a parent job is cancelled, any child jobs are also cancelled.</p>
Suspend	<p>You can suspend backup and restore any jobs that contain checkpoints.</p>
Restart	<p>You can restart the jobs that have completed, failed, or that have been cancelled or suspended.</p> <p>A new job ID is created for the new job.</p>
Resume	<p>You can resume the jobs that have been suspended or are in an incomplete state.</p>
Delete	<p>You can delete the jobs that have completed. When a parent job is deleted, any child jobs are also deleted.</p>

Search for or filter jobs in the jobs list

You can search for jobs in the Activity monitor or create filters to customize the jobs that are displayed.

Search for jobs in the jobs list

The search feature lets you search for the following job information: status code (complete status code #); policy name; client or display name; client; job ID (complete job ID #), or the job's parent ID.

Search for jobs in the jobs list

- 1 Click **Activity monitor > Jobs**.
- 2 In the **Search** box, type the keyword you want to find. For example, a client name or a status code number.

Filter the job list

To filter the job list

- 1 Click **Activity monitor > Jobs**.
- 2 In the toolbar, click the **Filter** icon.
- 3 Click on a filter that you created. Or, click **All jobs** to display all of the available jobs.

Create a jobs filter

You can create specific filters based on one or more query criteria.

To create a jobs filter

- 1 Click **Activity monitor > Jobs**.
- 2 In the toolbar, click the **Filter** icon.
- 3 If you have not created any filters yet, on the left click **Create filter**.

Otherwise, click **Actions > Create**.


- 4 Enter a name and an optional description for the filter.
- 5 In the **Query** pane, use the drop-down lists to create a condition.

For example, to jobs for the VMware policy type, **Policy type = VMware**.

Query

+ Condition

+ Sub-query

Policy Type ▾ = ▾ VMware ▾ 

- 6 Add any additional conditions for the filter or add a sub-query to apply to a condition.

For example, assume that you want to completed jobs that have a status code of 196 or 239. Create the following query:

```
State = Done
AND
  (Status code = 196
  OR
  Status code = 239)
```

Query

AND OR + Condition + Sub-query

State = Done

AND OR + Condition + Sub-query

Status code = 196

Status code = 239

- 7 Choose from the following options:

- To save this query and create another query, click **Save and add another**.
- To save this query and return to the **Jobs** list, click **Save and apply**.

Example 1 . Query filter for jobs with the VMare policy type.

Activity monitor

Jobs Daemons Processes Background tasks

Search...

All jobs < VMware

Job ID	Type ↑	Client or display name	Job state	Status code	Schedule	Policy Type	Sc
<input type="checkbox"/> 25694271	Snapshot	msdly15awd07 - wsd071302	Done	0	-	VMware	Fu
<input type="checkbox"/> 25694272	Snapshot	msdly15awd08 - wsd071302	Done	0	-	VMware	Fu
<input type="checkbox"/> 25825907	Snapshot	msdly15awd08 - wsd071302	Done	0	-	VMware	Fu
<input type="checkbox"/> 25825908	Snapshot	msdly15awd07 - wsd071302	Done	0	-	VMware	Fu
<input type="checkbox"/> 25665780	Snapshot	gsmd0715awd08 - wsd071302	Done	0	-	VMware	Dil
<input type="checkbox"/> 25674806	Snapshot	gsmd0715awd07 - wsd071302	Done	0	-	VMware	Dil
<input type="checkbox"/> 25674807	Snapshot	gsmd0715awd07 - wsd071302	Done	0	-	VMware	Dil
<input type="checkbox"/> 25674808	Snapshot	gsmd0715awd07 - wsd071302	Failed	4243	-	VMware	Dil
<input type="checkbox"/> 25674809	Snapshot	gsmd0715awd07 - wsd071302	Done	0	-	VMware	Dil

Jobs 346062 (Queued 0, Active 0, Waiting for retry 0, Suspended 0, Incomplete 0, Done 346062) Filter applied (683)

Example 2. Query filter for jobs that are done and have a status code of 196 or 239.

Activity monitor

Jobs Daemons Processes Background tasks

Search...

All jobs Standard Type=Backup Status code > 1 Code 239 or 196

Job ID	Type ↑	Client or display name	Job state	Status code	Schedule	Policy Type	Sc
<input type="checkbox"/> 25653771	Backup	BackupClient01	Failed	196	FULL	Standard	Fu
<input type="checkbox"/> 25654045	Backup	BackupClient01	Failed	196	-	Standard	Fu
<input type="checkbox"/> 25667318	Backup	BackupClient01	Failed	196	-	Hyper-V	Fu
<input type="checkbox"/> 25667831	Backup	BackupClient01	Failed	239	*NULL*		
<input type="checkbox"/> 25667832	Backup	BackupClient01	Failed	239	*NULL*		
<input type="checkbox"/> 25667841	Backup	BackupClient01	Failed	239	*NULL*		
<input type="checkbox"/> 25667886	Backup	BackupClient01	Failed	239	*NULL*		
<input type="checkbox"/> 25705499	Backup	BackupClient01	Failed	196	-	VMware	Dit
<input type="checkbox"/> 25722200	Backup	BackupClient01	Failed	196	-	Standard	Fu

Jobs 346062 (Queued 0, Active 0, Waiting for retry 0, Suspended 0, Incomplete 0, Done 346062) Filter applied (53)

Edit or delete a jobs filter

You can edit the query criteria for a jobs filter or delete a filter that you no longer need.

Edit a jobs filter

To edit a jobs filter

- 1 Click **Activity monitor > Jobs**.
- 2 In the toolbar, click the **Filter** icon.
- 3 Locate the filter that you want to apply and click **Actions > Edit**.
- 4 Make the changes that you want to the filter and click **Save and apply**.

Delete a jobs filter

To delete a jobs filter

- 1 Click **Activity monitor > Jobs**.
- 2 In the toolbar, click the **Filter** icon.
- 3 Locate the filter that you want to delete and click **Actions > Delete > Delete**.

Troubleshooting the viewing of jobs

You may see no job results because:

- The keyword or keywords that you searched for do not match any of the details for any jobs.
- You applied a search filter and no jobs match the filter criteria.
- The jobs in the hierarchy view have parent jobs, but you do not have permission to view the parent jobs.
Contact your NetBackup system administrator to get the necessary RBAC role permissions.
- NetBackup limits the number of tabs that you can have open with the Jobs hierarchy view.
If you cannot expand a parent job and see its child jobs, try closing any additional Jobs tabs that you have open.

Job notifications

The following types of email notifications are available for NetBackup jobs.

- Notifications when job failures occur. NetBackup supports the ticketing systems that use inbound email service for ticket creation.
See [“Send email notifications for job failures”](#) on page 33.
- Notifications to the backup administrator about backups with a non-zero status.
See [“Send notifications to the backup administrator about failed backups”](#) on page 36.
- Notifications to the host administrator about successful and failed backups for a specific host.
See [“Send notifications to a host administrator about backups”](#) on page 37.

Send email notifications for job failures

You can configure NetBackup to send email notifications when job failures occur. This way administrators spend less time monitoring NetBackup for job failures and manually creating tickets to track issues. NetBackup supports the ticketing systems that use inbound email service for ticket creation.

See [“Status codes that generate alerts”](#) on page 35.

NetBackup generates alerts based on certain job failure conditions or NetBackup status codes. Alerts that are similar or have a similar reason for failure are marked as duplicates. Email notifications for duplicate alerts are not sent for the next 24 hours. If a notification cannot be sent, NetBackup retries every 2 hours, up to three attempts.

NetBackup audits an event if changes are made to the alert settings or when it cannot generate an alert or send an email notification. See [“About NetBackup auditing”](#) on page 103.

Prerequisites

Review the following requirements before you configure email notifications using a ticketing system.

- The ticketing system is up and running.
- The SMTP server is up and running.
- A policy is configured in the ticketing system to create tickets (or incidents) based on the inbound emails that NetBackup sends.

To configure email notifications

- 1 At the top right, click **Settings > Email notifications**.
- 2 Go to the **Email notifications** tab.
- 3 Select **Send email notifications**.
- 4 Enter the email information including the recipient's email address, the sender's email address, and the email sender's name.
- 5 Enter the SMTP server details including the SMTP server name and port number.

Provide the SMTP username and password if you have specified the credentials earlier on the SMTP server.
- 6 Click **Save**.
- 7 Log on to the ticketing system to view the tickets that were created based on NetBackup alerts.

Exclude specific status codes from email notifications

You can exclude specific status codes so that email notifications are not sent for these errors.

To exclude specific status codes

- 1 At the top right, click **Settings > Email notifications**.
- 2 Locate **Exclude status codes**.
- 3 Enter the status codes or a range of status codes (separated by commas) for which you do not want to receive email notifications.
- 4 Click **Save**.

Sample email notification for an alert

An email notification for an alert contains information about the primary server, job, policy, schedule, and error. Emails may contain other information based on the type of job. For example, for VMware job failures, details such as vCenter Server and ESX host are present in the email notification.

Example email notification:

Primary Server: primary1.example.com

Client Name: client1.example.com

Job ID: 50

Job Start Time: 2018-05-17 14:43:52.0

Job End Time: 2018-05-17 15:01:27.0

Job Type: BACKUP

Parent Job ID: 49

Policy Name: Win_policy

Policy Type: WINDOWS_NT

Schedule Name: schedule1

Schedule Type: FULL

Status Code: 2074

Error Message: Disk volume is down

Status codes that generate alerts

The NetBackup web UI supports alerts for VMware job failures and retains the alerts for 90 days. NetBackup generates alerts for the supported status codes for following job types: backup, snapshot, snapshot replication, index from snapshot, and backup from snapshot. For the complete list of status codes for which alerts are generated, refer to the information for alert notification status codes in the [NetBackup Status Codes Reference Guide](#).

[Table 2-2](#) lists some of the conditions or status codes for which alerts are generated. These alerts are sent to the ticketing system through email notifications.

Table 2-2 Examples of status codes that generate alerts

Status code	Error message
10	Allocation failed

Table 2-2 Examples of status codes that generate alerts (*continued*)

Status code	Error message
196	Client backup was not attempted because backup window closed
213	No storage units available for use
219	The required storage unit is unavailable
2001	No drives are available
2074	Disk volume is down
2505	Unable to connect to the database
4200	Operation failed: Unable to acquire snapshot lock
5449	The script is not approved for execution
7625	SSL socket connection failed

Send notifications to the backup administrator about failed backups

You can send notifications to the backup administrator about backups with a non-zero status.

On UNIX, NetBackup uses the mail transfer agent sendmail to send email notifications. For Windows, NetBackup requires that an application to transfer messages using SMTP is installed and that the `nbmail.cmd` script is configured on the Windows hosts that send notifications.

See [“Configure the nbmail.cmd script on the Windows hosts”](#) on page 37.

To configure notifications for the backup administrator of a NetBackup host, see the following topic.

See [“Send notifications to a host administrator about backups”](#) on page 37.

To send notifications to the backup administrator about failed backups

- 1 On the left, select **Hosts > Host properties**.
- 2 Select the host and click **Connect**.
- 3 Click **Edit primary server**.
- 4 Click **Global attributes**.

- 5 Enter the email address of the administrator. (Separate multiple addresses with commas.)
- 6 Click **Save**.

Send notifications to a host administrator about backups

You can send notifications to the host administrator about successful and failed backups for a specific host.

On UNIX, NetBackup uses the mail transfer agent sendmail to send email notifications. Windows requires that an application to transfer messages with SMTP is installed. You also must configure the `nbmail.cmd` script on the Windows hosts that send notifications.

See [“Configure the nbmail.cmd script on the Windows hosts”](#) on page 37.

To send notifications for backups of a specific host

- 1 On the left, select **Hosts > Host properties**.
- 2 Select the host and click **Connect**.
- 3 Click **Edit client**.
- 4 Click **Universal settings**.
- 5 Choose how to send the email notifications.
 - To send email notifications from the client, select **Client sends email**.
 - To send email notifications from the server, select **Server sends email**.
- 6 Enter the email address of the host administrator. (Separate multiple addresses with commas.)
- 7 Click **Save**.

Configure the nbmail.cmd script on the Windows hosts

For Windows hosts to send and receive email notifications about backups, the `nbmail.cmd` script must be configured on the applicable hosts.

To configure the nbmail.cmd script on the Windows hosts

- 1 Create a backup copy of `nbmail.cmd`.
- 2 On the primary server, locate the following script:
`install_path\NetBackup\bin\goodies\nbmail.cmd`
- 3 Copy the script to the following directory on the applicable hosts:
`install_path\NetBackup\bin\`

Primary and media server	NetBackup sends notifications from the server if you configure the following setting: <ul style="list-style-type: none">■ The Administrator's email address in Global Attributes.■ The Server sends email option in the Universal Settings.
Client.	NetBackup sends notifications from the client if you configure the following setting: <ul style="list-style-type: none">■ The Client sends email option in the Universal Settings.

4 Use a text editor to open `nbmail.cmd`.

The following options are used in the script:

<code>-s</code>	The subject line of the email
<code>-t</code>	Indicates who receives the email.
<code>-i</code>	The originator of the email, though it is not necessarily known to the mail server. The default (<code>-i Netbackup</code>) shows that the email is from NetBackup.
<code>-server</code>	The name of the SMTP server that is configured to accept and relay emails.
<code>-q</code>	Suppresses all output to the screen.

5 Adjust the lines as follows:

- Remove `@REM` from each of the five lines to activate the necessary sections for BLAT to run.
- Replace `SERVER_1` with the name of the mail server. For example:

```
@IF "%~4"==" " (  
blat %3 -s %2 -t %1 -i Netbackup -server emailserver.company.com -q  
) ELSE (  
blat %3 -s %2 -t %1 -i Netbackup -server emailserver.company.com -q -attach %4  
)
```

6 Save `nbmail.cmd`.

NetBackup event notifications

To make NetBackup administrators aware of important system events, NetBackup regularly queries system logs and displays notifications about the events.

Note: Job events are not included with these notifications. See job details in the **Activity Monitor** for information about job events.

A **Notifications** icon is located at the top right in the web UI. You can click the icon to open the **Notifications** window and view a list of critical notifications 10 at a time. If a number is displayed with the icon, it indicates how many unseen critical messages exist. After you have opened the window, the number is reset.

From the window, you can choose to see a more comprehensive list of all notifications. Each event has a category for its NetBackup or external component and is assigned a severity level:

- Error
- Critical
- Warning
- Information
- Debug
- Notice

You can sort, filter, and search the list. The comprehensive list also lets you review details about each event. The details include the full description as well as any appropriate extended attributes.

NetBackup notifications are not available if the NetBackup Messaging Broker (`nbmqbroker`) is not running. See the *NetBackup Troubleshooting Guide* for information about restarting the service.

View notifications

To view notifications

- 1 At the top right, click the **Notifications** icon to view a list of critical notifications 10 at a time.

Note: If a number is displayed with the icon, it indicates how many unseen critical messages exist. After you have opened the **Notifications** window, the number is reset.

Click **Load 10 more** to view the next 10 notifications. After you have viewed 30 notifications, click **Show all** to view any remaining messages.

Use **Refresh** to load the most recent notifications again.

- 2 To view all notifications, click **Show all** to open the **Events** page. On the page, you can do the following:
 - Click an event to view its details. The details include the full description as well as extended attributes.
 - To sort the list, click any of the column headings except **Description**. Events are sorted by default by the date received.
 - To filter events, click **Filter**. You can filter by **Severity** and **Timeframe**. In the **Filters** menu, select the parameter values you want to filter by, and then click **Apply filters**.
To remove all filters, click **Clear all**.
 - To search for events, enter the search string in the **Search** field. You can search for values in all columns except **Description** and **Received**.

Modify or disable NetBackup event notifications in the web UI

You can disable specific types of NetBackup event notifications that appear in the web UI, or modify their severity and priority, by making changes to the `eventlog.properties` file on the NetBackup primary server:

- Windows:
`install_path\var\global\wmc\h2Stores\notifications\properties`
- UNIX:
`/usr/opensv/var/global/wmc/h2Stores/notifications/properties`

To disable event notifications

- ◆ Add a `DISABLE` entry in the `eventlog.properties` file in one of the following formats:


```
DISABLE.NotificationType = true
```

```
Or DISABLE.NotificationType.Action = true
```

```
Or DISABLE.namespace
```

For valid *NotificationType* and *Action* values, see the following topic.

See [Table 2-3](#) on page 42.

For example:

- To disable notifications about all storage unit events:

```
DISABLE.StorageUnit = true
```

- To disable only notifications about create storage unit events:

```
DISABLE.StorageUnit.CREATE = true
```

- To disable only notifications about update to storage unit events using a namespace:

```
DISABLE.eventlog.vrts.nbu.emm.storageunit.update = true
```

To modify the priority or severity of event notifications

- ◆ Add or change an entry in the `eventlog.properties` file in one of the following formats:

```
NotificationType.Action.priority = value
```

```
Or NotificationType.Action.severity = value
```

Valid priority values are: LOW, MEDIUM, HIGH

Valid severity values are: CRITICAL, ERROR, WARNING, INFO, DEBUG

For example:

- To set priority and severity for create storage unit events:

```
StorageUnit.CREATE.priority = LOW
```

```
StorageUnit.CREATE.severity = INFO
```

Note: It can take up to one minute for the events of type Policy, SLP, and Catalog to generate after the corresponding action has been performed.

Table 2-3 NetBackup event types supported with notifications

Event type and notification type value	Action	Severity	Sample notification message
Policy Policy Note: When possible, an aggregated policy event for two or more policy actions is created.	Create	INFO	The policy {Policy_Name} was created. Event for Policy received. No additional details found.
	Update	INFO or CRITICAL	The policy {Policy_Name} was activated. The policy {Policy_Name} was deactivated. The policy {Policy_Name} was updated. The client {Policy_Name} was added to the policy \${policyName}. The client {Policy_Name} was removed from the policy {Policy_Name}. The schedule {Policy_Name} was added to the policy \${Policy_Name}. The schedule {Policy_Name} was removed from the policy {Policy_Name}.
	Delete	CRITICAL	The policy {Policy_Name} was deleted.
Client ClientEvent	CREATE	INFO	The client {Client_Name} was created.
	DELETE	CRITICAL	The client {Client_Name} was deleted.
	UPDATE	INFO	The client {Client_Name} was updated.
Storage Unit StorageUnit Note: Any change to a basic disk staging schedule (DSSU), such as adding, deleting, or modifying, generates relevant storage unit notifications. With those notifications, some additional policy notifications are also generated with policy name __DSSU_POLICY_{Storage_Unit_Name}.	CREATE	INFO	The storage unit {Storage_Unit_Name} was created.

Table 2-3 NetBackup event types supported with notifications (*continued*)

Event type and notification type value	Action	Severity	Sample notification message
	DELETE	CRITICAL	The storage unit <i>{Storage_Unit_Name}</i> was deleted.
	UPDATE	INFO	The storage unit <i>{Storage_Unit_Name}</i> was updated.
Storage Unit Group <code>StorageUnitGroup</code>	CREATE	INFO	The storage unit group <i>{Storage_Unit_Group_Name}</i> was created.
	DELETE	CRITICAL	The storage unit group <i>{Storage_Unit_Group_Name}</i> was deleted.
	UPDATE	INFO	The storage unit group <i>{Storage_Unit_Group_Name}</i> was updated.
	UPDATE	INFO	The storage service <i>{Storage_Service_Name}</i> was updated.
Storage life cycle policy <code>SLP</code>	Create	INFO	Event for Storage Lifecycle Policy received. No additional details found. The Storage Lifecycle Policy <i>{Policy_Name}</i> was created.
	Delete	CRITICAL	The Storage Lifecycle Policy <i>{Policy_Name}</i> was deleted. The Storage Lifecycle Policy <i>{Policy_Name}</i> with version <i>Version_Number</i> was deleted.
Storage life cycle policy state change <code>SlpVersionActInactEvent</code>	UPDATE	INFO	The SLP version <i>{Version}</i> was changed.
cDOT Client <code>cDOTClientEvent</code>	CREATE	INFO	<i>{Cluster_Data_ONTAP_Client_Name}</i> was added as a cDOT client.
	DELETE	CRITICAL	<i>{Cluster_Data_ONTAP_Client_Name}</i> was deleted as a cDOT client.
Isilon Client <code>IsilonClientEvent</code>	CREATE	INFO	<i>{Isilon_Filer_Client_Name}</i> was added as an Isilon client.
	DELETE	CRITICAL	<i>{Isilon_Filer_Client_Name}</i> was deleted as an Isilon client.

Table 2-3 NetBackup event types supported with notifications (*continued*)

Event type and notification type value	Action	Severity	Sample notification message
Machine [Primary/Media/Cluster] Machine	CREATE	INFO	The host {Host_Name} was created.
	DELETE	CRITICAL	The host {Host_Name} was deleted.
Drive DriveChange	CREATE	INFO	The drive {Drive_Name} was created for host {Host_Name}.
	DELETE	CRITICAL	The drive {Drive_Name} was deleted for host {Host_Name}.
	UPDATE	INFO	The drive {Drive_Name} was updated for host {Host_Name}. Note: A notification message like this one is generated when a drive is updated for a particular host or when a drive state is changed to UP or DOWN.
Library Event - Robot Library	CREATE	INFO	The library {Library_Name} was created for host {Host_Name}.
	DELETE	CRITICAL	The library {Library_Name} was deleted for host {Host_Name}.
	UPDATE	INFO	The library {Library_Name} was updated for host {Host_Name}.
Media Media	CREATE	INFO	The media {Media_ID} was created.
	DELETE	CRITICAL	The media {Media_ID} was deleted.
	UPDATE	INFO	The media {Media_ID} was updated.
Media Group MediaGroup	CREATE	INFO	The media group {Media_Group_ID} was created.
	DELETE	CRITICAL	The media group {Media_Group_ID} was deleted.
	UPDATE	INFO	The media group {Media_Group_ID} was updated.

Table 2-3 NetBackup event types supported with notifications (*continued*)

Event type and notification type value	Action	Severity	Sample notification message
Media Pool MediaPool	CREATE	INFO	The media pool {Media_Pool_ID} was created.
	DELETE	CRITICAL	The media pool {Media_Pool_ID} was deleted.
	UPDATE	INFO	The media pool {Media_Pool_ID} was updated.
Retention Event RetentionEvent	UPDATE	INFO	Retention level has been changed.
VMware Discovery TAGSDISCOVERYEVENT	no actions	INFO	VMware tags cannot be retrieved.
Autodiscovery and Discover Now AutoDiscoveryEvent	no actions	INFO	An appropriate notification is generated when an autodiscovery action or a Discover Now action is performed for VMWare, RHV, or Cloud servers.
	no actions	CRITICAL	<p>Note: An appropriate notification is generated when an autodiscovery action or a Discover Now action fails for VMWare, RHV, Nutanix, or Cloud servers.</p> <p>Note: An appropriate notification is generated when an autodiscovery action or a Discover Now action fails for VMWare, RHV, or Cloud servers.</p>
KMS Certificate Expiration KMSCredentialStatus	EXPIRY	WARNING	The certificate that is used to communicate with the KMS server {KMS_Server_Name}\${server} is about to expire in {days_to_expiration}. If the certificate is not renewed on time, communication with the KMS server fails.
Message Broker Service Status ServiceStatus	RUNNING	INFO	The NetBackup Messaging Broker service is running. NetBackup internal notifications are now enabled.
	STOPPED	INFO	The NetBackup Messaging Broker service is stopped. NetBackup internal notifications are now disabled.

Table 2-3 NetBackup event types supported with notifications (*continued*)

Event type and notification type value	Action	Severity	Sample notification message
Protection Plan <code>ProtectionPlan</code>	Create	INFO	Received an event for protection plan. The protection plan <i>Protection_Plan_Name</i> is created. The protection plan <i>Protection_Plan_Name</i> is created from existing NetBackup policy.
	Update	INFO	The protection plan <i>Protection_Plan_Name</i> is updated.
	Delete	CRITICAL	The protection plan <i>Protection_Plan_Name</i> is deleted.
Protection Plan Subscription <code>ProtectionPlanSubscription</code>	Create	INFO	Received an event for protection plan subscription. The <i>Asset_Class</i> <i>Asset_Display_Name</i> is subscribed to protection plan <i>Protection_Plan_Name</i> .
	Update	INFO	The <i>Asset_Class</i> <i>Asset_Display_Name</i> subscription with protection plan <i>Protection_Plan_Name</i> is updated.
	Delete	CRITICAL	The <i>Asset_Class</i> <i>Asset_Display_Name</i> is unsubscribed from protection plan <i>Protection_Plan_Name</i> .
Catalog Image Expiration <code>Catalog</code> Note: Also applicable for manual image expiration.	Not applicable	CRITICAL	Event for Catalog Image received. No additional details found. Catalog Image <i>Image_Name</i> was modified. Catalog Image <i>Image_Name</i> expired.
Usage Reporting <code>UsageReportingEvent</code>	No actions	INFO or ERROR	The usage report generation has started. The usage report is generated successfully. Failed to generate the usage report. For more details, refer to the gather and report logs in the parent directory.

About configuring automatic notification cleanup tasks

By default, NetBackup runs event notification cleanup tasks every 4 hours. Up to 10,000 event records are stored for up to 3 days in the event database. During the cleanup tasks, NetBackup removes the older notifications from the database.

You can change how often the cleanup tasks run, how many event records are kept at one time, and the number of days a record is retained.

From a command line, use `bpsetconfig` or `bpgetconfig` to change the parameter values listed in [Table 2-4](#). See the *NetBackup Command Reference Guide* for more information about these commands.

You can also change the parameter values with the following APIs:

- `GET/config/hosts/{hostId}/configurations`
- `POST/config/hosts/{hostId}/configurations`
- `GET/config/hosts/{hostId}/configurations/configurationName` (for a specific property)
- `PUT/config/hosts/{hostId}/configurations/configurationName`
- `DELETE/config/hosts/{hostId}/configurations/configurationName`

See the *NetBackup 10.1 API Reference* on [SORT](#) for more information about these APIs.

Table 2-4 Configurable parameters for automatic notification cleanup tasks

Parameter and description	Minimum value	Default value	Maximum value
<code>EVENT_LOG_NOTIFICATIONS_COUNT</code> The maximum number of records that are stored, after which the cleanup process removes the oldest record, overriding the retention value.	1000	10000	100000
<code>EVENT_LOG_NOTIFICATIONS_RETENTION_IN_HOURS</code> The number of hours for which the events are stored in the database.	24 (hours)	72 (hours)	168 (hours)
<code>EVENT_LOG_NOTIFICATIONS_CLEANUP_INTERVAL_IN_HOURS</code> The frequency at which the event cleanup service runs.	1 (hour)	4 (hours)	24 (hours)

Managing hosts

- [Chapter 3. Managing host properties](#)
- [Chapter 4. Managing credentials for workloads and systems that NetBackup accesses](#)
- [Chapter 5. Managing deployment](#)

Managing host properties

This chapter includes the following topics:

- [Edit the host properties of a server or client](#)
- [Reset a host's attributes](#)

Edit the host properties of a server or client

The configuration options within the **Host properties** let an administrator customize NetBackup to meet specific site preferences and requirements. The NetBackup web UI displays properties for NetBackup primary servers, media servers, and clients.

Note: In a clustered environment, you must make changes to host properties separately on each node of the cluster.

Edit the host properties of the primary server

To edit the host properties of the primary server

- 1 On the left, click **Hosts > Host properties**.
- 2 At the top left, from the list select **Primary server**.
- 3 Select the primary server and click **Connect**.
- 4 Click **Edit primary server**.
- 5 Make any changes that you want. Then click **Save**.

Edit the host properties of a media server

To edit the host properties of a media server

- 1 On the left, click **Hosts > Host properties**.
- 2 At the top left, from the list select **Media server**.
- 3 Select the media server and click **Connect**.
- 4 Click **Edit media server**.
- 5 Make any changes that you want. Then click **Save**.

Edit the host properties of a client

To edit the host properties of a client

- 1 On the left, click **Hosts > Host properties**.
- 2 At the top left, from the list select **Client server**.
- 3 Select the client and click **Connect**.
- 4 Click **Edit client**.
- 5 Make any changes that you want. Then click **Save**.

Reset a host's attributes

In some cases you need to reset a host's attributes to allow successful communication with the host. A reset is most common when a host is downgraded to a 8.0 or earlier version of NetBackup. After the downgrade, the primary server cannot communicate with the client because the communication status for the client is still set to the secure mode. A reset updates the communication status to reflect the insecure mode.

When you reset a host's attributes:

- NetBackup resets the host ID to host name mapping information, the host's communication status and so on. It does not reset the host ID, host name, or security certificates of the host.
- The connection status is set to the insecure state. The next time the primary server communicates with the host, the connection status is updated appropriately.

To reset the attributes for a host

- 1** On the left, select **Security > Host mappings**.
- 2** Locate the host and click **Actions > Reset attributes**.
- 3** Choose if you want to communicate insecurely with 8.0 and earlier hosts.

NetBackup can communicate with a 8.0 or earlier host when the **Allow communication with NetBackup 8.0 and earlier hosts** option is enabled in the **Global Security Settings**. This option is enabled by default.

Note: If you unintentionally reset a host's attributes, you can undo the changes by restarting the `bpcd` service. Otherwise, the host attributes are automatically updated with the appropriate values after 24 hours.

Managing credentials for workloads and systems that NetBackup accesses

This chapter includes the following topics:

- [Overview of credential management in NetBackup](#)
- [Add a credential in NetBackup](#)
- [Add a credential for an external KMS](#)
- [Add a credential for NetBackup Callhome Proxy](#)
- [Edit or delete a named credential](#)
- [Add a credential for Network Data Management Protocol \(NDMP\)](#)
- [Edit or delete Network Data Management Protocol \(NDMP\) credentials in NetBackup](#)

Overview of credential management in NetBackup

Credential management lets you centrally manage the credentials that NetBackup uses to access systems and the workloads that it protects.

Credentials can be managed for the following workloads:

- Cassandra
- Cloud (for a cloud instance)
- Kubernetes

- Microsoft SQL Server
- Nutanix AHV
- Oracle
- SaaS

Credentials can also be managed for the following systems:

- A Call Home proxy server
- Disk arrays
- External Key Management Services (KMS)
- Malware detection (Malware scan host)
- NDMP

More information

See [“Add a credential for NetBackup Callhome Proxy”](#) on page 55.

See [“Add a credential for an external KMS”](#) on page 54.

See [“Add a credential for Network Data Management Protocol \(NDMP\)”](#) on page 56.

See the [Veritas Usage Insights Getting Started Guide](#) for details on using a Call Home proxy server.

To configure credentials for a workload (for example, SQL Server), refer to the guide for that workload for details.

Add a credential in NetBackup

You can use the **Credential management** node to add a credential that NetBackup uses to connect to a system or workload.

- See [“Add a credential for NetBackup Callhome Proxy”](#) on page 55.
- See [“Add a credential for an external KMS”](#) on page 54.
- See [“Add a credential for Network Data Management Protocol \(NDMP\)”](#) on page 56.

For SQL Server, Cloud, Kubernetes, and other workloads, refer to the guide for that workload for details.

[NetBackup documentation portal](#)

Add a credential for an external KMS

This type of credential allows you to access an external KMS server that you have configured.

To add a credential for an external KMS

- 1 On the left, click **Credential management**.
- 2 On the **Named credentials** tab, click **Add** and provide the following properties:
 - Credential name
 - Tag
 - Description (for example: This credential is used to access the external KMS.)
- 3 Click **Next**.
- 4 Select **External KMS**.
- 5 Provide the credential details that are needed for authentication.

These details are used to authenticate the communication between the NetBackup primary server and the external KMS server:

- Certificate - Specify the certificate file contents.
- Private key - Specify the private key file contents.
- CA Certificate - Specify the CA certificate file contents.
- Passphrase - Enter the passphrase of the private key file.
- CRL check level - Select the revocation check level for the external KMS server certificate.
 - CHAIN - The revocation status of all the certificates from the certificate chain are validated against the CRL.
 - DISABLE - Revocation check is disabled. The revocation status of the certificate is not validated against the CRL during host communication.
 - LEAF - The revocation status of the leaf certificate is validated against the CRL.

See the [NetBackup Security and Encryption Guide](#) for more information on external KMS configuration.

- 6 Click **Next**.
- 7 Add a role that you want to have access to the credential.
 - Click **Add**.
 - Select the role.

- Select the credential permissions that you want the role to have.
- 8 Click **Next** and follow the prompts to complete the wizard.

Add a credential for NetBackup Callhome Proxy

This type of credential provides the proxy server configuration that both the NetBackup Product Improvement Program and Usage Insights use.

To add a credential for NetBackup Callhome Proxy

- 1 On the left, click **Credential management**.
- 2 On the **Named credentials** tab, click **Add** and provide the following properties:
 - Credential name
 - Tag
 - Description
- 3 Click **Next**.
- 4 Select **Callhome proxy**.
- 5 Provide the credential details that are needed for authentication and click **Next**.
- 6 Add a role that you want to have access to the credential.
 - Click **Add**.
 - Select the role.
 - Select the credential permissions that you want the role to have.
- 7 Click **Next** and follow the prompts to complete the wizard.
- 8 After you create the credential, you must update the NetBackup configuration with an entry for `CALLHOME_PROXY_NAME`. Set the `CALLHOME_PROXY_NAME` to the credential name. From the primary server, use the command shown:

```
echo CALLHOME_PROXY_NAME = CredentialName |bpsetconfig.exe
```

Edit or delete a named credential

You can edit the properties for a named credential or delete a named credential NetBackup from the **Credential management**.

Edit a named credential

You can edit a named credential when you want to change the credential tag, description, category, authentication details, or permissions. You cannot change the credential name.

To edit a named credential

- 1 On the left, click **Credential management**.
- 2 On the **Named credentials** tab, locate and click on the credential that you want to edit.
- 3 Click **Edit** and update the credential as needed.
- 4 Review the changes and click **Finish**.
- 5 (Conditional) For any cloud workloads that use an agentless connection for instances, after you edit the credentials click the **Connect** button to reconnect the instances.

Delete a named credential

You can delete a named credential that you no longer need to use with NetBackup. Be sure to apply another credential to any assets that use the credential you want to delete. Otherwise, backups and restores may fail for those assets.

To delete a named credential

- 1 On the left, click **Credential management**.
- 2 On the **Named credentials** tab, locate and click on the credential that you want to delete.
- 3 Click **Delete**.
- 4 (Conditional) If the credential deleted was a proxy credential, you must remove the `CALLHOME_PROXY_NAME` entity. From the primary server, use the following command to remove the `CALLHOME_PROXY_NAME` entity.

```
echo CALLHOME_PROXY_NAME |bpsetconfig.exe
```

Add a credential for Network Data Management Protocol (NDMP)

You can add the credentials that NetBackup uses to connect to the Network Data Management Protocol (NDMP).

For more information about NDMP credentials, see the [NetBackup for NDMP Administrator's Guide](#).

To add an NDMP credential

- 1 On the left, click **Credential management**.
- 2 Click the **Client credentials** tab.
- 3 Click **Add**.
- 4 On the **Add NDMP host** screen, enter an NDMP host name and select the type of host credentials from the radio buttons.
 - **Use the following credentials for this NDMP host on all media servers** – This option uses the same credentials for all media servers.
 - **Use different credentials for this NDMP host on each media server** – This option lets you enter unique credentials for each media server. After you enter credentials for each of the media servers, click **Add**.
- 5 Click **Add**.

Edit or delete Network Data Management Protocol (NDMP) credentials in NetBackup

You can edit or delete credentials for any media servers that use the Network Data Management Protocol (NDMP).

For more information about NDMP credentials, see the [NetBackup for NDMP Administrator's Guide](#).

Edit an NDMP credential

To edit an NDMP credential

- 1 On the left, click **Credential management**.
- 2 Click the **Client credentials** tab.
- 3 Locate the host. Then click **Edit**.
- 4 Make any changes that you want, then click **Save**.

Delete an NDMP credential

To delete an NDMP credential

- 1 On the left, click **Credential management**.
- 2 Click the **Client credentials** tab.
- 3 Select one or more hosts. Then click **Delete > Delete**.

Managing deployment

This chapter includes the following topics:

- [Managing the NetBackup Package repository](#)
- [Update host](#)
- [Deployment policies](#)

Managing the NetBackup Package repository

The NetBackup Package repository provides a central location to add and remove NetBackup packages. Packages let you upgrade NetBackup or deploy emergency engineering binaries in your NetBackup environment.

The interface arranges packages by NetBackup version number. For a specific version of NetBackup, there are multiple child packages, one for each supported platform.

Select **Hosts > Deployment management** to review the packages that are available to deploy to computers in your NetBackup environment. Actions available from this interface include:

- Add new packages.
- Delete existing packages.

Before you can add packages to the repository, you must download VxUpdate formatted packages from the myveritas.com licensing portal. Place downloaded package in an accessible location on the primary server. For details on how to download packages, see the **Repository management** section of *NetBackup Upgrade Guide*. Specifically, refer to the **Downloading Veritas NetBackup approved media server and client packages** procedure.

To add packages

- 1 From **Hosts > Deployment management**, select **Add package** or **Add**, depending if there are already packages in the repository.
- 2 In the dialog box, navigate to where your VxUpdate packages are located and select them. Be aware that NetBackup can only add the packages that reside on the primary server's file system.

The interface displays only VxUpdate packages. A directory may have files but if there are no VxUpdate packages, it shows as empty.

- 3 Select **Ok** to add the packages.

Depending on the number and the size of packages you add, it may take a while for them to display in the repository.

To delete packages

- 1 From **Hosts > Deployment management**, select the packages you want to delete.
- 2 Select **Delete**.

Note: You can also delete individual packages from the action menu.

If you delete a parent package, all child packages that are associated with that parent are removed.

If you delete a server package, the associated client package is also deleted. For example, if you delete the Windows 8.3 server package, the Windows 8.3 client package is also removed.

Update host

The **Update host** option lets you launch immediate jobs to update or upgrade your NetBackup environment.

After you select **Hosts > Host Properties** and make one or more valid selections, the **Update host** option appears in the upper right. Certain restrictions apply to the use of the **Update host** option:

- All computers you select must be of the same type. Select either all client computers or all media servers. If you select mixed computer types, the **Update host** option disappears.
- Primary servers are not supported. If you select a primary server, the **Update host** option disappears.

- The operating system and versions column must contain data for the **Update host** option to appear. If these columns do not contain data, attempt to connect to the host.

After you specify computers to update, select **Update host** to launch the update process. You are prompted for the information shown:

- **Attributes**
On this screen, specify: The package you want deployed, the operation type, any limit on concurrent jobs, and how to handle Java and the JRE.
- **Hosts**
Displays the hosts you want to upgrade. From this screen, you can remove hosts.
- **Security options** (if it appears)
Either accept the default (**Use existing certificates when possible**) or specify the appropriate security information for your environment.
- **Review**
Displays all the options you selected on previous screens.

Select **Update** to start the deployment job.

Deployment policies

Under **Hosts > Deployment management**, you now have a **Deployment policies** tab. Use this tab to add, edit, copy, deactivate, delete, and launch your policies.

To add a new policy:

- 1 Navigate to **Hosts > Deployment management > Deployment policies** and select **Add**.
- 2 Enter the required information for deployment policies.
The required deployment policy information is similar to the update host information.
See [“Update host”](#) on page 59.
- 3 Select **Save**.

Similarly, to edit, copy, deactivate, or delete deployment policies, select the policy. Then select the appropriate action from banner.

To manually initiate policies, select the desired policy and select **Deploy now** from the menu.

Configuring storage and backups

- [Chapter 6. Configuring storage](#)
- [Chapter 7. Overview of backups in the web UI](#)
- [Chapter 8. Managing protection plans](#)
- [Chapter 9. Managing classic policies](#)
- [Chapter 10. Managing backup images](#)
- [Chapter 11. Pausing data protection activity](#)

Configuring storage

This chapter includes the following topics:

- [About storage configuration](#)
- [Create a Media Server Deduplication Pool \(MSDP\) storage server](#)
- [Create a Cloud storage, OpenStorage, or AdvancedDisk storage server](#)
- [Create a disk pool](#)
- [Create a storage unit](#)
- [Create a universal share](#)
- [Create a Media Server Deduplication Pool \(MSDP\) storage server for image sharing](#)
- [Using image sharing from the NetBackup web UI](#)
- [Troubleshooting storage configuration](#)
- [Troubleshooting universal share configuration issues](#)
- [Using instant access for MS-Windows and Standard policies](#)

About storage configuration

NetBackup lets you configure storage options for all protection plans and policies. You can set up the storage options using the storage option wizard. To access the wizard, on the left click on **Storage > Storage configuration**.

You can configure the following storage options:

- Media Server Deduplication Pool (MSDP)
- Media Server Deduplication Pool (MSDP) for image sharing

- AdvancedDisk
- Cloud storage
- OpenStorage

You can also configure NetBackup to work with your universal shares.

Note: If you use Key Management Service (KMS), it must be configured before you can select the KMS option in the storage server setup. Refer to [NetBackup Security and Encryption Guide](#) for more information.

To ensure that A.I.R. and other storage capabilities are displayed accurately for the storage servers on the NetBackup web UI, upgrade the media server. You must upgrade the media server that has NetBackup versions 8.2 or earlier. After you upgrade the media server then use the command line to update the storage server.

Use the following command to update the storage server:

```
/usr/opensv/netbackup/bin/admincmd/nbdevconfig -updatests
-storage_server <storage server name> -stype PureDisk
```

For more information, refer to the [NetBackup Deduplication Guide](#).

Create a Media Server Deduplication Pool (MSDP) storage server

Use this procedure to create a Media Server Deduplication Pool (MSDP) storage server. You have the option to create a disk pool (local storage or cloud storage) and storage unit after you create a storage server. The recommendation is that you create the disk pool and storage unit if they do not exist in NetBackup.

To add an MSDP storage server

- 1 Log into the NetBackup web UI.
- 2 On the left, click **Storage** > **Storage configuration** and then click **Add**.
- 3 Select **Media Server Deduplication Pool (MSDP)** from the list.
- 4 In **Basic properties**, enter all required information and click **Next**.

You must select your media server by clicking on the field. If you do not see the media server you want to use, you can use **Search** to find it.

- 5 In **Storage server options**, enter all required information and click **Next**.

If you use Key Management Service (KMS), it must be configured before you can select the **KMS** option.

- 6** (Optional) In **Media servers**, click **Add** to add any additional media servers you want to use.

Click **Next** after selecting additional media servers or if you want to continue without selecting additional media servers.

- 7** On the **Review** page, confirm that all options are correct and click **Save**.

If the MSDP storage server creation is unsuccessful, follow the prompts on the screen to correct the issue.

To configure MSDP to use cloud storage, use the following procedure (drop-down in **Volumes** step) to select an existing disk pool volume or create a new one.

See [“Create a disk pool”](#) on page 67.

- 8** (Optional) At the top, click on **Create disk pool**.

- 9** (Optional) To create a cloud logical storage unit and disk pool with replication, click on **Create disk pool**.

Enter the required information to create a disk pool.

In the next tab, select and add the required cloud volume. Select the cloud storage provider and the required details of the storage provider. Enter the credentials to access the cloud storage provider and then define the advanced settings.

Note: Currently, AWS S3 and Azure storage API types are supported.

Note: When you enable Server-Side Encryption, you can configure AWS Customer-Managed keys. These keys cannot be deleted once they are in use by NetBackup. Each object is encrypted with the key during upload and deleting the key from AWS causes NetBackup restore failures.

Note: NetBackup Recovery Vault supports multiple options such as Microsoft Azure and Amazon. Contact your Veritas NetBackup account manager for credentials or with any questions about the available options.

For more information on environments and deployment, refer to [Recovery Vault for NetBackup](#).

For more information, refer to the [NetBackup Cloud Administrator's Guide](#) and [NetBackup Deduplication Guide](#).

See [“Create a disk pool”](#) on page 67.

See [“Create a storage unit”](#) on page 68.

See [“Create a Cloud storage, OpenStorage, or AdvancedDisk storage server ”](#) on page 65.

See [“Create a protection plan”](#) on page 81.

Create a Cloud storage, OpenStorage, or AdvancedDisk storage server

Use the following procedures to create Cloud storage, OpenStorage, or an AdvancedDisk storage server.

Create a Cloud storage server

Follow this procedure to create a Cloud storage server.

To create a Cloud storage server

- 1 On the left, click **Storage > Storage configuration** and then click **Add**.
- 2 Select **Cloud storage** from the list.
- 3 In **Basic properties**, enter all required information and click **Next**.

You must select your **Cloud storage provider** by clicking on the field. If you do not see the cloud storage provider you want to use, you can use **Search** to find it.

If the **Region** information that you want to select does not appear in the table, use **Add** to manually add the required information. This option does not appear for every cloud storage provider.

You must select your media server by clicking on the field. If you do not see the media server you want to use, you can use **Search** to find it.

- 4 In **Access settings** enter the required access details for the selected cloud provider and click **Next**.

If you use `socks4`, `socks5`, or `socks4a`, some of the options in the **Advanced** section are not available.

- 5 In **Storage server options**, you can adjust the **Object size**, enable compression, or encrypt data and then click **Next**.

- 6 (Optional) In **Media servers**, click **Add** to add any additional media servers you want to use.

For Cloud storage servers, media servers with a NetBackup version older than primary server are not listed.

Click **Next** after selecting additional media servers or if you want to continue without selecting additional media servers.

- 7 On the **Review** page, confirm that all options are correct and click **Save**.

- 8 (Optional) At the top, click on **Create disk pool**.

Create an OpenStorage storage server

Follow this procedure to create an OpenStorage storage server.

To create an OpenStorage storage server

- 1 On the left, click **Storage > Storage configuration** and then click **Add**.

- 2 Select **OpenStorage** from the list.

- 3 In **Basic properties**, enter all required information and click **Next**.

You must select your media server by clicking on the field. If you do not see the media server you want to use, you can use **Search** to find it.

Use the drop-down to select the correct **Storage server type**.

- 4 (Optional) In **Media servers**, click **Add** to add any additional media servers you want to use.

Click **Next** after selecting additional media servers or if you want to continue without selecting additional media servers.

- 5 On the **Review** page, confirm that all options are correct and click **Save**.

After you click **Save**, the credentials you entered are validated. If the credentials are invalid, click **Change** and you can correct the issue with the credentials.

- 6 (Optional) At the top, click on **Create disk pool**.

Create an AdvancedDisk storage server

Follow this procedure to create an AdvancedDisk storage server.

To create an AdvancedDisk storage server

- 1 On the left, click **Storage > Storage configuration** and then click **Add**.

- 2 Select **AdvancedDisk** from the list.

- 3 Select a media server list and enter a **Storage server name** click **Select**.

Create a disk pool

Use this procedure to create a disk pool after you create any type of storage server. You can create a disk pool at any time, but disk pool creation requires that you have an existing storage server created.

You can configure MSDP storage server to use cloud storage. To configure, you can select an existing cloud volume or create a new one when you create a disk pool. Use the drop-down in **Volumes** step to select an existing cloud volume or create a new volume for the MSDP storage server.

When you view the **Disk pools** tab, the **Available space** column can be empty for a disk pool that uses a cloud storage provider. NetBackup cannot retrieve the information because the cloud provider does not supply an API for that information.

To create a disk pool

- 1 On the left, click **Storage > Storage configuration**, click the **Disk pools** tab, and then click **Add**.

Another way to create a disk pool is to click **Create disk pool** at the top of the screen after you have created a storage server.

- 2 In **Disk pool options**, enter all required information and click **Next**.

Click **Change** to select a storage server.

If **Limit I/O streams** is left cleared, the default value is **Unlimited** and may cause performance issues.

- 3 In **Volumes**, use the **Volume** drop down to select a volume or add a new volume. If you want to add a new disk pool volume, use the **Add volume** option.

Note: When you enable Server-Side Encryption, you can configure AWS Customer-Managed keys. These keys cannot be deleted once they are in use by NetBackup. Each object is encrypted with the key during upload and deleting the key from AWS causes NetBackup restore failures.

Note: NetBackup Recovery Vault supports multiple options such as Microsoft Azure and Amazon. Contact your Veritas NetBackup account manager for credentials or with any questions about the available options.

Enter all required information based on the selection and click **Next**.

- 4 In **Replication**, click **Add** to add replication targets to the disk pool.

This step lets you select a trusted primary server or add a trusted primary server. You can add a primary server that supports NetBackup Certificate Authority (NBCA), ECA, and ECA together with NBCA.

Replication is supported only on MSDP.

Review all the information that is entered for the replication targets and then click **Next**.

- 5 On the **Review** page, verify that all settings and information are correct. Click **Finish**.

The disk pool creation and replication configuration continue in the background if you close the window. If there is an issue with validating the credentials and configuration of the replication, you can use the **Change** option to adjust any settings.

Create a storage unit

Use this procedure to create a storage unit. You should create a storage unit after you create any type of storage server and disk pool. The steps in this procedure also work if you create a new storage unit without creating a storage server and disk pool.

When you view the **Storage units** tab, the **Used space** column can be empty for a storage unit that uses a cloud storage provider. NetBackup cannot retrieve the information because the cloud provider does not supply an API for that information.

To create a storage unit

- 1 On the left, click **Storage > Storage configuration**, click the **Storage units** tab, and then click **Add**.

Another way to create a storage unit is to click **Create storage unit** at the top of the screen after you have created a disk pool.

- 2 Select the storage unit from the list and click **Start**.
- 3 In **Basic properties**, enter all required information and click **Next**.

- 4 In **Disk pool**, select the disk pool you want to use in the storage unit and then click **Next**.

The **Enable WORM** option is activated when you select a disk pool that supports WORM (Write Once Read Many) storage.

For more information about WORM properties, refer to *Configuring immutability and indelibility of data in NetBackup* in the [NetBackup Administrator's Guide, Volume I](#) guide.

The **On demand only** option specifies whether the storage unit is available exclusively on demand. A policy or schedule must be explicitly configured to use this storage unit

- 5 In the **Media server** tab, select the media servers you want to use and then click **Next**.

You can have NetBackup select your media server automatically or you can select your media servers manually using the radio buttons.

- 6 Review the setup of the storage unit and then click **Save**.

See “[Create a disk pool](#)” on page 67.

See “[Create a Media Server Deduplication Pool \(MSDP\) storage server](#)” on page 63.

See “[Create a Cloud storage, OpenStorage, or AdvancedDisk storage server](#)” on page 65.

See “[Create a protection plan](#)” on page 81.

Create a universal share

A universal share offers the ability to ingest data directly into a space efficient SMB (CIFS) or NFS share. Space efficiency is achieved by storing the ingested data directly to an existing NetBackup deduplication pool (MSDP). No NetBackup software needs to be installed on the client that is mounting the share. Any operating system that is running a POSIX-compliant file system and can mount an SMB (CIFS) or NFS network share can write data to a universal share.

For more information about universal shares, see the [NetBackup Deduplication Guide](#)

With the NetBackup web UI, you can:

- Create, modify, view, and delete universal shares and manage them across NetBackup Appliance, Flex Appliance, Flex Scale, Flex WORM/non-WORM, MSDP AKS/EKS deployment, build-your-own (BYO) and BYO-In-Cloud servers.
- Change the quota settings, Active Directory (AD) user and group names, and any target hosts that pertain to the universal share.

Note: See the [NetBackup Deduplication Guide](#) for more information about universal share policies, universal share for cloud LSU limitation, prerequisites, and configuration.

To create a universal share in the NetBackup web UI

- 1 On the left, click **Storage > Storage Configuration > Universal Share** and then click **Add**.

If there are no storage servers, then configure an MSDP storage server:

See [“Create a Media Server Deduplication Pool \(MSDP\) storage server”](#) on page 63.

After you create the MSDP storage server, return to Universal Shares tab and click **Add** to add a universal share.

- 2 Provide the following required information:
 - Enter a **Display name**. This name is used in the universal share path.
 - Select the **Storage server**.
 - Select the **Disk volume**.
Click the search icon to get the volume list, and select the disk volume.
PureDiskVolume is selected by default.
This option is available only if universal share with object storage in cloud feature is enabled.. For more information, see the *NetBackup Deduplication Guide*.
 - Select the **Protocol**: NSF or SMB (CIFS)
 - Specify a **Host** that is allowed to mount the share and then click **Add to list**. You can use the host name, IP address, short name, or the FQDN to specify the Host. You can enter multiple hosts for each share.
- 3 At this point, continue to enter values in the remaining fields or click **Save** to save the universal share. You can update the remaining fields later from the universal share's details page:
 - Select a **Quota** type: Unlimited or Custom. If you select Custom, also specify the quota in MB, GB, or TB units.
The Custom quota value limits the amount of data that is ingested into the share. Quotas are enforced using the front-end terabyte (FETB) calculation method. They are Implemented per share and can be modified at any time. You do not need to remount the share for the change to a take effect.
To update the quote type or value from the universal share's details page, click **Edit** in the Quota section.

Create a Media Server Deduplication Pool (MSDP) storage server for image sharing

- Specify **User names** (Local or Active Directory) and **Group names** (Active Directory only). Only the specified users or groups can access the share. You can add and update the **User names** and **Group Names** later from the details page of an existing universal share.

Note: Currently, **User names** and **Group names** are supported only for the SMB (CIFS) protocol.

- 4 To view details about a universal share, click its name in the **Universal Shares** table.
- 5 To delete a universal share, select one or more and click **Delete** or select **Delete** from the action menu.

Deleting a universal share also deletes all data in the share. This action is irreversible and may take some time if the amount of data is large. Any active data transfers are immediately terminated, and any mounted shares are immediately removed.

Create a Media Server Deduplication Pool (MSDP) storage server for image sharing

Use this topic to create a cloud recovery server for image sharing. Refer to the *About image sharing using MSDP cloud* topic in the [NetBackup Deduplication Guide](#) for more information about a cloud recovery server.

To configure cloud recovery server:

- 1 On the left, click **Storage > Storage configuration** and then click **Add**. If you deleted a storage server, refresh this page.
- 2 Select **Media Server Deduplication Pool (MSDP) for image sharing** from the list.
- 3 In the **Basic properties**, enter all the required information and click **Next**.
You must select your media server by clicking on the field. If you do not see the media server you want to use, use the search option.
- 4 In the storage server options, enter all the required information except for **Encryption options** and **Encryption for local storage** and click **Next**.

If KMS encryption is enabled for the on-premises side, Key Management Service (KMS) must be configured before you can configure cloud recovery server. Then the KMS options from the on-premises side are selected and configured automatically in the cloud recovery server.

- 5 (Optional) In **Media servers**, click **Next**. As the cloud recovery server is an all-in-one NetBackup server, no additional media servers are added.
- 6 On the **Review** page, confirm that all options are correct and click **Save**.
If the MSDP with the image sharing creation is unsuccessful, follow the prompts on the screen to correct the issue.
- 7 At the top, click on **Create disk pool**.
Another way: On the left, click **Storage**, click the **Disk pools** tab, and then click **Add**.
- 8 In **Disk pool** options, enter all the required information and click **Next**.
Click **Change** to select a storage server.
- 9 In **Volumes**, use the **Volume** drop down to add a new volume. Enter all the required information based on the selection and click **Next**.
The volume name must be same as the volume name that is on the on-premises side or the sub bucket name.
- 10 In **Replication**, click **Next** to continue without adding any primary server.
- 11 On the **Review** page, verify that all settings and information are correct. Click **Save**.

See [“Using image sharing from the NetBackup web UI ”](#) on page 72.

Using image sharing from the NetBackup web UI

You can use the NetBackup web UI to share images from an on-premises location to the cloud. You can set up a cloud recovery server on demand and share the images to that server.

Use the information from the following topic from the [NetBackup Deduplication Guide](#) to set up a cloud recovery server:

About image sharing using MSDP cloud

Steps to complete from the NetBackup web UI after setting up the cloud recovery server

Before you begin, ensure that you have the required permissions in the web UI to import the image, restore, convert, and access the AMI ID or VHD.

Importing the images.

1. On the left, select **Storage > Storage configuration** and then **Disk pools**.
2. Select the volume pools that contain the images that you want to share.

3. In the Disk pool options, locate the disk pool name and click **Actions > Fast Import**.

Note: The fast import option is an import operation that is specific to image sharing. You can import the backed-up images from the cloud storage to the cloud recovery server that is used for image sharing. After a fast import, you can restore the images. For AWS cloud provider, you can also convert the VM image to an AWS AMI. For Azure cloud provider, you can convert the VM image to VHD.

4. In the **Fast import images** page, select the backup images that you want to import and click **Import**.
5. Verify the activity completion status in the **Activity Monitor**.

Converting the VM images to AWS AMI or VHD in Azure.

1. On the left select **VMware** and then select the imported VMware image to convert.
2. On the **Recovery point** tab, select the recovery date.
3. For the recovery point date, choose the required recovery point, click **Actions > Convert**.
4. Once the conversion is complete, an AMI ID or VHD URL is generated.
5. Use the AMI ID to locate the image in AWS and then use the AWS console to start the EC2 instance. Or use VHD URL to create virtual machine.

Troubleshooting storage configuration

The following table describes multiple issues that might occur when you configure storage:

Table 6-1 Storage configuration troubleshooting

Error message or cause	Explanation and recommended action
<p>The following error is displayed when you create a disk pool for a cloud volume:</p> <p>Disk is full</p>	<p>Workaround:</p> <p>Even if the disk is not full and you get the error, ensure that there is enough space available for creating the cloud volume.</p> <p>By default the cloud volume requires approximately 1 TB of free space.</p> <p>To reduce the cloud volume size, open the <code>contentrouter.cfg</code> file from <code>/msdp/etc/puredisk/</code> and change the values. After changing the values, restart the MSDP services and then create the cloud volume.</p>
<p>The local MSDP storage does not display the compression and the encryption values correctly.</p>	<p>In the Select long-term retention storage configuration page for protection plans, the local MSDP storage does not display the compression and the encryption values correctly.</p>

Troubleshooting universal share configuration issues

For more information about universal shares, see the [NetBackup Deduplication Guide](#)

How to troubleshoot a failed installation or configuration

To configure a universal share, ensure that instant access is enabled on the storage server. For more information about instant access, see the following guides:

- [NetBackup Web UI VMware Administrator's Guide](#)
- [NetBackup Web UI Microsoft SQL Administrator's Guide](#)

To ensure that instant access is enabled on the storage server

- 1** Log in to the storage server and run the following command (build your own (BYO) only):

```
/usr/opensv/pdde/vpfs/bin/ia_byo_precheck.sh
```

- 2** Review the pre-condition checking results and the configuration results:

```
/var/log/vps/ia_byo_precheck.log (BYO only)
```

```
/usr/opensv/pdde/vpfs/vpfs-config.log (BYO and appliance configurations)
```

In the following example, several required services are not running:

```
[root@rhelnbu06 ~]# /usr/opensv/pdde/vpfs/bin/ia_byo_precheck.sh
Mon Apr 13 12:42:14 EDT 2020 Try to get storagepath
Mon Apr 13 12:42:14 EDT 2020 Storage ContentRouter config path is
    /msdp/etc/puredisk/contentrouter.cfg
Mon Apr 13 12:42:14 EDT 2020 Storagepath is /msdp
Mon Apr 13 12:42:14 EDT 2020 File system for partition /msdp is
    ext2/ext3
Mon Apr 13 12:42:14 EDT 2020 File system for partition /msdp/data
    is ext2/ext3
Mon Apr 13 12:42:14 EDT 2020 **** Hardware Virtualization not
    supported, Instant Access browse may be slow ****
Mon Apr 13 12:42:14 EDT 2020 **** system memory support 50 vpfs
    livemounts ****
Mon Apr 13 12:42:14 EDT 2020 **** nginx service required by
    Instant Access is not running ****
Mon Apr 13 12:42:14 EDT 2020 **** smb service required by
    Instant Access is not running ****
Mon Apr 13 12:42:14 EDT 2020 **** docker service required by
    VMware Instant Access is not running ****
```

- 3** Resolve the issues that are identified in the log. For example, restart any services that are required for instant access.

How to check for universal share capability

To ensure that the storage server has universal share capability

- 1 Make sure that the storage service is running NetBackup 8.3 or later.
- 2 Log on to the storage server and run the following command:

```
nbdevquery -liststs -U
```

Make sure that the `InstantAccess` flag is listed in the command's output.

If the flag is not listed, see one of the guides mentioned above to enable instant access on the storage server.

- 3 Run the following command:

```
nbdevconfig -getconfig -stype PureDisk -storage_server  
storage_server_name
```

Make sure that the `UNIVERSAL_SHARE_STORAGE` flag is listed in the command's output.

If the flag is not listed, create a universal share on the storage server:

See [“Create a universal share”](#) on page 69.

How to start or to stop a universal share

A universal share can be started, restarted, or stopped with NetBackup services:

- Use the following command to start or restart a universal share:

```
netbackup start
```

- Use the following command to stop universal share:

```
netbackup stop
```

Whenever a universal share is created on the NetBackup web UI, a mount point is also created on the storage server.

For example:

```
[root@rsvlmc01vm309 vpfs.mnt]# mount | grep vpfs  
vpfsd on /mnt/vpfs type fuse.vpfsd (rw,nosuid,nodev,relatime,user_id=0,  
group_id=0,default_permissions,allow_other)  
vpfsd on /mnt/vpfs_shares/aa7e/aa7e83e5-93e4-57ea-a4a8-81ddbf5f819e  
type fuse.vpfsd (rw,nosuid,nodev,relatime,user_id=0,group_id=0,  
default_permissions,allow_other)
```

In this example, `aa7e83e5-93e4-57ea-a4a8-81ddbf5f819e` is the universal share's ID. This ID is found on the details page of the universal share in the NetBackup web UI: On the left, click **Storage > Storage Configuration > Universal Share** and then select the universal share to view its details.

Using instant access for MS-Windows and Standard policies

Instant access for unstructured data assets allows users to create instant access mounts from the backup images that are created with MS-Windows or Standard policies.

To manage instant access with a MS-Windows or Standard policy, a user must have the RBAC Administrator role. Or, a role with similar permissions.

You can instantly access backup copies from a local or a cloud LSU (logical storage unit) using NetBackup Instant Access APIs.

For more information about limitations of instant access for cloud LSU (logical storage unit), refer to the [NetBackup Deduplication Guide](#).

Note: Instant access on Flex WORM storage requires the following services: NGINX, NFS, SAMBA, WINBIND (if Active Directory is required), SPWS, VPFS.

Overview of backups in the web UI

This chapter includes the following topics:

- [Backups methods supported in the NetBackup web UI](#)
- [Protection plan vs. policy FAQs](#)
- [Support for NetBackup classic policies](#)

Backups methods supported in the NetBackup web UI

The NetBackup web UI offers the following methods to protect your data:

- **Protection plans.** Protection plans protect assets. For example, databases or virtual machines. Workload administrators are granted access to a protection plans through the available default RBAC roles. Then they can subscribe the assets to a plan.
- **Policies.** Policies protect data on clients. Some agents also have an intelligent policy that protects assets spread over multiple clients.

Protection plans and intelligent policies work with asset management to automatically discover assets in the NetBackup environment.

Protection plan vs. policy FAQs

You can protect an asset using a NetBackup classic policy, a protection plan, or both at the same time. This topic answers some common questions about NetBackup classic policies in the NetBackup web UI.

Table 7-1 Classic policy FAQ

Question	Answer
In the web UI's Protected by column, what does Classic policy only mean?	The asset is not currently subscribed to a protection plan. However, it was subscribed to a protection plan. Or, it was covered by a classic policy at one time and it has a Last backup status. There may or may not be an active classic policy protecting the asset (contact the NetBackup administrator to find out).
Where can I find the details of a classic policy?	The details of a classic policy are not visible in the web UI, with the exception of a few policy types. See "Support for NetBackup classic policies" on page 79.
How can I manage a classic policy?	Some policy types can be managed in the NetBackup web UI. See "Support for NetBackup classic policies" on page 79. For other classic policies, use the NetBackup Administration Console or the NetBackup CLIs. A user with the RBAC "Administrator" role can manage and create policies using the NetBackup APIs.
When should I subscribe an asset to a protection plan versus protecting the asset with a classic policy?	A protection plan lets you easily add and remove assets from the plan and see which assets are protected. A workload administrator can fully control who can view or manage protection plans and assets. Policies offer the classic method of data protection. However, they do not have RBAC control for individual policies or for the data you want to protect.
Can I use both a protection plan and a classic policy to protect an asset?	Yes. The web UI shows the details of the protection plan but not the details of the classic policy. You can contact the NetBackup administrator for the classic policy details.
What action should I take when an asset is unsubscribed from a protection plan and the web UI shows Classic policy only for that asset?	You can ask the NetBackup administrator if a classic policy protects the asset.

Support for NetBackup classic policies

The following policy types can be managed in the NetBackup web UI. Other policy types are available in the NetBackup Administration Console.

- BigData
- DB2
- Informix
- MS-Exchange-Server
- MS-SQL-Server
- MS-Windows
- NBU-Catalog
- NDMP
- Oracle
- SAP
- Standard
- Universal-Share
- VMware

Managing protection plans

This chapter includes the following topics:

- [Create a protection plan](#)
- [Customizing protection plans](#)
- [Edit or delete a protection plan](#)
- [Subscribe an asset or an asset group to a protection plan](#)
- [Unsubscribe an asset from a protection plan](#)
- [View protection plan overrides](#)
- [About Backup Now](#)

Create a protection plan

Note: After upgrade, the protection plans may not appear in the web UI. The conversion process may not have run but should run within 5 minutes of performing the upgrade.

Before you create a protection plan, you must configure all storage options.

See [“About storage configuration”](#) on page 62.

To create a protection plan

- 1 On the left, click **Protection > Protection plans** and then click **Add**.
- 2 In **Basic properties**, enter a **Name**, **Description**, and select a **Workload** from the drop-down list.

Optional selection:

- **Policy name prefix:**

Use this option for policy names. A prefix is added to the policy name when NetBackup automatically creates a policy when users subscribe assets to this protection plan.

- **Enable Continuous Data Protection**

For VMware workloads, select this option to use Continuous data protection for the workload. See the *Continuous data protection* chapter of the *NetBackup Web UI VMware Administrator's Guide* for details.

- **Protect PaaS assets only**

For Cloud workloads, you must select this option to protect non-RDS PaaS assets with non-snapshot based protection, using the protection plan. Do not select this option for RDS assets with snapshot-based protection. See the *Managing PaaS assets* chapter of the *NetBackup Web UI Cloud Administrator's Guide* for details.

3 In **Schedules**, click **Add**.

If you have selected cloud as workload of Azure or Azure Stack, see the *Configuring backup schedules for cloud workloads* section of the [NetBackup Web UI Cloud Administrator's Guide](#).

You can set up a daily, weekly, or monthly backup and then set retention and replication of that backup. Also depending on workload, you can set up the following backup schedules: a **Automatic**, **Full**, **Differential incremental**, **Cumulative Incremental**, or **Snapshot only**.

For more information about AWS snapshot replication, review the *Configure AWS snapshot replication* in the [NetBackup Web UI Cloud Administrator's Guide](#)

If you select **Monthly** as a frequency, you can select between **Days of the week** (grid view) or **Days of the month** (calendar view).

Note: If you select **Automatic** for the schedule type, then all schedules for this protection plan are **Automatic**. If you select a **Full**, **Differential incremental**, or **Cumulative Incremental** for the schedule type, then all schedules for this protection plan must be one of these options.

If you select **Automatic** for the schedule type, NetBackup automatically sets the schedule type for you. NetBackup calculates when to do a **Full** or **Differential incremental** based on frequency you specify.

Note: The protection plan creation does not work for the VMware workload when certain schedule frequencies are set with WORM storage lock duration. The protection plan creation does not work when: schedule frequencies are set to less than one week and WORM storage **Lock Maximum Duration** less than one week greater than the requested retention period.

If you use a protection plan to protect VMware with WORM capable storage, set the WORM storage **Lock Maximum Duration** to greater than one week. Or, explicitly select the schedule type in the protection plan.

In the **Attributes** tab:

- Select the **Backup type**, how often it runs, and how long to keep the backup for this schedule.
 - The selections in the **Backup type** are dependent on workload that is selected and any other backup schedules that are currently active in this protection plan.
- (Optional) To replicate the backup, select **Replicate this backup**.
 - To use the **Replicate this backup** option, the backup storage must be a source in a targeted A.I.R. environment. The **Replication target** is configured in step 4.
 - For more information about replication, review *About NetBackup Auto Image Replication* in the [NetBackup Administrator's Guide, Volume I](#).
- (Optional) To keep a copy in long-term storage, turn on **Duplicate a copy immediately to long-term retention**. This option is not available for all workloads.
 - NetBackup immediately duplicates a copy to long-term storage after the backup completes.
 - The schedule options that are available for long-term storage are based on the frequency and the retention levels for the regular backup schedules that you created.

In the **Start window** tab:

- Define a **Start day**, **Start time**, **End day**, and **End time** for this schedule using the options available on the screen. Or you can drag your cursor over the time boxes to create the schedule.
- Use the options on the right to duplicate, remove, or undo changes to a schedule.

Click **Save** after all options are selected in the **Attributes** and the **Start window** tabs.

Review the **Backup schedule preview** window and verify that all schedules are set correctly.

- 4 In **Storage options**, configure the storage type per schedule you configured in step 3.

The options vary depending on storage options currently setup to work with NetBackup.

A protection plan can only use the storage that a NetBackup 8.1.2 or newer media server can access.

Storage option	Requirements	Description
Snapshot storage only	Snapshot Manager is required for this option.	Configure Snapshot Manager in the NetBackup Administration Console using the Snapshot Management Server feature. If you use the Snapshot only storage option, no other storage option can be selected. Go to step 5.
Perform snapshot backups	Microsoft SQL Server is required for this option.	For instructions on configuring protection plans for Microsoft SQL Server, see the <i>NetBackup Web UI Microsoft SQL Server Administrator's Guide</i> .
Backup storage	OpenStorage is required for this option. Tape, storage unit groups, and Replication Director not supported.	<p>Click Edit to select the storage target. Click Use selected storage after selecting the storage target.</p> <p>The NetBackup Accelerator feature allows protection plans to execute faster than traditional backups, by creating a compact data stream that uses less network bandwidth. If the storage server on the NetBackup primary server supports NetBackup Accelerator, this feature is included in the protection plan. For more details on NetBackup Accelerator, contact the NetBackup administrator or see the NetBackup Administrator's Guide, Volume I or the NetBackup for VMware Administrator's Guide.</p> <p>The Instant access feature allows the plan's recovery points to support the creation of instant access VMs or databases.</p>
Replication target	The backup storage must be a source in a targeted A.I.R. environment.	<p>Click Edit to select the replication target primary server. Select a primary server and then select a storage lifecycle policy. Click Use selected replication target to return to the storage options screen.</p> <p>Cloud workloads support the MSDP and MSDP-C storage units for replication (AIR).</p> <p>If the replication target primary server is not in the list, you must add one in NetBackup. For more information on how to add a replication target primary server, review <i>Adding a trusted primary server</i> in the NetBackup Deduplication Guide.</p>

Storage option	Requirements	Description
Long-term retention storage	OpenStorage is required for this option. Tape, storage unit groups, and Replication Director not supported.	Click Edit to select the cloud storage provider. Click Use selected storage after selecting the cloud provider target. Cloud workloads support the AdvancedDisk, Cloud storage, MSDP, and MSDP-C as storage units for duplication.
Transaction log options	Microsoft SQL Server is required for this option.	If you use the option Select custom storage options , click Edit to select the backup storage.

- 5** In **Backup options**, configure all options based on your workload type. The options in this area change depending on workload, schedule, or storage options selected.

For the **Cloud** workload:

- For any of the selected cloud provider option, if you select **Enable granular recovery for files or folders**, ensure that you have opted to retain a snapshot while adding a backup schedule, as granular recovery can be performed only from a snapshot image.
- For any of the selected cloud provider option, if you select **Exclude selected disks from backups**, then the selected disks would not be backed-up and hence the VM would not be recovered completely. Any application running on the excluded disks might not work.

Note: The boot disks cannot be excluded from the backups even if they have data or tags associated with them.

- If you have selected the cloud provider as Google Cloud Platform, select **Enable regional snapshot**, to enable regional snapshots.
If the regional snapshot option is enabled, the snapshot is created in the same region in which the asset exists. Otherwise, the snapshot is created in a multi-regional location.
- (Microsoft Azure or Azure Stack Hub cloud provider) Select **Specify snapshot destination resource group** to associate snapshots to a particular peer resource group. This resource group is within the same region in which the asset exists. Select a configuration, subscription, and a resource group for a snapshot destination.
- If you have selected **Enable Continuous data protection** for a VMware workload, select a Continuous data protection gateway from the list. Click **Next**.

- For cloud workloads with PaaS assets, select a **Staging path** in the **Backup options** tab. This should be the export path of MSDP Universal Share storage residing on RHEL media server.

Note: If the MSDP STU is created on cloud storage, then universal shares from such storage servers are not listed in the DBPaaS protection plan. Because, the backup of universal shares from cloud storage unit are not supported by universal share backup mechanism.

- 6 In **Permissions**, review the roles that have access to protection plans.
To give another role access to this protection plan, click **Add**. Select the **Role** in the table and customize the role by adding or removing permissions in the **Select permissions** section.
- 7 In **Review**, verify that the protection plan details are correct and click **Finish**.

Customizing protection plans

After you create a protection plan, only certain settings are available to change or configure. See [Table 8-1](#).

Table 8-1 Protection plan settings that can be configured and edited

Protection plan setting	Setting is available when you...		Notes
	Edit a plan	Subscribe an asset	
Storage options	X		
Backup options		X	
Advanced options		X	
Schedules	X	X	Backup window only. For SQL Server, transaction log frequency, and retention.
Protected assets		N/A	
Permissions	X	N/A	Can add a role.

Edit or delete a protection plan

Edit a protection plan

You can make changes to the **Description**, **Storage options**, and **Schedules** (limited) for a protection plan.

Note: You cannot edit these settings in a protection plan: **Backup options** and **Advanced options**. If you want to adjust these settings and additional schedule settings, you must create a new protection plan and subscribe assets to the new plan. Or, you can customize the plan for the asset.

See [“Customizing protection plans”](#) on page 87.

To edit a protection plan

- 1 On the left, click **Protection > Protection plans**.
- 2 Click on the protection plan name that you want to edit.
- 3 Click **Edit description** to edit the description.
- 4 (Optional) In the **Storage options** section, click **Edit** to change the storage options.

Delete a protection plan

You cannot delete a protection plan unless all assets have been removed from the protection plan. If you want to maintain protection on the assets, add another protection plan to those assets before you delete the current protection plan.

See [“Unsubscribe an asset from a protection plan”](#) on page 90.

See [“Subscribe an asset or an asset group to a protection plan”](#) on page 89.

See [“Create a protection plan”](#) on page 81.

To delete a protection plan

- 1 On the left, click **Protection > Protection plans**.
- 2 Select the check box for the protection plan that you want to delete.
- 3 Click **Delete > Yes**.

Subscribe an asset or an asset group to a protection plan

You can subscribe a single asset or a group of assets to a protection plan. An asset or a group of assets can be subscribed to multiple protection plans. Before you can subscribe assets to a protection plan, you must create a protection plan.

NetBackup supports homogenous cloud asset subscriptions. When you subscribe an asset to a protection plan, the cloud provider of the asset must be the same as the cloud provider that is defined in the protection plan.

Note: You cannot edit these settings when you subscribe an asset: **Storage options** or **Permissions**. Changes to **Schedules** are limited. If you want to adjust these settings, you must create a new protection plan and subscribe assets to the new plan. Or, you can customize the plan for the asset.

See [“Customizing protection plans”](#) on page 87.

To subscribe an asset or an asset group to a protection plan

- 1 On the left, click **Workloads** then the workload type (for example: **VMware**).
- 2 Select an asset type (for example: **Virtual machines**, **Intelligent VM groups**).
- 3 Select one or more assets.
- 4 Click **Add protection**.

If you selected a Cloud workload asset or asset group, proceed to step 7.

- 5 In **Choose a protection plan**, select the name of the protection plan and click **Next**.
- 6 (Optional) Adjust any options in the **Backup options** or **Advanced options**.

- **Schedules**

Change the backup start window for full or incremental schedules.

For SQL Server transaction log schedules you can change the start window, the recurrence, and the retention period.

- **Backup options**

Adjust the backup options that were set up in the original protection plan. The options in this area change depending on workload.

- **Advanced**

Change or add any options that were set up in the original protection plan.

You need the following permissions to make these changes:

- **Edit attributes**, to edit **Backup options** and **Advanced options**.

- **Edit full and incremental schedules**, to edit the start window for these schedule types.
- **Edit transaction log schedules**, to edit the settings for SQL Server transaction log schedules.

7 Click **Protect**.

Unsubscribe an asset from a protection plan

You can unsubscribe individual assets or groups of assets from a protection plan.

Note: When you unsubscribe an asset from a protection plan, there is a possibility that the asset displays **Classic policy** in the web UI. This situation can happen when an asset is subscribed to a protection plan and a backup runs for that asset. Then the asset is unsubscribed from the protection plan while it has a valid backup image. The web UI displays **Classic policy**, but there may or may not be an active policy protecting the asset.

To unsubscribe a single asset from a protection plan

- 1 On the left, click **Workloads** then the workload type (for example: **VMware**).
- 2 Select a single asset type (for example: **Virtual machines**).
- 3 Click on the specific asset name.
- 4 Click **Remove protection** and click **Yes**.

To unsubscribe a group of assets from the protection plan

- 1 On the left, click **Workloads** then the workload type (for example: **VMware**).
- 2 Select a group asset type (for example: **Intelligent VM groups**).
- 3 Click on the specific group asset name.
- 4 Click **Remove protection** and click **Yes**.

View protection plan overrides

When you set permissions for protection plans, you can set the permissions to allow your workload administrator to customize assets a protection plan covers. The workload administrator can apply overrides to certain areas of schedules and backup options for an asset.

To view protection plan overrides

- 1** On the left, click **Protection > Protection plans** and then click the name of the protection plan.
- 2** In the **Protected assets** tab, click on **Applied** in the **Custom settings** column.
- 3** Review the original and the new settings in the **Schedules** and **Backup options** tabs.
 - **Original:** The setting when the protection plan was first created.
 - **New:** The last change that was made to the protection plan for that setting.

About Backup Now

With Backup Now, workload administrators can back up an asset immediately. For example, you can use Backup Now to prepare for the upcoming events that are outside scheduled backups, such as system maintenance. This type of backup is independent of scheduled backups and does not affect future backups. You can manage and monitor a Backup Now job in the same way you manage and monitor other NetBackup jobs.

Backup Now is supported for the following workloads:

- Cloud and PaaS
NetBackup supports homogenous cloud asset subscriptions. While you subscribe an asset to a protection plan, the cloud provider of the asset must be the same as the cloud provider defined in the protection plan.
- Microsoft SQL
- Nutanix AHV
- RHV
- VMware

Note: To use Backup Now you must have subscribe permissions for at least one protection plan. You can select only one asset at a time for each Backup Now operation.

Immediately back up an asset using Backup Now

You can start Backup Now for an asset from the list of assets. For example, from the list of virtual machines, intelligent groups, or databases. Or, you can start Backup Now from the asset's details. These details display all of the protection plans to

which the asset is subscribed. You can choose **Backup now** from any one of these protection plans.

To immediately back up an asset using Backup Now

- 1** On the left, select the workload and locate the asset that you want to back up.
- 2** Select **Actions > Backup now**
- 3** Choose a protection plan for the backup.

All protection plans to which the asset is subscribed are listed.

To back up an asset that is not subscribed to any protection plan, select **Backup now** and choose from the existing protection plans. You can also create a new protection plan and then use it with a **Backup now** operation.

Note: The option of **Backup type** is only available for Microsoft SQL Server assets. You can select the type of backup you want to perform using the drop-down. The drop-down only contains the backup types that are available in the protection plan.

- 4** Click **Start backup**.

Managing classic policies

This chapter includes the following topics:

- [Add a policy](#)
- [Example policy - Exchange Server DAG backup](#)
- [Example policy - Sharded MongoDB cluster](#)

Add a policy

Use the following procedure to create a backup policy in the NetBackup web UI. Example policies are also available.

See [“Example policy - Exchange Server DAG backup”](#) on page 94.

See [“Example policy - Sharded MongoDB cluster”](#) on page 95.

For details on policy options, refer to the *NetBackup Administrator's Guide, Volume I* and to the appropriate workload or database guides.

Note: You must have the RBAC Administrator role or similar permissions to create and manage policies.

To add a policy

- 1 On the left, select **Protection > Policies**.
- 2 Click **Add**.
- 3 On the **Attributes** tab, do the following:
 - Select the **Policy type** that you want to create.
 - Select the **Policy storage** that you want to use.
 - Select or configure any other policy attributes.

- 4 On the **Schedules** tab, configure all the necessary schedules. For example, Full and incremental schedules.
- 5 Depending on the policy type that you selected, add the clients, database instances, or virtual machines that you want to protect. Perform this configuration on the **Clients** or the **Instances and databases** tab.
 - For most policy types you configure a list of clients on the **Clients** tab.
 - For **Oracle** and **MS-SQL-Server** policy types, you select instances or databases on the **Instances and databases** tab. Or if you use scripts or batch files, you select clients on the **Clients** tab.
- 6 Depending on the policy type that you selected, add the files, database instances, or other objects that you want to protect. This configuration is performed on the **Backup selections** tab.
- 7 For the policy types that have additional tabs, review and select the other policy options that are needed to complete the setup.
- 8 Click **Create**.

Example policy - Exchange Server DAG backup

This example describes how to create a policy to back up all databases in an Exchange Server DAG.

To add a policy for an Exchange Server DAG backup

- 1 On the left, select **Protection > Policies**.
- 2 Click **Add**.
- 3 On the **Attributes** tab, select the following:
 - **Policy type**: MS-Exchange-Server
 - **Perform snapshot backups**: Must be enabled.
 - **Enable granular recovery**: Optional. Enable this option if you want to restore individual mailbox and public folder objects from the database backup.
 - **Database backup source**: Choose whether to back up the active or the passive copy of the database. Also configure the preferred list, depending on the backup source that you selected.

- 4 On the **Schedules** tab, configure all the necessary schedules. For example, Full and incremental schedules.

Name	Type	Frequency	Retention
Full-backup	Full backup	1 week	2 weeks
Incremental-backup	Differential incremental	1 day	2 weeks

- 5 On the **Clients** tab, add one or more DAG names.

Client name	Hardware	Operating system
dag1234.domain.com	Windows-x64	Windows2016
dag5678.domain.com	Windows-x64	Windows2016

- 6 On the **Backup selections** tab, add the following directive.

```
Microsoft Exchange Database Availability Groups:\
```

Backup selection list

```
Microsoft Exchange Database Availability Groups:\
```

- 7 Click **Create**.

Example policy - Sharded MongoDB cluster

This example describes how to create a policy to back up the primary configuration server in a Sharded MongoDB cluster.

To add a policy for a MongoDB cluster backup

- 1 On the left, select **Protection > Policies**.
- 2 Click **Add**.
- 3 On the **Attributes** tab, select the following:
 - **Policy type:** BigData

- 4 On the **Schedules** tab, configure all the necessary schedules. For example, Full and incremental schedules.

Name	Type	Frequency	Retention
Full-backup	Full backup	1 week	2 weeks
Incremental-backup	Differential incremental backup	1 day	2 weeks

- 5 On the **Clients** tab, add the client name. Use the format `MongoDBNode-portnumber`.

The following list backs up the primary configuration server on port 1.

Client name	Hardware	Operating system
primaryconfigserver-01	Linux	Red Hat 2.6.32

- 6 On the **Backup selections** tab, add the application type, the backup hosts, and manually add the ALL_DATABASES directive.

Backup selection list	Notes
Application_Type=mongodb	The parameter values are case-sensitive.
mongodbhost=mongodbhost.domain.com	Use the format <code>Backup_Host=<FQDN_or_hostname></code> . The backup host can be a NetBackup client or a media server.
ALL_DATABASES	

- 7 Click **Create**.

Managing backup images

This chapter includes the following topics:

- [About the NetBackup catalog](#)
- [Search for backup images](#)

About the NetBackup catalog

In the NetBackup web UI, use the **Catalog** utility to perform the following actions:

- Search for backup images to verify the contents of media with what is recorded in the NetBackup catalog.
- Duplicate a backup image.
- Expire backup images.
- Import expired backup images or images from another NetBackup server.

For more details on these actions and information on NetBackup catalog backups, see the [NetBackup Administrator's Guide, Volume I](#).

Search for backup images

To verify, duplicate, or import backup images, you first need to locate those images in the catalog.

For more details on these actions and on data-in-transit encryption (DTE) in your NetBackup environment, see the [NetBackup Administrator's Guide, Volume I](#) and [NetBackup Security and Encryption Guide](#).

To search for backup images

- 1 On the left, click **Catalog**.
- 2 From the **Action** list, select one of the following:

- **Verify.**
 - **Duplicate.**
 - **Phase 1 import.**
 - **Phase 2 import.**
- 3 Select the criteria for the search or the import.
 - 4 Click **Search** or **Import**.

Search results

When you search for backup images, the image list displays at the bottom of the screen. Click **Show or hide columns** to display additional information about the images.

The NetBackup web UI also indicates any image information for the **Copy DTE mode** and **Copy hierarchy DTE mode**. These attributes indicate if a copy or the ancestor copies are created securely.

Pausing data protection activity

This chapter includes the following topics:

- [Pause backups and other activity](#)
- [Allow NetBackup and authorized users to pause data protection activity](#)
- [Pause backups and other activity on a client](#)
- [View paused backups and other paused activities](#)
- [Resume data protection activity](#)

Pause backups and other activity

By default, NetBackup and authorized users are not allowed to pause data protection activities. Backups and other activities continue even if a scan detects malware in an image or a recovery point.

You can allow NetBackup and authorized users to automatically pause data protection activity on specific clients. For example, if a scan detects malware in backup images or recovery points for a specific client.

Data protection activity includes backups, duplication, replication, and image expiration. When it is enabled, a pause applies to scheduled backups and other automatic activities. It also applies to operations that a user initiates. Authorized users are those that have an RBAC role with the necessary security permissions to pause data protection activity.

Allow NetBackup and authorized users to pause data protection activity

You can choose to allow or not to allow NetBackup and authorized users to pause backups and other activity.

To allow NetBackup and authorized users to pause data protection activity

- 1 On the left, click **Protection > Protection status**.
- 2 Click **Edit settings** and click **Edit**.
- 3 Choose if you want to allow NetBackup or authorized users to pause data protection activity:
 - **Do not allow.** NetBackup and authorized users are not allowed to pause data protection activity.
 - **Allow.** NetBackup or authorized users can pause backups, duplication, and replication. Optionally, you can allow NetBackup or users to pause the expiration of backup images.

Pause backups and other activity on a client

Users can pause backups and other activity on a client until a certain date or indefinitely. This functionality is available in the API endpoint `POST /config/blocked-clients/`.

View paused backups and other paused activities

You can view a list of the clients or hosts where data protection activity is paused.

To view paused data protection activity

- 1 On the left, click **Protection > Protection status**.
- 2 The page displays the list of clients where the protection activity is paused. “Automatic” indicates that the pause was applied automatically by NetBackup. “User-initiated” indicates that a user manually applied the pause to the client.
 If you have not yet configured the setting, click **Edit settings**.
- 3 To see the details of the pause for a specific client, locate the client name. Then click **Actions > View pause details**.

Resume data protection activity

After performing maintenance or resolving any issues, you can resume the data protection activity where it is paused on a client. Perform this action from the **Protection > Protection status** node.

Note that when you resume data protection activity, this action also turns off any host property settings that disable backups on any clients.

To resume data protection activity for a client

- 1** On the left, click **Protection > Protection status**.
- 2** Select one or more clients and click **Resume**.

Managing security

- [Chapter 12. Security events and audit logs](#)
- [Chapter 13. Managing security certificates](#)
- [Chapter 14. Managing host mappings](#)
- [Chapter 15. Managing user sessions](#)
- [Chapter 16. Managing the security settings for the primary server](#)
- [Chapter 17. Using access keys, API keys, and access codes](#)
- [Chapter 18. Configuring authentication options](#)
- [Chapter 19. Managing role-based access control](#)

Security events and audit logs

This chapter includes the following topics:

- [View security events and audit logs](#)
- [About NetBackup auditing](#)
- [Send audit events to system logs](#)

View security events and audit logs

NetBackup audits user-initiated actions in a NetBackup environment to help answer who changed what and when they changed it. For a full audit report, use the `nbauditreport` command. See [“Viewing the detailed NetBackup audit report”](#) on page 108.

To view security events and audit logs

- 1 On the left, select **Security > Security events**.
- 2 The following options are available.
 - Click **Access history** to view the users that accessed NetBackup.
 - Click **Audit events** to view the events that NetBackup audited. These events include changes to security settings, certificates, and users who browsed or restored backups images.

About NetBackup auditing

Auditing is enabled by default in new installations. NetBackup auditing can be configured directly on a NetBackup master server.

Auditing of NetBackup operations provides the following benefits:

- Customers can gain insight from audit trails while they investigate unexpected changes in a NetBackup environment.
- Regulatory compliance.
The record complies with guidelines such as those required by the Sarbanes-Oxley Act (SOX).
- A method for customers to adhere to internal change management policies.
- Help for NetBackup Support in troubleshooting problems for customers.

About the NetBackup Audit Manager

The NetBackup Audit Manager (`nbaudit`) runs on the master server and audit records are maintained in the Enterprise Media Manager (EMM) database.

An administrator can search specifically for:

- When an action occurred
- Failed actions in certain situations
- The actions that a specific user performed
- The actions that were performed in a specific content area
- Changes to the audit configuration

Note the following:

- The audit record truncates any entries greater than 4096 characters. (For example, policy name.)
- The audit record truncates any restore image IDs greater than 1024 characters.

Actions that NetBackup audits

NetBackup records the following user-initiated actions.

Activity monitor actions	Canceling, suspending, resuming, restarting, or deleting any type of job creates an audit record.
Alerts and email notifications	If an alert cannot be generated or an email notification cannot be sent for NetBackup configuration settings. For example, SMTP server configuration and the list of excluded status codes for alerts.
Anomalies	When a user reports an anomaly as false positive, the action is audited and logged for that user.

Asset actions	<p>Deleting an asset, such as a vCenter server, as part of the asset cleanup process is audited and logged.</p> <p>Creating, modifying, or deleting an asset group as well any action on an asset group for which a user is not authorized is audited and logged.</p>
Authorization failure	Authorization failure is audited when you use the NetBackup web UI, the NetBackup APIs, or Enhanced Auditing.
Catalog information	<p>This information includes:</p> <ul style="list-style-type: none">■ Verifying and expiring images.■ Read the requests that are sent for the front-end usage data.
Certificate management	Creating, revoking, renewing, and deploying of NetBackup certificates and specific NetBackup certificate failures.
Certificate Verification Failures (CVFs)	<p>Any failed connection attempts that involve SSL handshake errors, revoked certificates, or host name validation failures.</p> <p>For certificate verification failures (CVFs) that involve SSL handshakes and revoked certificates, the timestamp indicates when the audit record is posted to the master server. (Rather than when an individual certificate verification fails.) A CVF audit record represents a group of CVF events over a time period. The record details provide the start and the end times of the time period as well as the total number of CVFs that occurred in that period.</p>
Disk pools and Volume pools actions	Adding, deleting, or updating disk or volume pools.
Hold operations	Creating, modifying, and deleting hold operations.
Host database	NetBackup operations that are related to the host database.
Logon attempts	Any successful or any failed logon attempts for the NetBackup Administration Console, the NetBackup web UI or the NetBackup APIs.
Policies actions	Adding, deleting, or updating policy attributes, clients, schedules, and backup selections lists.
Restore and browse image user actions	All the restore and browse image content (<code>bplist</code>) operations that a user performs are audited with the user identity.
Security configuration	Information that is related to changes that are made to the security configuration settings.
Starting a restore job	NetBackup does not audit when other types of jobs begin. For example, NetBackup does not audit when a backup job begins.
Starting and stopping the NetBackup Audit Manager (<code>nbaudit</code>).	Starting and stopping of the <code>nbaudit</code> manager is always audited, even if auditing is disabled.

Storage lifecycle policy actions	Attempts to create, modify, or delete a storage lifecycle policy (SLP) are audited and logged. However, activating and suspending an SLP using the command <code>nbslutil</code> are not audited. These operations are audited only when they are initiated from a NetBackup graphical user interface or API.
Storage servers actions	Adding, deleting, or updating storage servers.
Storage units actions	Adding, deleting, or updating storage units. Note: Actions that are related to storage lifecycle policies are not audited.
Token management	Creating, deleting, and cleanup of tokens and specific token issuing failures.
User management	Adding and deleting Enhanced Auditing users in the Enhanced Auditing mode.
User action that fails to create an audit record	If auditing is enabled but a user action fails to create an audit record, the audit failure is captured in the <code>nbaudit</code> log. NetBackup status code 108 is returned (<code>Action succeeded but auditing failed</code>). The NetBackup does not return an exit status code 108 when auditing fails.

Actions that NetBackup does not audit

The following actions are not audited and do not display in the audit report:

Any failed actions.	NetBackup logs failed actions in NetBackup error logs. Failed actions do not display in audit reports because a failed attempt does not bring about a change in the NetBackup system state.
The effect of a configuration change	The results of a change to the NetBackup configuration are not audited. For example, the creation of a policy is audited, but the jobs that result from its creation are not.
The completion status of a manually initiated restore job	While the act of initiating a restore job is audited, the completion status of the job is not audited. Nor is the completion status of any other job type, whether initiated manually or not. The completion status is displayed in the Activity Monitor.
Internally initiated actions	NetBackup-initiated internal actions are not audited. For example, the scheduled deletion of expired images, scheduled backups, or periodic image database cleanup is not audited.
Rollback operations	Some operations are carried out as multiple steps. For example, creating an MSDP-based storage server consists of multiple steps. Every successful step is audited. Failure in any of the steps results in a rollback, or rather, the successful steps may need to be undone. The audit record does not contain details about rollback operations.

Host properties actions

Changes made with the `bpsetconfig` or the `nbsetconfig` commands, or the equivalent property in host properties, are not audited. Changes that are made directly to the `bp.conf` file or to the registry are not audited.

User identity in the audit report

The audit report indicates the identity of the user who performed a specific action. The full identity of the user includes the user name and the domain or the host name that is associated with the authenticated user. A user's identity appears in the audit report as follows:

- Audit events always include the full user identity. Root users and administrators are logged as "root@hostname" or "administrator@hostname".
- In NetBackup 8.1.2 and later, image browse and image restore events always include the user ID in the audit event. NetBackup 8.1.1 and earlier log these events as "root@hostname" or "administrator@hostname".
- The order of the elements for the user principal is "domain:username:domainType:providerId". The domain value does not apply for Linux computers. For that platform, the user principal is :username:domainType:providerId.
- For any operations that do not require credentials or require the user to sign in, operations are logged without a user identity.

Audit retention period and catalog backups of audit records

The audit records are kept as part of the NetBackup database, for as long as the retention period indicates. The records are backed up as part of the NetBackup catalog backup. The NetBackup Audit Service (`nbaudit`) deletes expired audit records once every 24 hours at 12:00 A.M. (local time).

By default, audit records are kept for 90 days. Use an audit retention period value of 0 (zero) if you do not want to delete the audit records.

To configure the audit retention period

1 Log on to the master server.

2 Open the following directory:

Windows: *install_path\NetBackup\bin\admincmd*

UNIX: */usr/opensv/netbackup/bin/admincmd*

3 Enter the following command:

```
nbemmcmd -changesetting -AUDIT_RETENTION_PERIOD
number_of_days -machinename masterserver
```

Where *number_of_days* indicates (in days) how long audit records are to be retained for the audit report.

In the following example, the records of user actions are retained for 30 days and then deleted.

```
nbemmcmd -changesetting -AUDIT_RETENTION_PERIOD 30
-machinename server1
```

To ensure that audit records are not missed from a catalog backup, configure the catalog backup frequency to be less frequent or equal to the `-AUDIT_RETENTION_PERIOD`.

Viewing the detailed NetBackup audit report

To view the full audit report

1 Log on to the primary server.

2 Enter the following command to display the audit report in the summary format.

Windows: *install_path\NetBackup\bin\admincmd\nbauditreport*

UNIX: */usr/opensv/netbackup/bin/admincmd\nbauditreport*

Or, run the command with the following options.

```
-sdate
<"MM/DD/YY
[HH:[MM[:SS]]]">
```

The start date and time of the report data you want to view.

```
-edate  
<"MM/DD/YY  
[HH:[MM[:SS]]]">
```

The end date and time of the report data you want to view.

```
-ctgy category
```

The category of user action that was performed. Categories such as `POLICY` may contain several sub-categories such as `schedules` or `backup selections`. Any modifications to a sub-category are listed as a modification to the primary category.

See the [NetBackup Commands Guide](#) for `-ctgy` options.

```
-user  
<username[:domainname]>
```

Use to indicate the name of the user for whom you'd like to display audit information.

```
-fmt DETAIL
```

The `-fmt DETAIL` option displays a comprehensive list of audit information. For example, when a policy is changed, this view lists the name of the attribute, the old value, and the new value. This option has the following sub-options:

- `[-notruncate]` . Display the old and new values of a changed attribute on separate lines in the details section of the report.
- `[-pagewidth <NNN>]` . Set the page width for the details section of the report.

```
-fmt PARSABLE
```

The `-fmt PARSABLE` option displays the same set of information as the `DETAIL` report but in a parsable format. The report uses the pipe character (`|`) as the parsing token between the audit report data. This option has the following sub-options:

- `[-order <DTU|DUT|TUD|UDT|UTD>]`. Indicate the order in which the information appears.
 - D (Description)
 - T (Timestamp)
 - U (User)

3 The audit report contains the following details:

DESCRIPTION	The details of the action that was performed.
USER	The identity of the user who performed the action. See "User identity in the audit report" on page 107.
TIMESTAMP	The time that the action was performed.
The following information only displays if you use the <code>-fmt DETAIL</code> or the <code>-fmt PARSABLE</code> options.	
CATEGORY	The category of user action that was performed.
ACTION	The action that was performed.
REASON	The reason that the action was performed. A reason displays if a reason was specified for the operation that created the change.
DETAILS	An account of all of the changes, listing the old values and the new values.

Example of the audit report:

```
[root@server1 admincmd]# ./nbauditreport
TIMESTAMP      USER          DESCRIPTION
04/20/2018 11:52:43 root@server1  Policy 'test_pol_1' was saved but no changes were detected
04/20/2018 11:52:42 root@server1  Schedule 'full' was added to Policy 'test_pol_1'
04/20/2018 11:52:41 root@server1  Policy 'test_pol_1' was saved but no changes were detected
04/20/2018 11:52:08 root@server1  Policy 'test_pol_1' was created
04/20/2018 11:17:00 root@server1  Audit setting(s) of master server 'server1' were modified

Audit records fetched: 5
```

Send audit events to system logs

You can send NetBackup audit events to system logs. Ensure that you have the following permissions to carry out this task:

- View permission on the **Security > Security events UI**

- View, Create, Update, and Delete permissions on the **NetBackup management > NetBackup hosts** UI

To send audit events to system logs

- 1** On the left, select **Security > Security events**.
- 2** On the top right, click **Audit event settings**.
- 3** Enable **Send the audit events to the system logs** option.
- 4** In the **Audit event categories** dialog box, select the audit categories for which you want to send the audit events to the system logs.

To send audit events for all audit categories to the system logs, select the **Audit event categories** check box.

- 5** Click **Save**.

You can view NetBackup audit events in the system logs. For example:

On a Windows system, use **Windows Event Viewer** to view NetBackup audit events.

On a Linux system, you can view the system logs on the configured location.

Managing security certificates

This chapter includes the following topics:

- [About security management and certificates in NetBackup](#)
- [NetBackup host IDs and host ID-based certificates](#)
- [Managing NetBackup security certificates](#)
- [Using external security certificates with NetBackup](#)

About security management and certificates in NetBackup

NetBackup uses security certificates to authenticate the NetBackup hosts. These certificates must conform to the X.509 public key infrastructure (PKI) standard. With NetBackup 8.1, 8.1.1, and 8.1.2, NetBackup certificates are used for secure communication. In NetBackup 8.2 and later you can use NetBackup certificates or external certificates.

NetBackup certificates are issued to hosts by default and the NetBackup primary server acts as the CA and manages the Certificate Revocation List (CRL). The **NetBackup certificate deployment security level** determines how certificates are deployed to NetBackup hosts and how often the CRL is updated on each host. If a host needs a new certificate (the original certificate is expired or revoked), you can use an NetBackup authorization token to reissue the certificate.

External certificates are those that a trusted external CA signed. When you configure NetBackup to use external certificates, the primary server, media servers, and clients in the NetBackup domain use the external certificates for secure

communication. Additionally, the NetBackup web server uses these certificates for communication between the NetBackup web UI and the NetBackup hosts. Deployment of external certificates, updating or replacing external certificates, and CRL management for the external CA are managed outside of NetBackup.

For more information on external certificates, see the [NetBackup Security and Encryption Guide](#).

Security certificates for NetBackup 8.1 and later hosts

NetBackup 8.1 and later hosts can communicate with each other only in a secure mode. Depending on the NetBackup version, these hosts must have a certificate that the NetBackup CA issued or that another trusted CA issued. A NetBackup certificate that is used for secure communications over a control channel is also referred to as host ID-based certificate.

Security certificates for NetBackup 8.0 hosts

Any security certificates that NetBackup generated for 8.0 hosts are referred to as host name-based certificates. For more details on these certificates, refer to the [NetBackup Security and Encryption Guide](#).

NetBackup host IDs and host ID-based certificates

Each host in a NetBackup domain has a unique identity, which is referred to as a host ID or a Universally Unique Identifier (UUID). The host ID is used in many operations to identify the host. NetBackup creates and manages host IDs as follows:

- Maintains a list on the primary server of all of the host IDs that have certificates.
- Randomly generates host IDs. These IDs are not tied to any property of the hardware.
- By default, assigns NetBackup 8.1 and later hosts a host ID-based certificate that is signed by the NetBackup certificate authority.
- The host ID remains the same even when the host name changes.

In some cases a host can have multiple host IDs:

- If a host obtains certificates from multiple NetBackup domains, it has multiple host IDs that correspond to each NetBackup domain.
- When the primary server is configured as part of a cluster, each node in the cluster receives a unique host ID. An additional host ID is assigned for the virtual name. For example, if the primary server cluster is composed of N nodes, the number of host IDs that are allocated for the primary server cluster is $N + 1$.

Managing NetBackup security certificates

Note: The information here only applies to the security certificates that are issued by the NetBackup certificate authority (CA). More information is available for external certificates.

See [“Using external security certificates with NetBackup”](#) on page 118.

You can view and revoke NetBackup certificates and view information about the NetBackup CA. More detailed information about NetBackup certificate management and certificate deployment is available in the [NetBackup Security and Encryption Guide](#).

View a NetBackup certificate

You can view details of all host ID-based NetBackup certificates that are issued to NetBackup hosts. Note that only 8.1 and later NetBackup hosts have host ID-based certificates. The **Certificates** list does not include any NetBackup 8.0 or earlier hosts.

To view a NetBackup certificate

- 1 On the left, select **Security > Certificates**.
- 2 Click **NetBackup certificates**.
- 3 To view additional certificate details for a host, click on a host name.

Revoke a NetBackup CA certificate

When you revoke a NetBackup host ID-based certificate, NetBackup revokes any other certificates for that host. NetBackup ceases to trust the host, and it can no longer communicate with the other NetBackup hosts.

You may choose to revoke a host ID-based certificate under various conditions. For example, if you detect that client security has been compromised, if a client is decommissioned, or if NetBackup was uninstalled from the host. A revoked certificate cannot be used to communicate with primary server web services.

Security best practices suggest that the NetBackup security administrator explicitly revoke the certificates for any host that is no longer active. Take this action if whether or not the certificate is still deployed on the host.

Note: Do not revoke a certificate of the primary server. If you do, NetBackup operations may fail.

To revoke a NetBackup CA certificate

- 1 On the left, select **Security > Certificates**.
- 2 Click **NetBackup certificates**.
- 3 Select the host that is associated with the certificate that you want to revoke.
- 4 Click **Revoke certificate > Yes**.

View the NetBackup certificate authority details and fingerprint

For secure communication with the NetBackup certificate authority (CA) on the primary server, a host's administrator must add the CA certificate to an individual host's trust store. The primary server administrator must give the fingerprint of the CA certificate to the administrator of the individual host.

To view the NetBackup certificate authority details and fingerprint

- 1 On the left, select **Security > Certificates**.
- 2 Click **NetBackup certificates**.
- 3 In the toolbar, click **Certificate authority**.
- 4 Find the **Fingerprint** information and click **Copy to clipboard**.
- 5 Provide this fingerprint information to the host's administrator.

Reissue a NetBackup certificate

Note: The information here only applies to the security certificates that are issued by the NetBackup certificate authority (CA). External certificates must be managed outside of NetBackup.

In some cases a host's NetBackup certificate is no longer valid. For example, if a certificate is expired, revoked, or is lost. You can reissue a certificate either with or without a reissue token.

A reissue token is a type of authorization token that is used to reissue a NetBackup certificate. When you reissue a certificate, the host gets the host ID same as the original certificate.

Reissue a NetBackup certificate, with a token

If you need to reissue a host's NetBackup certificate NetBackup provides a more secure method to do this reissue. You can create an authorization token that the

host administrator must use to obtain a new certificate. This reissue token retains the same host ID as the original certificate. The token can only be used once. Because it is associated to a specific host, the token cannot be used to request certificates for other hosts.

To reissue a NetBackup certificate for a host

- 1 On the left, select **Security > Certificates**.
- 2 Click **NetBackup certificates**.
- 3 Select the host and click **Actions > Generate reissue token**.
- 4 Enter a token name and indicate how long the token should be valid for.
- 5 Click **Create**.
- 6 Click **Copy to clipboard** and click **Close**.
- 7 Share the authorization token so the host's administrator can obtain a new certificate.

Allow a NetBackup certificate reissue, without a token

In certain scenarios you need to reissue a certificate without a reissue token. For example, for a BMR client restore. The **Allow auto reissue certificate** option enables you to reissue a certificate without requiring a token.

To allow a NetBackup certificate reissue, without a token

- 1 On the left, select **Hosts > Host mappings**.
- 2 Locate the host and click **Actions > Allow auto reissue certificate > Allow**.

Once you set the **Allow auto reissue certificate** option, a certificate can be reissued without a token within the next 48 hours, which is the default setting. After this window to reissue expires, the certificate reissue operation requires a reissue token.
- 3 Notify the host's administrator that you allowed a NetBackup certificate reissue without a token.

Revoke the ability to reissue a NetBackup certificate without a token

After you allow a NetBackup certificate reissue without a token, you can revoke this ability before the window to reissue expires. By default, the window is 48 hours.

To revoke the ability to reissue a NetBackup certificate without a token

- 1 On the left, select **Hosts > Host mappings**.
- 2 Locate the host and click **Actions > Revoke auto reissue certificate > Revoke**.

Managing NetBackup certificate authorization tokens

Note: The information here only applies to the security certificates that are issued by the NetBackup certificate authority (CA). External certificates must be managed outside of NetBackup.

Depending on the security level for NetBackup certificate deployment, you may need an authorization token to issue a new NetBackup certificate to a host. You can create a token when it is required or find and copy a token if it is needed again. Tokens can be cleaned up or deleted if they are no longer needed.

To reissue a certificate, a reissue token is required in most cases. A reissue token is associated with the host ID.

Create an authorization token

Depending on the NetBackup certificate deployment security level, an authorization token may be required for a non-primary NetBackup host to obtain a host ID-based NetBackup certificate. The NetBackup administrator of the primary server generates the token and shares it with the administrator of the non-primary host. That administrator can then deploy the certificate without the presence of the primary server administrator.

Do not create an authorization token for a NetBackup host whose current certificate is not in a valid state because it is lost, corrupt, or expired. In these cases, a reissue token must be used.

See [“Reissue a NetBackup certificate”](#) on page 115.

To create an authorization token

- 1 On the left, select **Security > Tokens**.
- 2 On the top left, click **Add**.
- 3 Enter the following information for the token:
 - Token name
 - The maximum number of times you want the token to be used
 - How long the token is valid for
- 4 Click **Create**.

To find and copy an authorization token value

You can view the details of the tokens that you have created and copy the token value for future use.

To find and copy an authorization token value

- 1 On the left, select **Security > Tokens**.
- 2 Select the name of the token for which you want to view the details.
- 3 At the top right, click **Show token** and then click the **Copy to clipboard** icon.

Cleanup tokens

Use the Cleanup tokens utility to delete tokens from the token database that are expired or that have reached the maximum number of uses allowed.

To cleanup tokens

- 1 On the left, select **Security > Tokens**.
- 2 Click **Cleanup > Yes**.

Delete a token

You can delete a token can be deleted before it is expired or before the **Maximum uses allowed** is reached.

To delete a token

- 1 On the left, select **Security > Tokens**.
- 2 Select the name of the tokens that you want to delete.
- 3 On the top right, click **Delete**.

Using external security certificates with NetBackup

NetBackup 8.2 and later versions support the security certificates that are issued by an external CA. External certificates and the certificate revocation list for an external certificate authority must be managed outside of NetBackup. The **External certificates** tab displays details for the NetBackup 8.1 and later hosts in the domain and whether or not they use external certificates.

Before you can see external certificate information in **Certificates > External certificates**, you must first configure the primary server and the NetBackup web server to use external certificates.

See [“Configure an external certificate for the NetBackup web server”](#) on page 119.

See the video [External CA support in NetBackup](#).

Configure an external certificate for the NetBackup web server

By default, NetBackup uses the security certificates that the NetBackup CA has issued. If you have a certificate that an external CA has issued, you can configure the NetBackup web server to use it for secure communication.

Note: Windows certificate store is not supported as certificate source for the NetBackup web server.

To configure an external certificate for the web server

- 1 Ensure that you have valid certificate, private key of the certificate, and trusted CA bundle.

- 2 Run the following command:

```
configureWebServerCerts -addExternalCert -nbHost -certPath
certificate path -privateKeyPath private key path -trustStorePath
CA bundle path [-passphrasePath passphrase file path]
```

The `configureWebServerCerts` command does not support use of Windows certificate store paths.

Refer to the [NetBackup Commands Reference Guide](#) for more details on the command-line options.

- In a clustered setup, to avoid a failover run the following command on the active node:

```
install_path/netbackup/bin/bpclusterutil -freeze
```

- 3 Restart the NetBackup Web Management Console service to reflect the changes.

On UNIX, run the following commands:

- `install_path/netbackup/bin/nbwmc -terminate`
- `install_path/netbackup/bin/nbwmc start`

On Windows, use the **Services** application in the **Windows Control Panel**.

Location of the commands:

Windows `install_path\NetBackup\wmc\bin\install\`

UNIX `install_path/wmc/bin/install`

- In a clustered setup, unfreeze the cluster using the following command on the active node:

```
install_path/netbackup/bin/bpclusterutil -unfreeze
```

- 4 Verify that you can access the NetBackup web user interface using a browser, without a certificate warning message.

Remove the external certificate configured for the web server

You can remove the external certificate that is configured for the web server. NetBackup then uses the NetBackup CA-signed certificate for secure communication.

To remove the external certificate configured for the web server

- 1 Run the following command (in a clustered master server setup, run this command on the active node):

```
configureWebServerCerts -removeExternalCert -nbHost
```

- In a clustered master server setup, run the following command on the active node to freeze the cluster to avoid a failover:

```
install_path/netbackup/bin/bpclusterutil -freeze
```

- 2 Restart the NetBackup Web Management Console service.

- In a clustered master server setup, run the following command on the active node to unfreeze the cluster:

```
install_path/netbackup/bin/bpclusterutil -unfreeze
```

Update or renew the external certificate for the web server

You can update or renew the external certificate that you configured for the web server.

To update or renew the external certificate for the web server

- 1 Ensure that you have the latest external certificate, the matching private key, and the CA bundle file.
- 2 Run the following command (in a clustered setup, run the command on the active node):

```
configureWebServerCerts -addExternalCert -nbHost -certPath  
certificate_path -privateKeyPath private_key_path -trustStorePath  
CA_bundle_path
```


View external certificate information for the NetBackup hosts in the domain

Note: Before you can see external certificate information, you must configure NetBackup for external certificates. See the [NetBackup Security and Encryption Guide](#) for details.

As you add external certificates to the hosts in the NetBackup domain, use the **External certificates** dashboard to track which hosts need attention. To support an external certificate, a host must be upgraded and enrolled with an external certificate.

To view external certificate information for the hosts

- 1 On the left, select **Security > Certificates**.
- 2 Click **External certificates**.

In addition to hosts information and details for the hosts' external certificates, the following information is also included:

- The **NetBackup certificate status** column indicates if a host also has a NetBackup certificate.
- The **External certificate** dashboard contains the following information for NetBackup 8.1 and later hosts:
 - Total hosts. The total number hosts. The hosts must be online and able to communicate with NetBackup primary server.
 - Hosts with certificates. The number of hosts that have a valid external certificate enrolled with the NetBackup primary server.
 - Host missing certificates. Either the host supports external certificates, but does not have one enrolled. Or, an upgrade to NetBackup 8.2 is required for the host (applies to versions 8.1, 8.1.1, or 8.1.2). The **NetBackup upgrade required** total also includes any hosts that were reset or any hosts for which the NetBackup version is unknown. NetBackup 8.0 and earlier hosts do not use security certificates and are not reflected here.
 - Certificate expiry. The hosts that have an expired or expiring external certificate.

View details for a host's external certificate

You can view details of a host's certificate that was issued by an external certificate authority.

To view details for a host's external certificate

- 1** On the left, select **Security > Certificates**.
- 2** Click **External certificates**.
The list of external certificates displays for the primary server.
- 3** To view additional certificate details for a host, click on a host name.

Managing host mappings

This chapter includes the following topics:

- [View host security and mapping information](#)
- [Approve or add mappings for a host that has multiple host names](#)
- [Remove mappings for a host that has multiple host names](#)

View host security and mapping information

The **Hosts** information in **Host mappings** contains details about the NetBackup hosts in your environment, including the primary server, media servers, and clients. Only hosts with a host ID are displayed in this list. The **Host** name reflects the NetBackup client name of a host, also referred to as the primary name of the host.

Note: NetBackup discovers any dynamic IP addresses (DHCP or Dynamic Host Configuration Protocol hosts) and adds these addresses to a host ID. You should delete these mappings.

For host name-based certificates for 8.0 and earlier NetBackup hosts, refer to the respective version of the [NetBackup Security and Encryption Guide](#).

To view NetBackup host information

- 1 On the left, select **Security > Host mappings**.
Review the security status and any other host names that are mapped to this host.
- 2 For additional details for this host, click the name of the host.

Approve or add mappings for a host that has multiple host names

A NetBackup host can have multiple host names. For example, both a private and a public name or a short name and a fully qualified domain name (FQDN). A NetBackup host may also share a name with other NetBackup host in the environment. NetBackup also discovers cluster names, including the host name and fully qualified domain name (FQDN) of the virtual name of the cluster.

See [the section called “Examples of auto-discovered mappings for a cluster”](#) on page 126.

See [the section called “Example of auto-discovered mappings for a cluster in a multiple NIC environment”](#) on page 126.

See [the section called “Examples of auto-discovered mappings for SQL Server environments”](#) on page 127.

The NetBackup client name of a host (or the primary name) is automatically mapped to its host ID during certificate deployment. For successful communication between NetBackup hosts, NetBackup also automatically maps all hosts to their other host names. However, that method is less secure. Instead, you can choose to disable this setting. Then choose to manually approve the individual host name mappings that NetBackup discovers.

See [“Disable automatic mapping of NetBackup host names”](#) on page 134.

Approve the host mappings that NetBackup discovers

NetBackup automatically discovers many shared names or cluster names that are associated with the NetBackup hosts in your environment. Use the **Mappings to approve** tab to review and accept the relevant host names. When **Automatically map host names to their NetBackup host ID** is enabled, the **Mappings to approve** list shows only the mappings that conflict with other hosts.

Note: You must map all available host names with the associated host ID. When you deploy a certificate to a host, the host name must map to the associated host ID. If it does not, NetBackup considers the host to be a different host. NetBackup then deploys a new certificate to the host and issues it a new host ID.

To approve the host names that NetBackup discovers

- 1 On the left, select **Security > Host mappings**.
- 2 Click the **Mappings to approve** tab.
- 3 Click the name of the host.

- 4 Review the mappings for the host and click **Approve** if you want to use the discovered mapping.

Click **Reject** if you do not want to associate the mapping with the host.

The rejected mappings do not appear in the list until NetBackup discovers them again.

- 5 Click **Save**.

Map other host names to a host

You can manually map the NetBackup host to its host names. This mapping ensures that NetBackup can successfully communicate with the host using the other name.

To map a host name to a host

- 1 On the left, select **Security > Host mappings**.
- 2 Select the host and click **Manage mappings**.
- 3 Click **Add**.
- 4 Enter the host name or IP address and click **Save**.
- 5 Click **Close**.

Map shared or cluster names to multiple NetBackup hosts

Add a shared or a cluster name mapping if multiple NetBackup hosts share a host name. For example, a cluster name.

Note the following before you create a shared or a cluster name mapping:

- NetBackup automatically discovers many shared names or cluster names. Review the **Mappings to approve** tab.
- If a mapping is shared between an insecure and a secure host, NetBackup assumes that the mapping name is secure. However, if at run-time the mapping resolves to an insecure host, the connection fails. For example, assume that you have a two-node cluster with a secure host (node 1) and an insecure host (node 2). In this case, the connection fails if node 2 is the active node.

To map shared or cluster names to multiple NetBackup hosts

- 1 On the left, select **Security > Host mappings**.
- 2 Click **Add shared or cluster mappings**.

- 3
- Enter a **Shared host name or cluster name** that you want to map to two or more NetBackup hosts.
- For example, enter a cluster name that is associated with NetBackup hosts in your environment.
- 4
- On the right, click **Add**.
- 5
- Select the NetBackup hosts that you want to add and click **Add to list**.
- For example, if you entered a cluster name in step 3 select the nodes in the cluster here.
- 6
- Click **Save**.

Examples of auto-discovered mappings for a cluster

For a cluster with hosts `client01.lab04.com` and `client02.lab04.com`, you may see the following entries. For each host, approve the mappings that are valid.

Host	Auto-discovered mapping
client01.lab04.com	client01
client01.lab04.com	clustername
client01.lab04.com	clustername.lab04.com
client02.lab04.com	client02
client02.lab04.com	clustername
client02.lab04.com	clustername.lab04.com

When you have approved all valid mappings, you see the **Mapped host or IP address** settings that are similar to the following entries.

Host	Mapped Host Names/IP Addresses
client01.lab04.com	client01.lab04.com, client01, clustername, clustername.lab04.com
client02.lab04.com	client02.lab04.com, client02, clustername, clustername.lab04.com

Example of auto-discovered mappings for a cluster in a multiple NIC environment

Backups of a cluster in a multi-NIC environment require special mappings. You must map the cluster node names to the virtual name of the cluster on the private network.

Table 14-1 Mapping host names for a cluster in a multi-NIC environment

Host	Mapped Host Names
Private name of <i>Node 1</i>	Virtual name of the cluster on the private network
Private name of <i>Node 2</i>	Virtual name of the cluster on the private network

For example, for a cluster in a multi-NIC environment with hosts `client01-bk.lab04.com` and `client02-bk.lab04.com`, you may see the following entries. For each host, approve the mappings that are valid.

Host	Auto-discovered Mapping
client01-bk.lab04.com	clustername-bk.lab04.com
client02-bk.lab04.com	clustername-bk.lab04.com

When you have approved all valid mappings, you see the **Mapped host or IP address** settings that are similar to the following entries.

Host	Mapped Host Names/IP Addresses
client01-bk.lab04.com	clustername-bk.lab04.com
client02-bk.lab04.com	clustername-bk.lab04.com

Examples of auto-discovered mappings for SQL Server environments

In [Table 14-2](#), FCI is a SQL Server failover cluster instance. WSFC is Windows Server Failover Cluster.

Table 14-2 Example mapped host names for SQL Server environments

Environment	Host	Mapped Host Names
FCI (cluster with two nodes)	Physical name of <i>Node 1</i>	Virtual name of the SQL Server cluster
	Physical name of <i>Node 2</i>	Virtual name of the SQL Server cluster

Table 14-2 Example mapped host names for SQL Server environments
(continued)

Environment	Host	Mapped Host Names
Basic or advanced availability group (primary and secondary)	Primary name	WSFC name
	Secondary name	WSFC name
Basic or advanced availability group, with an FCI (primary FCI and secondary FCI)	Primary FCI name	WSFC name
	Secondary FCI name	WSFC name
	Physical name of <i>Node 1</i>	Virtual name of the SQL Server cluster
	Physical name of <i>Node 2</i>	Virtual name of the SQL Server cluster

Remove mappings for a host that has multiple host names

You can remove any host name mappings that NetBackup added automatically. Or, any host name mappings that you added manually for a host. Note that if you remove a mapping, the host is no longer recognized with that mapped name. If you remove a shared or a cluster mapping, the host may not be able to communicate with other hosts that use that shared or cluster name.

If you have issues with a host and its mappings, you can reset the host attributes. However, that resets other attributes like a host’s communication status.

See [“Reset a host’s attributes”](#) on page 50.

To remove a host name that NetBackup discovers

- 1 On the left, select **Security > Host mappings**.
- 2 Locate the host that you want to update.
- 3 Click **Actions > Manage mappings**.
- 4 Locate the mapping you want to remove and click **Delete > Save**.

Managing user sessions

This chapter includes the following topics:

- [Sign out a NetBackup user session](#)
- [Unlock a NetBackup user](#)
- [Configure when idle sessions should time out](#)
- [Configure the maximum of concurrent user sessions](#)
- [Configure the maximum of failed sign-in attempts](#)
- [Display a banner to users when they sign in](#)

Sign out a NetBackup user session

For security or maintenance purposes, you can sign out one or more NetBackup user sessions. To configure NetBackup to automatically sign out any idle user sessions, see the following topic.

See [“Configure when idle sessions should time out”](#) on page 130.

Note: Changes to a user’s roles are not immediately reflected in the web UI. An administrator must terminate the active user session before any changes take effect. Or, the user must sign out and sign in again.

To sign out a user session

- 1 On the left, select **Security > User sessions**.
- 2 Click **Active sessions**.
- 3 Select the user session that you want to sign out.
- 4 Click **Terminate session**.

To sign out all user sessions

- 1 On the left, select **Security > User sessions**.
- 2 Click **Active sessions**.
- 3 Click **Terminate all sessions**.

Unlock a NetBackup user

You can view the user accounts that are currently locked out of NetBackup and unlock one or more users.

By default a user's account only remains locked for 24 hours. You can change this time by adjusting the **User sessions > User account settings > User account lockout** setting.

See [“Configure the maximum of failed sign-in attempts”](#) on page 131.

To unlock out a locked user account

- 1 On the left, select **Security > User sessions**.
- 2 Click **Locked users**.
- 3 Select the user account that you want to unlock.
- 4 Click **Unlock**.

To unlock all locked user accounts

- 1 On the left, select **Security > User sessions**.
- 2 Click **Locked users**.
- 3 Click **Unlock all users**.

Configure when idle sessions should time out

You can customize when user sessions should time out and a user is automatically signed out. The setting you choose is applied to the NetBackup Administration Console and the NetBackup web UI. To configure this setting from the command line, use `nbsetconfig` to set the `GUI_IDLE_TIMEOUT` option.

To configure when idle sessions should time out

- 1 Select **Security > User sessions**.
- 2 Click **User account settings**.

- 3 Turn on **Session idle timeout** and click **Edit**.
- 4 Select the number of minutes and click **Save**.

For active users, the updates are applied the next time the user signs in.

Configure the maximum of concurrent user sessions

This setting limits the number of concurrent API sessions that a user can have active. API sessions are used for some applications in the NetBackup Administration Console.

This setting does not apply to API key sessions or to other applications like the NetBackup Backup, Archive, and Restore interface.

To configure this setting from the command line, use `nbsetconfig` to set the `GUI_MAX_CONCURRENT_SESSIONS` option.

To configure the maximum of concurrent user sessions

- 1 Select **Security > User sessions**.
- 2 Click **User account settings**.
- 3 Turn on **Maximum concurrent sessions** and click **Edit**.
- 4 Select the **Number of concurrent sessions per user** and click **Save**.

If you have signed in to the NetBackup Administration Console using the **Single Sign-on, Certificates, or Smart Cards through the Web UI** option, the concurrent user sessions that you set here include the web UI and NetBackup Administration Console user sessions.

For active users, the updates are applied the next time the user signs in.

Configure the maximum of failed sign-in attempts

You can customize the maximum number of NetBackup failed sign-in attempts. The setting you choose applies only to the NetBackup web UI. To configure this setting from the command line, use `nbsetconfig` to set the `GUI_MAX_LOGIN_ATTEMPTS` and `GUI_ACCOUNT_LOCKOUT_DURATION` options.

To configure the maximum of failed sign-in attempts

- 1 Select **Security > User sessions**.
- 2 Click **User account settings**.
- 3 Turn on **User account lockout** and click **Edit**.

- 4 Select the number of failed sign-in attempts that you want to allow before an account is locked.
- 5 To unlock a locked account after a period of time, select the number of minutes for **Unlock locked accounts after**.
- 6 Click **Save**.

For active users, the updates are applied the next time the user signs in.

Display a banner to users when they sign in

You can configure a sign-in banner that displays each time that any user signs in to the NetBackup web UI. A different banner can be configured for any primary server. This banner can also require the user to agree to the terms of service before the user signs in.

To configure the banner for the NetBackup Administration Console and the Backup, Archive, and Restore client, see the [NetBackup Administrator's Guide, Volume I](#). To migrate the banner that is used for the NetBackup Administration Console to the NetBackup web UI, see the `nbmlb` command in the [NetBackup Commands Reference Guide](#).

To display a banner to users when they sign in

- 1 Select **Security > User sessions**.
- 2 Click **User account settings**.
- 3 Turn on **Sign-in banner configuration** and click **Edit**.
- 4 Enter the text you want to use for the heading and the body of the message.
- 5 If you want to require the user to agree to the terms of service, select **Include "Agree" and "Disagree" buttons on the sign-in banner**.
- 6 Click **Save**.

For active users, the updates are applied the next time the user signs in.

Managing the security settings for the primary server

This chapter includes the following topics:

- [Certificate authority for secure communication](#)
- [Disable communication with NetBackup 8.0 and earlier hosts](#)
- [Disable automatic mapping of NetBackup host names](#)
- [Configure the global data-in-transit encryption setting](#)
- [About NetBackup certificate deployment security levels](#)
- [Select a security level for NetBackup certificate deployment](#)
- [About TLS session resumption](#)
- [Set a passphrase for disaster recovery](#)
- [About trusted primary servers](#)

Certificate authority for secure communication

In the global security settings, the **Certificate authority** information indicates the type certificate authorities that the NetBackup domain supports. Open **Security > Global security** to view these settings.

NetBackup hosts in the domain can use certificates as follows:

- NetBackup certificates.

By default, NetBackup certificates are deployed on the primary server and its clients.

- **External certificates.**
You can configure NetBackup to only communicate with the hosts that use an external certificate. Requires that a host is upgraded to 8.2 or later and has an external certificate that is installed and enrolled. In this case, NetBackup does not communicate with any hosts that use NetBackup certificates. However, you can enable **Allow communication with NetBackup 8.0 and earlier hosts** to communicate with any hosts that use NetBackup 8.0 or earlier.
- **Both NetBackup certificates and external certificates.**
With this configuration, NetBackup communicates with the hosts that use a NetBackup certificate or an external certificate. If a host has both types of certificates, NetBackup uses the external certificate for communication.

Disable communication with NetBackup 8.0 and earlier hosts

By default, NetBackup allows communication with NetBackup 8.0 and earlier hosts that are present in the environment. However, this communication is insecure. For increased security, upgrade all your hosts to the current NetBackup version and disable this setting. This action ensures that only secure communication is possible between NetBackup hosts. If you use Auto Image Replication (A.I.R.), you must upgrade the trusted primary server for image replication to NetBackup 8.1 or later.

To disable communication with NetBackup 8.0 and earlier hosts

- 1 At the top right, select **Security > Global security**.
- 2 Turn off **Allow communication with NetBackup 8.0 and earlier hosts**.
- 3 Click **Save**.

Disable automatic mapping of NetBackup host names

For successful communication between NetBackup hosts, all relevant host names and IP addresses need to be mapped to the respective host IDs. Use the **Automatically map host names to their NetBackup host ID** option to automatically map the host ID to the respective host names (and IP addresses) or disable it to allow the NetBackup security administrator to manually verify the mappings before approving them.

To disable automatic mapping of NetBackup host names

- 1 At the top right, click the **Settings > Global security**.
- 2 Turn off **Automatically map host names to their NetBackup host ID**.
- 3 Click **Save**.

Configure the global data-in-transit encryption setting

To configure the data-in-transit encryption (DTE) in your NetBackup environment, you need to first set the global DTE configuration setting (or global DTE mode) and then the client DTE mode.

Data-in-transit encryption decision for various NetBackup operations is carried out based on the global DTE mode, the client DTE mode, and the image DTE mode.

The supported values for the global DTE mode are as follows:

- **Preferred Off** (default): Specifies that the data-in-transit encryption is disabled in the NetBackup domain. This setting can be overridden by the NetBackup client setting.
- **Preferred On**: Specifies that the data-in-transit encryption is enabled only for NetBackup 9.1 and later clients.
This setting can be overridden by the NetBackup client setting.
- **Enforced**: Specifies that the data-in-transit encryption is enforced if the NetBackup client setting is either 'Automatic' or 'On'. With this option selected, jobs fail for the NetBackup clients that have the data-in-transit encryption set to 'Off' and for the hosts earlier than 9.1.

Note: By default, the DTE mode for 9.1 clients is set to `Off` and for 10.0 and later clients, it is set to `Automatic`.

RESTful API to be used for the global DTE configuration:

- GET - `/security/properties`
- POST - `/security/properties`

To set or view the global DTE mode using the NetBackup web UI

- 1 At the top right, select **Security > Global security**.
- 2 On the **Secure communication** tab, select one of the following global DTE settings:

- Preferred Off
- Preferred On
- Enforced

About NetBackup certificate deployment security levels

Security levels for certificate deployment are specific to NetBackup CA-signed certificates. If the NetBackup web server is not configured to use NetBackup certificates for secure communication, the security levels cannot be accessed.

The NetBackup certificate deployment level determines the checks that are performed before the NetBackup CA issues a certificate to a NetBackup host. It also determines how frequently the NetBackup Certificate Revocation List (CRL) is refreshed on the host.

NetBackup certificates are deployed on hosts during installation (after the host administrator confirms the master server fingerprint) or with the `nbcertcmd` command. Choose a deployment level that corresponds to the security requirements of your NetBackup environment.

Table 16-1 Description of NetBackup certificate deployment security levels

Security level	Description	CRL refresh
Very High	An authorization token is required for every new NetBackup certificate request.	The CRL that is present on the host is refreshed every hour.

Table 16-1 Description of NetBackup certificate deployment security levels
(continued)

Security level	Description	CRL refresh
High (default)	<p>No authorization token is required if the host is known to the master server. A host is considered to be known to the master server if the host can be found in the following entities:</p> <ol style="list-style-type: none"> 1 The host is listed for any of the following options in the NetBackup configuration file (Windows registry or the <code>bp.conf</code> file on UNIX): <ul style="list-style-type: none"> ■ APP_PROXY_SERVER ■ DISK_CLIENT ■ ENTERPRISE_VAULT_REDIRECT_ALLOWED ■ MEDIA_SERVER ■ NDMP_CLIENT ■ SERVER ■ SPS_REDIRECT_ALLOWED ■ TRUSTED_MASTER ■ VM_PROXY_SERVER <p>For more details on the NetBackup configuration options, refer to the NetBackup Administrator's Guide, Volume I.</p> 2 The host is listed as a client name in the <code>altnames</code> file (ALTNAMEESDB_PATH). 3 The host appears in the EMM database of the master server. 4 At least one catalog image of the client exists. The image must not be older than 6 months. 5 The client is listed in at least one backup policy. 6 The client is a legacy client. This is a client that was added using the Client Attributes host properties. 	The CRL that is present on the host is refreshed every 4 hours.
Medium	The certificates are issued without an authorization token if the master server can resolve the host name to the IP address from which the request was originated.	The CRL that is present on the host is refreshed every 8 hours.

Select a security level for NetBackup certificate deployment

NetBackup offers several security levels for the NetBackup certificate deployment. The security level determines what security checks the NetBackup certificate authority (CA) performs before it issues a certificate to a NetBackup host. The level also determines how frequently the Certificate Revocation List (CRL) for the NetBackup CA is refreshed on the host.

More details are available for security levels, NetBackup certificate deployment, and the NetBackup CRL:

- See [“About NetBackup certificate deployment security levels”](#) on page 136.
- See the [NetBackup Security and Encryption Guide](#).

To select a security level for NetBackup certificate deployment

- 1 At the top, click **Settings > Global security**.
- 2 Click **Secure communication**.
- 3 For **Security level for NetBackup certificate deployment**, select a security level.

If you choose to use NetBackup certificates, they are deployed on hosts during installation, after the host’s administrator confirms the primary server fingerprint. The security level determines if an authorization token is required or not for a host.

Very high	NetBackup requires an authorization token for every new NetBackup certificate request.
High (Default)	NetBackup does not require an authorization token if the host is known to the primary server, which means the host appears in a NetBackup configuration file, the EMM database, a backup policy, or the host is a legacy client.
Medium	NetBackup issues NetBackup certificates without an authorization token if the primary server can resolve the host name to the IP address from which the request was originated.

- 4 Click **Save**.

About TLS session resumption

NetBackup uses TLS (Transport Layer Security) to secure communications between NetBackup hosts and is enabled by default. Each new TCP connection between NetBackup hosts must perform a TLS handshake and verify the peer identity before NetBackup sends traffic across that connection.

TLS session resumption is an open standards optimization that allows a TLS client and server to reuse a secure session that is generated during a previous connection. Reusing a secure session allows NetBackup to use a streamlined handshake instead of a full handshake. Performing this action reduces both the host CPU and time that is required to establish the new connection.

At TLS version 1.2 (used by current NetBackup versions), this version reduces forward security for the interval between full handshakes. To limit this window while still benefitting from session reuse, NetBackup allows global configuration of the maximum interval between full TLS handshakes.

To use the options for **TLS session resumption**, navigate to **Settings > Global security > Secure communication**. You can use the **Perform full handshake every** option to set the security level as follows:

- **Default for current security level** – If you use this option, NetBackup defaults to the security setting as follows:
 - Very high - 10 minutes
 - High - 30 minutes
 - Medium - 60 minutes
- **Custom (overrides the security level settings)** - The value of this interval can be configured at a minute granularity, within the range of 1 minute to 720 minutes.

Note: If strict forward security is a concern, NetBackup also allows session resumption to be globally disabled.

Note: This feature currently only applies to NBQA. ECA to be supported in a future release.

Set a passphrase for disaster recovery

During a catalog backup, NetBackup creates a disaster recovery package and encrypts the backup with a passphrase that you set. The constraints for the

passphrase can be changed with the NetBackup APIs or the CLIs (`nbseccmd -setpassphraseconstraints`).

See the information for disaster recovery settings in the [NetBackup Security and Encryption Guide](#).

To set a passphrase for disaster recovery

- 1 At the top, click **Settings > Global security**.
- 2 Click **Disaster recovery**.
- 3 Enter and confirm a passphrase.

Note: The passphrase should meet additional constraints that you may have set. You can check the additional constraints using the `nbseccmd` command or the passphrase-constraints web API.

- 4 Click **Save**.

About trusted primary servers

A trust relationship between NetBackup domains lets you do the following:

- Select specific domains as a target for replication. This type of Auto Image Replication is known as targeted A.I.R.
Without a trust relationship, NetBackup replicates to all defined target storage servers. A trust relationship is optional for Media Server Deduplication Pool and PureDisk Deduplication Pool as a target storage. To use a Cloud Catalyst storage server, a trust relationship is required.
- Include usage reporting for multiple primary servers.

Primary servers can use a NetBackup certificate authority (CA) certificate or an external CA certificate. NetBackup determines the CAs used by the source and the target domains and selects the appropriate CA to use for communication between the servers. If the target primary server is configured for both CA types, NetBackup prompts you to select the CA that you want to use. To establish trust with a remote primary server using the NetBackup CA, the current primary and the remote primary must have NetBackup version 8.1 or later. To establish trust with a remote primary server using an external CA, the current primary and the remote primary must have NetBackup version 8.2 or later.

Table 16-2 Determining the certificate authority (CA) to use for a trust relationship between servers

Source primary server CA or CAs	Target primary server CA or CAs	Certificate authority that is selected
NetBackup CA and external CA	External CA	External CA
	NetBackup CA	NetBackup CA
	External CA and NetBackup CA	NetBackup prompts you to select the CA.
NetBackup CA	External CA	No trust is established.
	NetBackup CA	NetBackup CA
	External CA and NetBackup CA	NetBackup CA

Add a trusted primary server

Note: The NetBackup web UI does not support adding a trusted primary that uses version 8.0 or earlier.

You can create a trust relationship between the primary servers that use the NetBackup CA or an external CA.

To add a trusted primary server

- 1 For the servers that use the NetBackup certificate authority (CA), first obtain an authorization token for each server and the fingerprint for each server.
- 2 At the top, select **Settings > Global security**.
- 3 Select **Trusted primary servers**.
- 4 Click the **Add** button.
- 5 Follow the prompts in the wizard.
- 6 Repeat these steps on the remote primary server.

More information

For more information on using an external CA with NetBackup, see the [NetBackup Security and Encryption Guide](#).

Remove a trusted primary server

Note: Any trusted primary servers at NetBackup version 8.0 or earlier must be removed using the NetBackup Administration Console.

You can remove a trusted primary server, which removes the trust relationship between primary servers. Note the following implications:

- Any replication operations fail that require the trust relationship.
- A remote primary server is not included in any usage reporting after you remove the trust relationship.

To remove a trusted primary server

- 1 Ensure that all replication jobs to the target primary server are complete.
- 2 Delete all storage lifecycle policies (SLPs) that use the trusted primary as a destination. Before deleting an SLP, ensure that there are no backup policies or protection plans that use the SLP for storage.
- 3 At the top, select **Settings > Global security**.
- 4 Select **Trusted primary servers**.
- 5 Select **Actions > Remove**.
- 6 Click **Remove trust**.
- 7 Repeat step 3 through step 6 on the remote primary server.

Using access keys, API keys, and access codes

This chapter includes the following topics:

- [Access keys](#)
- [API keys](#)
- [Access codes](#)

Access keys

NetBackup access keys provide access the NetBackup interfaces through API keys and access codes.

See [“API keys”](#) on page 143.

See [“Access codes”](#) on page 148.

API keys

A NetBackup API key is a pre-authenticated token that identifies a NetBackup user to NetBackup RESTful APIs. The user can use the API key in an API request header when a NetBackup API requires authentication. API keys can be created for authenticated NetBackup users (groups are not supported). A specific API key is only created one time and cannot be recreated. Each API key has a unique key value and API key tag. NetBackup audits operations that are performed with that key with the full identity of the user.

The following actions are available for administrators and API key users.

- Administrators with the applicable role or RBAC permissions can manage API keys for all users. These roles are the Administrator, the Default Security Administrator, or a role with RBAC permissions for API keys.
- An authenticated NetBackup user can add and manage their own API key in the NetBackup web UI. If a user does not have access to the web UI, they can use the NetBackup APIs to add or manage a key.

More information

See [“User identity in the audit report”](#) on page 107.

See the [NetBackup Security and Encryption Guide](#) for information on using API keys with the `bpnbat` command.

Add an API key or view API key details (Administrators)

The API key administrator can manage the keys that are associated with all NetBackup users.

Add an API key

Note: Only one API key can be associated with a specific user at a time. If a user requires a new API key, the user or administrator must delete the key for that user. An expired API key can be reissued.

To add an API key

- 1 On the left, select **Security > Access keys > API keys**.
- 2 On left, click **Add**.
- 3 Enter a **Username** for which you want to create the API key.
- 4 (Conditional) If the API key is for a SAML user, select **SAML authentication**.
A new API key for a SAML user remains inactive until the user signs into the web UI.
- 5 Indicate how long you want the API key to be valid, from today's date.
NetBackup calculates the expiration date and displays it.
- 6 Click **Add**.
- 7 To copy the API key, click **Copy and close**.

Store this key in a safe place. After you click **Copy and close**, the key cannot be retrieved again. If this API key replaces a previous key for your account, you must update any scripts, etc. to reflect the new API key.

View API key details

An API key administrator can view the API key details that are associated with all NetBackup users.

To view API key details

- 1 On the left, select **Security > Access keys > API keys**.
- 2 Locate the API key that you want to view.
- 3 Click **Actions > Edit** to edit the date or description for the key.

Edit, reissue, or delete an API key (Administrators)

As an API key administrator, you can edit API key details and reissue or delete API keys.

Edit the expiration date or description for an API key

Note: For SAML users, avoid selecting an expiration date for the API key that occurs after the SAML session expires. If the date occurs after the session expires, this action can introduce a security risk with that API key.

You can edit the description of an API key or change the expiration date of an active API key.

To edit the expiration date or description for an API key

- 1 On the left, select **Security > Access keys > API keys**.
- 2 Locate the API key that you want to edit.
- 3 Click the **Actions** menu. Then select **Edit**.
- 4 Note the current expiration date for the key and extend the date as wanted.
- 5 Make any wanted changes to the description.
- 6 Click **Save**.

Reissue an API key after it expires

Note: For SAML users, avoid selecting an expiration date for the API key that occurs after the SAML session expires. If the date occurs after the session expires, this action can introduce a security risk with that API key.

When an API key expires you can reissue the API key. This action creates a new API key for the user.

To reissue an API key

- 1 On the left, select **Security > Access keys > API keys**.
- 2 Locate the API key that you want to edit.
- 3 Click the **Actions** menu. Then select **Reissue > Reissue**.

Delete an API key

You can delete an API key to remove access for the user or when the key is no longer used. The key is permanently deleted, meaning that the associated user can no longer use that key for authentication.

To delete an API key

- 1 On the left, select **Security > Access keys > API keys**.
- 2 Locate the API key that you want to view.
- 3 Click the **Actions** menu. Then click **Delete > Delete**.

Add an API key or view your API key details

You can create an API key to authenticate your NetBackup user account when using NetBackup RESTful APIs.

Add an API key

As NetBackup web UI user you can use the web UI to add or view the details for your own API key.

To add an API key

- 1 If your API key has expired you can reissue the key.
See [the section called “Reissue your API key after it expires”](#) on page 147.
- 2 On the top right, click the profile icon and click **Add API key**.
- 3 (Non-SAML users) Indicate how long you want the API key to be valid, from today's date.
NetBackup calculates the expiration date and displays it.
- 4 (SAML users) After NetBackup validates the token from the SAML session, then the expiration date for the API key can be determined.

- 5 Click **Add**.
- 6 To copy the API key, click **Copy and close**.

Store this key in a safe place. After you click **Copy and close**, the key cannot be retrieved again. If this API key replaces a previous key for your account, you must update any scripts, etc. to reflect the new API key.

View your API key details

To view your API key details

- ◆ On the top right, click the profile icon and select **View my API key details**.

Edit, reissue, or delete your API key

You can manage your own API key from the NetBackup web UI.

Edit the expiration date or description for your API key (non-SAML users)

Non-SAML users can change the expiration date for an active API key. After an API key expires, you can reissue the key.

To edit your API key details

- 1 On the top right, click the profile icon and click **View my API key details**.
Note: If your API key is expired, you can click **Reissue** to reissue the key.
See [the section called “Reissue your API key after it expires”](#) on page 147.
- 2 Click **Edit**.
- 3 Note the current expiration date for the key and extend the date as wanted.
- 4 Make any wanted changes to the description.
- 5 Click **Save**.

Reissue your API key after it expires

When your API key expires you can reissue the API key. This action creates a new API key for you.

To reissue your API key

- 1 On the top right, click the profile icon and click **View my API key details**.
- 2 On the top right, click **Reissue**.

- 3 (Non-SAML users) Note the current expiration date for the key and extend the date as wanted.
- 4 Make any wanted changes to the description.
- 5 Click **Reissue**.

Delete your API key

You can delete an API key if you no longer have access to the key or no longer use it. When you delete an API key, that key is permanently deleted. You can no longer use that key for authentication or with the NetBackup APIs.

To delete your API key

- 1 On the top right, click the profile icon and click **View my API key details**.
- 2 On the top right, click **Delete**. Then click **Delete**.

Use an API key with NetBackup REST APIs

After a key is created, the user can pass the API key in the API request headers. For example:

```
curl -X GET https://primaryservername.domain.com/netbackup/admin/jobs/5 \
-H 'Accept: application/vnd.netbackup+json;version=3.0' \
-H 'Authorization: <API key value>'
```

Access codes

To run certain NetBackup administrator commands, for example `bperor`, you need to authenticate through the web UI. You need to generate an access code through the command-line interface, get the access request approved from the administrator, and then access the command.

With the web UI authentication for CLI access, NetBackup administrators can delegate the associated privileges to other users. By default, only a root administrator or an administrator can perform NetBackup operations through the command-line interface. The web UI authentication support allows non-root users to administer NetBackup who have CLI access that the Security Administrator has granted. You can also administer NetBackup with a non-RBAC user role (such as Operating System Administrator) even though you are not registered as a NetBackup user. Each time you need to generate a new access code to access CLIs.

Get CLI access through web UI authentication

To get CLI access

- 1 Run the following command:

```
bpnbat -login -logintype webui
```

An access code is generated.

- 2 (Optional) Run the following command if you want to get the code approved from your security administrator:

```
bpnbat -login -logintype webui -requestApproval
```

- 3 If you have the Command Line (CLI) Administrator role, you can use the web UI to approve the CLI access request using the access code.

See [“Approve your CLI access request”](#) on page 149.

If you do not have the Command Line (CLI) Administrator role, request the administrator to approve the CLI access request.

See [“Approve CLI access requests of other users”](#) on page 149.

- 4 Once the CLI access request is approved, go to the command-line interface and run the required command.

By default, the CLI access session is valid for 24 hours.

See [“Edit access settings”](#) on page 150.

Approve your CLI access request

You can approve your CLI access request using the web UI.

To approve your CLI access request

- 1 On the right, click your user profile icon.
- 2 Click **Approve Access Request**.
- 3 Enter the CLI access code that you have received from the user, who requires CLI access and click **Review**.
- 4 Review the access request details.
- 5 Click **Approve**.

Approve CLI access requests of other users

If you have the Command Line (CLI) Administrator role, you can approve access requests of other users using the web UI.

To approve CLI access request of other user

- 1 On the left, select **Security > Access keys > Access codes**.
- 2 Enter the CLI access code that you have received from the user, who requires CLI access and click **Review**.
- 3 Review the access request details.
- 4 Provide comments, if any.
- 5 Click **Approve**.

Edit access settings

To edit access settings

- 1 On the left, select **Security > Access keys**.
- 2 On the right, select **Access settings**.
- 3 Click **Edit**.
- 4 Enter the time in minutes or hours for which the CLI access session will be valid. 1 minute is a minimum value and 24 hours is a maximum value.

Configuring authentication options

This chapter includes the following topics:

- [Sign-in options for the NetBackup web UI](#)
- [Configure user authentication with smart cards or digital certificates](#)
- [About Single Sign-On \(SSO\) configuration](#)
- [Configure NetBackup for Single Sign-On \(SSO\)](#)
- [Troubleshooting SSO](#)

Sign-in options for the NetBackup web UI

NetBackup supports authentication of local domain users and Active Directory (AD) or LDAP domain users. AD and LDAP domains, smart card, and Single Sign-On (SSO with SAML) requires separate configuration for each primary server domain where you want to use the authentication method.

NetBackup supports the following types of user authentication:

- Username and password
- Digital certificate or smart card, including CAC and PIV
This authentication method only supports one AD or LDAP domain for each primary server domain and is not available for local domain users.
See [“Configure user authentication with smart cards or digital certificates”](#) on page 152.
- Single sign-on, with SAML
Note the following requirements and limitations.

- To use SSO, you must have a SAML 2.0 compliant identity provider configured in your environment.
- Only one AD or LDAP domain is supported for each primary server domain. This feature is not available for local domain users.
- Configuration of the IDP requires the NetBackup APIs or the NetBackup command `nbidpcmd`.
- API keys are used to authenticate a user or a group and cannot be used with SAML-authenticated users or groups.
- Global logout is not supported.

See [“Configure NetBackup for Single Sign-On \(SSO\)”](#) on page 158.

Configure user authentication with smart cards or digital certificates

You can map smart card or certificate with AD or LDAP domain for user validation. Alternatively, you can configure smart card or certificate user authentication without AD or LDAP domain.

See [“Configure smart card authentication with domain”](#) on page 152.

See [“Configure smart card authentication without domain”](#) on page 153.

Configure smart card authentication with domain

If you want to map smart cards or certificates with AD or LDAP domain for user validation, add the AD or the LDAP domains that are associated with your NetBackup users. See the [NetBackup Security & Encryption Guide](#).

Note: Ensure that you complete the role-based access control (RBAC) configuration for the NetBackup users before you configure smart card or certificate authentication.

See [“Configuring RBAC ”](#) on page 174.

To configure NetBackup to authenticate users with a smart card or digital certificate

- 1 At the top right, select **Settings > Smart card authentication**.
- 2 Turn on **Smart card authentication**.
- 3 Select the required AD or LDAP domain from the **Select the domain** option.

- 4** Select a **Certificate mapping attribute**: Common name (CN) or Universal principal name (UPN).
- 5** Optionally, enter the **OCSP URI**.
If you do not provide the OCSP URI, the URI in the user certificate is used.
- 6** Click **Save**.
- 7** To the right of **CA certificates**, click **Add**.
- 8** Browse for or drag and drop the **CA certificates** and click **Add**.

Smart card authentication requires a list of trusted root or intermediate CA certificates. Add the CA certificates that are associated with the user digital certificates or the user smart cards.

Certificate file types must be .crt, .cer, .der, .pem, or PKCS #7 format and less than 64KB in size.
- 9** On the **Smart card authentication** page, verify the configuration information.
- 10** Before users can use a digital certificate that is not installed on a smart card, the certificate must be uploaded to the browser's certificate manager.

See the browser documentation for instructions or contact your certificate administrator for more information.
- 11** When users sign in, they now see an option to **Sign in with certificate or smart card**.

If you do not want users to have this sign-in option yet, turn off **Smart card authentication**. (For example, if all users do not yet have their certificates configured on their hosts.). The settings that you configured are retained even if you turn off smart card authentication.

For such users, the domain name and domain type are smart card.

Configure smart card authentication without domain

You can configure smart card or certificate user authentication without validating the users with AD or LDAP domain.

Only users are supported when there is no AD or LDAP domain is used for user validation. User groups are not supported.

To configure NetBackup to authenticate users with a smart card or digital certificate without domain

- 1** At the top right, select **Settings > Smart card authentication**.
- 2** Turn on **Smart card authentication**.

- 3 (Conditional step) If AD or LDAP domain is configured in your environment, select **Continue without the domain** option.
- 4 Select a **Certificate mapping attribute**: Common name (CN) or Universal principal name (UPN).
- 5 Optionally, enter the **OCSP URI**.
If you do not provide the OCSP URI, the URI in the user certificate is used.
- 6 Click **Save**.
- 7 To the right of **CA certificates**, click **Add**.
- 8 Browse for or drag and drop the **CA certificates** and click **Add**.
- 9 Smart card authentication requires a list of trusted root or intermediate CA certificates. Add the CA certificates that are associated with the user digital certificates or the user smart cards.

Certificate file types must be .crt, .cer, .der, .pem, or PKCS #7 format and less than 64KB in size.
- 10 On the **Smart card authentication** page, verify the configuration information.

Before users can use a digital certificate that is not installed on a smart card, the certificate must be uploaded to the browser's certificate manager.

See the browser documentation for instructions or contact your certificate administrator for more information.

<https://iase.disa.mil/pki-pke/Pages/web-browsers.aspx>
- 11 When users sign in, they now see an option to **Sign in with certificate or smart card**.

If you do not want users to have this sign-in option yet, turn off **Smart card authentication**. (For example, if all users do not yet have their certificates configured on their hosts.). The settings that you configured are retained even if you turn off smart card authentication.

Edit the configuration for smart card authentication

If the configuration changes for smart card authentication, you can edit the configuration details.

To edit user authentication configuration with domain

- 1 At the top right, select **Settings > Smart card authentication**.
- 2 You may want to edit the AD or LDAP domain selection in the following cases:
 - To select a domain that is different than the existing one

- The existing domain is deleted and you want to select a new domain
- You want to continue without the domain

Click **Edit**.

3 Select a domain.

Only the domains that are configured for NetBackup display in this list.

If you do not want to validate the users with domain, you can select **Continue without the domain**.

4 Edit the **Certificate mapping attribute**.

5 Leave the **OCSP URI** field empty if you want to use the **URI** value from the user certificate. Or, provide the URI that you want to use.

Add or delete a CA certificate that is used for smart card authentication

Add a CA certificate

Smart card authentication requires a list of trusted root or intermediate CA certificates. Add the CA certificates that are associated with the user digital certificates or the user smart cards.

To add a CA certificate

- 1** At the top right, select **Settings > Smart card authentication**.
- 2** Click **Add**.
- 3** Browse for or drag and drop the **CA certificates**. Then click **Add**.

Smart card authentication requires a list of trusted root or intermediate CA certificates. Add the CA certificates that are associated with the user digital certificates or the user smart cards.

Certificate file types must be in DER, PEM, or PKCS #7 format and no more than 1 MB in size.

Delete a CA certificate

You can delete a CA certificate if it is no longer used for smart card authentication. Note that if a user attempts to use the associated digital certificate or smart card certificate, they are not able to sign in to NetBackup.

To delete a CA certificate

- 1 At the top right, select **Settings > Smart card authentication**.
- 2 Select the CA certificates that you want to delete.
- 3 Click **Delete > Delete**.

Disable or temporarily disable smart card authentication

You can disable smart card authentication if you no longer want to use that authentication method for the primary server. Or, if you need to complete other configuration before users can use smart cards.

To disable smart card authentication

- 1 At the top right, select **Settings > Smart card authentication**.
- 2 Turn off **Smart card authentication**.

The settings that you configured are retained even if you turn off smart card authentication.

About Single Sign-On (SSO) configuration

You can configure Single Sign-On (SSO) with any identity provider (IDP) that uses the SAML 2.0 protocol for exchanging authentication and authorization information. Note that you can configure an IDP with more than one Veritas product. For example, the same IDP can be configured with NetBackup and with APTARE.

Note the following requirements and limitations:

- To use SSO, you must have a SAML 2.0 compliant identity provider configured in your environment.
- Only identity providers that use AD or LDAP directory services are supported.
- Configuration of the IDP requires the NetBackup APIs or the NetBackup command `nbidpcmd`.
- SAML users cannot use the APIs. API keys are used to authenticate a user and therefore cannot be used with a SAML-authenticated user.
- Global logout is not supported.

Figure 18-1 Example NAT configuration: Identity provider in a private network

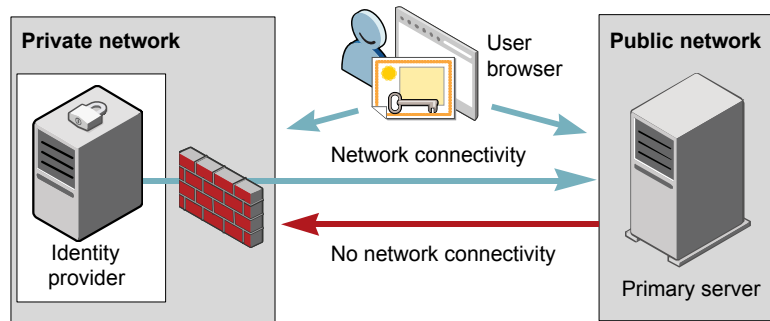


Figure 18-2 Example NAT configuration: Primary server in a private network

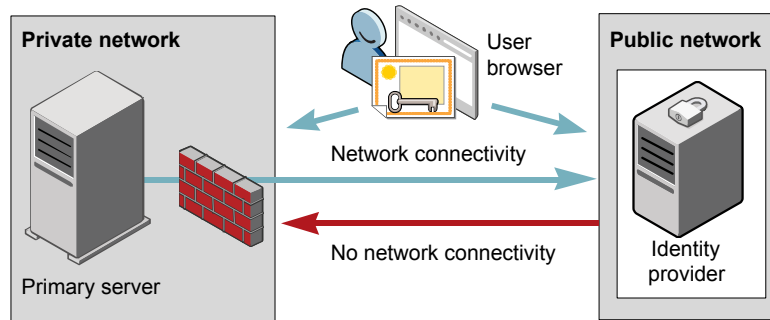


Figure 18-3 Example configuration: Primary server and identity provider in same network

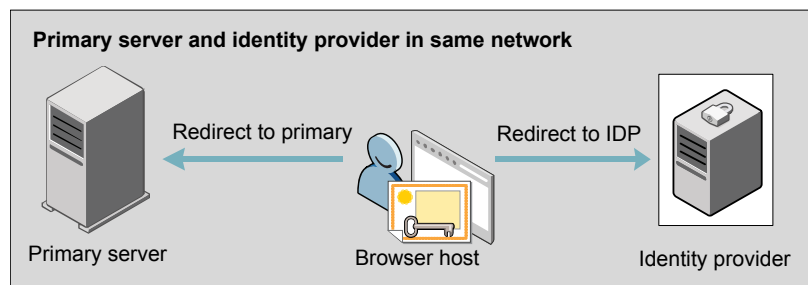
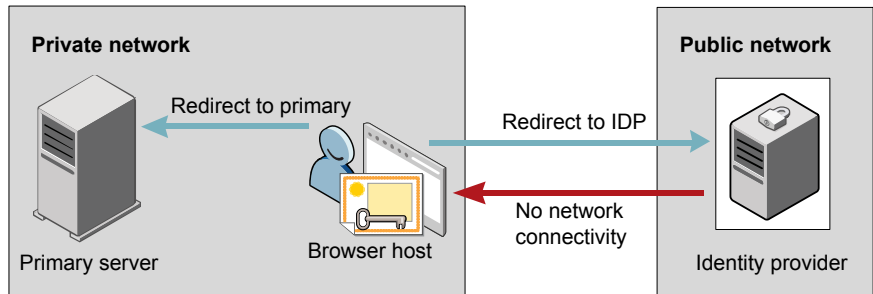


Figure 18-4 Example configuration: Primary server in private network and identity provider in public network



Configure NetBackup for Single Sign-On (SSO)

This section provides steps to set up trust and exchange configuration information between the IDP and the NetBackup primary server. Before proceeding with the steps, ensure that the following prerequisites are met in your environment:

- An IDP is set up and deployed in your environment.
- The IDP is configured to authenticate domain users of Active Directory (AD) or Lightweight Directory Access Protocol (LDAP).

Table 18-1 Steps to configure NetBackup for Single Sign-On

Step	Action	Description
1.	Download the IDP metadata XML file	<p>Download and save the IDP metadata XML file from the IDP.</p> <p>SAML metadata that is stored in XML files is used to share configuration information between the IDP and the NetBackup primary server. The IDP metadata XML file is used to add the IDP configuration to the NetBackup primary server.</p>
2.	Configure the SAML keystore, and add and enable the IDP configuration on the NetBackup primary server	<p>See “Configure the SAML KeyStore” on page 159.</p> <p>See “Configure the SAML keystore and add and enable the IDP configuration” on page 162.</p>

Table 18-1 Steps to configure NetBackup for Single Sign-On (*continued*)

Step	Action	Description
3.	Download the service provider (SP) metadata XML file	<p>The NetBackup primary server is the SP in the NetBackup environment. You can access the SP metadata XML file from the NetBackup primary server by entering the following URL in your browser:</p> <p><code>https://masterserver/netbackup/sso/saml2/metadata</code></p> <p>Where <i>masterserver</i> is the IP address or host name of the NetBackup primary server.</p>
4.	Enroll the NetBackup primary server as a service provider (SP) with the IDP	See “Enroll the NetBackup primary server with the IDP” on page 164.
5.	Add SAML users and the SAML groups that use SSO to the necessary RBAC roles	<p>SAML users and SAML user groups are available in RBAC only if the IDP is configured and enabled on the NetBackup primary server. For steps on adding RBAC roles, see the following topic.</p> <p>See “Add a user to a role (non-SAML)” on page 175.</p>

After the initial setup, you can choose to enable, update, disable, or delete the IDP configuration.

See [“Manage an IDP configuration”](#) on page 165.

After the initial setup, you can choose to update, renew, or delete the NetBackup CA SAML keystore. You can also configure and manage the ECA SAML keystore.

Configure the SAML KeyStore

To establish a trust between the NetBackup primary server and the IDP server, you must configure an SAML KeyStore on the NetBackup primary server. Depending on whether you are using the NetBackup CA or an external certificate authority (ECA), refer to either of the following sections:

Note: If you are using a combination of an ECA and NetBackup CA in your environment, by default, the ECA is considered while establishing trust with the IDP server.

Note: The SAML KeyStore configuration using batch files, such as `configureCerts.bat`, `configureCerts`, `configureSAMLECACert.bat`, `configureSAMLECACert` and their corresponding options is deprecated.

Configure a NetBackup CA KeyStore

If you are using the NetBackup CA, create the NetBackup CA KeyStore on the NetBackup primary server.

To create a NetBackup CA KeyStore

- 1 Log on to the NetBackup primary server as root or administrator.
- 2 Run the following command:

```
nbidpcmd -cCert -M master_server -f
```

`-f` is optional. Use the option for the forceful update.

Once the NetBackup CA KeyStore is created, ensure that you update the NetBackup CA KeyStore every time the NetBackup CA certificate is renewed.

To renew the NetBackup CA KeyStore

- 1 Log on to the NetBackup primary server as root or administrator.
- 2 Run the following command:

```
nbidpcmd -rCert -M master_server
```

- 3 Download the new SP metadata XML file from the NetBackup primary server by entering the following URL in your browser:

`https://primaryserver/netbackup/sso/saml2/metadata`

Where *primaryserver* is the IP address or host name of the NetBackup primary server.

- 4 Upload the new SP metadata XML file to the IDP.

See [“Enroll the NetBackup primary server with the IDP”](#) on page 164.

To remove the NetBackup CA KeyStore

- 1 Log on to the NetBackup primary server as root or administrator.
- 2 Run the following command

```
nbidpcmd -dCert -M master_server
```


- 3 Download the new SP metadata XML file from the NetBackup primary server by entering the following URL in your browser:

`https://primaryserver/netbackup/sso/saml2/metadata`

Where *primaryserver* is the IP address or host name of the NetBackup primary server.

- 4 Upload the new SP metadata XML file to the IDP.
- 5 See [“Enroll the NetBackup primary server with the IDP”](#) on page 164.

Configure an ECA KeyStore

If you are using an ECA, import the ECA KeyStore to the NetBackup primary server.

Note: If you are using a combination of an ECA and the NetBackup CA in your environment, by default, the ECA is considered while establishing trust with the IDP server. To use the NetBackup CA, you must first remove the ECA KeyStore.

To configure an ECA KeyStore

- 1 Log on to the primary server as root or administrator.
- 2 Depending on whether you want to configure SAML ECA keystore using the configured NetBackup ECA KeyStore or you want to provide the ECA certificate chain and private key, run the following commands:
 - Run the following command to use NetBackup ECA configured KeyStore:
`nbidpcmd -cECACert -uECA existing ECA configuration [-f] [-M primary_server]`
 - Run the following command to use ECA certificate chain and private key provided by the user:
`nbidpcmd -cECACert -certPEM certificate chain file -privKeyPath private key file [-ksPassPath Keystore Passkey File] [-f] [-M <master_server>]`
 - Certificate chain file specifies the certificate chain file path. The file must be in PEM format and must be accessible to the primary server on which the configuration is being performed.
 - Private key file specifies the private key file path. The file must be in PEM format and must be accessible to the primary server on which the configuration is being performed.
 - KeyStore passkey file specifies the KeyStore password file path and must be accessible to the primary server on which the configuration is being performed.

- Primary server is the host name or IP address of primary server on which you want to perform SAML ECA KeyStore configuration. The NetBackup primary server where you run the command is selected by default.

To remove the ECA KeyStore

- 1 Log on to the primary server as root or administrator.
- 2 Download the new SP metadata XML file from the NetBackup primary server by entering the following URL in your browser:

`https://primaryserver/netbackup/sso/saml2/metadata`

Where *primaryserver* is the IP address or host name of the NetBackup primary server.

- 3 Upload the new SP metadata XML file to the IDP.

See [“Enroll the NetBackup primary server with the IDP”](#) on page 164.

Configure the SAML keystore and add and enable the IDP configuration

Before proceeding with the following steps, ensure that you have downloaded the IDP metadata XML file and saved it on the NetBackup primary server.

To configure SAML keystore and add and enable an IDP configuration

- 1 Log on to the primary server as root or administrator.
- 2 Run the following command.

For IDP and NetBackup CA SAML KeyStore configuration:

```
nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata file
[-t SAML2] [-e true | false] [-u IDP user field] [-g IDP user
group field] [-cCert] [-f] [-M primary server]
```

Alternatively for IDP and ECA SAML KeyStore configuration:

Depending on whether you want to configure SAML ECA KeyStore using the configured NetBackup ECA KeyStore or you want to provide the ECA certificate chain and private key, run the following commands:

- Use NetBackup ECA configured keystore:

```
nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata
file[-t SAML2] [-e true | false] [-u IDP user field] [-g IDP
user group field] -cEACert -uECA existing ECA configuration
[-f] [-M Primary Server]
```

- Use ECA certificate chain and private key provided by the user:

```
nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata file [-t SAML2] [-e true | false] [-u IDP user field] [-g IDP user group field] -cEACert -certPEM certificate chain file -privKeyPath private key file [-ksPassPath KeyStore passkey file] [-f] [-M primary server]
```

Replace the variables as described below:

- *IDP configuration name* is a unique name provided to the IDP configuration.
- *IDP XML metadata file* is the path to the XML metadata file, which contains the configuration details of the IDP in Base64URL-encoded format.
- *-e true | false* enables or disables the IDP configuration. An IDP configuration must be added and enabled, otherwise users cannot sign in with the Single Sign-On (SSO) option. Even though you can add multiple IDP configurations on a NetBackup primary server, only one IDP configuration can be enabled at a time.
- *IDP user field* and *IDP user group field* are the SAML attribute names, which are mapped to the `userPrincipalName` and the `memberOf` attributes of the AD or LDAP.

Note: Ensure that the SAML attribute names are defined in the format of ***username@domainname*** and ***(CN=group name, DC=domainname)*** respectively.

- *primary Server* is the host name or IP address of primary server to which you want to add or modify the IDP configuration. The NetBackup primary server where you run the command is selected by default.
- *Certificate Chain File* is the certificate chain file path. The file must be in PEM format and must be accessible to the primary server on which the configuration is being performed.
Private Key File is the private key file path. The file must be in PEM format and must be accessible to the primary server on which the configuration is being performed.
KeyStore Passkey File is the KeyStore passkey file path and must be accessible to the primary server on which the configuration is being performed.

Fore example: `nbidpcmd -ac -n veritas_configuration -mxp file.xml -t SAML2 -e true -u username -g group-name -cCert -M primary_server.abc.com`

Enroll the NetBackup primary server with the IDP

The NetBackup primary server must be enrolled with the IDP as a service provider (SP). For step-by-step procedures that are specific to a particular IDP, see the following table:

Table 18-2 IDP-specific steps for enrolling the NetBackup primary server

IDP name	Link to steps
ADFS	https://www.veritas.com/docs/100047744
Okta	https://www.veritas.com/docs/100047745
PingFederate	https://www.veritas.com/docs/100047746
Azure	https://www.veritas.com/docs/100047748
Shibboleth	https://www.veritas.com/docs/00047747

Enrolling an SP with an IDP typically involves the following operations:

Uploading the SP metadata XML file to the IDP

The SP metadata XML file contains the SP certificate, the entity ID, the Assertion Consumer Service URL (ACS URL), and a log out URL (SingleLogoutService). The SP metadata XML file is required by the IDP to establish trust, and exchange authentication and authorization information with the SP.

Mapping the SAML attributes to their AD or LDAP attributes

Attribute mappings are used to map SAML attributes in the SSO with its corresponding attributes in the AD or LDAP directory. The SAML attribute mappings are used for generating SAML responses, which are sent to the NetBackup primary server. Ensure that you define SAML attributes that map to the `userPrincipalName` and the `memberOf` attributes in the AD or LDAP directory. The SAML attributes must adhere to the following formats:

Table 18-3

Corresponding AD or LDAP attribute	SAML attribute format
<code>userPrincipalName</code>	<code>username@domainname</code>
<code>memberOf</code>	<code>(CN=group name, DC=domainname)</code>

Note: While adding the IDP configuration to the NetBackup primary server, the values entered for the user (-u) and user group (-g) options must match the SAML attribute names that are mapped to the `userPrincipalName` and the `memberOf` attributes in the AD or LDAP.

See [“Configure the SAML keystore and add and enable the IDP configuration”](#) on page 162.

Manage an IDP configuration

You can manage the identity provider (IDP) configurations on the NetBackup primary server by using the enable (-e true), update (-uc), disable (-e false), and delete (-dc) options of the `nbidpcmd` command.

Enable an IDP configuration

By default, an IDP configuration is not enabled in the product environment. If you did not enable the IDP when you added it, you can use the `-uc -e true` options to update and enable the IDP configuration.

To enable an IDP configuration

- 1 Log on to the primary server as root or administrator.
- 2 Run the following command:

```
nbidpcmd -uc -n IDP configuration name -e true
```

Where *IDP configuration name* is a unique name provided to the IDP configuration.

Note: Even though you can configure multiple IDPs on a NetBackup primary server, only one IDP can be enabled at a time.

Update an IDP configuration

You can update the XML metadata file associated with an IDP configuration.

To update the IDP XML metadata file in an IDP configuration

- 1 Log on to the primary server as root or administrator.
- 2 Run the following command:

```
nbidpcmd -uc -n IDP configuration name -mxp IDP XML metadata file
```

Replace the variables as described below:

- *IDP configuration name* is a unique name provided to the IDP configuration.

- *IDP XML metadata file* is the path to the XML metadata file, which contains the configuration details of the IDP in Base64URL-encoded format.

If you want to update the IDP user or IDP user group values in an IDP configuration, you must first delete the configuration. The Single Sign-On (SSO) option is not available for users until you re-add the configuration with the updated IDP user or IDP user group values.

To update IDP user or IDP user group in an IDP configuration

- 1 Log on to the primary server as root or administrator.
- 2 Delete the IDP configuration.

```
nbidpcmd -dc -n IDP configuration name
```

Where *IDP configuration name* is a unique name provided to the IDP configuration.

- 3 To add and enable the configuration again, run the following command:

```
nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata file
[-t SAML2] [-e true | false] [-u IDP user] [-g IDP user group
field] [-M Master Server]
```

Replace the variables as described below:

- *IDP configuration name* is a unique name provided to the IDP configuration.
- *IDP XML metadata file* is the path to the XML metadata file, which contains the configuration details of the IDP in Base64URL-encoded format.
- *-e true | false* enables or disables the IDP configuration. An IDP must be available and enabled otherwise users cannot sign in with the Single Sign-On (SSO) option. Even though you can add multiple IDP configurations on a NetBackup primary server, only one IDP configuration can be enabled at a time.
- *IDP user field* and *IDP user group field* are the SAML attribute names, which are mapped to the `userPrincipalName` and the `memberOf` attributes in the AD or LDAP.

Note: Ensure that the SAML attribute names are defined in the format of ***username@domainname*** and ***(CN=group name, DC=domainname)*** respectively.

- *Master Server* is the host name or IP address of the primary server to which you want to add or modify the IDP configuration. The NetBackup primary server where you run the command is selected by default.

Disable an IDP configuration

If an IDP configuration is disabled in the product environment, the Single Sign-On (SSO) option of that IDP is not available for users when they sign in.

To disable an IDP configuration

- 1 Log on to the primary server as root or administrator.
- 2 Run the following command:

```
nbidpcmd -uc -n IDP configuration name -e false
```

Where *IDP configuration name* is a unique name provided to the IDP configuration.

Delete an IDP configuration

If an IDP configuration is deleted, the Single Sign-On (SSO) option of that IDP is not available for users when they sign in.

To delete an IDP configuration

- 1 Log on to the primary server as root or administrator.
- 2 Run the following command:

```
nbidpcmd -dc -n IDP configuration name
```

Where *IDP configuration name* is a unique name provided to the IDP configuration.

Video: Configure Single Sign-On in NetBackup

In this video, you will see an overview of how to configure Single Sign-On (SSO) in NetBackup.

[Video link](#)

Depending on which IDP you are using, see the following articles for steps on downloading the IDP metadata XML file and enrolling the NetBackup primary server with the IDP:

- ADFS: <https://www.veritas.com/docs/100047744>
- Okta: <https://www.veritas.com/docs/100047745>
- PingFederate: <https://www.veritas.com/docs/100047746>

- Azure: <https://www.veritas.com/docs/100047748>
- Shibboleth: <https://www.veritas.com/docs/100047747>

For more information about SSO in NetBackup, see the *NetBackup Web UI Administrator's Guide*.

Troubleshooting SSO

This section provides steps for troubleshooting issues related to SSO.

Redirection issues

If you are facing issues with redirection, check the error messages in web services log files to narrow down the cause of the issue. NetBackup creates logs for the NetBackup web server and for the web server applications. These logs are written to the following location:

- UNIX: `/usr/openv/logs/nbweb service`
- Windows: `install_path\NetBackup\logs\nbweb service`

NetBackup web UI does not redirect to the IDP sign in page

The IDP metadata XML file contains the IDP certificate, the entity ID, the redirect URL, and the logout URL. The NetBackup web UI can fail to redirect to the IDP sign in page, if the IDP XML metadata file is outdated or corrupted. The following message is added to the web service log:

```
Failed to redirect to the IDP server.
```

To ensure that the latest configuration details are available to the NetBackup primary server, download the latest copy of the XML metadata file from the IDP. Use the IDP XML metadata file to add and enable the latest IDP configuration on the NetBackup primary server. See [“Configure the SAML keystore and add and enable the IDP configuration”](#) on page 162.

IDP sign in page does not redirect to the NetBackup web UI

When you enter your credentials in the IDP sign in page, your browser might display an **Authentication failed** error, instead of redirecting to the NetBackup web UI. Refer to the following table for resolution steps based on the error found in the web service log.

Table 18-4

Web Service log error message	Explanation and recommended action
<code>userPrincipalName not found in response.</code>	While adding the IDP configuration to the NetBackup primary server, the value entered for the user (-u) option must match the SAML attribute name, which is mapped to the <code>userPrincipalName</code> attribute in AD or LDAP. For more information, See “Configure the SAML keystore and add and enable the IDP configuration” on page 162.
<code>userPrincipalName is not in expected format</code>	The IDP sends SAML responses to the NetBackup primary server, which contains SAML user and SAML user group information. To enable the IDP to successfully send this information, ensure the value of <code>userPrincipalName</code> attribute sent by the IDP is defined in the format of <i>username@domainname</i> . For more information, See “Enroll the NetBackup primary server with the IDP” on page 164.
<code>Authentication issue instant is too old or in the future</code>	This error can occur because of the following reasons: <ul style="list-style-type: none"> ■ The date and time of IDP server and the NetBackup primary server is not synchronized. ■ By default, the NetBackup primary server allows a user to remain authenticated for a period of 24 hours. You might encounter this error, If an IDP allows a user to remain authenticated for a period longer than 24 hours. To resolve this error, you can update the SAML authentication lifetime of the NetBackup primary server to match that of the IDP. Specify the new SAML authentication lifetime in the <code><installpath>\var\global\wsl\config\web.conf</code> file on the NetBackup primary server. For example, If your IDP has an authentication lifetime as 36 hours, update the entry in the <code>web.conf</code> file as follows: <code>SAML_ASSERTION_LIFETIME_IN_SECS=129600</code>
<code>Response is not success</code>	This error can occur because of the following reasons: <ul style="list-style-type: none"> ■ The IDP metadata XML file contains an IDP certificate. If you are using a NetBackup CA, ensure that the IDP certificate is updated with latest NetBackup CA certificate information. For more information, See “Configure the SAML KeyStore” on page 159. ■ The Certificate Revocation List (CRL) must be disabled in the IDP if you are using a NetBackup CA keystore.

Unable to sign in due to authorization-related issues

To sign in with SSO, you must add SAML users and the SAML user groups to the necessary RBAC roles. If the RBAC roles are not correctly assigned, you might encounter the following error while signing into NetBackup web UI.

You are not authorized to access this application. Contact your NetBackup security administrator to request RBAC permissions for the NetBackup web user interface.

Refer to the table below to troubleshoot authorization-related issues:

Table 18-5

Cause	Explanation and recommended action
RBAC roles are not assigned to the SAML users and the SAML groups.	<p>After an IDP configuration is added and enabled on the NetBackup primary server, ensure that necessary RBAC roles are assigned to SAML users and SAML user groups that use SSO. Note that SAML users and SAML user groups are available in RBAC only after the IDP configuration is added and enabled on the NetBackup primary server.</p> <p>For steps on adding users, See “Add a user to a role (non-SAML)” on page 175.</p>
RBAC roles are assigned to SAML users and SAML user groups associated with an IDP configuration that is not currently added and enabled.	<p>When you add a SAML users or SAML user group in RBAC, the SAML user or SAML user group entry is associated with the IDP configuration that is added and enabled at that time.</p> <p>If you add and enable a new IDP configuration, ensure that you also add another entry for the SAML user or SAML user group. The new entry is associated with the new IDP configuration.</p> <p>For example, NBU_user is added to RBAC and assigned the necessary permissions, while an ADFS IDP configuration is added and enabled. If you add and enable an Okta IDP configuration, you must add a new user entry for NBU_user. Assign the necessary RBAC roles to the new user entry, which is associated with the Okta IDP configuration.</p> <p>For steps on adding users, See “Add a user to a role (non-SAML)” on page 175.</p>

Table 18-5 (continued)

Cause	Explanation and recommended action
RBAC roles are assigned to local domain users or Active Directory (AD) or LDAP domain users (instead of SAML users and SAML user groups).	<p>SAML user or SAML user group records might appear similar to corresponding local domain users or AD or LDAP domain users already added in the RBAC.</p> <p>After an IDP configuration is added and enabled on the NetBackup primary server, ensure that you add SAML users and SAML user groups in RBAC and assign the necessary permissions. Note that SAML users and SAML user groups are available in RBAC only after the IDP configuration is added and enabled on the NetBackup primary server.</p> <p>For steps on adding SAML users and user groups, See “Add a user to a role (non-SAML)” on page 175.</p>
The NetBackup primary server is unable to retrieve user group information from the IDP	<p>The IDP sends SAML responses to the NetBackup primary server, which contains SAML user and SAML user group information. To enable the IDP to successfully send this information, ensure the following:</p> <ul style="list-style-type: none">■ The IDP is configured to authenticate domain users from AD or LDAP.■ The value of <code>memberOf</code> attribute sent by the IDP is in the X.500 distinguished format, that is, {cn=groupname,dc=domain}.■ While adding the IDP configuration to the NetBackup primary server, the values entered for the user group (-g) option matches the SAML attribute name, which is mapped to the <code>memberOf</code> attribute in AD or LDAP. For more information, See “Configure the SAML keystore and add and enable the IDP configuration” on page 162.

Managing role-based access control

This chapter includes the following topics:

- [RBAC features](#)
- [Authorized users](#)
- [Configuring RBAC](#)
- [Default RBAC roles](#)
- [Add a custom RBAC role](#)
- [Role permissions](#)
- [Manage access permission](#)
- [View access definitions](#)

RBAC features

The NetBackup web user interface provides the ability to apply role-based access control in your NetBackup environment. Use RBAC to provide access for the users that do not currently have access to NetBackup. Or, for current NetBackup users with administrator access you can provide limited access and permissions, based on their role in your organization.

For information on access control methods for the NetBackup Administration Console and access control and auditing information for root users and administrators, refer to the [NetBackup Security and Encryption Guide](#).

Table 19-1 RBAC features

Feature	Description
Roles allow users to perform specific tasks	Add users to one or more default RBAC roles or create custom roles to fit the role of your users. Add a user to the Administrator role to give full NetBackup permissions to that user. See “ Default RBAC roles ” on page 179.
Users can access NetBackup areas and the features that fit their role	RBAC users can perform common tasks for their business role, but are restricted from accessing other NetBackup areas and features. RBAC also controls the assets that users can view or manage.
Auditing of RBAC events	NetBackup audits RBAC events.
DR ready	RBAC settings are protected with the NetBackup catalog.
Enhanced Auditing or authorization (<code>auth.conf</code>) configurations still available for older interfaces	Enhanced Auditing is supported across all interfaces. You can continue to use the authorization (<code>auth.conf</code>) configurations with the NetBackup Administration Console and the CLIs. With these older interfaces you can manage access to workflows that are not yet supported in the NetBackup web UI and NetBackup APIs. Note that the <code>auth.conf</code> file does not restrict access to the NetBackup web UI or the NetBackup APIs.

Authorized users

The following users are authorized to sign in to and use the NetBackup web UI.

Table 19-2 Users that are authorized to use the NetBackup web UI

User	Access	Notes
Root OS administrators Enhanced Auditing users Users with the RBAC Administrator role	Full	You can disable automatic access for OS administrators. See “ Disable web UI access for operating system (OS) administrators ” on page 178. For details on Enhanced Auditing, see the NetBackup Security and Encryption Guide .
nbasecadm Appliance user appadmin Flex Appliance user	Default Security Administrator role	This role can grant access to other appliance users. The default admin user for the NetBackup appliance does not have access to the web UI.
Users that have an RBAC role that gives access to the web UI	Varies	See “ Configuring RBAC ” on page 174.

Configuring RBAC

To configure role-based access control for the NetBackup web UI, perform the following steps.

Table 19-3 Steps to configure role-based access control

Step	Action	Description
1	Configure any Active Directory or LDAP domains.	Before you can add domain users, Active Directory or LDAP domains must be authenticated with NetBackup. See the NetBackup Security & Encryption Guide .
2	Determine the permissions that your users need.	Determine the permissions that your users need to perform their daily tasks. You can use the default RBAC roles or use a default role as a template to create a new role. Or, you can create a completely custom role to fit your needs. See "Role permissions" on page 185. See "Default RBAC roles" on page 179. See "Add a custom RBAC role" on page 181.
3	Add users to the appropriate roles.	See "Add a user to a role (non-SAML)" on page 175. See "Add a user to a role (SAML)" on page 177. See "Add a smart card user to a role (non-SAML, without AD/LDAP)" on page 176.
4	Determine the permissions that you want for OS administrators	See "Disable web UI access for operating system (OS) administrators" on page 178. See "Disable command-line (CLI) access for operating system (OS) administrators" on page 178.

Notes for using NetBackup RBAC

Note the following when you configure the permissions for RBAC roles:

- RBAC only controls access to the web UI and not the NetBackup Administration Console.
- When you create roles, be sure to enable the minimal number of permissions so the user can sign in to and use the web UI. Some individual permissions do not have a direct correlation with a screen in the web UI. Users that attempt to sign in but that only have a permission of this kind receive an "Unauthorized" message.

- If a user is added to or removed from a role, the user must sign out and sign in again before the user's permissions are updated.
- Most permissions are not implicit.
In most cases a **Create** permission does not give a user **View** permission. A **Recovery** permission does not give a user **View** permission or other recovery options like **Overwrite**.
- Not all RBAC-controlled operations can be used from the NetBackup web UI. These types of operations are included in RBAC so a role administrator can create roles for API users as well as for web UI users.
- Some tasks require a user to have permissions in multiple RBAC categories. For example, to establish a trust relationship with a remote primary server, a user must have permissions for both **Remote primary servers** and **Trusted primary servers**.

Add AD or LDAP domains

NetBackup supports Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) domain users. Before you can add domain users to RBAC roles, you must add the AD or the LDAP domain. A domain also must be added before you can configure that domain for smart card authentication.

You can use the `POST /security/domains/vxat` API or the `vssat` command to configure domains.

For more information on the `vssat` command and more of its options, see the [NetBackup Command Reference Guide](#). For troubleshooting information, see the [NetBackup Security & Encryption Guide](#).

View users in RBAC

You can view the users that have been added to RBAC and the roles that they are assigned to. The **Users** list is view-only. To edit the users that are assigned to a role, you must edit the role.

To view the users in RBAC

- 1 On the left, click **Security > RBAC**.
- 2 Click on the **Users** tab.
- 3 The **Roles** column indicates each role to which the user is assigned.

Add a user to a role (non-SAML)

This topic describes how to add a non-SAML user or group to a role.

Non-SAML users use one of the following sign-in methods: **Sign in with username and password** or **Sign in with smart card**.

To add a user to a role (non-SAML)

- 1 On the left, click **Security > RBAC**.
- 2 Click the **Roles** tab.
- 3 Click on the role name, then click on the **Users** tab.
- 4 (Conditional) From the **Sign-in type** list, select from the following:
 - **Default sign-in**. For a user that signs into NetBackup with their username and password.
 - **Smart card user**. For a user that uses a smart card to sign into NetBackup.

Note: The **Sign-in type** list is only available if there is an IDP configuration available for NetBackup.

- 5 Enter the user or the group name that you want to add.

For this type of user	Use this format	Example
Local user or group	<i>username</i>	jane_doe
	<i>groupname</i>	admins
Windows user or group	<i>DOMAINusername</i>	WINDOWS\jane_doe
	<i>DOMAINgroupname</i>	WINDOWS\Admins
UNIX user or group	<i>username@domain</i>	john_doe@unix
	<i>groupname@domain</i>	admins@unix

- 6 Click **Add to list**.
- 7 The user must sign out and sign in again before the user's permissions are updated.

Add a smart card user to a role (non-SAML, without AD/LDAP)

This topic describes how to add a smart card user to a role. In this case the user is a non-SAML user and there is no AD or no LDAP domain association or mapping. User groups are not supported with this type of configuration.

This type of user uses the following sign-in method: **Sign in with smart card**.

To add a smart card user to a role (non-SAML, without AD/LDAP)

- 1 On the left, click **Security > RBAC**.
- 2 Click the **Roles** tab.
- 3 Click on the role name, then click on the **Users** tab.
- 4 (Conditional) From the **Sign-in type** list, select **Smart card user**.

Note: The **Sign-in type** list is available only if there is an IDP configuration available for NetBackup. The smart card user option in the **Sign-in type** list is available when the smart card configuration is done without AD or LDAP domain mapping.

- 5 Enter the username that you want to add.
Provide the exact common name (CN) or the universal principal name (UPN) that is available in the certificate.
- 6 Click **Add to list**.
- 7 The user must sign out and sign in again before the user's permissions are updated.

Add a user to a role (SAML)

This topic describes how to add a SAML user or group to a role.

SAML users use one of the following sign-in methods: **SAML user** or **SAML group**.

To add a user to a role (SAML)

- 1 On the left, click **Security > RBAC**.
- 2 Click the **Roles** tab.
- 3 Click on the role name, then click on the **Users** tab.
- 4 From the **Sign-in type** list, select the sign-in method **SAML user** or **SAML group**.
- 5 Enter the user or the group name that you want to add.
For example, nbuadmin@my.host.com.
- 6 Click **Add to list**.
- 7 The user must sign out and sign in again before the user's permissions are updated.

Remove a user from a role

You can remove a user from a role when you want to remove permissions for that user.

If a user is removed from a role, the user must sign out and sign in again before the user's permissions are updated.

To remove a user from a role

- 1 On the left, click **Security > RBAC**.
- 2 Click the **Roles** tab.
- 3 Click on the role that you want to edit, select the **Users** tab.
- 4 Locate the user you want to remove and click **Actions > Remove > Remove**.

Disable web UI access for operating system (OS) administrators

By default, an OS administrator (user or group member) has access to the NetBackup web UI and does not need to be a member of an RBAC role.

If you do not want an OS administrator to automatically have this access, you can disable it. An OS administrator must then have the RBAC Administrator role to be able to access the web UI.

To disable web UI access control for the OS administrators

- 1 On the left, select **Security > RBAC**.
- 2 On the top right, click **Role-based access control settings**.
- 3 Turn off **Web UI access for Operating System Administrator**.

Disable command-line (CLI) access for operating system (OS) administrators

By default, an OS administrator (user or group member) has access to the NetBackup CLI and does not need to be a member of an RBAC role.

If you do not want an OS administrator to automatically have this access, you can disable it. An OS administrator must then log in with `bpbabat -login` to access the CLI.

To disable CLI access for OS administrators

- 1 On the left, select **Security > RBAC**.
- 2 On the top right, click **Role-based access control settings**.
- 3 Turn off **CLI access for Operating System Administrator**.

Default RBAC roles

The NetBackup web UI provides the following default RBAC roles with preconfigured permissions and settings.

Table 19-4 Default RBAC roles in the NetBackup web UI

Role name	Description
Administrator	The Administrator role has full permissions for NetBackup and can manage all aspects of NetBackup.
Default Apache Cassandra Administrator	This role has all the permissions that are necessary to manage and protect Apache Cassandra assets with protection plans.
Default AHV Administrator	This role has all the permissions that are necessary to manage Nutanix Acropolis Hypervisor and to back up those assets with protection plans.
Default Cloud Administrator	<p>This role has all the permissions that are necessary to manage cloud assets and to back up those assets with protection plans.</p> <p>Note that a PaaS administrator requires additional permissions that you can add to a custom role</p> <p>See “Add a custom RBAC role for a PaaS administrator” on page 184.</p>
Default Kubernetes Administrator	This role has all the permissions that are necessary to manage Kubernetes and to back up those assets with protection plans. The permissions for this role give a user the ability to view and manage jobs for Kubernetes assets. To view all jobs for this asset type, a user must have the default role for that workload. Or, a similar custom role must have the following option applied when the role is created: Apply selected permissions to all existing and future workload assets .
Default Microsoft SQL Server Administrator	<p>This role has all the permissions that are necessary to manage SQL Server databases and to back up those assets with protection plans. In addition to this role, the NetBackup user must meet the following requirements:</p> <ul style="list-style-type: none"> ■ Member of the Windows administrator group. ■ Have the SQL Server “sysadmin” role.
Default MySQL Administrator	This role has all the permissions that are necessary to manage MySQL instances and databases and to back up those assets with protection plans.
Default NetBackup Command Line (CLI) Administrator	<p>This role has all the permissions that are necessary to manage NetBackup using the NetBackup command line (CLI). With this role a user can run most of the NetBackup commands with a non-root account.</p> <p>Note: A user that has only this role cannot sign into the web UI.</p>
Default Oracle Administrator	This role has all the permissions that are necessary to manage Oracle databases and to back up those assets with protection plans.

Table 19-4 Default RBAC roles in the NetBackup web UI (*continued*)

Role name	Description
Default PostgreSQL Administrator	This role has all the permissions that are necessary to manage PostgreSQL instances and databases and to back up those assets with protection plans.
Default Resiliency Administrator	This role has all the permissions to protect Veritas Resiliency Platform (VRP) for VMware assets.
Default RHV Administrator	<p>This role has all the permissions that are necessary to manage Red Hat Virtualization machines and to back up those assets with protection plans. This role gives a user the ability to view and manage jobs for RHV assets.</p> <p>To view all jobs for RHV assets, a user must have this role. Or, the user must have a similar custom role with following option applied when the role was created: Apply selected permissions to all existing and future RHV assets.</p>
Default SaaS Administrator	This role has all the permissions to view and manage SaaS assets.
Default Security Administrator	This role has permissions to manage NetBackup security including role-based access control (RBAC), certificates, hosts, identity providers and domains, global security settings, and other permissions. This role can also view settings and assets in most areas of NetBackup: workloads, storage, licensing, and other areas.
Default Storage Administrator	This role has permissions to configure disk-based storage and storage lifecycle policies. SLP settings are managed with the Administrator role.
Default Universal Share Administrator	This role has the permissions to manage policies and storage servers. It also can manage the assets for Windows and Standard client types and for universal shares.
Default VMware Administrator	This role has all the permissions that are necessary to manage VMware virtual machines and to back up those assets with protection plans. To view all jobs for VMware assets, a user must have this role. Or, the user must have a similar custom role with following option applied when the role was created: Apply selected permissions to all existing and future VMware assets.

Note: Veritas reserves the right to update the RBAC permissions for default roles in future releases. Any revised permissions are automatically applied to users of these roles when NetBackup is upgraded. If you have copies of default roles these roles are not updated automatically. (Or, if you have any custom roles that are based on default roles.) If you want these custom roles to include changes to default roles, you must manually apply the changes or recreate the custom roles.

Add a custom RBAC role

Create a custom RBAC role if you want to manually define the permissions and the access that users have to workload assets, protection plans, or credentials.

Note: Veritas reserves the right to update the RBAC permissions for default roles in future releases. Any revised permissions are automatically applied to users of these roles when NetBackup is upgraded. Any copies of default roles (or any custom roles that are based on default roles) are not automatically updated.

To add a custom RBAC role

1 On the left, select **Security > RBAC** and click **Add**.

2 Select the type of role that you want to create.

You can make a copy of a default role that contains all the preconfigured permissions and settings for that type of role. Or, select **Custom role** to manually configure all the permissions for a role.

3 Provide a **Role name** and a description.

For example, you may want to indicate that role is for any users that are backup administrators for a particular department or region.

4 Under **Permissions**, click **Assign**.

The permissions that you select determine the other settings that you can configure for the role.

If you select a default role type, certain permissions are enabled only if they are required for that type of role. (For example, the **Default Storage Administrator** does not require permissions for protection plans. The **Default Microsoft SQL Server Administrator** requires credentials.)

- **Workloads** are enabled when you select **Asset** permissions.
- **Protection plans** are enabled when you select **Protection plans** permissions.
- **Credentials** are enabled when you select **Credentials** permissions.

5 Configure the permissions for the role.

See [“Role permissions”](#) on page 185.

See [“Notes for using NetBackup RBAC”](#) on page 174.

6 Under **Users**, click **Assign**.

7 When you are done configuring the role, click **Save**.

Note: After a role is created, you must edit permissions for assets, protection plans, or credentials directly from the applicable node in the web UI. For example, to edit permissions for VMware, go to **Workloads > VMware** and then select **VMware settings > Manage permissions**. Or, open the details for a VM and click on the **Permissions** tab.

Edit or remove a role a custom role

You can edit or remove a custom role when you want to change or remove permissions for users with that role. Default roles cannot be edited or removed. You can only add or remove users from default roles.

Edit a custom role

Note: When you change permissions for a custom role, the changes affect all users that are assigned to that role.

To edit a custom role

- 1** On the left, click **Security > RBAC**.
- 2** On the **Roles** tab, locate and click on the custom role that you want to edit.
- 3** To edit the role description, click **Edit name and description**.
- 4** Edit the permissions for the role. You can edit the following details for a role:

Global permissions for the role

On the **Global permissions** tab, click **Edit**.

Users for the role

Click the **Users** tab.

Access definitions for the role

Click the **Access definitions** tab.

See [“Role permissions”](#) on page 185.

See [“Notes for using NetBackup RBAC”](#) on page 174.

- 5** To add or remove users for the role, click the **Users** tab.

See [“Add a user to a role \(non-SAML\)”](#) on page 175.

See [“Remove a user from a role”](#) on page 178.

- 6** Permissions for assets, protection plans, and credentials must be edited directly in the applicable node in the web UI.

Remove a custom role

Note: When you remove a role, any users that are assigned to that role lose the permissions that the role provided.

To remove a custom role

- 1 On the left, click **Security > RBAC**.
- 2 Click the **Roles** tab.
- 3 Locate the custom role that you want to remove and select the check box for it.
- 4 Click **Remove > Yes**.

Add a custom RBAC role to restore Azure-managed instances

To restore Azure-managed instances, users must have the view permission for these instances. Administrators and similar users can provide other users with a custom role and this permission.

To assign the view permission for Azure-managed instances

- 1 To get the access control ID of the managed instance, enter the following command:

```
GET /asset-service/workloads/cloud/assets?filter=extendedAttributes/managedInstanceName eq 'managedInstanceName'
```

Search for *accessControlId* field in the response. Note down the value of this field.

- 2 To get the role ID, enter the following command:

```
GET /access-control/roles
```

Search for the *id* field in the response. Note down the value of this field.

- 3 Create an access definition, as follows:

```
POST /access-control/managed-objects/{objectId}/access-definitions
```

Request payload

```
{
  "data": {
    "type": "accessDefinition",
    "attributes": {
```

```

        "propagation": "OBJECT_AND_CHILDREN"
    },
    "relationships": {
        "role": {
            "data": {
                "id": "<roleId>",
                "type": "accessControlRole"
            }
        },
        "operations": {
            "data": [
                {
                    "id": "|OPERATIONS|VIEW|",
                    "type": "accessControlOperation"
                }
            ]
        },
        "managedObject": {
            "data": {
                "id": "<objectId>",
                "type": "managedObject"
            }
        }
    }
}

```

Use the following values:

- `objectId`: Use the value of *accessControlId* obtained from step 1.
- `roleId`: Use the value of *id* obtained from step 2.

Note: For an alternate restore, provide the `|OPERATIONS|ASSETS|CLOUD|RESTORE_DESTINATION|` permission in the *operations* list.

Add a custom RBAC role for a PaaS administrator

A PaaS administrator needs additional storage permissions. You can use the **Default Cloud Administrator** role as a template to create a custom role.

To add a custom RBAC role

- 1 On the left, select **Security > RBAC** and click **Add**.
- 2 Select **Default Cloud Administrator**.
- 3 Provide a **Role name** and a description.
 For example, you may want to indicate that the role is for any users that are PaaS administrators.
- 4 Under **Permissions**, click **Assign**.
- 5 On the **Global** tab, expand the **Storage** section. Select the following permissions.

Disk pools	View
Storage servers	View
Storage universal shares	View, Create
- 6 Click **Assign**.
- 7 Under **Users**, click **Assign**. Then add each user that you want to have access to this custom role.
- 8 When you are done configuring the role, click **Add role**.

Role permissions

Role permissions define the operations that roles users have permission to perform.

For details on individual RBAC permissions and dependencies, refer to the NetBackup API documentation.

<http://sort.veritas.com>

Table 19-5 Role permissions for NetBackup RBAC

Category	Description
Global	<p>Global permissions apply to all assets or objects.</p> <p>BMR - Configuration and management of BMR.</p> <p>NetBackup Web Management Console Administration - With guidance from Veritas Support, create diagnostic files to troubleshoot NetBackup and perform JVM garbage collection.</p> <p>These operations are only available from the NetBackup APIs. Refer to the following guides for information on JVM tuning options: NetBackup Installation Guide, NetBackup Upgrade Guide.</p> <p>NetBackup management - Configuration and management of NetBackup.</p> <p>Protection - NetBackup backup policies and storage lifecycle policies.</p> <p>Security - NetBackup security settings.</p> <p>Storage - Manage backup storage settings.</p>
Assets	Manage one or types of assets. For example, VMware assets.
Protection plans	Manage how backups are performed with protection plans.
Credentials	Manage credentials for assets and for other features of NetBackup.

Manage access permission

The **Manage access** permission allows a user to manage who can access a specific part of NetBackup. Users that manage access also need **Access control** permissions. This permission is available for each permission category. However, for some categories the **Manage access** functionality is only available from the NetBackup APIs and not the NetBackup web UI.

For example, a user that has **Manage access** on VMware assets can add or remove the custom roles that have access to VMware assets. This user can also add or remove the specific permissions that a custom role has on VMware assets.

Add the manage access permission to a custom role

If a default role does not have the **Manage access** permission that a user needs, you can create a custom role with that permission. Also give the user the permissions for **User** and **Roles**. These permissions allow the user to view and add users to roles and to add and manage roles.

Assign permissions [Learn about permissions](#)

Global
Assets
Protection plans
Credentials

RHV assets [All](#) | [None](#)

☐ View
☐ Create
☐ Update
☐ Delete

☐ Manage access
☐ Protect
☐ View restore targets
☐ Restore

☐ Allow restore to overwrite
☐ Cancel Jobs
☐ Restart Jobs
☐ View Jobs

VMware assets [All](#) | [None](#)

☒ View
☐ Create
☐ Update
☐ Delete

☒ Manage access
☐ Protect
☐ View restore targets
☐ Restore to cloud

☐ Granular restore
☐ Instant access - Download files
☐ Instant access - Restore files
☐ Instant access

☐ Restore
☐ Allow restore to overwrite
☐ Cancel Jobs
☐ Restart Jobs

☐ View Jobs

Assign permissions

Global
Assets
Protection plans
Credentials

NetBackup management

Protection

Security

Access control

Users

☒ View
☐ Manage access
☒ Assign to role

Roles

☒ Create
☒ Update
☒ Delete
☐ Manage access

Remove access for a custom role

You can remove access to an area of the web UI for a custom role. For each category for which you want to remove the manage access permission, clear the **Manage access** permission. You must edit permissions for assets, protection plans, or credentials directly from the applicable node in the web UI.

For example, to remove manage access permissions for VMware, go to **Workloads > VMware** and then select **VMware settings > Manage permissions**. Or, open the details for a VM and click on the **Permissions** tab.

- 1 On the left, select **Security > RBAC** and click on the **Roles** tab.
- 2 Click on the role.
- 3 Click on the **Access definitions** tab.
- 4 Locate the namespace you want to remove.
- 5 Click **Actions > Remove**.

Detection and reporting

- [Chapter 20. Detecting malware](#)
- [Chapter 21. Detecting anomalies](#)
- [Chapter 22. Usage reporting and capacity licensing](#)

Detecting malware

This chapter includes the following topics:

- [About malware detection](#)
- [Configure a new scan host pool](#)
- [Add an existing scan host](#)
- [Manage credentials](#)
- [Remove the scan host](#)
- [Deactivate the scan host](#)
- [Scan a policy client backup images for malware](#)
- [Perform malware scanning](#)
- [Scan a VMware asset for malware](#)
- [View the malware scan status](#)
- [Actions for malware scanned images](#)
- [Recover from malware-affected images \(clients protected by policies\)](#)
- [Recover a VMware asset affected by malware](#)
- [Troubleshooting](#)

About malware detection

NetBackup finds malware in supported backup images and finds the last good-known image that is malware free.

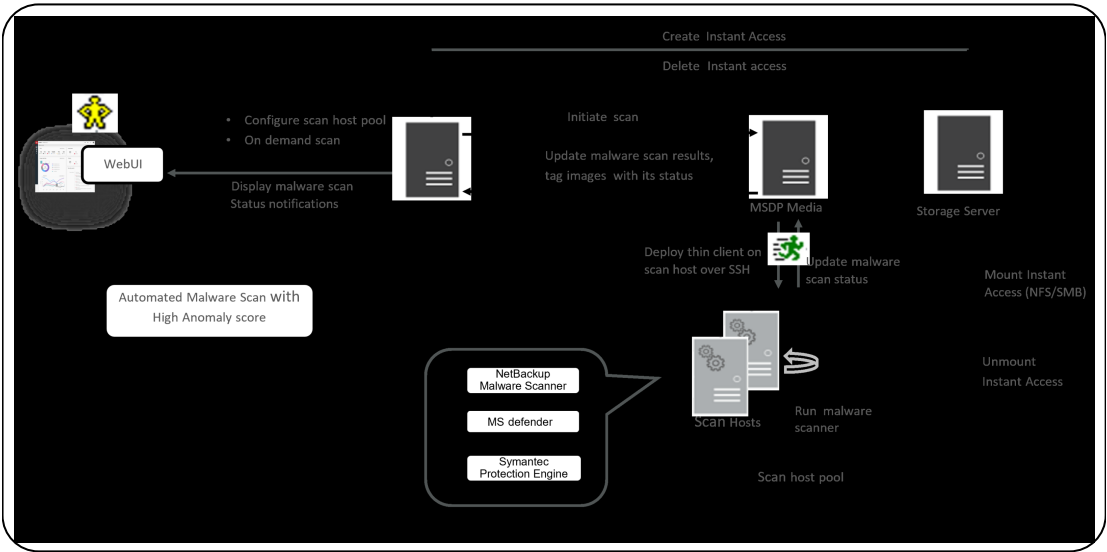
Malware detection provides the following benefits:

- You can select one or more backup images of the supported policy-types for an on-demand scan. You can use a predefined list of scan hosts.
- If malware is detected during the scanning, a notification is generated in the web UI.

Note: During recovery if user starts recovery from a malware-affected backup image, a warning message is shown and confirmation is required for proceeding with recovery. Only users with permission to restore from malware-affected images can proceed with recovery.

The following steps depict the malware workflow:

Figure 20-1 Malware detection workflow



1. Primary server identifies the available scan host from the specified scan host pool. A maximum of three scans can be initiated on a scan host at a given point of time.

Note: The backup images that fail validation are ignored.

2. After the backup images are queued for an on-demand scan, the primary server identifies the storage server. An instant access mount is created on the storage server of the configured share type that is specified in scan host pool.
3. Primary server identifies available MSDP media server and instructs the media server to initiate the malware scan.
4. MSDP media server deploys the thin client on the scan host over SSH.
5. Thin client mounts the instant access mount on the scan host.
6. Scan is initiated using the malware tool that is configured in the scan host pool.
7. After the scan is completed, the scan host unmounts the instant access mount from the scan host.
8. Malware scan status is updated to the media server over SSH. Scan logs are copied to the media server log directory.
9. Media server updates the scan status and the infected file list (if there are any infected files) to the primary server.
10. Primary server updates the scan results and deletes instant access.
11. Malware scan status notification is generated.

Malware detection performs an automated cleanup of scan jobs that are older than 30 days.

Note: You can download a malware scanner from the Microsoft Azure Marketplace and the AWS Marketplace. Follow the instructions on how to install, configure, and use the malware scanner for AWS and Azure.

Refer to the following for more information about AWS:

[AWS Marketplace](#)

[Cloud NetBackup Marketplace Deployment on AWS](#)

Refer to the following for more information about Microsoft Azure:

[Microsoft Azure Marketplace](#)

[NetBackup Marketplace Deployment on Azure Cloud](#)

Configure a new scan host pool

- 1 On left, click **Detection and reporting > Malware detection**.
- 2 On the **Malware detection** page, click **Configure a scanner host pool** or **Malware settings** on the top-right corner to go to host pool list page.
 For configuration details, see the [NetBackup Security and Encryption Guide](#).
- 3 On the **Malware scanner host pools** page, click **Add** to add a new host pool.
- 4 On the **Add malware scanner host pools** page, enter the details such as **Host pool name**, **Malware scanner**, and **Type of share**.
- 5 Click **Save and add hosts**.

Add an existing scan host

Use this procedure to add a same scan host in another scan host pool of same share type.

To configure an existing scan host

- 1 On left, click **Detection and reporting > Malware detection**.
- 2 Click **Malware detection** page, click **Malware settings** on the top right corner.
- 3 On the **Malware scanner host pools** page, select the desired scan host pool and click **Manage hosts** from the action menu.
- 4 On the **Manage malware scanner hosts** page, click **Add existing** to select pre-existing host.

Note: List includes all scan hosts from all scan host pools.

- 5 On the **Add existing malware scanner host** window, select the desired one or more scan hosts.
- 6 Click **Add**.

Manage credentials

Add new credentials

- 1 On the **Manage credentials** page, select **Add new credentials** and click **Next**.
- 2 On the **Manage credentials** page, add the details such as **Credential name**, **tag**, **description**.

- 3 On the **Host credentials** tab, add **Host username**, **Host password**, **SSH port**, **RSA key**, and **Share type**, .
 - Ensure the SSH connection between MDSP media server and host is working. To ensure run `ssh username@remote_host_name`
 - ■ Run `ssh-keyscan scan_host_name 2>/dev/null | grep ssh-rsa` command to verify that it is listing the RSA key for remote scan host.
 - To get the RSA key for the remote scan host, use `ssh-keyscan scan_host_name 2>/dev/null | grep ssh-rsa | awk '{print $3}' | base64 -d | sha256sum` on linux MSDP media server.
For example, the output is
33f697637ab3f0911c1d462d4bde8be3eec61a33403e8f6a88daecb415a31eef
- where the RSA key is
33f697637ab3f0911c1d462d4bde8be3eec61a33403e8f6a88daecb415a31eef

Note: Ensure that you remove the character – from RSA key when you copy.

- 4 For share type **SMB**, enter additional details such as:
 - **Active directory domain**
It is a domain to which storage server has joined for the authenticating mounts on scan host.
 - **Active directory group**
It is a group name which is available in active directory domain.
 - **Active directory user**
It is an active directory user added in selected active directory group.
 - **Password**
- 5 Click **Save**.

Select existing credentials

- 1 On the **Manage credentials** page, select **Select existing credentials** and click **Next**.
- 2 On the **Select credentials** tab, select the desired credential and click **Save**.

Remove the scan host

- 1 On left, click **Detection and reporting > Malware detection**.
- 2 Click **Malware detection** page, click **Malware detection settings** on the top right corner.
- 3 On the **Malware scanner host pools** page, select the desired scan host pool and click **Manage hosts** from the action menu.
- 4 Select the desired host and click **Remove**.

Deactivate the scan host

- 1 On left, click **Detection and reporting > Malware detection**.
- 2 Click **Malware detection** page, click **Malware detection settings** on the top right corner.
- 3 On the **Malware scanner host pools** page, select the desired scan host pool and click **Manage hosts** from the action menu.
- 4 Select the desired host and click **Deactivate**.

Scan a policy client backup images for malware

- 1 On left, click **Detection and reporting > Malware detection**.
- 2 On the **Malware detection** page, click **Scan for malware**.
- 3 From the **Search by** option, select **Backup images**.
- 4 In the search criteria, review and edit the following:

- **Policy name**

Note: Only supported policy types are listed.

- **Client name**

Note: Shows clients which contains supported policy type backup images.

- **Policy type**

- **Type of backup**

Note: Incremental backup images without accelerator feature enabled are not supported for VMware workload.

- **Copies**

Note: If the selected copy is not an instant access capable copy, the backup image is skipped for the malware scan.

- **Disk pool**

Note: Only MSDP (PureDisk) storage type disks pools are listed.

- **Malware scan status.**

- On the **Select the timeframe of backups** verify the date and time range or update.

5 Click **Search**.

Note: Select the search criteria accordingly and also ensure enough scan host availability and active in selected scan host pool.

- 6** From the **Select the backups to scan** table select one or more images for scan.

- 7** In the **Select a malware scanner host pool**, **Select** the appropriate host pool name.

Note: Scan host from the selected scan host pool must be able to access the instant access mount created on MSDP storage server with configured share type NFS/SMB.

8 Click **Scan for malware**.

Note: The malware scanner host can initiate a scan of three images at the same time.

9 This scan status is at backup image level and it is applicable to all copies of backup image. Once the scan initiated you can see **Malware Scan Progress** on **Malware Detection**, you can see the following fields:

- **Not scanned**
- **Not infected**
- **Infected**
- **Failed**

Note: When we hover on failed status tool tip displays the reason of failed scan.

Note: The backup images which failed in validation, are ignored. Malware scanning is supported for backup image stored on MSDP storage with instant access capability for the supported policy type only.

- **In progress**
- **Pending**

Note: You can cancel the malware scan for one or more In progress and pending jobs.

Perform malware scanning

You can start the malware scanning to detect the malware.

- 1 On left, click **Detection and reporting > Malware detection**.
- 2 On the **Malware detection** page, click **Scan for malware**.
- 3 From the **Search by** option, select one of the following:
 - **Backup images**.

See [“Scan a policy client backup images for malware”](#) on page 196.

- **Assets by policy type**

Note: NetBackup supports MS-windows and standard policy types for malware scan.

- **Assets by protection plans**

Note: NetBackup support VMware assets for malware scan.

- 4 From the **Client/Asset** table, select a client/Asset to scan.
- 5 Click **Next**.
- 6 On the **Start date/time** and **End date/time** verify the date and time range or update.

Note: According to selection criteria, scan gets initiated to maximum of 100 images.

- 7 In the **Scanner host pool**, **Select** the appropriate host pool name.
- 8 From the **Current status of malware scan**, select one of the following:
 - **Not scanned**
 - **Not infected**
 - **Infected**
 - **All**
- 9 Click **Scan for malware**.

Warning: There are more than 100 images in your search. Unable to scan more than 100 images. Adjust the date range and try again.

Note: Malware scanner host can initiate the scanning of three images at the same time.

- 10 Once Scan initiated you can see **Malware Scan Progress** on **Malware Detection**, you can see the following fields:
 - **Not scanned**

- **Not infected**
- **Infected**
- **Failed**

Note: When we hover on failed status tool tip displays the reason of failed scan.

Note: The backup images which failed in validation, are ignored. Malware scanning is supported for backup image stored on MSDP storage with instant access capability for the supported policy type only.

Scan a VMware asset for malware

The following requirements exist before you can scan for malware:

- The primary server must be at NetBackup 10.0.1 or later.
- The backups were performed with a storage server at NetBackup 10.1 or later.
- Backup images are stored on MSDP storage with instant access capability, for the supported policy type only.
- The scan host pool must be configured with scan hosts.
- The last backup must be successful.
- You must have an RBAC role with permissions to perform malware scans.

To scan a VMware asset for malware

- 1 On left, click **VMware > Virtual machines**.
- 2 Locate and click on the VM.
- 3 Select **Actions > Scan for malware**.
- 4 On the **Malware scan** page, do the following:
 - Select the date range for the scan by selecting **Start date/time** and **End date/time**.
 - Select **Scanner host pool**
 - From the **Select current status of malware scan** list select one of the following:
 - **Not scanned**

- Not infected
- Infected
- All

5 Click **Scan for malware**.

Note: The malware scanner host can initiate a scan of three images at the same time.

6 After the scan starts, you can see the **Malware Scan Progress** on **Malware Detection**, you can see the following fields:

- Not scanned
- Not infected
- Infected
- Failed

Note: Any backup images that fail validation are ignored.

- In progress
- Pending

View the malware scan status

To view the malware scan status

- ◆ On the left, click **Detection and reporting > Malware detection**.

The following columns are displayed:

- Client - Name of the NetBackup client where the malware is detected.
- Backup time - Time when the backup was performed.
- Malware scan status - The scan status of the backup image. The different statuses are infected, not infected, failed, in progress, pending, canceled, and cancellation in progress.
- Schedule type - The backup type of the associated backup job
- Date of the scan - Date when the scan was performed.

- Malware scanner - Name of the malware scanner that was used for scanning.
- Files infected - Indicates the number of files that were found infected during the scan.

Actions for malware scanned images

Once you scan the backup images for malware detection, a tabular data is available on the **Malware detection** home page. See [“View the malware scan status”](#) on page 201.

For each backup image, the following quick configuration are available:

Expire all copies

- 1 On the left, select **Detection and reporting > Malware detection**
- 2 For the desired scan result, from the right, select **Expire all copies**
- 3 Confirm to expire all the copies of the selected backup image.

View infected files

- 1 On the left, select **Detection and reporting > Malware detection**
- 2 For the desired scan result, select **View infected files**

Note: This option is available only for infected files.

- 3 In the **Infected files** table, search or the desired file, if needed.
- 4 If needed, click **Export list**.

Note: A list of infected files from the selected malware scanning result is exported in `.csv` format. The file name is of following format:

backupid_infected_files_timestamp.csv

Export infected files list

- 1 On the left, select **Detection and reporting > Malware detection**
- 2 For the desired malware affected , from the right, select **Export Infected files list**

Note: `.csv` file contains backup time and names of the infected files.

Cancel malware scan

- 1 On the left, select **Detection and reporting > Malware detection**
- 2 For desired client, from actions menu, click **Cancel malware scan**.

Note: You can cancel the malware scan only from in progress and pending states.

- 3 Click **Cancel scan** to confirm.

Note: The status changes to Cancellation in progress.

Recover from malware-affected images (clients protected by policies)

By default during recovery, NetBackup only displays the backup images that are scanned and free from malware.

To restore from malware-affected images, you must have the Administrator role or equivalent RBAC permissions. To recover a VMware asset that is affected by malware, see the following topic.

See [“Recover a VMware asset affected by malware”](#) on page 204.

To recover from malware-affected images (clients protected by policies)

- 1 On the left, click **Recovery**.
- 2 Under **Regular recovery**, click **Start recovery**.
- 3 Select the following properties:

Source client	The client that performed the backup.
Destination client	The client to which you want to restore the backup.
Policy type	The type of policy that is associated with the backup you want to restore.
Restore type	The type of restore that you want to perform. The restore types that are available depend on the policy type that you choose.

4 Click **Next**.

5 Select the **Start date** and **End date**.

Or, click **Backup history** to view and select specific images. Click **Select** to add the selected images for recovery.

Note: The table displays all the backup image details for selected time frame. You can filter and sort the images. For example, based on the malware scan results, schedule type, or policy name.

6 To include any malware-infected images in the recovery, select **Allow the selection of images that are malware-affected**.

7 On the left, expand the **Source client** directory. Select any directories that you want to restore. Or in the right pane, select any files or directories. Click **Next**.

8 Select the recovery target.

9 To restore any files that are malware-infected, click **Allow recovery of files infected with malware**. Otherwise, NetBackup only restores the files that are scanned and free from malware.

10 Select any other recovery options that you want. Then click **Next**.

11 Review the recovery settings and then click **Start recovery**.

Recover a VMware asset affected by malware

By default during recovery, NetBackup only displays the recovery points that are scanned and free from malware.

To restore from malware-affected recovery points, you must have the Administrator role or equivalent RBAC permissions. To recover a VMware asset that is affected by malware, see the following topic.

See [“Recover from malware-affected images \(clients protected by policies\)”](#) on page 203.

To recover a VMware asset affected by malware

1 On left, click **VMware > Virtual machine**.

2 Locate the VM. Then click **Actions > Recover**.

3 On the **Recovery points** tab you can see **Malware scan** status of each recovery point, as follows:

- **Not scanned**

- **Not infected**
 - **Infected**
 - **Failed**
- 4 Select the recovery point.
- 5 Select **Allow the selection of recovery of points that are malware-affected**. This option only displays if there are recovery points that contain malware-affected images.
-
- Note:** To restore from malware-affected recovery points, you must have the Administrator role or equivalent RBAC permissions.
-
- 6 Click **Recover** and select the type of recovery. Then follow the prompts.
- For more details on recovering a VM, see the [NetBackup Web UI VMware Administrator's Guide](#)

Troubleshooting

Table 20-1

Error	Description
Too many infected files in the selected time range.	<p>Review the <code>nbmalwarescanner</code> to view the infected files list for the backup images in the selected date range. Update the date range or recovery files and folders selection to reduce the number of infected files. Retry the operation. You can also perform one of the following:</p> <ul style="list-style-type: none">■ Select the Allow recovery of files impacted by malware option which can be used to recover selective clean files.■ Skip that backup image from recovery.

Detecting anomalies

This chapter includes the following topics:

- [About backup anomaly detection](#)
- [How a backup anomaly is detected](#)
- [View anomalies](#)
- [Configure anomaly detection settings](#)

About backup anomaly detection

NetBackup can now detect anomalies in backup metadata. It can detect any unusual job data in the data backup flow. For example, it can detect a file count or a file size that is different than the usual count or size.

Note: By default, the anomaly detection algorithm runs on the NetBackup master server. If you see any impact on the master server because of the anomaly detection process, you can configure a media server to detect anomalies.

The following backup job metadata, attributes, or features are verified during backup anomaly detection:

- Backup image size
- Number of backup files
- Data that is transferred in KB
- Deduplication rate
- Backup job completion time

Any unusual deviation in these backup job attributes is considered to be an anomaly and is notified using the NetBackup web UI.

Workflow of backup anomaly detection and notification

The workflow of the backup anomaly detection and notification is as follows:

Table 21-1 Workflow

Step	Description
Step 1	<p>Install or upgrade NetBackup software on the master server and the media server.</p> <p>See the NetBackup Installation or Upgrade Guide.</p>
Step 2	<p>Enable the master server to detect backup anomalies.</p> <p>By default, the anomaly detection algorithm runs on the NetBackup master server. If you see any impact on the master server because of the anomaly detection process, you can configure a media server to detect anomalies.</p> <p>See the NetBackup Security and Encryption Guide.</p>
Step 3	<p>Configure anomaly detection settings using the NetBackup web UI.</p> <p>See “Configure anomaly detection settings” on page 209.</p>
Step 4	<p>View the anomalies using the NetBackup web UI.</p> <p>See “View anomalies” on page 208.</p>

How a backup anomaly is detected

Consider the following example:

In an organization, around 1 GB of data is backed up every day for a given client and backup policy with the schedule type FULL. On a particular day, 10 GB of data is backed up. This instance is captured as an image size anomaly and notified. The anomaly is detected because the current image size (10 GB) is much greater than the usual image size (1 GB).

Significant deviation in the metadata is termed as an anomaly based on its anomaly score.

An anomaly score is calculated based on how far the current data is from the cluster of similar observations of the data in the past. In this example, a cluster is of 1 GB of data backups. You can determine the severity of anomalies based on their scores.

For example:

Anomaly score of Anomaly_A = 7

Anomaly score of Anomaly_B = 2

Conclusion - Anomaly_A is severer than Anomaly_B

NetBackup takes anomaly detection configuration settings (default and advanced if available) into account during anomaly detection.

See the [NetBackup Security and Encryption Guide](#).

View anomalies

NetBackup can now detect anomalies in backup metadata. It can detect any unusual job data in the data backup flow. For example, it can detect a file count or a file size that is different than the usual count or size.

See [“About backup anomaly detection”](#) on page 206.

Note: An anomalies count of 0 indicates there are no anomalies generated or that the anomaly detection services are not running.

To view anomalies

- 1 On the left, select **Detection and reporting > Anomaly detection**.

The following columns are displayed:

- Job ID - Job ID of the job for which the anomaly is detected
- Client name - Name of the NetBackup client where the anomaly is detected
- Policy type - The policy type of the associated backup job
- Count - The number of anomalies that are detected for this job
- Score - Severity of the anomaly. The score is higher if the severity of the anomaly is more.
- Anomaly severity - Severity of the anomalies that are notified for this job
- Anomaly summary - Summary of the anomalies that are notified for this job
- Received - Date when the anomaly is notified
- Review status - Indicates whether the detected anomaly is reported as a false positive, an actual anomaly, or it can be ignored.
- Policy name - The policy name of the associated backup job
- Schedule name - The schedule name of the associated backup job

- Schedule type - The schedule type of the associated backup job
- 2 Expand a row to see the details of the selected anomaly.
 For each anomaly record, the current value of that feature and its actual range based on the past data are displayed.
 Consider the following example:
 An anomaly of the image size feature is displayed as 100MB (Usual 350MB, 450MB). This information implies that the current image size that is reported as anomaly is 100 MB. However, the usual image size range is 350 MB - 450 MB that is derived from the analysis of past data. Because of the significant difference between the current images size and usual image size range, NetBackup notifies it as an anomaly.
 - 3 You can perform the following actions on the anomaly record:
 - Click **Mark as ignore** when you can ignore the anomaly condition.
 The **Review status** of the anomaly record appears as *Ignore*.
 - Click **Confirm as anomaly** when you want to take some action on the anomaly condition.
 The **Review status** of the anomaly record appears as *Anomaly*.
 - Click **Report as false positive** if the anomaly is a false positive. Similar anomalies are not shown in the future.
 The **Review status** of the anomaly record appears as *False positive*.

Configure anomaly detection settings

Once you enable anomaly detection setting, anomaly data gathering, detection service, and events are enabled. Basic and advanced anomaly detection settings are available.

See [“About backup anomaly detection”](#) on page 206.

To configure anomaly detection settings

- 1 On the left, select **Detection and reporting > Anomaly detection**.
- 2 On the top right, Click **Anomalies settings**.
- 3 Click **Edit** on the right to configure anomaly detection settings by selecting one of the following options:
 - **Disable all**
 - **Enable anomaly data gathering**
 - **Enable anomaly data gathering and detection service**

- **Enable anomaly data gathering and detection service and events**
- 4 Click **Save**.
 - 5 Click **Edit** to modify the following **Basic Settings**:
 - **Anomaly detection sensitivity**
 - **Data retention settings**
 - **Data gathering settings**
 - **Anomaly proxy server settings**
 - 6 Click **Save**.
 - 7 Click **Advanced settings**.
 - 8 Edit **Disable anomaly settings for clients**.
 - 9 Click **Save**.
 - 10 Edit **Disable policy type or specific features for machine learning**.
 - 11 Click **Save**.

Usage reporting and capacity licensing

This chapter includes the following topics:

- [Track protected data size on your primary servers](#)
- [Add a local primary server](#)
- [Select license types to display in usage reporting](#)
- [Scheduling reports for capacity licensing](#)
- [Other configuration for incremental reporting](#)
- [Troubleshooting failures for usage reporting and incremental reporting](#)

Track protected data size on your primary servers

The Usage reporting application displays the primary servers that are configured for capacity licensing and their respective consumption details. This reporting provides the following benefits:

- Ability to plan for capacity licensing.
- On a weekly basis, NetBackup gathers and reports usage and trend information. The `nbdeployutil` utility has scheduled runs to gather data for the report (enabled by default).
- A link to the [Veritas NetInsights Console](#). The Usage Insights tool within the NetInsights Console tool NetBackup customers to proactively manage their license use through near real-time visibility of consumption patterns.
- Reporting is done for all policy types that are used for data protection.

Requirements

NetBackup automatically collects data for the usage reporting, provided the following requirements are met:

- The primary servers (or primary servers) are at NetBackup 8.1.2 or later.
- You use capacity licensing.
- You use automatic, scheduled reports. If you manually generate capacity license reports, the data does not display in the usage report in the NetBackup web UI.
- The following file exists:
UNIX: `/usr/openv/var/global/incremental/Capacity_Trend.out`
Windows: `install_path\var\global\incremental\Capacity_Trend.out`
The **Usage** tab displays an error if the backup data is not available. Or, if the usage report is not generated (file does not exist).
- If you want one of your primary servers to gather usage reporting data for other remote primary servers, additional configuration is required. You must create a trust relationship between the primary servers. You must also add the local primary server (where you plan to run `nbdeployutil`) to the **Servers** list on each remote primary server.
See [“Add a local primary server”](#) on page 212.
See [“Add a trusted primary server”](#) on page 141.

Additional information

- [Scheduling capacity licensing reports](#). Details on capacity licensing, scheduling, and options for capacity licensing reports.
- *Veritas Usage Insights Getting Started Guide*. Details on how to use [Usage Insights](#) to manage your NetBackup deployment and licensing. This tool provides accurate, near real-time reporting for the total amount of data that is backed up.

Add a local primary server

If you want to add usage reporting information for a primary server but that server does not have an internet connection, you need to add the name of the local primary server to the servers list of the remote primary server. The local primary server is where you plan to run the usage reporting tool.

To add a local primary server

- 1 On the left, click **Hosts > Host Properties**.
- 2 Select the host and click **Connect**.
- 3 Click **Edit primary server**.

- 4 Click **Servers**.
- 5 On the **Additional Servers** tab, click **Add**.
- 6 Enter the name of the primary server where you plan to run `nbdeployutil`.
- 7 Click **Add**.

Select license types to display in usage reporting

You can select the license types for which you want to generate usage reports using the `netbackup_deployment_insights` utility.

Some license types cannot be configured with other types on a primary server. For example, you cannot select traditional licensing if you select any type of capacity licensing. For details, see the NetBackup Licensing Guide.

To select license types to display in usage reporting

- 1 On the left, click **Detection and reporting > Usage**.
- 2 On the top right, click **Usage reporting settings**.

License settings with the license type and license model are displayed for the primary server.
- 3 Click **Edit**.
- 4 Select the license types that you want to use. Then click **Save**.

Scheduling reports for capacity licensing

By default, NetBackup triggers `nbdeployutil` to run on a specified schedule to incrementally gather data and to generate licensing reports. For the first run, the duration of the report uses the frequency that is specified in the configuration file.

For capacity licensing, the report duration is always for the last 90 days based on the availability of the gathered data. Any data older than 90 days is not considered in the report. Each time `nbdeployutil` runs, it gathers information for the time between the latest run of `nbdeployutil` and the previous successful run.

Licensing report location

The current capacity licensing report resides in the following directory:

On Windows: `install_path\NetBackup\var\global\incremental`

On UNIX: `/usr/openv/var/global/incremental`

It contains the following files:

- The generated report for the latest `nbdeployutil` result.
- Folders containing incrementally gathered data.
- The archive folder that contains the older generated reports.
- `nbdeployutil` log files.

The older reports are placed in the archive folder. Veritas recommends that you retain at least 90 days of reporting data. Data can be kept longer than 90 days, depending on the requirements of your environment. Older reports can help to show how the capacity usage has changed over time. Delete the reports or the folder when they are no longer required.

Use Case I: Using the default values for the licensing report

The `nbdeployutilconfig.txt` file is not required when you use the default parameters. `nbdeployutil` uses the following default values for capacity licensing:

- `FREQUENCY_IN_DAYS=7`
- `MASTER_SERVERS=local_server`
- `PARENTDIR=folder_name`
For Windows: `install_path\NetBackup\var\global\incremental`
For UNIX: `/usr/opensv/var/global/incremental`
- `PURGE_INTERVAL=120` (number of days)
- `MACHINE_TYPE_REQUERY_INTERVAL = 90` (number of days)

Use Case II: Using custom values for the licensing report

If the file `nbdeployutilconfig.txt` is not present, create a file using the following format:

```
[NBDEPLOYUTIL_INCREMENTAL]
MASTER_SERVERS=<server_names>
FREQUENCY_IN_DAYS=7
PARENTDIR=<folder_name_with_path>
PURGE_INTERVAL=120
MACHINE_TYPE_REQUERY_INTERVAL=90
```

To use custom values for the licensing report

- 1 Copy the `nbdeployutilconfig.txt` file to the following location:
For Windows: `install_path\NetBackup\var\global`
For UNIX: `/usr/opensv/var/global`
- 2 Open the `nbdeployutilconfig.txt` file.

- 3 Edit the `FREQUENCY_IN_DAYS` value to reflect how often you want the report to be created.

Default 7
(recommended)

Minimum 1

Value of 0 Disables the incremental reporting and no licensing information is captured.

Parameter deleted `nbdeployutil` uses the default value.

- 4 Edit the `MASTER_SERVERS` value to include a comma-separated list of the master servers you want to include in the report.

Note: Veritas Usage Insights requires that master servers be at NetBackup 8.1.2 or later.

No value `nbdeployutil` uses the default value.

Parameter deleted `nbdeployutil` uses the default value.

For example:

- `MASTER_SERVERS=newserver, oldserver`
- `MASTER_SERVERS=newserver, oldserver.domain.com`
- `MASTER_SERVERS=myserver1.somedomain.com, newserver.domain.com`

- 5 Edit the `PARENTDIR` value to include the full path for location where the data is gathered and reported.

No value `nbdeployutil` uses the default value.

Parameter deleted `nbdeployutil` uses the default value.

- 6 Edit the `PURGE_INTERVAL` to indicate the interval (in days) for how often you want to delete the report data. Data that is older than 120 days is automatically purged.

Default	120
Minimum	90
No value	<code>nbdeployutil</code> uses the default value.
Parameter deleted	<code>nbdeployutil</code> uses the default value.

- 7 Edit the `MACHINE_TYPE_REQUERY_INTERVAL` to indicate how often to scan physical clients for updates to the machine type.

Default	90
Minimum	1
No value	<code>nbdeployutil</code> uses the default value.
Parameter deleted	<code>nbdeployutil</code> uses the default value.

Other configuration for incremental reporting

To change the directory of the gathered data and capacity licensing report

- 1 If you have older gathered data and licensing reports, copy the complete directory to the new location.
- 2 Edit `nbdeployutilconfig.txt` and change the location of the gathered data and licensing report in the `PARENTDIR=folder_name` field.

To use the data that was gathered previously to generate a capacity licensing report

- 1 Locate the folder that was generated for the gathered data after the previous run of `nbdeployutil` and copy it to the following location:

On Windows: `install_path\NetBackup\var\global\incremental`

On UNIX: `/usr/openv/var/global/incremental`

- 2 Create the `gather_end.json` file inside the copied folder and add the following text:

```
{"success":0}
```

The next incremental run considers the data inside the copied folder to generate a capacity licensing report.

Note: Delete any other gather folders inside the copied folder to avoid gaps for the period in which data is gathered. The missing data is automatically generated during the next incremental run.

To create a custom interval report using existing gathered data for capacity licensing

- ◆ To create a report for a time interval that is different than the default interval of 90 days, run the following command:

On Windows:

```
nbdeployutil.exe --capacity --incremental --report --inc-settings  
"install_dir\netbackup\var\global\nbdeployutilconfig.txt"  
--hoursago <custom-time-interval>
```

On UNIX:

```
nbdeployutil.exe --capacity --incremental --report --inc-settings  
"/usr/openv/var/global/nbdeployutilconfig.txt"  
--hoursago <custom-time-interval>
```

The number of hours specified in `--hoursago` must be fewer than the `purge-interval` that is specified in the `nbdeployutilconfig.txt` file.

Note: `nbdeployutil` uses existing gathered data to generate the custom interval report. You are not required to use the `--gather` option.

Troubleshooting failures for usage reporting and incremental reporting

- For incremental runs of `nbdeployutil`, notifications are sent to the NetBackup web UI. The notification details include, status of the run, duration, start time, and end time.
- `nbdeployutil` fails to gather data and generate the report for your environment. Refer to the logs to understand when the task failed and the reason for the failure.
- `nbdeployutil` fails with a `bpimagelist` error with status 37 after you run the utility manually. Ensure that you added the master servers to the additional servers list.
See [“Add a local primary server”](#) on page 212.
- The following error displays because of internal web service communication failures:
Internal Web API error occurred for master server `SERVER_NAME`. Run `nbdeployutil` again with the `gather` option on master server `SERVER_NAME`.
- For VMware or NDMP, when the backup agent fails to post licensing information to the database, a status code 5930 or 26 displays in the Activity Monitor: For more information, see the [NetBackup Status Codes Reference Guide](#).

You can use `netbackup_deployment_insights` with the same troubleshooting points.

NetBackup workloads and NetBackup Flex Scale

- [Chapter 23. NetBackup SaaS Protection](#)
- [Chapter 24. NetBackup Flex Scale](#)
- [Chapter 25. NetBackup workloads](#)

NetBackup SaaS Protection

This chapter includes the following topics:

- [Overview of NetBackup for SaaS](#)
- [Adding NetBackup SaaS Protection Hubs](#)
- [Configuring the autodiscovery frequency](#)
- [Viewing asset details](#)
- [Configuring permissions](#)
- [Troubleshooting SaaS workload issues](#)

Overview of NetBackup for SaaS

The NetBackup web UI provides the capability to view the assets of NetBackup SaaS Protection. The assets configured to protect SaaS applications data are automatically discovered in the NetBackup web UI.

The NetBackup SaaS Protection assets comprise of the assets such as, Hubs, StorSites, Stors, and Services.

The following assets details are displayed:

- Storage size
- Storage tier details
- Number of items in the storage
- WORM details
- Write, delete, stub policies details

- Schedule for the next backup
- Status of the last backup

The NetBackup web UI lets you perform the following operations:

- Add a NetBackup SaaS Protection Hub.
- View assets in the Hub.
- Launch the NetBackup SaaS Protection web UI.
- Delete the added Hub.

Note: If a SaaS asset is deleted from NetBackup SaaS Protection web UI, the deleted asset is not removed from the NetBackup database immediately. The deleted asset remains in the NetBackup database for 30 days.

The following table describes the features of NetBackup for SaaS:

Table 23-1 Features of NetBackup for SaaS

Features	Description
Integration with NetBackup role-based access control (RBAC)	The NetBackup web UI provides RBAC roles, which enable its users to view assets in SaaS workload. The user does not need to be a NetBackup administrator to add a NetBackup SaaS Protection Hub or view assets in the Hub.
NetBackup SaaS Protection-specific credentials	NetBackup SaaS Protection service accounts are used to authenticate the Hubs.
Autodiscovery of assets	NetBackup automatically discovers StorSites, Stors, and Services in the Hubs. You can also perform manual discovery. After the assets are discovered, you can view assets details.
Cross Launch	<p>You can cross launch the NetBackup SaaS Protection web UI.</p> <p>If SSO is configured the user is redirected to the NetBackup SaaS Protection UI without entering the credentials for each login.</p>

About NetBackup SaaS Protection

NetBackup SaaS Protection is a cloud-based data protection solution that is deployed on Microsoft Azure. It is used to protect the data of the on-premises application and SaaS applications.

NetBackup SaaS Protection protects data of the following SaaS applications:

- Box
- Exchange
- Google Drive
- SharePoint sites
- OneDrive sites
- Teams sites and chats
- Slack

NetBackup SaaS Protection supports bulk or granular data restore at the required locations. It also supports restore of the last updated data or any specific point-in-time data.

An account is configured for a customer, which is referred to as a tenant. The assets are configured for the tenant to protect the required data.

For more information, refer to the NetBackup SaaS Protection administrator's guide.

Adding NetBackup SaaS Protection Hubs

You can add NetBackup SaaS Protection Hubs and autodiscover all the assets inside the Hub.

To add NetBackup SaaS Protection Hubs

- 1 On the left, click **Workloads > SaaS**.
- 2 On the **Hubs** tab, click **Add**.
- 3 On the **Add a NetBackup SaaS Protection Hub** page, enter the name of the Hub.
 - To use the existing credential, click **Select existing credentials**.
On the next page, select the required credentials, and click **Select**.
 - To create a new credential, click **Add a new credential**.
On the **Add credential** page, enter the following:
 - **Credentials name**: Enter a name for the credential.
 - **Tag**: Enter a tag to associate with the credential.
 - **Description**: Enter a description of the credential.
 - **Username**: Enter the username, which is configured as a service account in NetBackup SaaS Protection.

- **Password:** Enter the password.
- 4 Click **Add**.
 After the credentials are successfully validated, the Hub is added and autodiscovery runs to discover available assets in the Hub.
 See [“Configure NetBackup for Single Sign-On \(SSO\)”](#) on page 158.

Configuring the autodiscovery frequency

Autodiscovery keeps a count of the assets in Hubs. NetBackup web UI refreshes Hubs at intervals to get the updates from NetBackup SaaS Protection for any addition or removal of assets. By default, the interval for refresh is 8 hours.

To configure the autodiscovery frequency

- 1 On the left, click **Workloads > SaaS**.
- 2 On the top-right, click **SaaS settings > Autodiscovery**.
- 3 Click **Edit**.
- 4 Enter the number of hours after which NetBackup should run autodiscovery and click **Save**.

Proxy configuration for autodiscovery

To discover SaaS applications of NetBackup SaaS Protection, you are required to connect the primary server to the NetBackup SaaS Protection server. Direct internet traffic from the primary server must be open, otherwise the discovery fails. To allow discovery of NetBackup SaaS Protection assets, configure a proxy server to reroute the traffic. The discovery plug-in supports proxy server types HTTP and SOCKS.

Configuring the proxy setting on primary server using the bpsetconfig utility

To configure the proxy setting on primary server using the bpsetconfig utility

- 1 Open a command prompt in primary server.
- 2 Change the directory to the following path:
 - For Windows: **C:\Program Files\Veritas\NetBackup\bin\ admincmd**

- For Linux: `/usr/opensv/netbackup/bin/admincmd/`

3 Execute the `bpsetconfig` command and provide the following proxy details.

```
bpsetconfig> SAAS_PROXY_HOST = X.X.X.X
bpsetconfig> SAAS_PROXY_PORT = 3128
bpsetconfig> SAAS_PROXY_TYPE = HTTP
bpsetconfig> SAAS_PROXY_TUNELLING = 1
```

The following are the proxy configuration keys:

Table 23-2 Proxy configuration keys

Proxy configuration keys	Supported values
SAAS_PROXY_TYPE	HTTP, SOCKS, SOCKS4, SOCKS4A, SOCKS5
SAAS_PROXY_HOST	IP address or FQDN of the proxy host
SAAS_PROXY_TUNNELING	0 or 1
SAAS_PROXY_PORT	Any valid port (1- 65535). The default port is 3128.

Viewing asset details

The NetBackup SaaS Protection assets are displayed in two tabs, **Services** tab and **Hubs** tab.

To view asset details

1 On the left, click **Workloads > SaaS**.

The **Services** tab is displayed. It displays the services configured for the Hub.

You can perform the following actions on the tab:

- View the list of services configured for the Hub.
- Search the required service in the list of services.
- Filter the list of services based on the status of the services.
- Sort columns.
- View the following service details:
 - Application type for which the service is configured.
 - Date and time of the last backup and the next scheduled backup.

- Criteria set for write, stub, and delete policy.
- WORM details.

2 Click the **Hubs** tab to view details on Hubs, StorSites, and Stors.

You can navigate to the required asset using the left panel. You can perform the following actions on the **Hubs** tab:

- View a list of the Hubs.
- Search for a Hub in the list.
- Add new Hubs.
- Validate the credentials.
- Sort columns.
- Click **Actions** to perform the following:
 - Edit credentials.
 - Delete the Hub.
 - Manually discover assets in the Hub.
- View the following asset details:
 - Associated Stors, last backup details, and so on for the Services.
 - Version, ID, and state of the Hub.
 - State, tier details, and so on for the StorSite.
 - State, policy details, and so on for the Stors.
 - Launch the NetBackup SaaS Protection web UI. You can cross launch the NetBackup SaaS Protection web UI from Services, Stors, and Hubs page.

For more information, refer to the NetBackup SaaS Protection administrator's guide.

Configuring permissions

Using the NetBackup web UI, you can assign different access privileges to the user roles on the assets. For example, view, update, delete, and manage access.

See [“Manage access permission”](#) on page 186.

Note: The user with access permission on the SaaS workload in NetBackup, and no or limited permissions in NetBackup SaaS Protection can still view the NetBackup SaaS Protection assets on the NetBackup web UI.

Troubleshooting SaaS workload issues

Check the following locations for logs of the SaaS workload:

- PiSaaS
 - Windows: <install path>\Veritas\NetBackup\logs\ncfnbcs
 - UNIX: <install path>/openv/netbackup/logs/ncfnbcs
- bpVMUtil
 - Windows: <install path>\Veritas\NetBackup\logs\bpVMutil
 - UNIX: <install path>/openv/netbackup/logs/bpVMutil
- APIs/nbWebServices
 - Windows: <install path>\Veritas\NetBackup\logs\nbweb service
 - UNIX: <install path>/openv/logs/nbweb service

Use the following information to troubleshoot issues.

Table 23-3 Troubleshooting issues in SaaS Workload

Problems	Recommended actions
Failed to add a Hub due to incorrect Hub name or invalid user credentials.	Enter appropriate Hub name and valid credentials.
Failed to add a Hub due to issue in credential validation.	Check if the credentials are not expired. Also check if the credentials are valid.
Failed to add a Hub due to limited permissions.	Assign appropriate permissions to the user on the SaaS workload. See “Role permissions” on page 185.
Failed to delete a Hub due to limited permissions.	Assign appropriate permissions to the user on the SaaS workload. See “Role permissions” on page 185.

Table 23-3 Troubleshooting issues in SaaS Workload (*continued*)

Problems	Recommended actions
Failed to perform discovery on the Hub due to limited permissions.	Assign appropriate permissions to the user on the SaaS workload. See “Role permissions” on page 185.
The services are not deleted from NetBackup after deleted the associated Connector from NetBackup SaaS Protection.	The services get removed from NetBackup after 30 days from Connector deletion.
Failed to launch the NetBackup SaaS Protection web UI using the Launch NSP option. Credentials are required while launching the NetBackup SaaS Protection web UI.	Check if SSO is configured correctly. If SSO is configured correctly, check if the user has appropriate permissions to access the NetBackup SaaS Protection web UI. See “Configure NetBackup for Single Sign-On (SSO)” on page 158.
Connecting to the proxy host X.X.X.X on port 3128 with type SOCKS5	Configure proxy settings on the primary server using the bpsetconfig utility.

NetBackup Flex Scale

This chapter includes the following topics:

- [Managing NetBackup Flex Scale](#)

Managing NetBackup Flex Scale

The Flex Scale appliance administrator (**appadmin**) can monitor and manage their cluster nodes and disks from the Flex Scale infrastructure page in the NetBackup web UI. The **appadmin** has the **Default Security Administrator** role for the NetBackup web UI and can also manage all of NetBackup.

For full instructions on managing NetBackup Flex Scale, see the following resources.

NetBackup Flex Scale Installation and Configuration Guide

NetBackup Flex Scale Administrator's Guide

Table 24-1 Accessing Flex Scale and NetBackup

Interface and URL	Access to Flex Scale or NetBackup
NetBackup web UI https://primaryserver/webui/login	To open Flex Scale, click the Appliance management node. This action opens the NetBackup Flex Scale infrastructure management console in a new browser tab. See “Access NetBackup Flex Scale from the NetBackup web UI” on page 229.
Flex Scale infrastructure management console IPv4: https://ManagementServerIPorFQDN:14161/ IPv6: https://ManagementServerIP:14161/	To open NetBackup, click the NetBackup node. This action launches the NetBackup Flex Scale UI in the same browser tab. To access the Flex Scale infrastructure management console again, click Cluster Monitor > Infrastructure and then Cluster Dashboard . See “Access NetBackup from the Flex Scale infrastructure management console” on page 230.

Table 24-1 Accessing Flex Scale and NetBackup (*continued*)

Interface and URL	Access to Flex Scale or NetBackup
Flex Scale UI https://ManagementServerIPorFQDN	<p>To view the Flex Scale infrastructure, on the left click Cluster Monitor > Infrastructure.</p> <p>From that page you can also open the Flex Scale UI infrastructure management console. Click Cluster Dashboard at the top right.</p> <p>See “Manage NetBackup and the Flex Scale cluster infrastructure from the Flex Scale UI” on page 231.</p>

Access NetBackup Flex Scale from the NetBackup web UI

You can open Flex Scale from the NetBackup web UI when you click on the **Appliance management** node.

The screenshot shows the Veritas NetBackup web UI. The left sidebar contains the following menu items: Dashboard, Activity monitor, Recovery, Protection, Workloads, Storage, Catalog, Detection and reporting, Credential management, Hosts, Bare Metal Restore, **Appliance management** (highlighted with a red box), Resiliency, and Security. The main dashboard area displays the following sections:

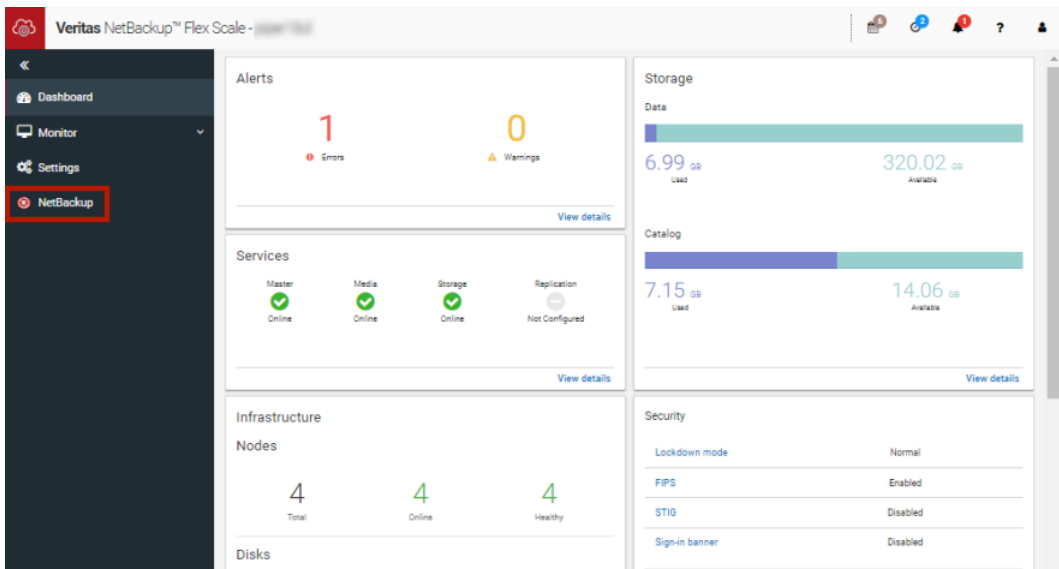
- JOBS** (Last 72 hours): 0 Active, 0 Queued, 2 Failed, 78 Success, 0 Partial success, 1 Retries.
- MALWARE DETECTION** (Last 24 hours): 0 Impacted, 0 Not impacted, 0 Pending, 0 In progress, 0 Failed.
- ANOMALY DETECTION** (Last 24 hours): 0 Not reviewed, 0 High severity, 0 Medium severity, 0 Low severity.
- CERTIFICATES** (NetBackup/External): 6 All, 0 Revoked, 6 Valid, 0 Expired.
- TOKENS**: 0 All, 0 Not valid, 0 Valid.
- Veritas™ NetInsights Console** (bottom left): A widget showing a line graph and a pie chart.
- SECURITY EVENTS** (bottom right): A log of events including authentication successes and failures for 'admin_user' on Jan 21, Jan 20, and Jan 19.

To access Flex Scale from the NetBackup web UI

- 1 In a web browser, enter the URL for the NetBackup web UI.
 The primaryserver is the host name or IP address of the NetBackup primary server that you want to sign in to.
 See [“Sign in to the NetBackup web UI”](#) on page 18.
- 2 Enter the credentials for the **appadmin** user and click **Sign in**.
- 3 On the left, click **Appliance management**.
 In a new browser window, the NetBackup Flex Scale infrastructure management console opens.

Access NetBackup from the Flex Scale infrastructure management console

You can open NetBackup from the Flex Scale infrastructure management console when you click on the **NetBackup** node.



To access NetBackup from the Flex Scale infrastructure management console

- 1 In a web browser, enter the URL for the Flex Scale infrastructure management console.

`https://ManagementServer/IPorFQDN:14161/`

The *ManagementServer/IP* is the public IP address or FQDN that you specified for the NetBackup Flex Scale management server.

- 2 Enter the credentials for the **appadmin** user and click **Sign in**.
- 3 On the left, click **NetBackup**.

This action launches the Flex Scale web UI in the same browser tab, where you can manage both NetBackup and Flex Scale.

Manage NetBackup and the Flex Scale cluster infrastructure from the Flex Scale UI

You can manage both NetBackup and the Flex Scale infrastructure management from the Flex Scale UI.

Veritas NetBackup™ Flex Scale

Cluster dashboard

Console IP
Console node
Cluster ID

560.00 GB
Total Storage

Nodes
4 4 0 4
Total Healthy Unhealthy Online

Disks
56 56 0 56
Total Healthy Unhealthy Online

VCIDRAVMware-42352f602e08e6...

Nodes

Status	Name	Node serial numb	Health	Product version	Management IP (CPU utilization	Memory utilizatio
Online	pipe16cl-03	VMware-423598ae010...	Healthy	3.0		20.87%	14.67%
Online	pipe16cl-04	VMware-42358e3c948...	Healthy	3.0		46.82%	14.63%
Online	pipe16cl-01	VMware-423568cbcca...	Healthy	3.0		77.41%	17.18%
Online	pipe16cl-02	VMware-42352f602e0...	Healthy	3.0		61.13%	27.73%

Items per page: 5

Discovered nodes

No new nodes.
No new nodes have been discovered.

Scan for nodes

To manage NetBackup and Flex Scale cluster infrastructure from the Flex Scale UI

- 1** In a web browser, enter the URL for the Flex Scale UI.

`https://ManagementServerIPorFQDN`

The *ManagementServerIPorFQDN* is the host name or IP address of the NetBackup Flex Scale server that you want to sign in to.

- 2** Enter the credentials for the **appadmin** user and click **Sign in**.

The web UI displays both NetBackup functionality and the Flex Scale infrastructure.

To view the cluster infrastructure, click **Cluster Monitor > Infrastructure**.

To open the Flex Scale management console, from the Infrastructure page, click **Cluster Dashboard** at the top right.

NetBackup workloads

This chapter includes the following topics:

- [Protection of other asset types and clients](#)

Protection of other asset types and clients

The NetBackup web UI protects assets like databases, virtual machines, and clients through either protection plans or policies. Some workloads support both protection plans and policies. For more information on performing backups and restores, refer to the associated guide for that workload or agent. Protection of **Standard** and **MS-Windows** clients are covered in the *NetBackup Administrator's Guide, Volume I*.

Disaster recovery and troubleshooting

- [Chapter 26. Managing Resiliency Platforms](#)
- [Chapter 27. Managing Bare Metal Restore \(BMR\)](#)
- [Chapter 28. Troubleshooting the NetBackup Web UI](#)

Managing Resiliency Platforms

This chapter includes the following topics:

- [About Resiliency Platform in NetBackup](#)
- [Understanding the terms](#)
- [Configuring a Resiliency Platform](#)
- [Troubleshooting NetBackup and Resiliency Platform issues](#)

About Resiliency Platform in NetBackup

You can integrate NetBackup and Veritas Resiliency Platform to manage your disaster recovery operations. Veritas Resiliency Platform provides a single console from which you can proactively maintain business uptime across private, public, and hybrid clouds. Integrating NetBackup and Resiliency Platform lets you leverage the capabilities, such as complete automation, visualizing and monitoring DR specific information for all resiliency operations for the virtual machines in your data center.

Note the following points:

- You can integrate more than one Resiliency Platform with your NetBackup primary server.
- You can have more than one data centers for a Resiliency Platform.
- You can use Resiliency Platform with Veritas Resiliency Platform version 3.5 and later in NetBackup.
- After you add a Resiliency Platform, the assets are automatically discovered and displayed on the **Virtual machines** tab.

- You can view detailed information alerts and error messages in the **Notifications** section.

Understanding the terms

The following table explains the key components related to Veritas Resiliency Platform and NetBackup integration.

Term	Description
Resiliency Platform	The Veritas Resiliency Platform integrated with your NetBackup primary server. The Resiliency Manager provides the services required for protecting assets, such as virtual machines, within a resiliency domain. It also provides workload automation services.
Resiliency manager	The component that provides resiliency capabilities within a resiliency domain. It is composed of loosely coupled services, a distributed data repository, and a management console.
Infrastructure management server (IMS)	The component that discovers, monitors, and manages the asset infrastructure within a data center. The IMS transmits information about the asset infrastructure to the Resiliency Manager. The IMS is deployed as a virtual appliance. To achieve scale, multiple IMSs can be deployed in the same data center.
Data center	The location that contains source data center and a target data center. Each data center has one or more IMSs.
Resiliency group	The unit of management and control in Resiliency Platform. You organize related assets into a resiliency group and manage and monitor them as a single entity.
Automated virtual machines	The assets that are a part of a resiliency group and you can perform actions, such as migrate, recover, and rehearsal.
Recovery readiness	Measured based on migrate, recover or rehearsal operations. <ul style="list-style-type: none">■ Low - If no operations are performed or failed.■ High - If at least one operation is performed successfully in the past 7 days.■ Medium - If the recovery readiness does not fall in either high or low category.

Term	Description
Recovery Point Object (RPO)	<p>Recovery Point Objective is the point in time you can recover to in the event of a disaster.</p> <p>For example, if you have an RPO of 4 hours on your critical virtual machines then you lose 4 hours of data, as 4 hours ago is the last point in time to which you can recover data on your VMs.</p>

Configuring a Resiliency Platform

You can add, edit, delete, or refresh a Resiliency Platform. You can add more than one Resiliency Platform in NetBackup.

Add a Resiliency Platform

You can add one or more than one Resiliency Platforms in NetBackup. The Resiliency Platform lets you add virtual machines and automate protection. If the resiliency manager is using a third-party certificate, see the [NetBackup Web UI Administrator's Guide](#).

To add a Resiliency Platform

- 1 On the left, click **Resiliency**.
- 2 Click the **Resiliency Platform** tab.
- 3 Click **Add Resiliency Platform**.
- 4 Read the instructions on the **Add Resiliency Platform** dialog box and click **Next**.
- 5 In the **Add credentials** dialog box, enter a value in the following fields and click **Next**:
 - **Resiliency manager host name or IP address**
 - **Resiliency Platform API access key**
 - **NetBackup API access key**
- 6 In the **Add data center and Infrastructure management** server dialog box, select a data center.
- 7 In the **Infrastructure management server** section, select a preferred server.
- 8 Click **Add**.

After you add the Resiliency Platform in NetBackup, the NetBackup primary server will be configured automatically in the Resiliency Platform.

Note: If the NetBackup has FIPS mode enabled and you need to fetch the respective certificates, refer *Integrating with NetBackup* topic in *Resiliency Platform* product documentation. You need to install Resiliency Platform certificates in FIPS trust store and then add the Resiliency Platform. (Only done when NetBackup has FIPS mode enabled)

Configure a third-party CA certificate

You can use a self-signed or a third-party certificate to validate your Resiliency manager.

Consider the following points:

- For Windows, you can give a certificate as a file path or install the third-party certificate in the Trusted root certificates authorities.
- To switch from a self-signed certificate to a third-party certificate for an already added Resiliency Platform, you can edit the Resiliency Platform.

To configure a third-party CA certificate

- 1 Copy a PKCS #7 or P7B file having certificates of the trusted root certificates authorities that are bundled together. This file may either be PEM or DER encoded.
- 2 Create a CA file containing the PEM encoded certificates of the trusted root certificate authorities that are concatenated together.
- 3 In the `bp.conf` file, create the following entries, where `/certificate.pem` is the file name:
 - `ECA_TRUST_STORE_PATH = /certificate.pem`
 - Verify that the `nbwebsvc` account has the permissions to access the path that `ECA_TRUST_STORE_PATH` refers.

Edit or delete a Resiliency Platform

After you add a Resiliency Platform, you can edit the Resiliency Platform and NetBackup API access keys. You cannot change or update the Resiliency manager host name or IP address. However, you can delete the Resiliency Platform and add it to NetBackup again. If you refresh the Resiliency Platform, the discovery of assets on the Resiliency Platform is triggered.

To edit a Resiliency Platform

- 1 On the left, click **Resiliency**.
- 2 Click the **Resiliency Platform** tab.

- 3 Click the **Actions** menu for the Resiliency Platform that you want to edit and select **Edit**.
- 4 Enter the updated **Resiliency Platform API access key** and **NetBackup API access key**.
- 5 Click **Next**.
- 6 In the **Edit data center and Infrastructure management server** dialog box, select the **Data center** and then select the preferred infrastructure management server.
- 7 Click **Save**.
- 8 To delete a Resiliency Platform, from the **Actions** menu, select **Delete**.

View the automated or not-automated VMs

The virtual machines that belong to a resiliency group in Veritas Resiliency Platform are discovered and displayed on the **Automated** tab and the VMs that don't belong any resiliency group are displayed on the **Not automated** tab. You can view the status of the assets and perform various actions. You can search for a VM or apply filters too.

The following table lists the columns displayed on the **Automated** and **Not automated** tabs:

Table 26-1

Tab	Column	Description
<ul style="list-style-type: none"> ■ Automated ■ Not automated 	Name	Name of the virtual machine.
<ul style="list-style-type: none"> ■ Automated 	RPO	<p>Recovery Point Objective is the point in time you can recover to in the event of a disaster.</p> <p>For example, if you have an RPO of 4 hours on your critical virtual machines then you lose 4 hours of data, as 4 hours ago is the last point in time to which you can recover data on your VMs.</p>
<ul style="list-style-type: none"> ■ Automated ■ Not automated 	State	Whether the VM is switched on or off.

Table 26-1 (continued)

Tab	Column	Description
<ul style="list-style-type: none"> Automated 	Recovery readiness	<p>Measured based on migrate, recover or rehearsal operations.</p> <ul style="list-style-type: none"> Low - If no operations are performed or failed. High - If at least one operation is performed successfully in the past 7 days. Medium - If the recovery readiness does not fall in either high or low category.
<ul style="list-style-type: none"> Automated Not automated 	Platform	The platform that the VM belongs to.
<ul style="list-style-type: none"> Automated Not automated 	Server	The server name of the VM.
<ul style="list-style-type: none"> Automated 	Protection	Protection status of the VM.
<ul style="list-style-type: none"> Automated 	Resiliency group	Name of the resiliency group to which the VM belongs.
<ul style="list-style-type: none"> Not automated 	Recovery action	Launch the Resiliency Platform to add the VM to a resiliency group.

To view and perform actions on automated VMs

- 1 On the left, click **Resiliency**.
- 2 On the **Virtual machines** tab, click **Automated**.
- 3 To view more details about a VM, in the **Name** column, click a VM.
- 4 To view all VMs that are a part of the same resiliency group, click the preferred resiliency group.

- 5 To perform disaster recovery operation, such as rehearse, restore, or recover, click **Launch Resiliency Platform**.

To enable single-sign, same authentication domain must be configured NetBackup and Veritas Resiliency Platform. If not configured, you must login with username and password to access Veritas Resiliency Platform web console.
- 6 Log on to your Resiliency Platform and perform the preferred action. See the *Veritas Resiliency Platform User Guide*.

To view and perform actions on not automated VMs

- 1 On the left, click **Resiliency**.
- 2 On the **Virtual machines** tab, click **Not automated**.
- 3 To add the VM to a resiliency group, in the **Recovery action** column, click **Automate Recovery**.
- 4 Perform the preferred action for your Resiliency Platform. See, the *Veritas Resiliency Platform User Guide*.

Troubleshooting NetBackup and Resiliency Platform issues

Use the following information to troubleshoot issues.

Table 26-2 Troubleshooting issues

Issue	Action
Failed to configure the current NetBackup primary server with the Resiliency Platform.	<div>Check the logs at the following location in Veritas Resiliency Platform's Resiliency manager:</div> <div><ul style="list-style-type: none">■ /var/opt/VRTSitrp/logs/copydata-service.log■ /var/opt/VRTSitrp/logs/api-service.log</div>
Failed to establish a persistent connection between the current NetBackup primary server and the Resiliency Platform.	<div><ul style="list-style-type: none">■ Verify that the logged in user has permissions in credentials namespace.■ Check the logs at the following location on the NetBackup primary server:<ul style="list-style-type: none">■ /usr/openv/logs/nbweb service/ in NetBackup installation directory■ C:\Program Files\Veritas\NetBackup\logs\nbweb service in NetBackup windows</div>

Table 26-2 Troubleshooting issues (*continued*)

Issue	Action
Failed to launch the Veritas Resiliency Platform	Verify that same authentication domain is used to configure Veritas Resiliency Platform and NetBackup.

Managing Bare Metal Restore (BMR)

This chapter includes the following topics:

- [About Bare Metal Restore \(BMR\)](#)
- [Add a custom role for a Bare Metal Restore \(BMR\) administrator](#)

About Bare Metal Restore (BMR)

NetBackup Bare Metal Restore (BMR) is the server recovery option of NetBackup. BMR automates and streamlines the server recovery process so you do not have to reinstall the operating systems or configure the hardware manually. BMR restores the operating system, the system configuration, and all the system files and the data files with the following steps.

For complete information on BMR, refer to the [NetBackup Bare Metal Restore Administrator's Guide](#).

In the NetBackup web UI, you can perform the following BMR operations:

- View and manage the clients that are backed up for VM conversion.
- Convert BMR-enabled backups to a virtual machine using the Virtual Machine Conversion wizard.
- Create point-in-time restore configurations.
- View and manage VM conversion tasks.
- View and manage the BMR clients and configurations.
- Run pre-restore operations on the client configuration and the VM conversion client's configurations. For example, prepare-to-restore, prepare-to-discover, and dissimilar disk restore operations.

- View and manage boot servers.
- View and manage resources like shared resource trees, discovered configurations, and Windows device driver packages.
- View and manage BMR restore or discover tasks.
- View and manage the BMR clients and configurations.
- Run pre-restore operations on the client configuration and the VM conversion client's configurations. For example, prepare-to-restore, prepare-to-discover, and dissimilar disk restore operations.
- View and manage boot servers.
- View and manage resources like shared resource trees, discovered configurations, and Windows device driver packages.
- View and manage BMR restore or discover tasks.

Add a custom role for a Bare Metal Restore (BMR) administrator

To add a custom RBAC role

- 1 On the left, select **Security > RBAC** and click **Add**.
- 2 Select **Custom role** to manually configure all the permissions for the role.
- 3 Provide a **Role name** and a description.
 For example, you may want to indicate that the role is for any users that are BMR administrators.
- 4 On the **Global** tab, expand the **BMR** section and select all the permissions for **BMR**.

Boot servers	View, Delete
Clients	View, Create, Update, Delete, Pre restore
VM conversion	View, Delete, VM conversion

- 5 Expand the **NetBackup management** section.
 - Locate the **NetBackup hosts** group.
 - Select the following permissions:

NetBackup hosts	View, Update
-----------------	--------------

- Locate the **NetBackup backup images** group.
- Select the following permissions:

NetBackup backup images	Image Requests > View
-------------------------	-----------------------

NetBackup backup images	View
-------------------------	------

6 For ESXi servers, additional permissions are needed for **Host properties**.

- On the **Global** tab, expand the **NetBackup management** section.
- Select the following permissions:

Access hosts	View, Create, Update, Delete
--------------	------------------------------

7 On the **Assets** tab, select the following permissions.

VMware assets	View, Update, View restore targets
---------------	------------------------------------

8 Click **Assign**.

9 Under **Workloads**, click **Assign**.

Select the VMware assets that you want the role to have access to.

- To give the role access to all VMware assets and future assets that you add, select **Apply selected permissions to all existing and future VMware assets**.
- To select individual assets, deselect **Apply selected permissions to all existing and future VMware assets** and click **Add**.
 For example, you can select one or more: datastores, datastore clusters, ESXi servers, ESXi clusters, resource pools, vApps.

10 When you have added all the assets, click **Assign**.

11 On the **Users** card, click **Assign**. Then add each user that you want to have access to this custom role.

12 When you are done configuring the role, click **Save**.

Troubleshooting the NetBackup Web UI

This chapter includes the following topics:

- [Tips for accessing the NetBackup web UI](#)
- [If a user doesn't have the correct permissions or access in the NetBackup web UI](#)
- [Unable to validate the user or group when configuring LDAP server](#)

Tips for accessing the NetBackup web UI

When NetBackup is properly configured, a user can access the primary server at the following URL:

`https://primaryserver/webui/login`

If the web UI on a primary server does not display, follow these steps to troubleshoot the issue.

Browser displays an error that the connection was refused or that it cannot connect to the host

Table 28-1 Solutions when the web user interface does not display

Step	Action	Description
Step 1	Check the network connection.	
Step 2	Verify that the firewall is open for port 443.	Refer to the following article: https://www.veritas.com/docs/100042950

Table 28-1 Solutions when the web user interface does not display
(continued)

Step	Action	Description
Step 3	If port 443 is in use, configure another port for the web UI.	Refer to the following article: https://www.veritas.com/docs/100042950
Step 4	Verify that the nbweb service is up.	Check the nbweb service logs for more details.
Step 5	Verify that the vnetd -http_api_tunnel is running.	Verify that the vnetd -http_api_tunnel service is running. For more details, check the vnetd -http_api_tunnel logs with OID 491.
Step 6	Ensure that the external certificate for the NetBackup web server is accessible and has not expired.	<ul style="list-style-type: none"> Use the Java Keytool commands to validate the following file: Windows: <code>install_path\var\global\wsl\credentials\nbweb service.jks</code> UNIX: <code>/usr/openv/var/global/wsl/credentials nbweb service.jks</code> Check whether the nbweb group has a permission to access the nbweb service.jks file. Contact Veritas Technical Support.

Cannot access web UI when you use a custom port

- Restart the vnetd service.
- Follow the steps in [Table 28-1](#).

Certificate warning displays when you try to access the web UI

The certificate warning displays if the NetBackup web server uses a certificate that is issued by a CA that is not trusted by the web browser. (Including the default NetBackup web server certificate that the NetBackup CA issued.)

To resolve a certificate warning from the browser when you access the web UI

- Configure the external certificate for the NetBackup web server.
See [“Configure an external certificate for the NetBackup web server”](#) on page 119.
- If the problem persists, contact Veritas Technical Support.

If a user doesn't have the correct permissions or access in the NetBackup web UI

Note that only administrators, root users, or Enhanced Auditing users automatically have full access to the web UI. Other users must be configured in RBAC to have access and permissions for the web UI.

See [“Configuring RBAC”](#) on page 174.

If a user does not have the correct permissions or cannot access the workload assets that they should have access to, do the following:

- Verify that the user's credentials match the username (or the username and the domain name) that is specified in the user's role.
- Review the roles for the user in **Security > RBAC**. You may need to change the role permissions. However, be aware that those kinds of changes also affect any other users that belong to those roles.
- Any user account changes with the identity provider are not synchronized with the user's roles. If a user account changes with the identity provider, the user may not have the correct permissions or access. The NetBackup security administrator must edit each role for the user to remove the existing user account and re-add the new account.
- Changes to a user's roles are not immediately reflected in the web UI. A user with an active session must sign out and sign in again before any changes take effect.

Unable to validate the user or group when configuring LDAP server

When the administrator configures the LDAP server, they must specify the `-d DomainName` option. `DomainName` can be the LDAP server name or the domain name. Whatever name is specified for `-d DomainName` is the domain name that an administrator should use when they add users to an RBAC role.

If you specify the incorrect domain, you may see the error `Unable to validate the user or group`. Review the following:

- The username and domain name are typed correctly.
- You specified the correct domain name.
 The domain name that you should specify depends on how the LDAP server is configured in NetBackup. Contact your administrator for help with adding users to RBAC.