Veritas NetBackup™ OpsCenter Administrator's Guide

Windows and UNIX

Release 8.1.1

VERITAS™

Veritas NetBackup™ OpsCenter Administrator's Guide

Document version: NetBackup 8.1.1

Legal Notice

Copyright © 2018 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
500 E Middlefield Road
Mountain View, CA 94043

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 Overview of NetBackup OpsCenter 19

About OpsCenter 19
About OpsCenter functions 20
About OpsCenter Analytics functions 20
About monitoring and managing NetBackup and NetBackup appliances 22
About alerting in OpsCenter 22
About reporting in OpsCenter Analytics 22
About OpsCenter components 24
About the OpsCenter Server 24
About the OpsCenter Agent 27
About the OpsCenter OpsCenter View Builder 30
About using the OpsCenter console 30
About starting the OpsCenter console 31
About web browser considerations 31
About accessing the OpsCenter console 34
Logging on to the OpsCenter console as a default admin user 42
Customizing the OpsCenter login page 46
Logging out of the OpsCenter console 46
Configuring the OpsCenter session timeout interval 47
Possible OpsCenter console issues 47
About OpsCenter console components 48
About using the links on the title bar 50
About using tabs and subtabs 51
About refreshing the OpsCenter console 51
Changing the Task pane 52
About the View pane 52
Using the quick links in the Task pane 56
Viewing alerts from the Alert Summary pane 56
Sizing the Content pane 57
About the OpsCenter status bar 59
Status icons and colors in the console 59
About using tables 61
Common tasks in OpsCenter 65
About using Web browser bookmarks 67

About OpsCenter documentation 68

Chapter 2 Installing OpsCenter 70

About planning an OpsCenter installation 70
Software components that OpsCenter uses 71
About the Java Runtime Environment 72
About the OpsCenter licensing model 73
OpsCenter DVDs 76
Managed NetBackup master server considerations 77
About designing your OpsCenter Server 79
Supported upgrade paths in OpsCenter 79
About planning an OpsCenter Agent deployment 80
Preparation for installation or upgrade 82
Installing OpsCenter on Windows and UNIX 87
About installing OpsCenter on Windows 88
About installing OpsCenter on UNIX 94
About installing OpsCenter silently on Windows 97
About OpsCenter upgrade on Windows and UNIX 115
About importing authentication settings during OpsCenter upgrade 116
Upgrading OpsCenter on Windows 121
Upgrading OpsCenter on UNIX 129
About files and folders that are protected during OpsCenter upgrade 131
About OpsCenter upgrade failure scenarios 133
About post-installation tasks 135
Setting up trust between OpsCenter and NBAC-enabled NetBackup or PureDisk 135
Verifying that OpsCenter is running properly 135
About starting to use OpsCenter 136
About the start up tasks that OpsCenter performs 137
About uninstalling OpsCenter on Windows and UNIX 137
Uninstalling OpsCenter on Windows 137
Uninstalling OpsCenter on UNIX 138
About clustering OpsCenter 139
About OpsCenter clusters 139
Supported platforms for cluster solutions 140
About running commands on the active node 141
Connecting Authentication Service and Veritas Private Branch Exchange 141
Clustering OpsCenter on Windows 143
Uninstalling OpsCenter from the Windows cluster 151

Chapter 3 OpsCenter Getting Started feature 153

About the OpsCenter Getting Started feature 153
OpsCenter user roles 155
Learn more about adding NetBackup Master Servers 157
Learn more about OpsCenter Views 157
Add Users 158
Edit User 159
Reset password 160
Add NetBackup Master Server 160
Add OpsCenter Agent 161
Add OpsCenter Views/Groups 161
Configure SMTP Server 162

Chapter 4 Administering OpsCenter 163

About the services and processes used by OpsCenter 163
Services used by OpsCenter on Windows 164
Controlling the OpsCenter services 164
Processes used by OpsCenter on UNIX 165
OpsCenter server scripts on Windows and UNIX 166
Commands to control OpsCenter services and processes 168
About dependency of services 169
About nbproxy processes on NetBackup master servers 170
About OpsCenter database administration 171
OpsCenter database commands 171
Moving the OpsCenter database and database logs to a different hard disk 174
Moving OpsCenter server to a different computer 178
About database troubleshooting 183
About backup and restore of OpsCenter and OpsCenter Analytics 184
Backing up OpsCenter in case of a disaster 184
Restoring OpsCenter 186
About communication ports and firewall considerations in OpsCenter 188
Communication ports used by key OpsCenter components 189
Ports required to communicate with backup products 191
Web browser to launch OpsCenter user interface 192
About OpsCenter user interface and OpsCenter server software communication 192
About OpsCenter server to NetBackup master server (NBSL) communication 192
About SNMP traps 193

About communication between OpsCenter and Sybase database ... 193
About email communication in OpsCenter ... 193
Gathering troubleshooting data with the support script ... 193
About OpsCenter log files ... 197
VxUL log files ... 197
OpsCenter application log files ... 199
About OpsCenter log files on Windows servers ... 200
About OpsCenter log files on UNIX servers ... 202

Chapter 5 Understanding OpsCenter settings ... 205

OpsCenter settings ... 206
Setting user preferences ... 207
Settings > User Preferences options ... 208
Changing your OpsCenter password ... 211
About managing licenses ... 212
Settings > Configuration > License options ... 212
Adding OpsCenter license keys ... 213
Viewing OpsCenter license keys ... 213
Deleting OpsCenter license keys ... 214
Configuring the data purge period on the OpsCenter Server ... 214
Settings > Configuration > Data Purge options ... 214
About storing the SMTP Server configurations in OpsCenter ... 216
Configuring SMTP server settings for OpsCenter ... 216
Settings > Configuration > SMTP server options ... 217
Adding host aliases in OpsCenter ... 218
Settings > Configuration > Host Alias options ... 218
Merging objects (hosts) in OpsCenter ... 219
Settings > Configuration > Object Merger options ... 220
Modifying tape library information in OpsCenter ... 220
Settings > Configuration > Tape Library options ... 221
Copying a user profile in OpsCenter ... 221
Settings > Configuration > Copy User Profile options ... 222
Setting report export location in OpsCenter ... 222
Settings > Configuration > Report Export Location options ... 223
About managing Object Types in OpsCenter ... 223
Settings > Configuration > Object Type options ... 223
Adding object types in OpsCenter ... 224
Deleting object types in OpsCenter ... 224
Modifying object types in OpsCenter ... 225
Adding attributes to object types in OpsCenter ... 225
Deleting attributes from object types in OpsCenter ... 225

About managing OpsCenter users 226
About managing user password 226
About adding AD / LDAP user groups in OpsCenter 227
Settings > Users > Users options 229
User access rights and functions in OpsCenter user interface ...
2 3 1
Viewing OpsCenter user account information 235
Adding new users to OpsCenter 236
Editing OpsCenter user information 238
Resetting an OpsCenter user password 238
Resetting password of the OpsCenter Security Admin 239
Deleting OpsCenter users 240
Viewing OpsCenter user groups 241
Settings > Users > User Groups options 241
Adding OpsCenter user groups 241
Editing OpsCenter user groups 242
Deleting OpsCenter user groups 242
About managing recipients in OpsCenter 242
Viewing email recipients in OpsCenter 243
Settings > Recipients > Email options 243
Viewing SNMP trap recipients in OpsCenter 244
Settings > Recipients > SNMP trap recipient options 244
Creating OpsCenter email recipients 245
Settings > Recipients > Email > Add Email Recipient options 245
Creating OpsCenter SNMP trap recipients 246
Settings > Recipients > SNMP > Add SNMP trap recipient options
..... 247
Modifying OpsCenter Email or SNMP recipient information 248
Deleting OpsCenter Email or SNMP trap recipient 248
About managing cost analysis and chargeback for OpsCenter Analytics
..... 249
Setting the default currency for OpsCenter cost reports 249
Settings > Chargeback > Currency Settings options 250
Editing the OpsCenter global currency list 250
Settings > Chargeback > Currency Settings > Edit Currency List
options 251
Settings > Chargeback > Cost Variable options 251
Creating cost variables in OpsCenter 252
Modifying cost variables in OpsCenter 254
Deleting cost variables in OpsCenter 254
Settings > Chargeback > Cost Formulae options 255
Creating cost formulae in OpsCenter 255
Modifying cost formulae in OpsCenter 255

Deleting a cost formulae in OpsCenter 256
Estimating chargeback costs using the OpsCenter Formula Modeling Tool 256
Settings > Chargeback > Cost Estimation options 257

Chapter 6 Understanding data collection 259

About data collection in OpsCenter 259
About OpsCenter Agents 260
About OpsCenter Agent logs 260
OpsCenter Data Collector types 260
About managing OpsCenter Agents 264
Settings > Configuration > Agent options 264
Viewing OpsCenter Agent status 265
Configuring an OpsCenter Agent 265
Settings > Configuration > Agent > Create Agent or Edit Agent options 265
Modifying an OpsCenter Agent 266
Deleting OpsCenter Agents 266
About managing OpsCenter Data Collectors 267
Viewing OpsCenter Data Collector status 267
Configuring an OpsCenter Data Collector 268
Data Collector Wizard settings 269
Modifying an OpsCenter Data Collector configuration 270
Deleting OpsCenter Data Collectors 271
About configuring data collection for NetBackup 271
Settings > Configuration > NetBackup options 273
NetBackup data collection view 274
How OpsCenter collects data from NetBackup 275
About the Breakup Jobs option 276
Viewing master server details and data collection status 281
Adding a master server or appliance in OpsCenter 285
Adding a NetBackup master server 286
Configuring a master server or appliance master server for server access and data collection by OpsCenter 288
Settings > Configuration > NetBackup > Add Master Server options 290
Adding a master server or an appliance master server in the OpsCenter console 291
Editing a master server or an appliance master server in OpsCenter 292
Deleting a master server or an appliance master server in OpsCenter 292

Controlling data collection for a master server in OpsCenter 293
Configuring Backup Exec data collector 293
Collecting data from PureDisk 295
Setting up a trust between the PureDisk SPA host and the OpsCenter OpsCenter host 296
Configuring PureDisk data collector 297

Chapter 7 Managing OpsCenter views 299

About OpsCenter views 299
Settings > Views options 300
OpsCenter view types 302
OpsCenter user interface access for specific view types 303
About access rights for a view 304
About OpsCenter view levels 305
About nodes and objects 306
About managing OpsCenter views 306
Settings > Views > Manage Nodes and Objects options 307
Looking at OpsCenter views and their details 307
Creating OpsCenter views 307
Modifying OpsCenter views 308
Deleting OpsCenter views 309
Modifying alias view levels in OpsCenter 309
About managing nodes and objects in OpsCenter 310
Adding nodes to a view in OpsCenter 311
Modifying node details in OpsCenter 311
Deleting nodes in OpsCenter 312
Adding objects to a view node in OpsCenter 312
Deleting objects from a view node in OpsCenter 313
View filters in OpsCenter 314
Creating a view object filter in OpsCenter 314
Modifying view object filters in OpsCenter 315
Deleting view object filters in OpsCenter 316
Setting up logging for OpsCenter View Builder 316

Chapter 8 Monitoring NetBackup using OpsCenter 318

About the Monitor views 320
Controlling the scope of Monitor views 320
About time frame selection 321
About monitoring NetBackup using the Overview tab 322
Viewing the Job Summary by State 323
Viewing the Media Summary by Status 323
About Top 7 Job Error Log Summary 324

Viewing the Services Summary 325
Viewing the Master Server Summary 325
Viewing the Job Summary by Job Status 326
Viewing the Drive Summary by Status 327
Top 7 Policies by Failed Jobs 328
Viewing the Alert Summary by Severity 328
About monitoring NetBackup jobs 329
Monitor > Jobs List View options 329
About monitoring jobs using the List View 332
Viewing the details for a single NetBackup job 332
Viewing the details for a master server associated with a job 333
Viewing policy information for a job 333
Filtering on NetBackup job type and state 334
Controlling NetBackup jobs 335
Reconciling NetBackup jobs 335
Changing the job priority 336
Change Job Priority dialog box options 337
Exporting NetBackup job logs 337
About using the Summary View for monitoring jobs 338
Viewing the Job Summary by Job Status 338
Viewing the Job Summary by State 339
Viewing the Job Summary by Type 340
About the Group Component Summary table 341
About using the Hierarchical View for monitoring jobs 343
Viewing the details for a single NetBackup job 344
Viewing the details for a master server associated with a job 345
Viewing policy information for a job 345
Filtering on NetBackup job state 346
Monitor > Services view 347
Filtering on NetBackup service type 348
Controlling NetBackup services 348
About monitoring NetBackup policies 349
Monitor > Policies List View 350
About using the List View to monitor NetBackup policies 352
Filtering on NetBackup policy type 353
Monitor > Policies page 354
Viewing details for a single NetBackup policy 354
Viewing the details for a master server associated with a policy 355
Viewing the details for a volume pool associated with a policy 355
Activating or deactivating a job policy 355
Starting a manual backup 356

Viewing the history for a single job policy 356
Monitor > Policies Summary View 357
About Top 5 Policies by Data Backed up 357
About Top 7 Policies by Failed Jobs 357
About Top 7 Policies by No. of Jobs 358
About monitoring NetBackup media 358
Monitor > Media List View options 359
About using the List View to monitor NetBackup media 362
Viewing the details for NetBackup media 362
Viewing the details for a master server associated with the media 362
Filtering on NetBackup media type 363
Controlling media 364
Monitor > Media Summary View options 364
Hierarchical View by Volume Pool for monitoring media 365
Viewing the details for volume pool 366
Viewing the details for media 366
Controlling media 366
Hierarchical View by Volume Group for monitoring media 367
Viewing the details for a volume group 368
Viewing the details for media 368
Controlling media in OpsCenter 368
Monitoring NetBackup devices 369
Monitor > Devices > Drives List View options 370
About using the List View for monitoring drives 371
Viewing the details for a single drive 372
Viewing the details for a master server associated with a drive 372
Filtering on NetBackup drive category 372
Controlling drives 373
Monitor > Devices > Drives Summary View 374
Viewing the Drive Summary by Status 374
Monitor > Devices > Disk Pools options 375
Viewing the details for a single disk pool 376
About monitoring NetBackup hosts 377
Monitor > Hosts > Master Servers view 377
Filtering by NetBackup master server type and status 378
Monitor > Hosts > Media Servers view 379
Viewing the details of a master server that is associated with a media server 380
Monitor > Hosts > Clients view 380
Viewing the details for a single master server 381
About monitoring NetBackup alerts 381
Monitor > Alerts List View 382

About using the List View to monitor NetBackup alerts 383
Viewing the details for a single alert 384
Viewing the details of a single alert for Appliance hardware failure 384
Viewing the details of the alert policy associated with an alert 385
Filtering by alert type 386
Responding to alerts 387
Summary View for monitoring NetBackup alerts 390
Viewing alerts by severity 391
Viewing alerts by NetBackup Master Server 391
About monitoring Audit Trails 392
Additional information about the Audit Trails report 392
What Audit Trails track 392
Audit Trails report 393
About OpsCenter features for Audit Trails 394
Creating a custom filter to view audit trail data 394
About managing Audit Trails settings 395
Monitor > Appliance Hardware > Master Server 395
Monitor > Appliance Hardware > Media Server 398
Monitor > Appliance Hardware > NetBackup 401
Monitor > Appliance Hardware > Deduplication 405
Appliance hardware details 408
Monitor > Cloud options 413

Chapter 9 Managing NetBackup using OpsCenter 415

About the Manage views 415
Controlling the scope of Manage views 416
About managing alert policies 417
About OpsCenter alert policies 417
Manage > Alert Policies view 418
Viewing the details for a single alert policy 419
Filtering on type of alert policy 419
About creating (or changing) an alert policy 420
Managing an alert policy 436
Viewing the alerts associated with an alert policy 437
About managing NetBackup storage 438
Manage > Storage > Storage Unit view 438
Manage > Storage > Storage Unit Group view 440
Manage > Storage > Storage Lifecycle Policy view 442
About managing NetBackup devices 443
Manage > Devices > Drive view 444
Manage > Devices > Robot view 448

Manage > Devices > Disk Pool view 450
Manage > Devices > SAN Client view 452
Manage > Devices > FT Server view 454
About Operational Restore and Guided Recovery operations 456
About Operational Restores from OpsCenter 456
About OpsCenter Guided Recovery 487
About managing NetBackup Hosts 497
Managing audit trails settings 497
About managing NetBackup Deployment Analysis 498
About the traditional license report 498
Prerequisites and data collection for a traditional licensing report 500
Traditional Licensing page 500
Create Traditional Licensing Report Wizard 500
Generating a Traditional Licensing report 503
Traditional Licensing report and log file locations 504
Possible Traditional License report issues 505
Capacity License report 506
Data compilation for the Capacity License report 507
Generating a Capacity Licensing report 508
Possible Capacity License report issues 510

Chapter 10 Supporting Replication Director in OpsCenter 512

About monitoring Replication Director from OpsCenter 512
About the Open Storage alert condition 512
How the events are generated 513
Adding an alert policy 514
About monitoring replication jobs 515
Disk pool monitoring 516
Storage lifecycle policy reporting 517
Reporting on storage units, storage unit groups, and storage lifecycle policies 518

Chapter 11 Understanding and configuring OpsCenter alerts 520

About using SNMP 520
About SNMP 521
About SNMP versions 521
SNMP versions supported in OpsCenter 522

About the Management Information Base (MIB) and OpsCenter support 522
SNMP traps 522
Alert descriptions in OpsCenter 525
Configuring the SNMP trap community name for OpsCenter 537
Configuring the SNMP version for sending SNMP traps 538
About customizing Alert Manager settings 539
Frequently asked SNMP and OpsCenter questions 540
About managing OpsCenter alerts using Microsoft System Center Operations Manager 2007 541
About managing OpsCenter alerts using HP OpenView Network Node Manager 7.50/7.51 on Windows 541

Chapter 12 Reporting in OpsCenter 543

About OpsCenter reports 543
OpsCenter reporting user interface 544
Report creation wizards in OpsCenter 545
Reports > Report Templates 545
About custom reports in OpsCenter Analytics 546
About custom SQL query in OpsCenter Analytics 547
About supporting OpsCenter custom reports and custom SQL queries 547
Report Templates in OpsCenter 547
About report filters in OpsCenter 549
Creating an OpsCenter report using a Report Template 550
Using report formats 550
About managing reports in OpsCenter 551
Save report and email report dialog boxes 552
Saving an OpsCenter report 554
Exporting an OpsCenter report 554
File formats available in OpsCenter 555
Emailing a report in OpsCenter 556
Configuring number of rows in a tabular report for email or export 557
Adding email recipients to an OpsCenter report mailing 559
Add email recipients dialog box options 559
Creating a custom report in OpsCenter 559
About Custom Report Wizard parameters 566
Creating an OpsCenter report using SQL query 573
About managing My Reports 575
Creating a report using the My Reports tab 575
Deleting a saved report using the My Reports tab 575

Viewing a saved report using the My Reports tab 576
Editing a saved report using the My Reports tab 576
Exporting a saved report 576
Emailing a saved report 577
About managing My Dashboard 578
Reports > My Dashboard options 578
Adding reports to a dashboard 579
Modifying a dashboard section 579
Deleting a dashboard section 579
Emailing dashboard sections 580
Refreshing My Dashboard 580
About managing reports folders in OpsCenter 580
Reports > Manage Folders options 580
Adding a reports folder in OpsCenter 581
Editing a reports folder in OpsCenter 581
Deleting reports folders in OpsCenter 581
Deleting reports from a folder in OpsCenter 582
Using report schedules in OpsCenter 582
Reports > Schedules options 584
About managing report schedules in OpsCenter 585
Viewing report schedule details in OpsCenter 586
Report Schedule Wizard 586
Creating a report schedule in OpsCenter 588
Editing a report schedule in OpsCenter 589
Deleting a report schedule in OpsCenter 589
Enabling or disabling a report schedule 589
About managing time schedules in OpsCenter 590
Reports > Schedules > Create or Edit Time Schedule options 590
Viewing time schedule details 591
Creating a time schedule 591
Editing a time schedule 591
Deleting a time schedule 592

Appendix A Additional information on PureDisk data collection 593

About AT configuration in OpsCenter 593
About Scenario 1: Root brokers on local hosts 594
About Scenario 2: Local root broker for OpsCenter server and remote root broker for PureDisk SPA 594
Setting up a trust between the PureDisk SPA AT host and the OpsCenter Server host 595

Appendix B Attributes of NetBackup data 597

Backup data attributes 597

Appendix C Man pages for CLIs 628

changedbpassword 629
configurePorts 630
dbbackup 631
dbdefrag 633
nbfindfile 634
opsadmin 638
opsCenterAgentSupport 640
opsCenterSupport 641
runstoredquery 644
startagent 645
startdb 646
startgui 647
startserver 648
stopagent 649
stopdb 650
stopgui 651
stopserver 652
view_exportimport 653

Appendix D Creating views using CSV, TSV, and XML files 658

About using CSV, TSV, and XML files to create views 659
About creating CSV files 659
About creating TSV files 662
About creating XML files 664
XML DTD structure 665
DTD elements 666
DTD <application> element 666
DTD <objects> and <object> elements 667
DTD <attribute> elements 668
DTD <view> element 668
DTD <node> elements 669
DTD <aliaslevel> elements 670
Examples of XML files 670
Example 1: Adding an object 670
Example 2: Adding a view 671
Example 3: Updating an object 672

Example 4: Merging objects 674

Appendix E Error messages in OpsCenter 675

OpsCenter Error Messages 675

OpsCenter Glossary 693

Index 694

Chapter 1

Overview of NetBackup OpsCenter

This chapter includes the following topics:

- About OpsCenter
- About OpsCenter components
- About using the OpsCenter console
- About starting the OpsCenter console
- About OpsCenter console components
- Common tasks in OpsCenter
- About using Web browser bookmarks
- About OpsCenter documentation

About OpsCenter

OpsCenter is a web-based software application that helps organizations by providing visibility into their data protection environment. By using OpsCenter, you can track the effectiveness of backup operations by generating comprehensive reports.

OpsCenter is available in the following two versions:

OpsCenter	This OpsCenter version does not require any license. OpsCenter provides single deployment configuration and user interface for monitoring, alerting, and reporting functionality.

OpsCenter Analytics	OpsCenter Analytics is the licensed version of OpsCenter. In addition to the features available in the unlicensed OpsCenter version, Analytics offers report customization, and chargeback reporting.

About OpsCenter functions

The unlicensed version of Veritas NetBackup OpsCenter is called OpsCenter.

OpsCenter can perform the following functions:

- Monitor NetBackup and NetBackup Appliance setups.
- Manage or administer NetBackup and NetBackup Appliance setups.
  Note that OpsCenter can only monitor and manage NetBackup or NetBackup Appliance. It cannot monitor or manage other products like NetBackup PureDisk, deduplication appliance and so on.
- Generate alerts depending on the conditions that you have defined.
- Create and customize views using OpsCenter View Builder (formerly called Java View Builder).

  Note: Where Amazon is the cloud service provider, OpsCenter cannot report on the data that MSDP cloud storage servers upload to the cloud.

- Provide operational reporting on the following Veritas products:
  - Veritas NetBackup
  - Veritas NetBackup Appliance
  - Veritas NetBackup PureDisk
  - Veritas Backup Exec

About OpsCenter Analytics functions

The licensed version of Veritas NetBackup OpsCenter is called OpsCenter Analytics.

OpsCenter Analytics can perform the following functions:

- Monitor NetBackup and NetBackup Appliance setups.
- Manage or administer NetBackup and NetBackup Appliance setups.
  See " About monitoring and managing NetBackup and NetBackup appliances" on page 22.

Note that OpsCenter Analytics can only monitor and manage NetBackup or NetBackup Appliance. It cannot monitor or manage other products like NetBackup PureDisk, Backup Exec, Deduplication Appliance and so on.

- Generate alerts depending on the conditions that you have defined.
  See "About alerting in OpsCenter" on page 22.
- Create and customize views using OpsCenter View Builder.
- Provide operational and business-level reporting on the following Veritas products:
  - Veritas NetBackup
  - Veritas NetBackup Appliance
  - Veritas NetBackup PureDisk
  - Veritas Backup Exec
- Provide chargeback, custom, and custom SQL reports

OpsCenter Analytics displays customizable, multi-level views of backup resources and customizable reports for tracking service usage and expenditures. It also contains tools for defining cost metrics and chargeback formulas or handling alerts.

A wide range of audiences can benefit from the reporting capabilities and management capabilities of OpsCenter Analytics. The audiences include IT (Information Technology) managers, application owners, IT finance teams, external compliance auditors, legal teams, line-of-business managers, external customers, IT architects, and capacity planning teams.

The primary objectives of OpsCenter Analytics are as follows:

- Help organizations assess their compliance with business standards by allowing them to accomplish the following:
  - Help organizations to establish the Service Level Agreements by reporting on them
  - Report to legal departments, auditors, IT managers, and administrators
  - Verify compliance with internal as well as external business-level regulations.
  - Identify risks in terms of shortfall of backup resources.
  - Assess the recovery of clients and applications.
- Assist organizations in effective business planning by enabling them to do the following:
  - Estimate future backup requirements with the help of backup trend analysis.

- Calculate the cost of data protection management and chargeback to customers and business units.

About monitoring and managing NetBackup and NetBackup appliances

OpsCenter can manage and monitor NetBackup master and media servers, clients, policies, and additionally appliance master and media servers. It can manage up to 100 NetBackup master servers that are distributed across multiple locations. It does not require you to separately log on to each NetBackup master or media server.

OpsCenter lets you view the operational status and health of your distributed data protection environment.

OpsCenter focuses on how to maintain your backup environment after you complete the NetBackup configuration. You need to use the NetBackup Administration Console and command-line interfaces for core NetBackup administrative functions such as configuring media, storage units, and policies.

About alerting in OpsCenter

OpsCenter provides a policy-based alert system, which monitors and notifies you before serious problems happen to your backup environment. You can use predefined alert conditions to create alert policies to monitor typical issues or thresholds within NetBackup, NetBackup Appliance or other products. You can send an email or SNMP notification in response to an actual alert, which lets administrators focus on other job responsibilities. They no longer need to be logged on to a terminal to monitor systems continuously.

See “About managing alert policies” on page 417.

About reporting in OpsCenter Analytics

These topics state the benefits that you can get from the OpsCenter Analytics reports.

See “About OpsCenter reports” on page 543.

See “About compliance reporting” on page 23.

See “About business planning” on page 23.

About compliance reporting

OpsCenter Analytics helps organizations evaluate their compliance with internal and external business standards by providing accurate and customizable reports. By using internal compliance reports, you can measure system performance against a service level agreement (SLA). You can then use the results to optimize data protection management. Reports such as history or trend analysis ensure your compliance with the SLA. By using these reports, you can track the use of backup resources and identify the risks involved. For example, you can generate a report that anticipates a shortfall of resources in the future based on the current backup trend. This report is then used to determine the time that is required to purchase new tape drives, master servers, or media servers.

External compliance reports help you follow the policies that are laid down by various federal regulations. Such policies include the Sarbanes-Oxley Act (SOX) and the Health Insurance Portability and Accountability Act (HIPAA).

In addition to tracking the backup information, OpsCenter reports ensure recovery of key information assets. The reports can help you ensure that the data recovery meets the recovery-time and recovery-point objectives.

OpsCenter can generate reports that are filtered by views. A view shows a set of enterprise assets (hosts or file systems) organized in logical groups. For example, you can create views to display assets according to their locations in the organization, the line of business they represent, or the applications that are installed. OpsCenter can generate reports according to views created. These reports help you identify locations or departments containing assets with critical data. These reports are then used in resource planning.

About business planning

OpsCenter Analytics is a management tool that helps you optimize your data protection environment with effective business planning. It delivers backup services to organizations, which include reporting on backup and recovery trends and managing datacenters . This product supports a wide range of backup and recovery solutions including NetBackup and Backup Exec. It seamlessly integrates with backup products and provides consistent reporting across them. It can collect data from the following target products:

- Veritas NetBackup
- Veritas NetBackup Appliance
- Veritas Backup Exec
- Veritas NetBackup PureDisk

OpsCenter's ability to forecast backup resource requirements helps datacenter executives to decide whether to maintain the existing resources or add new capacity. The detailed, drill-down OpsCenter reports help you determine the applications, databases, or business departments that are the heaviest consumers of backup resources. For example, in an environment running 20 instances of Oracle applications, you can generate a report showing resource consumption by department, server, or location. Depending on this information, organizations can provide appropriate resource planning in advance.

OpsCenter Analytics offers you a set of chargeback reports that detail backup service expenditures. By using these reports, you can track the backup use and recovery use and the associated cost. By using the chargeback function, you can define pricing models for backup service delivery and allocate costs to customers based on these models. For example, you can create a formula that determines charges based on kilobytes of backed up data over a period of time. Using this chargeback data, you can then present itemized invoices to internal customers, export chargeback tables to third-party billing systems, or use the data to analyze and justify expenditures.

About OpsCenter components

This section describes the following OpsCenter components:

About the OpsCenter Server

The OpsCenter Server, the core of the architecture, is a Web application that normalizes backup data that it collects from various applications. This normalized data is used for reporting on backup-related information.

OpsCenter Server is supported on Windows and UNIX platforms.

Note: You must install OpsCenter Server, Agent, and View Builder of the same versions. For example, OpsCenter Server 7.7 is compatible only with Agent 7.7 and View Builder 7.7.

The OpsCenter Server comprises the following components:

OpsCenter database

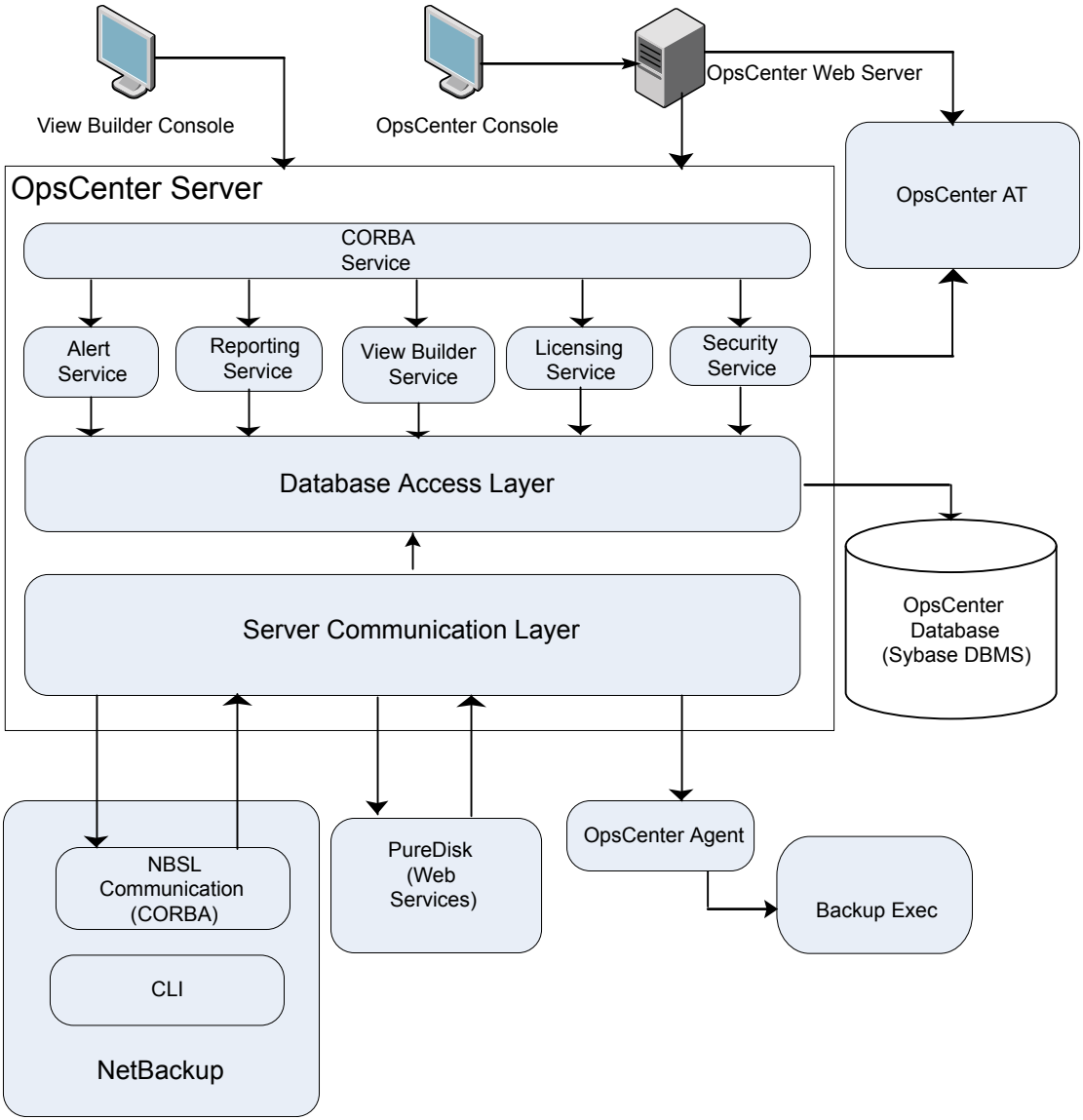
A Sybase SQL Anywhere database management system containing data related to back up service usage and expenditure, cost metrics and chargeback formulas, and alerts.

See "About the OpsCenter database" on page 26.

OpsCenter AT	A set of common authentication runtime libraries and processes that enable users to log on once to access multiple products. OpsCenter AT validates identities based on external name spaces. Examples of name spaces are Active Directory or other LDAP servers, UNIX identities based on password files, NIS/NIS+ repositories, or any identities that can be authenticated through PAM (Pluggable Authentication Module). It also provides a private user repository for service identities. See "About OpsCenter AT" on page 27.
Alert Manager	A component that provides policy-based alert management, including notification, custom actions, and SNMP management capabilities.
Web Server and Java Runtime Environment (JRE)	A common web server (that uses Java Server Pages) and JRE to serve the OpsCenter console. See "About the Java Runtime Environment" on page 72.
Veritas Licensing Manager	A common Veritas Licensing Module and API used to add, change, and remove Veritas product license keys.
Veritas Private Branch Exchange	A common component that uses socket passing to reduce the number of ports that are required to be open across a firewall. Veritas Private Branch Exchange uses a paradigm similar to the paradigm of a telephone switchboard. Calls placed to a switchboard are redirected to a known extension. In the PBX exchange, client connections that are sent to the exchange's port are redirected to an extension that is associated with the OpsCenter Server.

Figure 1-1 shows the architecture of the OpsCenter Server.

Figure 1-1 OpsCenter Server architecture



About the OpsCenter database

OpsCenter uses Sybase SQL Anywhere database management system as a repository for the backup data, such as backup service usage and expenditure reports, cost metrics, chargeback formulae, and alerts.

OpsCenter uses a Sybase SQL Anywhere database installation that is separate from the NetBackup database.

Except for a very small number of system settings, all information that is in the Web user interface is contained in the OpsCenter database, which consists of a single cross-platform database file.

The OpsCenter database is completely embedded and requires no additional installation steps. The Sybase database is also self tuning and does not require a database administrator to maintain it.

About OpsCenter AT

The Authentication Service (AT), which consists of Root Broker and Authentication Broker is embedded with the OpsCenter Server software. This AT service is very specific to OpsCenter and therefore, it is called OpsCenter AT.

Note: No other Veritas product can use OpsCenter AT for user authentication.

In a clustered OpsCenter setup, each cluster node has an embedded AT binary. All cluster nodes share the same AT configuration and the authentication data exists on a shared disk.

Name of the OpsCenter Authentication Service is `ops_atd`.

About the OpsCenter Agent

The OpsCenter Agent collects data from Backup Exec. The OpsCenter Agent relies on the Java Runtime Environment (JRE) to perform its functions.

See "About the Java Runtime Environment" on page 72.

It also requires embedded AT (Authentication Service) to authenticate itself with the OpsCenter Server. Both JRE and AT libraries are installed automatically with the Agent installation.

OpsCenter Agent is supported on Windows.

Note: You must install OpsCenter Server, Agent, and View Builder of the same versions. For example, Server 7.7 is compatible only with Agent 7.7 and View Builder 7.7.

OpsCenter formats the information collected from the following target products and displays it through the OpsCenter console:

- NetBackup and NetBackup Appliance

Note: You do not need to install and configure OpsCenter Agent to collect data from NetBackup. OpsCenter uses NetBackup's NBSL component or bpjava protocol to collect data from NetBackup.

- Backup Exec (Windows only)

OpsCenter Server collects NetBackup data using NBSL in the following scenarios:

- If you want to collect tape drive information, media, policy and schedule, job, or skipped file data from a NetBackup master server of any supported version.
- If you want to collect any data type (except traditional and capacity license data) from NetBackup master servers of 7.6 or later version.

The core of the OpsCenter Agent is a Java Virtual Machine (JVM) on which you run different data collectors. The OpsCenter Agent communicates with the OpsCenter Server, schedules backup data collection data types, and receives commands through the CORBA API.

As the OpsCenter Server relies on AT to authenticate connections between the OpsCenter Server and OpsCenter Agent, the AT client libraries reside on the Agent host.

The OpsCenter Agent consists of the scheduler, CORBA Client/Server, and data collectors that collect backup data from all available backup applications. The Scheduler and CORBA form the agent core.

These parts of the agent are described in the following topics:

See “About the scheduler” on page 28.

See “About the CORBA Client/Server ” on page 29.

See “About data collectors” on page 29.

About the scheduler

The scheduler performs three basic functions for the OpsCenter Agent:

- Checks and queues the data collection schedules of all running data collectors.
- Sends periodic heartbeat messages to the OpsCenter server to ensure the reliability of communications between the Agent and the Server.
- Monitors modifications that are made to the Agent configuration using the OpsCenter console, which are stored on the OpsCenter Server.

About the CORBA Client/Server

The OpsCenter Agent implements a CORBA server that listens on a configurable port that allows the OpsCenter console to get the runtime status of the Agent. (The default port is 7806.) When you send a request to get the Agent status through the OpsCenter user interface, the OpsCenter Server sends the request to the CORBA Server to receive the requested information.

The Agent behaves as a CORBA client when sending data or alerts to the OpsCenter Server.

About data collectors

The data collectors convert the data specific to back up products into a format that can be used by the OpsCenter Server. Each data collector must conform to an interface that defines its interaction with the OpsCenter Agent. The data collector is implemented in a way that suits the underlying backup product.

Data collector configurations consist of general parameters, such as log configurations and data collection event definitions, which are shared by all data collectors, and product-specific values.

You must configure a data collector on the OpsCenter Agent host that collects data from a backup product host.

About Agent configuration and logging

Agent configuration settings are stored in the OpsCenter database. The OpsCenter Agent also caches the latest version of the configuration settings in the `agent.conf` file. The agent compares the local `agent.conf` file with the one stored in the database when the agent process is started. If the agent process has already started, any changes made to the local `agent.conf` file do not take place until the agent is restarted.

Note: You should not modify the `agent.conf` file. You should change the agent configuration settings using the OpsCenter Agent configuration user interface.

Any changes that you make to the Agent configuration settings are reflected after the next heartbeat.

A heartbeat is a request that the OpsCenter Agent sends to the OpsCenter Server to check for any new changes in the configuration settings. By default, a heartbeat is sent every minute.

Logging for the agent core and individual data collector is administered in the same fashion but written to different log files.

About the OpsCenter OpsCenter View Builder

The OpsCenter View Builder is an application in which an administrator creates, modifies, and manages access to the OpsCenter views that users see in the console.

The OpsCenter View Builder relies on the AT client libraries which is installed automatically to communicate properly with the OpsCenter Server. To use the OpsCenter View Builder, you need to provide logon credentials as you do while logging onto the OpsCenter console.

See "Logging on to the OpsCenter console as a default admin user" on page 42.

When you run the OpsCenter View Builder `.exe` file, it is directly connected to the OpsCenter Server. The View Builder fetches the existing object view definitions from the OpsCenter database and displays them in the OpsCenter console. The actions that you perform using the View Builder console are then stored in the OpsCenter database.

Note: You must install OpsCenter Server, Agent, and View Builder of the same versions. For example, Server 7.7 is compatible only with Agent 7.7 and View Builder 7.7.

About using the OpsCenter console

The following sections describe how to access and use OpsCenter. They include how to log on and log off and how the console works.

For information on how to understand and use the various OpsCenter views and related tasks, see the OpsCenter online Help. Context-sensitive help is available for all console views, task dialog boxes, and wizard task screens.

To access the online Help, use the **Help** option in most dialog boxes and wizard screens. You can also use the **Help** option on the title bar of OpsCenter views.

The OpsCenter online documentation assumes that the user has a good working knowledge of NetBackup and its concepts and components.

Portions of the online Help may refer the user to other NetBackup documentation for descriptions of NetBackup fields and components.

The following NetBackup documents are referenced in the OpsCenter online Help:

- *NetBackup Administration Console Help*
- *NetBackup Administrator's Guide for UNIX, Windows, and Linux, Volume I*
- *NetBackup Troubleshooting Guide for UNIX, Windows, and Linux*

About starting the OpsCenter console

The OpsCenter Server is the focal point for centralized management of the NetBackup servers in your backup environment.

When you install OpsCenter, you select the computer that serves as the OpsCenter server. When you start the OpsCenter console to manage and monitor your NetBackup environment, you open a connection to the OpsCenter web interface.

About web browser considerations

Consider the following recommendations and requirements for the web browser to be able to access the OpsCenter console.

The following requirements and recommendations should be considered for the web browser to access OpsCenter console:

- The web browser cache must be cleared.
  After you upgrade to OpsCenter 8.0, you may see the old user interface with the Symantec logo. You need to clear the web browser cache to view the new user interface with the Veritas logo.
- The OpsCenter console uses pop-up menus. If you use pop-up blockers with your web browser, some of these menus may not display properly. You must disable pop-up blocking or add the OpsCenter web address to the list of acceptable sites in your browser.
- JavaScript should be enabled for all the browsers.
- In case Win2000, WinXP SP3, Win2003, or WinCE clients need to connect to the OpsCenter server using Internet Explorer version 6,7,or 8 with 128 bit cipher configuration, then following steps need to be followed:
  - Find **server.xml** file at
    OpsCenter\gui\webserver\conf for Windows server
    /opt/SYMCOpsCenterGUI/gui/webserver/conf for UNIX/Linux server.
  - Find below cipher configuration in **server.xml** file.

```
<Connector SSLEnabled="True" URIEncoding="UTF-8"
acceptCount="100" ciphers="SSL_RSA_WITH_RC4_128_MD5,
SSL_RSA_WITH_RC4_128_SHA, TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA"
compressableMimeType="text/html,text/xml,text/javascript,text/css"
compression="on" compressionMinSize="10"
```

```
connectionTimeout="20000" disableUploadTimeout="true"
enableLookups="false"
keystoreFile="C:\PROGRA~1\Symantec\OpsCenter\gui\Security\Keystore"
keystorePass="opscenter" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25"
noCompressionUserAgents="gozilla, traviata" port="443"
protocol="HTTP/1.1" scheme="https" secure="true"
sslProtocol="TLS" useBodyEncodingForURI="true"/>
```

- Append below list of ciphers in 'ciphers' attribute.

```
SSL_RSA_WITH_RC4_128_MD5,
SSL_RSA_WITH_RC4_128_SHA,
SSL_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
```

- Restart OpsCenter WebServer service.

- In case of Internet Explorer 7.0, ActiveX should be enabled. This is because Ajax is supported through ActiveX for Internet Explorer 7.0.
- Ensure that the character encoding for the browser is Unicode (UTF 8) before you access the OpsCenter console.
  Open the Internet Explorer browser and select **View > Encoding > Unicode (UTF-8)**.
  Open the Mozilla Firefox browser and select **View > Character Encoding > Unicode (UTF 8)**.
- On some server systems, you may see a blank page when you try to access OpsCenter using Internet Explorer 7.0 and above versions. This issue is caused due to high security level in server systems. If you encounter this issue, open Internet Explorer and click **Tools > Internet Options**. Click the **Security** tab and select 'Internet' icon as the zone. Click **Custom Level...**. In the **Security Settings** dialog box, browse to **Miscellaneous** > **Allow META REFRESH** and select **Enable**. Click **Yes** to confirm that you want to change the security settings for the zone, and then click **OK**.

  Note: In case you do not want to change your security settings, you must manually append `/opscenter` to the OpsCenter URL. This action must be taken every time you access OpsCenter and face this issue.

- On some server-class systems, an enhanced security configuration can cause some pages to not display properly in Internet Explorer. If you encounter this

issue, add the OpsCenter URL to the Trusted-sites list and lower the security setting. To resolve this issue, open Internet Explorer and select **Tools > Internet Options > Security** to configure the Trusted-sites list and lower the security level.

- If you use Internet Explorer 8.0 or 9.0 to access the OpsCenter console, security certificate warnings appear when you access a pop-up menu. Select **Continue to this website (not recommended)** to open the pop-up menu. Once you select this option, the security certificate warnings do not appear on the pop-up menus.
- If you use Internet Explorer 9.0 to access the OpsCenter console, you may not be able to download or view reports, jobs, or audit trails data when you export it from OpsCenter. More details on how to resolve this issue are available.
  See "Exporting OpsCenter reports or data with IE 9.0" on page 36.
- If you use Internet Explorer 8.0 or 9.0 to access the OpsCenter console, ensure that you select the standard versions of IE 8.0 or 9.0 and not their compatibility mode.
  To select the standard version on your IE 8.0 or 9.0 window, press F12. The **F12** window opens. From the Menu bar click **Browser Mode:**, you can view the different IE versions - **Internet Explorer 7**, **Internet Explorer 8**, **Internet Explorer 9**, **Internet Explorer 9 Compatibility View**. Select **Internet Explorer 8** or **Internet Explorer 9** to access the OpsCenter console.
- If you use Internet Explorer 10 to access the OpsCenter console, you must change the default browser mode from Internet Explorer 10 Compatibility View to Internet Explorer 10.
  To change the browser compatibility view mode, press **F12** from the browser to open the Developer Tools window. From the Menu bar, click **Browser Mode:Internet Explorer Compat View**, and then select **Internet Explorer 10**.
- A known issue in Firefox 8.x causes the downloaded attachments to be named as `ExportReportAction.do` or some other file name and type which cannot be opened. This issue affects you if you use Firefox 8.x to access the OpsCenter console and generally occurs when you export a report or export job and audit logs. Because of the Firefox 8.x issue, when you export an OpsCenter report for instance, the report is saved by the name `ExportReportAction.do` and does not open if you try to open it.
  To resolve this issue, Veritas recommends that you upgrade to Firefox 9.0.
  In case you want to continue using Firefox 8.x, when you export a report or job logs using Firefox 8.x and are prompted to open or save the exported file, click **Save File**. In the **Enter name of file to save to** dialog box, select the **Save as type** as **All Files** and then rename the file with the proper extension (like replace the default name `ExportReportAction.do` with `filecount.pdf`) and click **Save**. You can then open this report.

Note: If you do not see **Enter name of file to save to** dialog box, click **Firefox > Options > General** and check **Always ask me where to save files** option.

Note: Refer to the compatibility matrix that is posted on the Veritas Support web site for the latest information on the browsers that OpsCenter supports. This document is posted at the following URL:

http://www.netbackup.com/compatibility

About accessing the OpsCenter console

Before accessing the OpsCenter console, review the following section thoroughly.

See "About web browser considerations" on page 31.

On a system that has a network connection to the OpsCenter server, start a Web browser.

In the Web browser address bar, enter the following: https://*host.domain*/opscenter

`host.domain` is the fully qualified domain name of the OpsCenter server and can also be an IP address.

Note: By default, OpsCenter tries to run on port 443 (HTTPS). If port 443 is not available, OpsCenter can use a different port. To learn more about the HTTPS ports that OpsCenter uses, run the `configurePorts` utility. Run the following command:

On Windows: `<INSTALL_PATH>\OpsCenter\gui\bin\goodies\configurePorts.bat -status`

On UNIX: `<INSTALL_PATH>/SYMCOpsCenterWebGUI/bin/goodies/configurePorts.sh -status`

If OpsCenter uses HTTPS port 8443, then use https://host.domain:8443/opscenter.

You can also use the URL that is presented at the end of the OpsCenter server installation to access OpsCenter.

You must supply logon credentials on the OpsCenter logon screen. For an administrator initial logon, the user name is `admin` and the password is `password` or any custom password that you chose during the installation.

Select **OpsCenterUsers(vx)** from the **Domain** drop-down list and click **Log On**.

See "Logging on to the OpsCenter console as a default admin user" on page 42.

Disabling the Untrusted Connection page in Mozilla Firefox

When you access OpsCenter in Mozilla Firefox, you may see the following Untrusted Connection page.

```
-------------------------------------------------------------

This Connection is Untrusted

You have asked Firefox to connect
securely to <OpsCenterhost.domain>, but we can't confirm
that your connection is secure.

Normally, when you try to connect securely,
sites will present trusted identification to prove that you are
going to the right place. However, this site's identity can't be verified.

What Should I do?
If you usually connect to
this site without problems, this error could mean that someone is
trying to impersonate the site, and you shouldn't continue.

Technical Details
   I Understand the Risks

-------------------------------------------------------------
```

Your choice is either to click **Get me out of here**, which takes you to the Mozilla Firefox start page, or to click **Add Exception** (when you expand the **I Understand the Risks** section) and permanently disable the page.

To disable the Untrusted Connection page in Mozilla Firefox

1. On the Untrusted Connection page, expand **I Understand the Risks** section and click **Add Exception**.
2. In the **Add Security Exception** dialog box, click **Get Certificate**.
3. To make this exception permanent, make sure that the **Permanently store this exception** option is checked. This option is checked by default.
4. Click **Confirm Security Exception**.
5. Restart your browser for the changes to take effect.

Exporting OpsCenter reports or data with IE 9.0

When you are using IE 9.0, you may not be able to download or view reports, audit trails, or jobs data when you export them from OpsCenter on HTTPS.

This problem occurs if the **Do not save encrypted pages to disk** option in Internet Explorer is checked. This issue is explained in detail on the following Web site:

http://support.microsoft.com/kb/2549423

File downloads in Internet Explorer require a cache or temporary file to succeed. In IE9, if the file is delivered over HTTPS with any response headers set to prevent caching and the Do not save encrypted pages to disk option is set, then a cache file is not created. Therefore, the download fails.

Use any one of the following procedures to resolve this issue.

To uncheck encrypted pages to disk

1. Open Internet Explorer. Go to **Tools** > **Internet Options** > **Advanced**.
2. Uncheck **Do not save encrypted pages to disk** option.

To bypass the cache check in IE 9

1. Start the Registry Editor.
2. For a per-user setting, locate the following registry key:

   HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings

   For a per-computer setting, locate the following registry key:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
3. On the **Edit** menu, click **Add Value** and add the following value:

   "BypassSSLNoCacheCheck"=Dword:00000001
4. Quit Registry Editor.

Possible OpsCenter console access issues

Table 1-1 describes possible OpsCenter console access issues and their solution.

Table 1-1 OpsCenter console access issues, causes, and solution

Issue and Cause	Solution

You cannot connect to the Web interface. Your Web browser displays a "page cannot be displayed" or "connection was refused."message.
 	
This issue happens when the OpsCenter Web interface (the OpsCenter console) is not running or is inaccessible on the network.
	To connect to the Web interface
	
	1 Verify that the OpsCenter Web server Service is running.
	
	You can check the status of all OpsCenter processes on UNIX by entering the following command:
	
	`<INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh monitor`
	
	2 Verify that a Web browser on the OpsCenter server can connect to the OpsCenter console by using the following address:
	
	https://localhost/opscenter
	
	Note: By default, OpsCenter tries to run on port 443 (HTTPS). If port 443 is not available, OpsCenter can use a different port. To learn more about the HTTPS ports that OpsCenter uses, run the `configurePorts` utility. Run the following command:
	
	On Windows:
	`<INSTALL_PATH>\OpsCenter\gui\bin\goodies\configurePorts.bat -status`
	
	On UNIX:
	`<INSTALL_PATH>/SYMCOpsCenterWebGUI/bin/goodies/configurePorts.sh -status`

Table 1-1 OpsCenter console access issues, causes, and solution *(continued)*

Issue and Cause	Solution

The OpsCenter Web interface is running, but the OpsCenter console is not available. Your Web browser displays an HTTP STATUS 404 error.
 	
This issue happens when the OpsCenter console application is not loaded.
	To resolve an HTTP STATUS 404 error on Windows
	
	1 Locate the `opscenter.war` file in the following directory to verify that the OpsCenter application is installed:
	
	`INSTALL_PATH\OpsCenter\gui\webserver\webapps`
	
	2 Verify that all the OpsCenter server services are running.
	
	3 Start all the OpsCenter Server services by using the following command:
	
	`INSTALL_PATH\OpsCenter\server\bin\opsadmin.bat start`
	
	To resolve an HTTP STATUS 404 error on UNIX:
	
	1 Locate the `opscenter.war` file in the following directory to verify that the OpsCenter application is installed:
	
	`<INSTALL_PATH>/SYMCOpsCenterGUI`
	
	2 To verify that all OpsCenter Server processes are running, use the following command:
	
	`<INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin monitor`
	
	3 Start all the OpsCenter Server processes by using the following commands:
	
	`<INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh start`

Table 1-1 OpsCenter console access issues, causes, and solution *(continued)*

Issue and Cause	Solution
You see a blank page when you try to access OpsCenter using Internet Explorer 7.0 and later versions.	To resolve blank page issues when using Internet Explorer 7.0 and later **1** Open Internet Explorer . On the **Tools** menu, click **Internet Options**. **2** Click the **Security** tab. **3** Under **Select a Web content zone to specify its security settings**, click the **Internet**, icon and then click **Custom Level**. **4** In the **Security Settings** dialog box, browse to **Miscellaneous > Allow META REFRESH** and select **Enable**. **5** Click **Yes** to confirm that you want to change the security settings for the zone, and then click **OK**. **Note:** If you do not want to change your security settings, you must manually append `/opscenter` to the OpsCenter URL. Without the changes to the security settings, the issue recurs every time that you accessOpsCenter, and you must add `/opscenter` to the URL.

Table 1-1 OpsCenter console access issues, causes, and solution *(continued)*

Issue and Cause	Solution
You get the following error when you access OpsCenter by clicking **Start > Programs > OpsCenter > WebUI Login** on Windows: `Windows cannot find https://<MACHINE_NAME>:<PORT_NUMBER>/opscenter. Make sure you typed the name correctly, and then try again. To search for a file, click the Start button and then click Search.`	

Table 1-1 OpsCenter console access issues, causes, and solution *(continued)*

Issue and Cause	Solution
	To fix the Web user interface login error for Windows XP **1** Open Windows Explorer (or My Computer). **2** Go to **Tools > Folder Options > File Types**. **3** Select **Extension**: **(NONE)** and **File Type**: **URL:HyperText Transfer Protocol** **4** Click **Advanced**. In the **Edit File Type** window, select **Open** and click **Edit**. **5** Uncheck **Use DDE** (the dialog should then hide the lower part). **6** Click **OK** for that dialog and the next one (afterwards, the **Use DDE** box is still checked but the **DDE Message** box will be cleared). **7** Repeat for Extension: **(NONE)** File Type: **URL:HyperText Transfer Protocol with Privacy** (and any other protocols you want to fix). **8** Repeat for Extension: **(NONE)** File Type: **Firefox URL**. **9** Repeat for Extension: **HTM** (or **HTML**) File Type: **Firefox Document**. Note that the File Types user interface that allows you to uncheck the **Use DDE** option, as described above, is not available in Windows Vista. You need to edit the registry to remove the `ddeexec` key. You need to manually edit the registry in Windows Vista or in cases where the File Types listing is missing certain entries such as `URL:HyperText Transfer Protocol with Privacy`(HTTPS). **Note:** Editing the registry incorrectly can damage your system. Do not attempt these steps if you are inexperienced or uncomfortable using the Registry Editor. Use the following resolution on Windows Vista or in cases where the **File Types** listing is missing certain entries such as `URL:HyperText Transfer Protocol with Privacy` (HTTPS): **1** Go to **Start > Run**, then type `regedit` and click **OK**. **2** Use the directory tree hierarchy to navigate to **HKEY_CLASSES_ROOT\HTTP\shell\open\ddeexec**. **3** Delete the `ddeexec` registry key. **4** Repeat for

Table 1-1 OpsCenter console access issues, causes, and solution *(continued)*

Issue and Cause	Solution
	HKEY_CLASSES_ROOT\HTTPS\shell\open\ddeexec (and any other protocols you want to fix). **5** Repeat for **HKEY_CLASSES_ROOT\FirefoxURL\shell\open\ddeexec**. **6** Repeat for **HKEY_CLASSES_ROOT\FirefoxHTML\shell\open\ddeexec**.

Logging on to the OpsCenter console as a default admin user

This section provides the procedure to logon to OpsCenter. After successful installation, you can log on to the OpsCenter user interface with default admin user account credentials.

To log on to the OpsCenter console as a default admin user

1. Enter a user name and password, and select a domain from the **Domain** drop-down list. For administrator initial logon, the user name is `admin` and the password is `password` or any custom password that you chose during the installation.
2. Select **OpsCenterUsers(vx)** from the **Domain** drop-down list.

   The domains that appear in the **Domain** drop-down list include the **OpsCenterUsers(vx)** domain and domains of the users that are added to the OpsCenter console.

3 Click **Log On**. The Change Password page is displayed that prompts you to change your default password for security purposes.

Note: The new OpsCenter users (including the default 'admin' user) require to change the password before logging on to the OpsCenter user interface. After a new user enters the default user credentials, the Change Password page is displayed that prompts the user to change the default password for security purposes. However, the users whose accounts existed in the previous OpsCenter version and were upgraded can logon to OpsCenter user interface with their old passwords.

The password rules are also provided on the Change Password page.

---

4 On the Change Password page, enter the old password and new password. Re-enter the new password for confirmation and click **OK**.

See "Changing your OpsCenter password" on page 211.

After successfully changing the password you are able to logon to the OpsCenter user interface. At the time of first login, Home > Getting Started page is displayed where you can do initial OpsCenter configuration.

For the next login, a monitoring overview of the NetBackup master servers appears on the OpsCenter user interface. When you log off from the console, OpsCenter saves your settings and preferences and uses these settings when you restart the console again.

Note: The first time you log on, OpsCenter uses the default language of the Web browser. If OpsCenter does not support this language, it uses English.

After initial logon, you can specify a default language or locale from **Settings > User Preferences > General**. If you do not set a default language, OpsCenter uses the Web browser language (or English).

See "Setting user preferences" on page 207.

Possible OpsCenter console logon issues

Table 1-2 describes the issues you may find when you log on to the console and their solution.

Table 1-2 OpsCenter console logon issues

Issue	Cause	Solution
You have a user authentication error. The logon screen displays the message "User authentication failed. Please enter valid user name and password. If problem persists contact your system administrator."	The OpsCenter Authentication Service cannot validate the user name and password for the selected domain.	Enter a valid user name, password, and domain. Ensure that the OpsCenter Authentication Service is started and running properly. You can start the authentication service by running `net start ops_atd` on Windows and `<INSTALL_PATH SYMCOpsCenterServer/authbroker/bin/ops_atd` on UNIX.
The entered user name is not a registered OpsCenter user. The logon screen displays the message "This user is not authorized to use OpsCenter. Please contact the OpsCenter Administrator for adding this user."	The user name and domain are valid, but the user was not added to the list of users for OpsCenter.	Log on as the OpsCenter admin user and add the user to the list of OpsCenter users.

Table 1-2 OpsCenter console logon issues *(continued)*

Issue	Cause	Solution
You cannot connect to the OpsCenter server. The logon screen displays the message "Error occurred while connecting to the OpsCenter Server. Please ensure that the server is running."	This issue may occur due to any of the following reasons: ■ The OpsCenter server is not running. ■ If PBX server goes down or restarts when OpsCenter services were running.	Start the OpsCenter Server Service and verify that it is running properly. See 'Controlling OpsCenter services and processes' section in the Administration chapter of the *OpsCenter Administrator's Guide*. Check your network configuration. Verify that the `hosts` file has the correct IP address to host name mapping. The `hosts` file is located in `C:\WINDOWS\system32\drivers\etc` directory on Windows. If PBX server gets restarted while OpsCenter services were running, you must restart all OpsCenter services. Use the following procedure to restart all OpsCenter services. ■ First stop all OpsCenter server services, by using the following command for Windows and UNIX: INSTALL_PATH\OpsCenter\server\bin\opsadmin.bat stop <INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh stop ■ Start all OpsCenter server services, use the following command for Windows and UNIX: INSTALL_PATH\OpsCenter\server\bin\opsadmin.bat start <INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh start
Either the user name or password or both have not been entered. The logon screen displays the message "Please enter valid user name and password. "	Username and/or password has not been specified.	Enter a valid user name and password.
Authentication service is down "Error occurred while connecting to the OpsCenter Authentication Service (AT). Please ensure that the AT service is running."	Authentication service is down	Verify that the OpsCenter Authentication Service is running. You can start the authentication service by running `net start ops_atd` on Windows or <INSTALL_PATH>/SYMCOpsCenterServer/authbroker/bin/ops_atd on UNIX.

Customizing the OpsCenter login page

OpsCenter provides you a way of customizing the login page as per your requirements. You can define customized login message

To customize the OpsCenter login page

1. Using a text editor, create a file named `customerpreferences.conf` at the following location:

Windows	*`install_path`*`\opscenter\server\config` *install_path* is the location where OpsCenter is installed.
UNIX	`/opt/SYMCOpsCenterServer/config`

2. Add the following contents in the `customerpreferences.conf` file:

   SHOW_MESSAGE_IN_LOGIN_DIALOG=true

   LOGIN_DIALOG_MESSAGE_TEXT=*Login dialog message*

   SHOW_LOGIN_MESSAGE=true

   IS_LOGIN_MESSAGE_TYPE_CONFIRM=false

   LOGIN_MESSAGE=*Login message*

   SHOW_MESSAGE_IN_HEADER_AND_FOOTER=true

   HEADER_FOOTER_MESSAGE_TEXT=*Header footer message*

   SHOW_CUSTOMIZED_INVALID_CREDENTIAL_MESSAGE=true

   INVALID_CREDENTIAL_MESSAGE=*Invalid credential message*

3. Save the `customerpreferences.conf` file.
4. Stop and restart the OpsCenter services.

Logging out of the OpsCenter console

When you log out from the console, OpsCenter saves most of the settings and changes you make in an OpsCenter session.

To log out from OpsCenter

- Click **Logout** located on the right side of the title bar.

Configuring the OpsCenter session timeout interval

When the timeout interval is left at its default value, users are automatically logged out of the OpsCenter console when a session is left inactive for 30 minutes. However, the session timeout interval can be reconfigured.

To configure the session timeout interval

1. Open the `web.xml` configuration file in a text editor from the following locations:

   For Windows: *INSTALL_PATH*`\OpsCenter\gui\webserver\conf\web.xml`

   For UNIX: `<INSTALL_PATH>/SYMCOpsCenterGUI/webserver/conf/web.xml`

2. In the `web.xml` file, locate the session-timeout parameter:

```
<session-config>

<session-timeout>30</session-timeout>

</session-config>
```

3. Change the session timeout parameter value to the desired length by changing the number that is encapsulated by the XML tags for session-timeout (in the example above, change `30` to the desired value).

   This value is set in minutes.

4. Stop the OpsCenter services. Enter the following command:

   Windows *INSTALL_PATH*`\OpsCenter\server\bin\opsadmin.bat stop`

   UNIX `<INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh stop`

5. Restart the OpsCenter services. Enter the following command:

   Windows *INSTALL_PATH*`\OpsCenter\server\bin\opsadmin.bat start`

   UNIX `<INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh start`

Possible OpsCenter console issues

Table 1-3 describes the issues you may find when you use the console.

Table 1-3 Issues when you use OpsCenter console

Issue	Cause	Solution
Your OpsCenter console session times out. The logon screen appears when you try to change views or refresh the current view.	After 30 minutes of inactivity, the OpsCenter user automatically logs out of the console. Any attempt to use OpsCenter, displays the OpsCenter logon screen.	Log on again. After successful logon, you then return to the OpsCenter view that you last visited. You can also configure the session timeout interval. See "Configuring the OpsCenter session timeout interval" on page 47.
An internal error occurs in the OpsCenter console. An exception error message appears in the OpsCenter console. You receive the message "An unknown error has occurred. Click here to log on and retry. "	This error results from an internal issue in the OpsCenter console application.	Click the link in the message and try to logon again.
You receive the message "Active scripting is required to use this application. Enable active scripting in the browser."	Active scripting is disabled in the Web browser.	Enable active scripting in the Web browser. You must enable it to use OpsCenter.

About OpsCenter console components

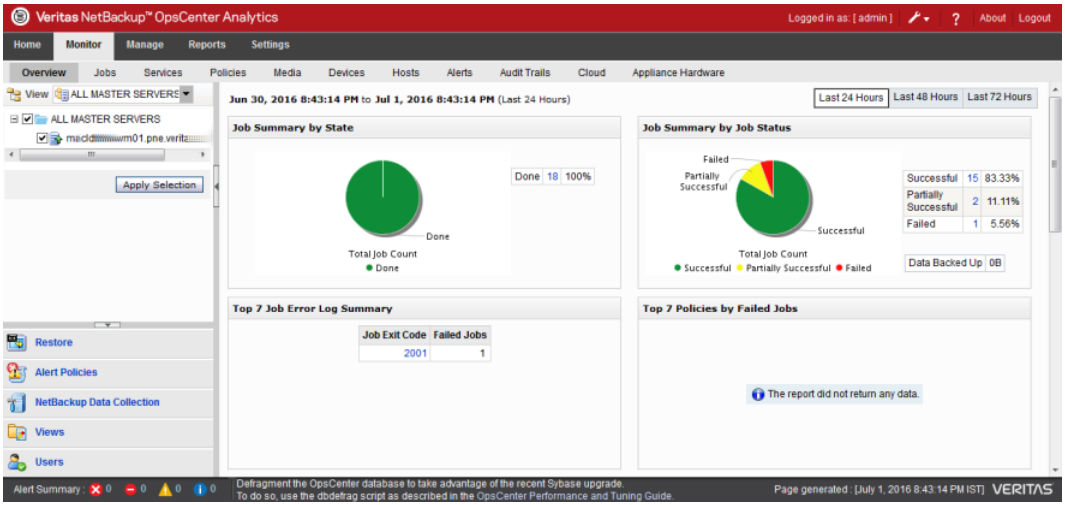
This section provides information on the panes and navigation features available in the OpsCenter console. You can view the console by using a Web browser.

When you log on initially, the **Monitor > Overview** view appears.

When you change the settings and preferences they are saved and if you log out and log on again these settings are used.

The following is an example view that shows the OpsCenter console components.

Figure 1-2 OpsCenter console components



The following sections describe the main elements of the console in greater detail.

Table 1-4 lists the topics that describe the main elements of the console in greater detail.

Table 1-4 Topics covered in this section

Topic Description	Link
Use the links available from the title bar, such as **Logout** and **Help**.	See “About using the links on the title bar” on page 50.
Overview about the tabs and subtabs available in the console.	See “About using tabs and subtabs” on page 51.
Control the frequency that the OpsCenter console refreshes to reflect changes in your backup environment.	See “About refreshing the OpsCenter console” on page 51.
Overview about the **Task** pane.	See “Changing the Task pane” on page 52.
Overview about the **View** pane.	See “About the View pane” on page 52.
Overview about quick links in the task panes.	See “Using the quick links in the Task pane” on page 56.
Use the pane that displays a quick visual summary of any current alerts.	See “Viewing alerts from the Alert Summary pane” on page 56.
Use the main data display pane that OpsCenter uses.	See “Sizing the Content pane” on page 57.

Table 1-4 Topics covered in this section *(continued)*

Topic Description	Link
Use the status bar at the bottom of the OpsCenter console.	See "About the OpsCenter status bar" on page 59.
Use the visual keys that OpsCenter uses to help you understand displayed information.	See "Status icons and colors in the console" on page 59.
Use tables, select rows, and use filters.	See "About using tables" on page 61.

About using the links on the title bar

On the title bar of the OpsCenter console, the **Logged in as** value shows the user name that is logged on to the OpsCenter server.

To adjust the screen space that is used by the tabs and sub-tabs, click the **Customize Tabs** drop-down list. You can select the following options:

Small — Only the selected tab and sub-tab are shown in a single row. To display the remaining tabs in a drop-down list, click the arrow next to the selected tab. To display the remaining sub-tabs in a drop-down list, click the arrow next to the selected sub-tab.

Medium — The tabs and sub-tabs appear in two separate rows. The tabs do not have any icons above them.

Large — The tabs and sub-tabs appear in two separate rows. The tabs have icons placed above them.

Use the links available in the title bar at the top of the console for the following tasks:

- To access documentation, product information, How To links, support links, and other information click **Tools**.
- To see OpsCenter product version and copyright information, click **About**.
- To access OpsCenter help, click **Help**. Context-sensitive help for all views, wizards, and dialog boxes is available.
  More information about online Help is available.
  See "About OpsCenter documentation" on page 68.
- To disconnect from the OpsCenter server to end your session, click **Logout**.

About using tabs and subtabs

Table 1-5 describes the main tabs that provide access to the major areas of the OpsCenter console.

Table 1-5 Tabs and subtabs in the OpsCenter console

Tab	Description
Monitor	From this tab, you can monitor the status of NetBackup or NetBackup Appliance jobs, services, policies, media, devices, and hosts. You can also display and respond to any OpsCenter alerts.
Manage	From this tab, you can manage alert policies, NetBackup job policies, storage units, and devices. You can also restore data.
Reports	From this tab, you can view standard OpsCenter reports, create and run custom reports, and schedule reports. **Note:** You can use custom report functionality only with a licensed OpsCenter version (OpsCenter Analytics).
Settings	From this tab, you can customize the OpsCenter server, add OpsCenter users, define user preferences, add master servers or appliance master servers, add and configure views, set up email and SNMP recipients, view chargeback settings, and so on.

Under each main tab is a series of subtabs. The contents of these subtabs vary depending on the current view and represent the views accessible from each main tab. For example, the **Monitor** tab includes subtabs such as **Overview**, **Jobs**, **Services**, and **Policies**.

Your selection on the **View** pane determines what data is shown in OpsCenter views.

More information about the **View** pane is available.

See "About the View pane" on page 52.

About refreshing the OpsCenter console

As you use OpsCenter, the status of your backup environment is likely to change. Devices go online and offline, OpsCenter generates alerts, media usage fluctuates, and so on. You can control when the information in the console refreshes to reflect the changes in your backup environment.

You can change the refresh setting from **Settings > User Preferences > General** view in the OpsCenter console.

See "Setting user preferences" on page 207.

Changing the Task pane

In many views in the console, a **Task** pane is available.

The **Task** pane is located on the left side of the console and contains the **View** pane and Quick Links at the bottom.

To change the Task pane

1. To enlarge the Task pane, click the **Collapse Task Panel** icon between the **Task** pane and the **Content** pane.
2. To show all panes after you enlarged the **Task** pane, click the **Collapse Task Panel** icon again.
3. To resize the **Task** pane, drag the line separating the **Task** pane and the **Content** pane.

   The minimize or maximize settings are applicable only for the current session.

   You cannot resize the **Task** pane from the **Monitor > Overview** page.

About the View pane

The **View** pane is a key navigation and configuration tool in OpsCenter. This pane lets you select the views to control the scope of your console views.

Using OpsCenter views, you can view NetBackup information for your entire management domain (with the **ALL MASTER SERVERS** view), a specific view type, an individual server, or NetBackup appliances.

A Security Administrator or an Administrator can create views from **Settings > Views** or by using the OpsCenter View Builder. For example, an admin can create a view named Geography to display details about master servers in a particular region, such as Europe. An admin can also create client or policy views.

More information about how to create views from **Settings > Views** is available.

See "About OpsCenter views" on page 299.

See the OpsCenter View Builder Help for more information about creating views using OpsCenter View Builder.

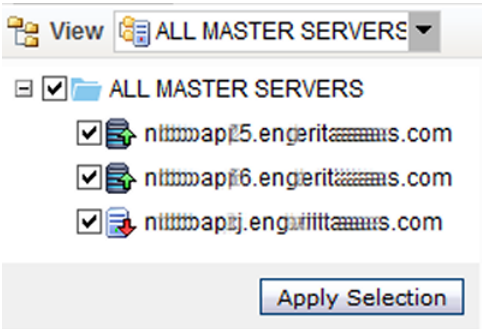
The **View** pane has the following features:

- It is available in any OpsCenter view where you can change the view.

- It uses unique icons and colors to convey operational states.
  For example, an icon with a red-dashed-circle represents a managed server that is Not Connected. Similarly, a disabled master server is shown as a gray-colored icon.
  See "Status icons and colors in the console" on page 59.
- It lets you access and change the views that you monitor or manage.
  As you navigate within the OpsCenter console, your view selection applies for any subsequent screens until you select a different view.
  The **View** pane is one method that you can use to determine the scope of information that you view.
  See "About making multiple or single-click selections in the View pane" on page 53.
  See "About selecting views from the View pane when the multiple selection option is checked" on page 55.

Figure 1-3 shows a sample **View** pane in which **ALL MASTER SERVERS** view is selected.

Figure 1-3 View pane description



About making multiple or single-click selections in the View pane

You can make either multiple selections or single-click selections in the **View** pane. The **Allow Multiple Selection In View Pane** option governs how you can make selections in the **View** pane. To see the **Allow Multiple Selection In View pane** option, click **Settings > User Preferences > General** in the OpsCenter console.

You can make selections in the **View** pane in the following ways, based on whether you check or uncheck the multiple selection option:

Select the **Allow Multiple Selection In View Pane** option	With the multiple-selection option selected, you can select multiple nodes or view objects from the View pane. The multiple-selection option is selected by default. You also see a check box next to each master server or node in the **View** pane. To view data for multiple master servers and nodes, select the corresponding check boxes and click **Apply Selection**.
Clear the **Allow Multiple Selection In View Pane** option	With the multiple-selection option cleared, you can only select a single node or view object from the **View** pane. Each node or a view object is a link. You can click a node or a view object to view data for the respective node or view object. For example, you can click a master server in the **View** pane to view data for the specific master server. **Note:** When you clear the multiple-selection option, a **Group Component Summary** table is displayed when you click **Monitor > Jobs > Summary View**. See "About the Group Component Summary table" on page 341.

Figure 1-4 shows how you can select the **Allow Multiple Selection In View Pane** option and make multiple selections. The **Allow Multiple Selection in View Pane** option is selected by default.

Figure 1-4 Making multiple selections in the View pane

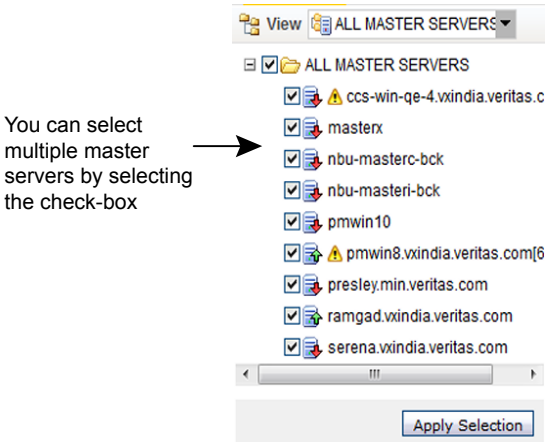
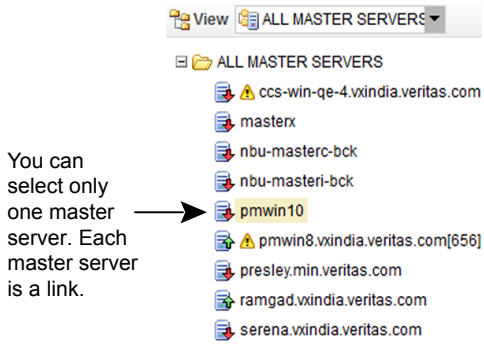


Figure 1-5 shows how you can clear the **Allow Multiple Selection in View Pane** option and make single-click selections.

Figure 1-5 Making single-click selections in the View pane



About selecting views from the View pane when the multiple selection option is checked

From the **View** pane, you can select a view and a node that contains a group of master servers and also specific objects. For example, you can select the default view, **ALL MASTER SERVERS**. When you select a view such as **ALL MASTER SERVERS** or a node that contains a group of master servers, all the master servers that are currently in the view or node are automatically selected. The master servers that you may add later to this view or node are also automatically selected.

You also have the option to select only specific objects of a particular view or node. For example, you may select only specific master servers under the default view **ALL MASTER SERVERS**. To select a specific master server, first deselect the view or node that contains the master server and then select the master server.

You may also deselect a specific master server from a view by selecting the view and then deselecting the specific master server.

Consider a scenario in which `server A` and `server B` exist in a particular view, such as **ALL MASTER SERVERS**. Suppose that you select the **ALL MASTER SERVERS** view and then specifically deselect `server B`. Then, you select a node that also contains `server B`. In this case, even though `server B` is part of the selected view or node, it is not considered. It is not considered because you specifically excluded `server B` from the **ALL MASTER SERVERS** view. When you specifically deselect a master server from a view, and that master server is also part of another selected view, the exclusion (the deselection) has a higher priority. For this reason, it is recommended that you do not repeat a master server across groups.

Using the quick links in the Task pane

In many views in the console, a **Task** pane is available. At the bottom of the **Task** pane, there are quick links to the most common tasks in OpsCenter.

Table 1-6 shows the quick links available in OpsCenter and where they take you when you click them.

Table 1-6 Quick links and their destinations

Quick Link	Destination
Restore Files and Directories or Oracle Cloning	**Manage** > **Restore**
Alert Policies	**Manage** > **Alert Policies**
NetBackup Data Collection	**Settings > Configuration > NetBackup**
Views	**Settings > Views**
Users	**Settings > Users > Users**
Cloud	**Monitor > Cloud**
Appliance Hardware	**Monitor > Appliance Hardware**

To use the quick links in the Task pane

1. Click the minimize icon (the down arrow) located on top of the quick links. Only the icons for quick link tasks are visible when the quick links are minimized.
2. Click the maximize icon (the up arrow) again to view the quick links.

Note: The quick links are shown by default in a maximized state. The minimize or maximize settings are applicable only for the current session.

Viewing alerts from the Alert Summary pane

The **Alert Summary** pane provides a visual summary of the critical, major, warning, and informational alerts for the NetBackup master servers to which you are connected. This pane is available in the **Monitor** view and **Manage** view of the OpsCenter console.

The Alert Summary pane displays all the alerts in the OpsCenter database.

To view alerts from the Alert Summary pane

- Click any of the four available alert counts.

  A filtered detail view for that alert category appears. This view is a shortcut to the **Monitor > Alerts** view.

Sizing the Content pane

When you initially log on to Veritas NetBackup OpsCenter, the content pane displays a summary of information for all master servers in the OpsCenter console.

Initially, a monitoring overview appears (**Monitor > Overview**). Information in the content pane varies and is context-sensitive to current selections in the **View** pane, the tabs and subtabs, and the time frame.

To size the Content pane

1. To enlarge the Content pane, click the **Collapse Task Panel** icon between the **Task** pane and the **Content** pane.
2. To show all panes after you enlarged the **Content** pane, click the **Collapse Task Panel** icon again.
3. To resize the **Content** pane, drag the line separating the **Task** pane and the **Content** pane.

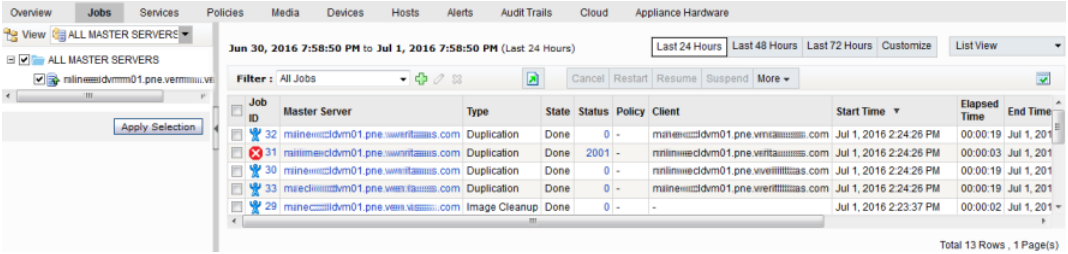
   The minimize or maximize settings are applicable only for the current session.

   Note: You cannot resize the **Content** pane from **Monitor > Overview** page.

Using the List, Summary, Hierarchical, and Details views

Most of the OpsCenter **Monitor** views and **Manage** views present information in three main viewing modes: **List View**, **Summary View**, and **Hierarchical View**. You can view information about your NetBackup environment in any of the available views. Use the drop-down list on the top-right corner of the OpsCenter console to switch these views.

Note: Not all viewing modes are available for all **Monitor** views and **Manage** views. If the viewing modes are available, the drop-down list is displayed.

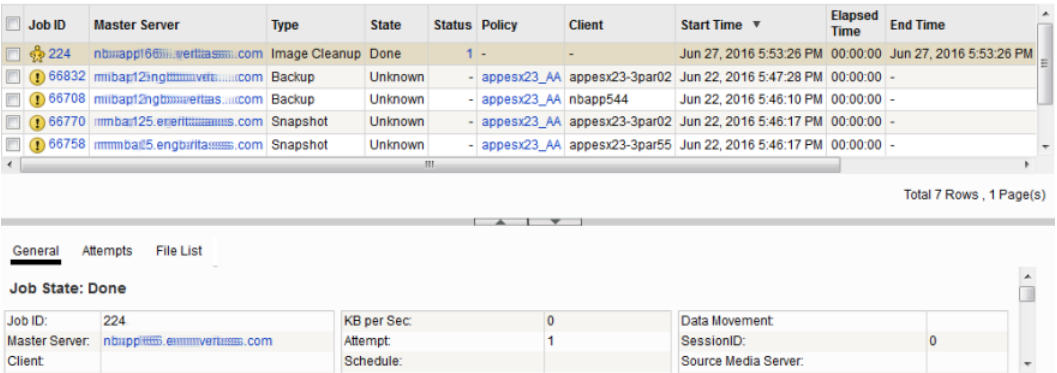


The **Summary View** presents information in a graphical format as pie charts. The **List View** and **Hierarchical View** present information in tabular formats.

For example, you can show any of the following views on the **Monitor > Jobs** page:

- To view details about all NetBackup jobs for a master server in a tabular format, click **List View**
- To view a summary of all NetBackup jobs for a master server in the form of pie charts, click **Summary View**.
- To view details about all NetBackup jobs and relationships between jobs for a master server in a tabular format, click **Hierarchical View**.

A **Details** view is available on some of the **Monitor** views, **Manage** views, and **Settings** views. The following figure shows the **Details** view.



The **Details** view presents detailed information about an entity and shows contents of all the tabular columns for the specific entity. The view presents details on the displayed information and on the available information for the specific entity. For example, the **Details** view on the **Monitor > Jobs** page (**List View**) shows detailed information about a specific job ID. Information in the **Details** view can be viewed from tabs available in the view.

To change the Details view

1. To minimize the **Details** view, click the icon (the down arrow) between the **Details** view and the upper part of the **Content** pane.
2. To maximize the **Details** view, click the icon (the up arrow) between the **Details** view and the upper part of the **Content** pane.

   The minimize or maximize settings are applicable only for the current session.
3. To resize the **Details** view, drag the line separating the upper part of the **Content** pane and **Details** view.

About the OpsCenter status bar

The status bar at the bottom of the OpsCenter console shows a **Page generated** value. The **Page generated** value shows the date and time on the OpsCenter server to which you logged on. The date and time are adjusted to match your time zone. This value updates when the view changes or refreshes.

More information on how to specify your time zone is available.

See "Setting user preferences" on page 207.

Status icons and colors in the console

To help you understand the information it presents, OpsCenter uses status icons and color. Tool tips provide brief descriptions of the tool and the status icons that appear in OpsCenter views. A tool tip appears when you place the mouse over an icon.

When OpsCenter detects a condition for a managed NetBackup server, job, drive, or drive path, you see a status icon. The icons use colors to represent critical, warning, or informational conditions. Together, the icons and colors let you quickly determine the status of a particular area in your NetBackup environment. For example, the **Monitor > Jobs** view contains green icons for running jobs.

Unique icons appear in the drive details view for shared drives available with the NetBackup Shared Storage Option (SSO). These icons represent the shared drives that are operating on all servers that share the drive. Icons also appear for shared drives where the drive status is mixed (operating on some servers and not operating on other servers that share the drive).

Table 1-7 lists the icons that are used for managed NetBackup master servers in the **View** pane.

Table 1-7 Icons used for managed NetBackup master servers

Icon	Description
	A blue server icon with a green upward arrow means that the master server is connected.
	A blue server icon with a red downward arrow means that the connection to the master server is lost. OpsCenter tries to connect again after 10 minutes.
	A gray server icon with a line means that data collection for the master server was disabled by the user.
	A gray server icon with a red cross means that the master server is retired.
	A gray server icon with blue question mark means that the master server state is unknown.
	A blue server icon with a green upward arrow means that the NetBackup Appliance master server is connected.
	A blue server icon with a red downward arrow means that the connection to the NetBackup Appliance master server is lost. OpsCenter tries to connect again after 10 minutes.
	A gray server icon with a line means that data collection for the NetBackup Appliance master server was disabled by the user.
	A gray server icon with a red cross means that the NetBackup Appliance master server is retired.
	A gray server icon with blue question mark means that the NetBackup Appliance master server state is unknown.

OpsCenter uses the following colors in the interface:

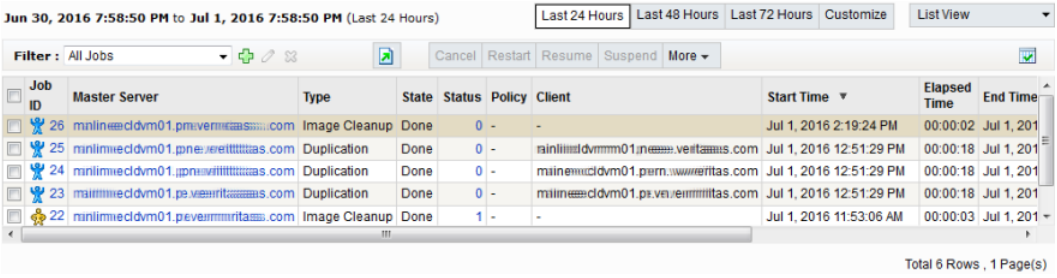
- Red indicates a critical condition that may cause the system to be unable to perform an important function. Investigate critical conditions immediately.
- Green indicates a normal condition, result, or operation.
- Blue-gray generally indicate conditions such as enabled or assigned, while gray indicates conditions such as disabled or unassigned.

About using tables

OpsCenter collects information about aspects of your NetBackup environment and presents much of this information in tables. The following is a sample table showing task icons.

Figure 1-6 shows the task options for tables.

Figure 1-6 Sample screen with task options for tables



Customizing tables for your needs

You can customize the tables in the following manner.

You can perform the following operations to a table:

Add or remove columns	See "Specifying which columns appear in a table" on page 62.
Rearrange the order of the columns for your individual requirements	See "Moving a column" on page 62.
Choose the number of rows and columns to display	See "Choosing the number of table rows that appear per page" on page 62.
Sort columns in ascending or descending order	See "Sorting the contents of a table column" on page 62.
Change the widths of columns	See "Changing the width of a column" on page 63.
Configure pagination	See "Accessing multiple pages of data in a table" on page 63.
Select rows in tables	See "Selecting rows in tables" on page 63.

The table refreshes after the operation and shows the changes you made.

For these operations, OpsCenter saves and reloads your customized settings when you log on to the OpsCenter server again. Each user can have different customized table settings.

Specifying which columns appear in a table

Use the following procedure to specify which columns appear in a table.

To specify which columns appear in a table

1. Click the **Change Table Settings** icon at the top-right corner of the table.
2. Initially, some OpsCenter tables do not show all available columns. To view any of these columns, you may first have to remove one or more columns from the table and then add the missing columns.

   To remove columns you do not want to appear, select the column in **Selected Columns** and click **Remove**.

   To add any columns that currently do not appear, select the column in the **Available Columns** list and click **Add**. Added columns appear as the last column in the table.

Moving a column

Use the following procedure to move columns in a table.

To move a column

1. Click the **Change Table Settings** icon at the top of the table.
2. Select the name of the column in Selected Columns.
3. Click **Move Up** to move the column to the left in the table.

   Click **Move Down** to move the column to the right in the table.

Choosing the number of table rows that appear per page

Use the following procedure to choose the number of table rows that appear per page.

To choose the number of table rows that appear per page

1. Click the **Change Table Settings** icon at the top of the table.
2. Select a number from the Rows Per Page drop-down list .
3. Select **Apply To All Tables** if you want the **Rows Per Page** setting to apply to all tables in OpsCenter. The setting applies to reports also.

Sorting the contents of a table column

Use the following procedure to sort the contents of a column or multiple columns.

To sort the contents of a column or multiple columns

- In a table, click the column name. The column sorts in ascending order by default.

  To sort in descending order, click the column name again.

Changing the width of a column

Use the following procedure to change the width of a column.

To change the width of a column

1. Select the edge of the column heading and hold down the left mouse option.
2. Drag the edge of the column heading to the right or left.

Accessing multiple pages of data in a table

Much of the monitoring information appears in a table format. OpsCenter tables display 10 rows at one time by default. To change the number of rows that are displayed, use the **Change Table Settings** icon.

When you have more data to display than can fit in a table, the table contains multiple pages. Use the table page controls that are located below the table to help you navigate the pages.

To display the next 10 rows or to return to a previous set of rows in large tables, use the table page controls.

To access a specific page in a table

- Click the page number.

To access the previous or the next page in a table

- Click the left arrow or the right arrow.

To access the first or the last page in a table

- Click the double left arrow or the double right arrow.

Selecting rows in tables

For many tables in OpsCenter, you must select a row or rows to enable the tasks.

To select a row in a table

- Click the check box for that row. Click the check box again to deselect the selected row.

To select all rows on the current page of the table

- Click the check box in the header row of the table. Click the check box again to deselect all selected rows.

Creating, applying, editing, and removing custom view filters

Many tables in OpsCenter let you display a subset of the information available by creating and using custom filters, or by using the predefined (ready-to-use) filters. A filter screens information that is based on a set of conditions that you define. Once you create a filter, you can save it, edit it, or remove it.

In the views that allow filtering, filtering icons appear above the table.

The following procedures describe how you can create, apply, edit, or remove a filter.

To create a custom filter

1. Select the **Create Filter** icon.
2. Type a name for the filter in the **Name** field.
3. For Column, select the column name that you want to filter on from the drop-down list.

   For Operator, select an operator. Use != if you do not want to match a specific value.

   For Value, enter or select a value.

   If you select Start Time or End Time for Column, a calendar icon appears for Value. Click the calendar icon to choose a date and time and then click **OK**.
4. From the drop-down list, select **And** or **Or** to build the filter query.

   For Link, click **Add** to add another clause to the query. If the clause is not what you want, click **Remove** to remove the clause from the query.
5. To continue building the filter, select another column.

   Repeat 3 and 4.
6. Click **OK** when you finish building the filter. Your new filter is available in the filter drop-down list.

To apply a filter

- From the drop-down list, select a custom filter or a OpsCenter built-in filter.

  OpsCenter filters the table according to the criteria you specify. The view remains in effect until you change it by selecting another filter.

To edit a custom filter

1 From the drop-down list, select a custom filter.

Note: You cannot modify the predefined OpsCenter filters. You can only modify custom filters.

---

2 Click the **Edit filter** icon.

3 See "To create a custom filter" on page 64.

This lists the instructions for using the dialog to edit a filter.

4 Make your changes and click **OK**.

To remove a custom filter

1 From the drop-down list, select a custom filter.

Note: You cannot delete the predefined filters.

---

2 Click the **Delete filter** icon.

3 Click **OK** to remove the filter.

Common tasks in OpsCenter

Table 1-8 lists common tasks and corresponding links to the documentation.

Table 1-8 Quick links to the OpsCenter documentation

OpsCenter functions	Tasks	Go to this topic
User Management	Create, update, delete users Create, update, delete user groups Add, remove users from user groups Assign, remove roles to users and user groups	See "About managing OpsCenter users " on page 226. See "Setting user preferences" on page 207.

Table 1-8 Quick links to the OpsCenter documentation *(continued)*

OpsCenter functions	Tasks	Go to this topic
OpsCenter Management	Add, update, or delete master servers Add, update, or delete OpsCenter Agents Set default currency, SNMP, SMTP server	See "Adding a master server or appliance in OpsCenter" on page 285. See "Editing a master server or an appliance master server in OpsCenter" on page 292. See "Deleting a master server or an appliance master server in OpsCenter" on page 292. See "About managing OpsCenter Agents" on page 264. See "About managing cost analysis and chargeback for OpsCenter Analytics" on page 249. See "About managing recipients in OpsCenter" on page 242. See "Configuring SMTP server settings for OpsCenter" on page 216.
NetBackup Operations	Change states of the NetBackup entities as follows: Policy (Activate or deactivate) Job (Stop, start, suspend, or resume) Media (Assign, freeze, unfreeze) Drives (Up or down)	See "Activating or deactivating a job policy" on page 355. See "Controlling NetBackup jobs" on page 335. See "Controlling media" on page 364. See "Controlling drives" on page 373.
Backup and Recovery	Execute manual backups Search and restore files, directories, or application (Oracle)	See "Starting a manual backup" on page 356. See "About Operational Restores from OpsCenter" on page 456.

Table 1-8 Quick links to the OpsCenter documentation *(continued)*

OpsCenter functions	Tasks	Go to this topic
Views Management	Create, update, delete OpsCenter views and nodes Assign read or write permissions to users on OpsCenter views and nodes	See "About managing OpsCenter views" on page 306. See "User access rights and functions in OpsCenter user interface" on page 231. See " Adding new users to OpsCenter" on page 236.
Report Execution	Execute report templates and custom reports Schedule canned and custom reports Create, update Dashboard Schedule when you want a report to run	See "Creating an OpsCenter report using a Report Template" on page 550. See "Creating a custom report in OpsCenter" on page 559. See "About managing My Dashboard" on page 578. See "About managing report schedules in OpsCenter" on page 585.
Monitoring	View entities (Dashboards, Summary, Details): Job, Policy, Services etc.	See "About monitoring NetBackup using the Overview tab" on page 322. See "About monitoring NetBackup jobs" on page 329. See "About monitoring NetBackup policies" on page 349. See "Monitor > Services view" on page 347.
Alert Management	Create, update, delete alert policies Assign, acknowledge, and clear alerts	See "About creating (or changing) an alert policy" on page 420. See "Managing an alert policy " on page 436. See "About managing recipients in OpsCenter" on page 242. See "Configuring SMTP server settings for OpsCenter" on page 216.

About using Web browser bookmarks

Use your Web browser to add a bookmark for any view in the OpsCenter console and return to it as needed.

You can use the bookmark to return to the same view when you log onto the console again.

About OpsCenter documentation

NetBackup OpsCenter documentation set comprises the following:

- The *OpsCenter Administrator's Guide* (`NetBackup_AdminGuide_OpsCenter.pdf`) provides information on how to use OpsCenter. It includes information about how to monitor and manage NetBackup, collect data from Veritas products, generate alerts, and create various reports. It also provides details on the new enhancements in and also how you can install OpsCenter.
  The online version of the *OpsCenter Administrator's Guide* can be found at:
  http://www.veritas.com/docs/000003387
- The *OpsCenter Reporting Guide* (`NetBackup_OpsCenter_Reporting.pdf`) provides information on all OpsCenter reports. The online version of the OpsCenter *OpsCenter Reporting Guide* can be found at:
  http://www.veritas.com/docs/000003387
- The new *OpsCenter Performance and Tuning Guide* provides information on how to tune OpsCenter for improved performance. The online version of the *OpsCenter Performance and Tuning Guide* can be found at:
  http://www.veritas.com/docs/000003387
- Refer to the NetBackup hardware and software compatibility matrix for the latest information on the backup products, operating systems, and web browsers that OpsCenter supports. This document is posted at the following URL:
  http://www.netbackup.com/compatibility
- You can find more information about OpsCenter in *NetBackup Release Notes*. Always refer to the OpsCenter sections of this document for any last-minute changes to the information that is presented in this document. The Release Notes also include any restrictions or limitations for OpsCenter. The online version of the *NetBackup Release Notes* can be found at:
  http://www.veritas.com/docs/000003214

In addition to the PDFs, OpsCenter is also shipped with the following online help documents:

OpsCenter context-sensitive help	This Help provides information about the OpsCenter user interface. It provides context-sensitive help pages for all screens.

OpsCenter Analytics View Builder context-sensitive help	This Help provides information about all OpsCenter Analytics View Builder procedures and dialog boxes. To access the Help, click **Help** in a dialog box in the OpsCenter Analytics View Builder console.
NetBackup Status Codes Help	This Help provides descriptions of NetBackup status codes and possible actions to take when a code appears. To access the Help, click **Monitor > Jobs**. Click a status code link in the jobs table to view its details.
OpsCenter Table Settings Help	This Help provides information on how to change the settings of a table in the OpsCenter console. To access the Help, click **Help** on the **Table Settings** pop-up dialog box.

Chapter 2

Installing OpsCenter

This chapter includes the following topics:

- About planning an OpsCenter installation
- Installing OpsCenter on Windows and UNIX
- About OpsCenter upgrade on Windows and UNIX
- About files and folders that are protected during OpsCenter upgrade
- About OpsCenter upgrade failure scenarios
- About post-installation tasks
- About uninstalling OpsCenter on Windows and UNIX
- About clustering OpsCenter

About planning an OpsCenter installation

The following topics provide information on concepts to understand and steps to take before you install or upgrade OpsCenter.

See “Software components that OpsCenter uses” on page 71.

See “About the Java Runtime Environment” on page 72.

See “About the OpsCenter licensing model” on page 73.

See “ OpsCenter DVDs” on page 76.

See “Managed NetBackup master server considerations” on page 77.

See “About designing your OpsCenter Server” on page 79.

See “Supported upgrade paths in OpsCenter” on page 79.

See “About planning an OpsCenter Agent deployment” on page 80.

See "Preparation for installation or upgrade" on page 82.

For sizing guidelines, refer to the new *OpsCenter Performance and Tuning Guide* at the following location:

http://www.veritas.com/docs/000003387

Refer to the NetBackup hardware and software compatibility matrix for the latest information on the backup products, operating systems, and web browsers that OpsCenter supports. This document is posted at the following URL:

http://www.netbackup.com/compatibility

Software components that OpsCenter uses

Along with OpsCenter-specific components, OpsCenter uses some Veritas components that are shared.

Components that are shared with other Veritas applications

OpsCenter uses the following components that are also shared with other Veritas applications:

- Veritas Private Branch Exchange (PBX)
  PBX lets applications share a common TCP/IP port, which reduces the required number of open ports in firewalls. PBX also integrates with the Veritas Product Authentication Service to allow for authenticated connections and non-authenticated connections.
  Because PBX is an independent component, its port number can be changed using PBX configuration files.

  Note: If you change the PBX port number on the OpsCenter server, OpsCenter may fail.
- JRE (Java Runtime Environment)
  The Veritas NetBackup OpsCenter Web server and the OpsCenter application require this component.
  See "About the Java Runtime Environment" on page 72.

Note: The NetBackup Access Control (NBAC) does not need to be configured on your managed NetBackup master servers.

See the *NetBackup Security and Encryption Guide* for information about NBAC.

OpsCenter components

OpsCenter uses the following components that are not shared with other Veritas applications:

- Apache Tomcat Web server
  The OpsCenter user interface runs under the Apache Tomcat Web server.
- Veritas Unified Logging (VxUL)
  VxUL is installed with the OpsCenter Server and the Agent. OpsCenter uses VxUL to configure and view logs.
  See the *NetBackup Troubleshooting Guide* for more information about VxUL logs.
  http://www.veritas.com/docs/000003214
- Sybase database
  OpsCenter uses a Sybase SQL Anywhere database installation that is separate from the NetBackup database.
  More information about the Sybase component is available at the following location:
  http://www.sybase.com/support/manuals

About the Java Runtime Environment

OpsCenter software installer installs a customized version of Java Runtime Environment (JRE) when you install the following:

- OpsCenter Server
- OpsCenter Agent
- OpsCenter View Builder

The customized version of JRE does not include some directories that a standard JRE version includes. For example, man, plugin, and so on.

Until OpsCenter 8.0, the JRE package that was bundled along with the OpsCenter installer was updated only when you upgraded to a later OpsCenter release. You can use the `nbcomponentupdate` utility to update the JRE to a supported version for the following OpsCenter components: OpsCenter Server, OpsCenter Agent, and View Builder

If your system is running OpsCenter 8.0 or later, the `nbcomponentupdate` utility is available in the OpsCenter installer at the following locations:

Table 2-1

OpsCenter Component	Operating System	Path
OpsCenter Server	Windows	*Install_path*\server\bin\nbcomponentupdate.exe
	UNIX	SYMCOpsCenterServer/bin/nbcomponentupdate

Table 2-1 *(continued)*

OpsCenter Component	Operating System	Path
OpsCenter Agent	Windows	`Install path\agent\bin\nbcomponentupdate.exe`
OpsCenter View Builder	Windows	`Install_path\viewbuilder\bin\nbcomponentupdate.exe`

Note: If you update the JRE, and then later upgrade OpsCenter, the software upgrade overwrites the JRE update. Run the utility again to update the JRE. You can download and run the `nbcomponentupdate.exe` from the following location:

https://www.veritas.com/support/en_US/article.000115043

For more details on the `nbcomponentupdate` command and its parameters, refer to the *NetBackup™ Commands Reference Guide*.

Note: The JRE version in the OpsCenter installer is the supported major version for that OpsCenter release. Use this utility to update to a minor version of the supported major JRE version. Veritas recommends that you update to another major JRE version only if the installed version is end-of-life. For example, if OpsCenter 8.0 installer has JRE 1.8.0.31, the supported major version is 1.8. You can use this utility to update to a minor version of JRE 1.8, for example, 1.8.0.92.

You may have additional versions of the JRE installed on your system for different applications. The OpsCenter JRE does not interfere with these other installations. The OpsCenter JRE does not provide integration with web browsers and does not allow Java Applets or Web Start to run. For that reason, the OpsCenter JRE cannot be used in a browser-based attack that uses Java Applet or Web Start vulnerabilities.

For more information about such alerts, see the following article:

https://www.veritas.com/support/en_US/article.TECH50711

About the OpsCenter licensing model

OpsCenter requires no license. You need a license key to enable OpsCenter Analytics that provides additional functionality.

The licensed version of OpsCenter is called OpsCenter Analytics. The unlicensed version of OpsCenter is called Veritas NetBackup OpsCenter. The product name is visible from the title bar and logon page of the OpsCenter console.

The charges for Veritas NetBackup OpsCenter licenses are based on how many entities you report on.

For backup environments, the charges are based on the number of backup clients.

OpsCenter Analytics license keys

OpsCenter Analytics has two types of license keys:

Demo key — The demo key is valid for 60 days from the day the key is generated. The demo key lets you try the product before you purchase it.

Permanent key — A permanent key does not have an expiry date.

- NetBackup ENT Capacity key enables all the features of OpsCenter Analytics like business reporting, etc.
- GOLD key enables all the features of OpsCenter Analytics.

You can access the licensed features with both demo keys and permanent keys. With OpsCenter Analytics, you can perform advanced reporting and create custom reports.

See "OpsCenter Analytics licensed features" on page 75.

You can also add, delete, or view license keys after installation from the OpsCenter console.

See "About managing licenses" on page 212.

Differences between OpsCenter and OpsCenter Analytics

Table 2-2 lists the differences between Veritas NetBackup OpsCenter and OpsCenter Analytics.

Table 2-2 Differences between Veritas NetBackup OpsCenter and OpsCenter Analytics

Veritas NetBackup OpsCenter	OpsCenter Analytics
Veritas NetBackup OpsCenter is visible from the title bar and logon page of the OpsCenter console.	OpsCenter Analytics is visible from the title bar and logon page of the OpsCenter console.

Table 2-2 Differences between Veritas NetBackup OpsCenter and OpsCenter Analytics *(continued)*

Veritas NetBackup OpsCenter	OpsCenter Analytics
Veritas NetBackup OpsCenter lets you do operational reporting.	OpsCenter Analytics lets you perform advanced, business-level reporting. With OpsCenter Analytics, you have an additional reporting functionality that includes (but is not limited to) the following: ■ Creating custom reports ■ Creating reports using SQL queries ■ Running or configuring charge back reports ■ Viewing report data for any previous date More information about the licensed features is available. See "OpsCenter Analytics licensed features" on page 75.

OpsCenter Analytics licensed features

Table 2-3 shows the list of licensed features, where they are located in the OpsCenter console, and how they appear in the unlicensed version.

Table 2-3 Licensed features in OpsCenter Analytics

Licensed feature	Access on the OpsCenter Analytics console	Access on the unlicensed Veritas NetBackup OpsCenter console
Create a Custom Report	**Reports > Report Templates > Create a New Report > Create a Custom Report** **Reports > My Reports > Create a New Report > Create a Custom Report**	Create a custom report option is disabled.
Create a report using SQL query	**Reports > Report Templates > Create a New Report > Create a report using SQL query** **Reports > My Reports > Create a New Report > Create a report using SQL query**	Create a report using SQL query option is disabled.

Table 2-3 Licensed features in OpsCenter Analytics *(continued)*

Licensed feature	Access on the OpsCenter Analytics console	Access on the unlicensed Veritas NetBackup OpsCenter console
Run or view charge back reports	**Report > Report Templates > Charge back Reports**	Charge back reports are disabled.
Control charge back settings	**Settings > Charge back**	Charge back settings are disabled.
Full control over report time frame selection. You can view report data for any previous date.	**Report > Report Templates > Create New Report** (**Relative and Absolute Time frame** window on the **Select Parameters** page.) **Reports > My Reports > Create New Report** (**Relative and Absolute Time frame** window on the **Select Parameters** page.) **Report > Report templates** (Run a report, click **Edit Report** and then **Relative and Absolute Time frame** window.) **Reports > My Reports** (Run a report, click **Edit Report** and then **Relative and Absolute Time frame** window.)	You cannot view data older than 60 days.
Reconcile Task	**Monitor > Jobs**. The **Reconcile** option under the **More** drop-down list is disabled.	The **Reconcile** option is disabled.
Edit View level Alias tab	**Settings > Edit View level Alias**	The **Edit View level Alias** tab is disabled.
Object Types	**Settings > Configuration > Object Types**	The **Object Types** tab is disabled.

OpsCenter DVDs

The OpsCenter software application is shipped with two DVDs that are part of the NetBackup media kit. The NetBackup media kit comprises NetBackup DVDs as well as OpsCenter DVDs.

Table 2-4 describes the contents of each DVD.

Table 2-4 OpsCenter DVD contents

DVD	Platform OS	Contents
OpsCenter (1 of 2)	Windows (32-bit and 64-bit)	■ 32-bit Windows platforms (x86) ■ 64-bit Windows platforms (x64) ■ OpsCenter documentation
OpsCenter (2 of 2)	UNIX	■ RedHat ■ SUSE ■ OpsCenter documentation

You can either install an unlicensed OpsCenter version, a demo version, or purchase a OpsCenter Analytics license key and install the licensed version. With the demo version, you can access the OpsCenter Analytics features for 60 days (starting from the day you install the demo key).

See "About the OpsCenter licensing model" on page 73.

See "Exporting authentication settings" on page 119.

Managed NetBackup master server considerations

Starting from 8.0 version, Veritas does not recommend the OpsCenter server and the NetBackup master server to be on the same host. For more information, refer to the following article:

https://www.veritas.com/support/en_US/article.100033419

The following recommendations and requirements should be considered for your managed master servers:

- OpsCenter does not collect data from the managed servers that are configured within a network address translation (NAT) network.
- The OpsCenter server should be configured as a fixed host with a static IP address.
- Veritas recommends that any NetBackup master server is monitored by only one OpsCenter server.
- The OpsCenter Server must be of the same or later version than the NetBackup master server version that it monitors. For example, OpsCenter 8.0 can monitor NetBackup 8.0 and earlier master servers.
- If a NetBackup master Server that was added in OpsCenter is upgraded to a newer version, you should disable and then enable the master server in the OpsCenter user interface.

- If you plan to upgrade the backup product like NetBackup, Backup Exec, or PureDisk and the OpsCenter components, it is recommended that you upgrade OpsCenter components first. By upgrading OpsCenter components before the backup product, OpsCenter can start collecting data from the backup product once it is added to the console.

  You must perform upgrades in the following order:

Serial No.	Steps to upgrade	Reference
1.	Upgrade the OpsCenter Server	See "Upgrading OpsCenter on Windows" on page 121.
2.	Upgrade the OpsCenter Agent	See "Upgrading OpsCenter on Windows" on page 121.
3.	Upgrade the OpsCenter View Builder	See "Upgrading OpsCenter on Windows" on page 121.
4.	Upgrade the backup product that you are using like NetBackup.	Refer to the appropriate product manuals.

  The order also holds true if you plan to upgrade only OpsCenter and not the backup product. Always upgrade the OpsCenter Server first followed by the Agent and the View Builder.

- OpsCenter can be used to monitor a NetBackup cluster.

  See *NetBackup High Availability Administrator's Guide* for more details on setting up a NetBackup cluster environment.

More information about adding managed NetBackup master servers in OpsCenter is available.

See "Adding a master server or an appliance master server in the OpsCenter console" on page 291.

About using NBSL to collect data from NetBackup master servers

The OpsCenter Server uses the NetBackup Service Layer (NBSL) to collect most of the data types from a NetBackup master server.

To collect the data types like capacity and traditional license from NetBackup, OpsCenter uses the bpjava protocol.

OpsCenter requires NBSL for all NetBackup monitoring, managing, and control functions. OpsCenter is affected if NBSL stops running on a managed NetBackup server.

If NBSL stops, OpsCenter may not capture any changes that were made to the NetBackup configuration. When NBSL restarts, OpsCenter correctly recaptures the latest state.

About designing your OpsCenter Server

Before setting up an OpsCenter Server, review the recommendations and requirements that are listed in the earlier sections.

See "Managed NetBackup master server considerations" on page 77.

About the OpsCenter database requirements

The Sybase database that OpsCenter uses is similar to the database that NetBackup uses. The database is installed as part of the OpsCenter server installation.

Note the following:

- After you configure OpsCenter, OpsCenter disk space depends on the volume of data initially loaded on the OpsCenter server from the managed NetBackup servers.
  The initial data load on the OpsCenter server is in turn dependent on the following data present in the managed master servers:
  - Number of policy data records
  - Number of job data records
  - Number of media data records
- The rate of OpsCenter database growth depends on the quantity of managed data. This data can be policy data, job data, or media data.

For information on how to adjust database values for better OpsCenter performance, refer to the new *OpsCenter Performance and Tuning Guide* at the following location:

http://www.veritas.com/docs/000003387

Supported upgrade paths in OpsCenter

OpsCenter supports direct upgrades from the following versions:

- OpsCenter 7.7.x to OpsCenter 8.1.1
- OpsCenter 8.0 to OpsCenter 8.1.1
- OpsCenter 8.1 to OpsCenter 8.1.1

About planning an OpsCenter Agent deployment

Before deploying an OpsCenter Agent, you must decide if you need an OpsCenter Agent. To make this decision, you must examine the following parameters:

Do I need an Agent?	See "When do you need an Agent?" on page 80.
Can a single Agent monitor multiple product versions?	See "Can a single Agent monitor different product versions?" on page 80.
Should I install the Agent on the product host? Should I install the Agent on a different platform?	See "Where should I install the Agent?" on page 80.
Quickly glance through the Agent deployment matrix	See "About the OpsCenter Agent deployment matrix" on page 82.

Caution: OpsCenter does not support Backup Exec.

Refer to the *NetBackup Compatibility Guide* for information on supported products and their versions.

http://www.veritas.com/docs/DOC5332

When do you need an Agent?

You do not need an OpsCenter Agent to collect data from PureDisk or NetBackup.

Can a single Agent monitor different product versions?

A single Agent can monitor multiple versions of backup products.

Note: PureDisk data collection does not require a separate Agent. You can use the Integrated Agent of the OpsCenter Server for data collection. To create or configure the data collector, select the Agent that is installed as the Integrated Agent.

See "Configuring PureDisk data collector" on page 297.

Where should I install the Agent?

Installing the OpsCenter Agent has an impact on the backup environment. The OpsCenter Agent must be compatible with the operating system of the backup application host.

You can deploy the OpsCenter Agent on any of the following hosts:

Product host

The product host is the host where the backup product is installed.

Advantages of installing OpsCenter Agent on a product host are the following:

- Ease of maintenance for upgrades, because you only service one host.
- Minimal intrusion on backup hosts, because only one agent is installed on a backup host.

Disadvantages of installing OpsCenter Agent on the product host are the following:

- The Agent may use significant system resources, which can affect the product host's performance.

OpsCenter Server host or a separate host

The OpsCenter Agent can be installed on a host different from the product host; this is sometimes called a Remote Agent. The different host may be the OpsCenter Server host or a separate host.

You should deploy a Remote Agent in the following situations:

- When the OpsCenter Agent is not compatible with the operating system of the product (such as HP-UX).
- When the product host system has insufficient resources to support co-location of the OpsCenter Agent and the backup application.

In such situations, the Agent should remotely communicate with backup products.

Advantages of installing OpsCenter Agent on the Server host or a separate host are the following:

- You do not have to install additional software on backup application hosts, because the backup data is gathered remotely.
- If you install Agent on the OpsCenter Server host, you need to maintain only one host for both the OpsCenter Agent and the Server, which avoids the maintenance that might otherwise be involved in upgrading the Agent.

Disadvantages of installing OpsCenter Agent on the Server host include the following:

- You must install a component of the backup application on the OpsCenter Server host.
- In some situations, a backup application license is required for the component that is installed on the OpsCenter Server host.

Note the following points about installing an OpsCenter Agent:

- Only one OpsCenter Agent can be installed on any host.

- A single Agent can be configured for multiple data collectors which collect data from the respective product hosts.

About the OpsCenter Agent deployment matrix

Table 2-5 compiles Agent-related information for each backup product. The Agent deployment matrix can help you in deploying the OpsCenter Agent.

Table 2-5 Agent deployment matrix

Product	Is an Agent Required?	Can a single Agent monitor multiple product versions?	Should Agent be deployed on the product host?	Can Agent be installed on any platform?
PureDisk	Not Required	None	None	Windows

Preparation for installation or upgrade

Review the following checklists before installing OpsCenter.

Table 2-6 lists the things you must check before you install OpsCenter on a Windows server.

Table 2-6 OpsCenter installation and upgrade checklist for Windows

Item	Task
1.	Ensure that you install OpsCenter software on a compatible platform. http://www.netbackup.com/compatibility
2.	Ensure that no other installation is in progress while you install OpsCenter. In addition, Veritas recommends that you do not stop the installer forcefully while the OpsCenter upgrade is in progress.

Table 2-6 OpsCenter installation and upgrade checklist for Windows *(continued)*

Item	Task
3.	If 8.3 file name creation is disabled on a Windows host, it is recommended that you enable it and restart the Windows host before installing or upgrading to OpsCenter components. If you install or upgrade to OpsCenter components on a Windows host where 8.3 name creation is disabled, then you must do the following: ■ Install OpsCenter components on a customized (non-default) location like `D:\Favorites`. The default installation location of OpsCenter components is `C:\Program Files\Symantec`. ■ The customized location that you provide should not contain spaces or special characters like (, % etc.
4.	Ensure that the antivirus software is disabled before you install OpsCenter.
5.	Ensure that your OpsCenter server is configured as a fixed host with a static IP address.
6.	Ensure that the fully qualified domain name (FQDN) of your OpsCenter Server has no more than 44 characters.
7.	For a new OpsCenter installation, ensure that the database directory has at least 20 MB of available space. Note that after you install and start using OpsCenter, the database grows in size, and requires more space. See "Supported upgrade paths in OpsCenter" on page 79.
8.	If you plan to upgrade OpsCenter, ensure the following: You should take care of these disk space requirements before you upgrade.
9.	Before upgrading to OpsCenter, Veritas recommends that you take a hot backup of the OpsCenter database (without stopping OpsCenter) using the `dbbackup` utility. See "Backing up the OpsCenter database" on page 184.

Table 2-6 OpsCenter installation and upgrade checklist for Windows *(continued)*

Item	Task
10.	If you plan to upgrade both the backup product like NetBackup, Backup Exec, or PureDisk and the OpsCenter components, it is recommended that you upgrade OpsCenter components first. By upgrading OpsCenter components before the backup product, OpsCenter can start collecting data from the backup product once it is added to the console. You must perform upgrades in the following order: ■ Upgrade the OpsCenter Server ■ Upgrade the OpsCenter Agent ■ Upgrade the OpsCenter View Builder ■ Upgrade the backup product that you are using like NetBackup. The above order also holds true if you plan to upgrade only OpsCenter and not the backup product. Always upgrade the OpsCenter Server first followed by the Agent and the View Builder.
11.	If you plan to upgrade OpsCenter and have installed the OpsCenter database on a custom location, ensure that the free space on the drive where OS is installed is equal to or more than size of the current OpsCenter database. In case free space on the drive where OS is installed is less than size of the current OpsCenter database, use the following procedure before you upgrade: **1** Create a directory (say temp) where the OpsCenter database is installed: <*OpsCenterDatabaseCustomLocation*>\temp. **2** Create a new system variable with variable name `SATMP` and value as: <*OpsCenterDatabaseCustomLocation*>\temp. **3** Run the OpsCenter installer. **4** After successful upgrade, delete the environment variable `SATMP` and the directory `temp` from <*OpsCenterDatabaseCustomLocation*>.
12.	Ensure that the necessary ports are opened before you install OpsCenter on a hardened server. See "About communication ports and firewall considerations in OpsCenter" on page 188.
13.	Ensure that the name of the folder in which you install OpsCenter does not contain any special characters such as %, ~, !, @, $, &, ^, or #.
14.	If a file called `program` exists in the `C:` folder of your OpsCenter Server, rename or delete the file before you install OpsCenter.

Table 2-6 OpsCenter installation and upgrade checklist for Windows *(continued)*

Item	Task
15.	Ensure that the system on which the OpsCenter server is installed has valid values for the following OS parameters: ■ Display language ■ Location Check your respective OS documentation for more information on these parameters.
16.	Install OpsCenter Server, Agent, and View Builder of the same versions. For example, Server 7.7 is compatible only with Agent 7.7 and View Builder 7.7.
17.	Also in case OpsCenter components are installed on a dual stack IPv4 and IPv6 host, the default IP must be IPv4 and the hostname of the system must be configured accordingly.
18.	In a clustered environment, first upgrade OpsCenter Server on the active node and then on the passive nodes.
19.	To install OpsCenter on Windows 2008 or later version, you must log on as the official administrator. Users that are assigned to the Administrators Group but are not the official administrator cannot install OpsCenter in UAC-enabled environments. To allow users in the Administrators Group to install OpsCenter, disable UAC.

Table 2-7 lists the things you must check before you install OpsCenter on a UNIX server.

Table 2-7 OpsCenter installation and upgrade checklist for UNIX

Item	Task
1.	Ensure that you install OpsCenter software on a supported platform. http://www.netbackup.com/compatibility
2.	Ensure that no other installation is in progress while you install OpsCenter. In addition, Veritas recommends that you do not stop the installer forcefully while the OpsCenter upgrade is in progress.
3.	Ensure that your OpsCenter Server is configured as a fixed host with a static IP address.
4.	Ensure that `/opt` is a directory and not a symbolic link to another directory.
5.	Ensure that the fully qualified domain name (FQDN) of your OpsCenter Server has no more than 44 characters.

Table 2-7 OpsCenter installation and upgrade checklist for UNIX *(continued)*

Item	Task
6.	Ensure that ksh (Korn shell) is installed on the host where you want to install or upgrade OpsCenter Server. **Warning:** If you fail to install ksh before installation or upgrade, you may not be able to logon to OpsCenter user interface.
7.	For OpsCenter installation on UNIX, a minimum space of approximately 2.5 GB is required at root folder before starting the installation process. This space is necessary for installing components like PBX, Perl, and VRTSvlic. In addition, the space is required to copy installation related logs at root location. If the space is not available at the root location, installation cannot proceed.
8.	For a new OpsCenter installation, ensure that the database directory has at least 20 MB of available space. Note that once you install and start using OpsCenter, the database grows in size, and requires more space. See "About designing your OpsCenter Server" on page 79.
9.	Ensure that the necessary ports are opened before you install OpsCenter on a hardened server. See "About communication ports and firewall considerations in OpsCenter" on page 188.
10.	If you need to monitor a single master server, install OpsCenter on the NetBackup master server or media server (recommended).
11.	Ensure that the name of the folder in which you install OpsCenter does not contain any special characters such as %, ~, !, @, $, &, ^, or #.
12.	Ensure that the system on which the OpsCenter server is installed has valid values for the following OS parameters: ■ Display language ■ Location Check your respective OS documentation for more information on these parameters.
13.	Ensure that the available disk space is at least two times the database size. This should be done before the upgrade.
14.	Before upgrading OpsCenter, Veritas recommends that you take a hot backup of the OpsCenter database (without stopping OpsCenter) using the `dbbackup` utility. See "Backing up the OpsCenter database" on page 184.

Table 2-7 OpsCenter installation and upgrade checklist for UNIX *(continued)*

Item	Task
15.	If you plan to upgrade both the backup product like NetBackup, Backup Exec, PureDisk, or OpsCenter, it is recommended that you upgrade OpsCenter components first. By upgrading OpsCenter components before the backup product, OpsCenter can start collecting data from the backup product once it is added to the console. You must perform upgrades in the following order: ■ Upgrade the OpsCenter Server ■ Upgrade the backup product that you are using like NetBackup.

16.	If you plan to upgrade OpsCenter and have installed the OpsCenter database on a custom location, ensure that the free space on /tmp is equal to or more than the size of current OpsCenter database.
	In case the free space on /tmp is less than size of the current OpsCenter database, use the following procedure before you upgrade:
	1 Create a directory (say temp) where the OpsCenter database is installed: <*OpsCenterDatabaseCustomLocation*>/temp.
	2 Export a variable named `SATMP` with the value of this variable as <*OpsCenterDatabaseCustomLocation*>/temp.
	Use the following command:
	`export SATMP=<OpsCenterDatabaseCustomLocation>/temp`
	3 Run the OpsCenter installer.
	4 After successful upgrade, unset the environment variable `SATMP` and remove the `temp` directory from <*OpsCenterDatabaseCustomLocation*>.
	Use the following command to unset the `SATMP` variable:
	`unset SATMP`

17.	If OpsCenter components are installed on a dual stack IPv4 and IPv6 host, the default IP must be IPv4 and the hostname of the system must be configured accordingly.
18.	In a clustered environment, first upgrade OpsCenter Server on the active node and then on the passive nodes.

Installing OpsCenter on Windows and UNIX

This section describes the procedures for fresh installation of OpsCenter on Windows and UNIX hosts.

Note: After you install OpsCenter, when you install a language pack do not stop the OpsCenter services. To verify if the language pack has been installed successfully, go to **Settings** > **User Preferences** > **General** > **Default Locale** and check if you see the locale that you installed.

See "About OpsCenter upgrade on Windows and UNIX" on page 115.

See "About clustering OpsCenter" on page 139.

Table 2-8 provides steps to install OpsCenter components. You can use this table as a checklist while installing OpsCenter.

Table 2-8 Steps to install, upgrade, and cluster OpsCenter

Step number	Step	Reference topic
1	■ Review the hardware requirements and software requirements for OpsCenter Server and Agent hosts, carefully. ■ Make sure that you satisfy the operating system requirements. ■ Go through the firewall settings and port number information. ■ Go through the Agent deployment section. ■ Review the Install/Upgrade checklists before installing OpsCenter.	■ See "About planning an OpsCenter installation" on page 70. ■ http://www.netbackup.com/compatibility ■ See "About communication ports and firewall considerations in OpsCenter" on page 188. ■ See "About planning an OpsCenter Agent deployment" on page 80. ■ See "Preparation for installation or upgrade" on page 82.
2	Go through the appropriate installation section. Different sections are available for fresh installation, upgrade, and clustering. **Note:** After installation, verify if OpsCenter is running properly.	See "About installing OpsCenter on Windows" on page 88. See "About installing OpsCenter on UNIX" on page 94. See "About OpsCenter upgrade on Windows and UNIX" on page 115. See "About clustering OpsCenter" on page 139.

About installing OpsCenter on Windows

Use the Installation Wizard to install OpsCenter on a Windows host. The two OpsCenter DVDs contain OpsCenter software for all available platforms.

Review the following considerations before installing OpsCenter components on Windows:

- Veritas recommends that you enable 8.3 file name creation before installing OpsCenter components. If 8.3 file name creation is disabled, enable it and restart the Windows host before installing or upgrading to OpsCenter components.
- You must not run any other installation while installing OpsCenter components. Additionally after an installation is complete, you should wait for some time before installing other OpsCenter components.

Note: Veritas recommends that you do not cancel or interrupt the installation process once it is started.

See "Installing OpsCenter Server on Windows" on page 89.

See "Installing OpsCenter Agent on Windows" on page 91.

See "Installing OpsCenter View Builder on Windows" on page 92.

Installing OpsCenter Server on Windows

Use the following procedure to install OpsCenter Server on Windows hosts.

Note: If you install OpsCenter components on a system where the same version of OpsCenter is already installed, the installer runs in a Maintenance mode. Maintenance mode lets you repair or remove the OpsCenter component that is installed on your system.

To install OpsCenter Server on Windows

1. On a Windows host where you want to install OpsCenter Server, insert the OpsCenter product DVD in the DVD drive.
2. - If autorun is enabled, the Veritas DVD Browser appears.
   - If autorun is not enabled, click **Start > Run**. On the **Run** dialog box, in the **Open** text box, type ***D***`:\Browser.exe` and press **Enter**:
     Where *D* is the DVD drive.
     The Veritas DVD Browser appears.
3. On the Veritas DVD browser, click the **Installation** link.
4. Click the **OpsCenter Server Installation** link to install Veritas NetBackup OpsCenter server.
5. The OpsCenter Installation Wizard appears. Click **Next**.

6 Read the license agreement, check **I accept the terms of the license agreement**, and click **Next**.

You may opt to check or uncheck **Participate in the NetBackup Product Improvement Program**. This option is checked by default.

If you check this option, the installer uploads installation deployment and product usage information to Veritas automatically and in a secured manner. This data helps Veritas to guide future product development and also analyze issues.

7 The following options are displayed on the Installation Choice screen:

Install to this computer only	Select this option to install OpsCenter Server on this host.
Install a clustered OpsCenter Server	Select this option to install OpsCenter Server on all selected nodes, in a clustered mode. You need to install OpsCenter Server manually on each node of the cluster. This option is enabled if you have Cluster Server installed. See "Clustering OpsCenter on Windows" on page 143.

Select **Install to this computer only**.

In the Installation Method section, click **Typical** to use the default settings, installation location, or port numbers. Compare the space that the installation requires with the actual space available in the installation directory.

Click **Custom** if you want to change the default settings, locations, or port numbers.

Click **Next**.

8 On the **License Keys** panel, enter your demo or permanent key that you have received with the purchase of OpsCenter and click **Add Key**.

See "OpsCenter Analytics license keys" on page 74.

You can also add the license keys later from the OpsCenter console.

See "About managing licenses" on page 212.

9 Click **Next**. The installer shows the summary of the settings that you have selected for installation.

Check **Save Summary to** field to save the installation summary. Click **Browse** to save the installation summary in your preferred location.

10 Click **Install**.

The installer starts installing the OpsCenter Server software.

Note: The default OpsCenter database location on Windows is:

`C:\Program Files\Symantec\OpsCenter\server\db\data`

---

11 After successful installation, you can view the OpsCenter console or view installation logs.

The installation logs are generated in the following location:`%ALLUSERSPROFILE%\Symantec\OpsCenter\INSTALLLOGS\OpsCenterServerInstallLog.htm`.

If you run the installer in a maintenance mode later,`OpsCenterServerMaintenanceInstallLog.htm` is also generated in the same location.

Note: After successful installation, the OpsCenter database password is set to an auto-generated string. Veritas recommends that you change the database password after the installation.

See "Changing the OpsCenter database administrator password" on page 172.

---

12 Click **Finish**.

Installing OpsCenter Agent on Windows

Use the following procedure to install OpsCenter Agent on a Windows host.

To install OpsCenter Agent on Windows

1 You can install the OpsCenter Agent either on the OpsCenter Server host, product host, or a separate host. To decide where you want to install the OpsCenter Agent, review the information on Agent deployments.

See "About planning an OpsCenter Agent deployment" on page 80.

2 On a Windows host where you want to install OpsCenter Agent, insert the OpsCenter product DVD in the DVD drive.

3
- If autorun is enabled, the Veritas DVD Browser appears.
- If autorun is not enabled, click **Start > Run**. On the **Run** dialog box, in the **Open** text box, type ***D*:\Browser.exe** and press **Enter**:
  Where *D* is the DVD drive.

The Veritas DVD Browser appears.

4 On the Veritas DVD Browser, click the **Installation** link.

5 Click the **OpsCenter Agent Installation** link to install OpsCenter Agent.

6 The OpsCenter Installation Wizard appears. Click **Next**.

7 Read the license agreement, check **I accept the terms of the license agreement** and click **Next**.

You may opt to check or uncheck **Participate in the NetBackup Product Improvement Program**. This option is checked by default.

If you check this option, the installer uploads installation deployment and product usage information to Veritas automatically and in a secured manner. This data helps Veritas to guide future product development and also analyze issues.

8 The default installation location is `C:\Program Files\Symantec`. To install OpsCenter to a different directory, click **Browse**.

Click **Next**.

9 The installer shows the summary of the settings that you have selected for Agent installation.

Check **Save Summary to** field to save the installation summary. Click **Browse** to save the installation summary in your preferred location.

10 Click **Install**.

The installer starts installation of OpsCenter Agent.

11 After successful installation, you can view Agent installation logs or open the readme file.

The installation logs are generated at the following location:
`%ALLUSERSPROFILE%\Symantec\OpsCenter\INSTALLLOGS\OpsCenterAgentInstallLog.htm`.

If you run the installer in a maintenance mode later,`OpsCenterAgentMaintenanceInstallLog.htm` is also generated in the same location.

12 Click **Finish**.

Installing OpsCenter View Builder on Windows

Use the following procedure to install Veritas NetBackup OpsCenter View Builder.

To install OpsCenter View Builder on Windows

1. On the OpsCenter Server host, insert the OpsCenter product DVD in the DVD drive.
2. - If autorun is enabled, the Veritas DVD Browser appears.
   - If autorun is not enabled, click **Start > Run**. On the **Run** dialog box, in the **Open** text box, type ***D*:\Browser.exe** and press **Enter**:
     Where *D* is the DVD drive.
     The Veritas DVD Browser appears.
3. On the Veritas DVD Browser, click the **Installation** link.
4. Click the **OpsCenter View Builder Installation** link to install Veritas NetBackup OpsCenter View Builder.
5. The OpsCenter Installation Wizard appears. Click **Next**.
6. Read the license agreement, check '**I accept the terms of the license agreement**' and click **Next**.

   You may opt to check or uncheck **Participate in the NetBackup Product Improvement Program**. This option is checked by default.

   If you check this option, the installer uploads installation deployment and product usage information to Veritas automatically and in a secured manner. This data helps Veritas to guide future product development and also analyze issues.
7. On the Installation Location screen, click **Browse** if you want to change the default location for Veritas NetBackup OpsCenter View Builder installation.

   Note: The default installation location on a Windows 64-bit computer is `C:\Program Files (x86)\Symantec`.

   ---

8. Select a new location and click **Next**.
9. The installer shows the summary of the settings that you have selected for Veritas NetBackup OpsCenter View Builder installation.

   Check **Save Summary to** field to save the installation summary. Click **Browse** to save the installation summary in your preferred location.
10. Click **Install**.

    The installer starts installation of Veritas NetBackup OpsCenter View Builder.

11 After successful installation, you can view the installation logs or open the readme file.

The installation logs are generated in the following location:`%ALLUSERSPROFILE%\Symantec\OpsCenter\INSTALLLOGS\OpsCenterViewBuilderInstallLog.htm`.

If you run the installer in a maintenance mode later,`OpsCenterViewBuilderMaintenanceInstallLog.htm` is also generated in the same location.

12 Click **Finish**.

About installing OpsCenter on UNIX

This section provides you with the procedure to install OpsCenter on a UNIX host.

You can install OpsCenter components from the OpsCenter DVD's. Three DVD's for OpsCenter are available—one for Windows and two for UNIX. Select the appropriate OpsCenter DVD based on the platform on which you plan to install.

Note: Veritas recommends that you do not cancel or interrupt the installation process once it is started.

See "Installing OpsCenter Server on UNIX" on page 94.

Installing OpsCenter Server on UNIX

Use the following procedure to install OpsCenter Server software on UNIX hosts.

To install OpsCenter Server on UNIX

1 Open a UNIX console and log on as `root` on the target host.

2 Mount the appropriate OpsCenter product DVD on the computer where you are installing OpsCenter.

3 Type the following command: `./install`. Press **Enter**.

4 The Welcome message is displayed. Press **Enter** to continue.

5 The installer then checks if OpsCenter Server is installed on the system or not. It prompts you in case OpsCenter Server is already installed. The installer also examines the system for existing packages.

6 The installer displays a list of components that get installed like PBX, AT, OpsCenter Server, OpsCenter GUI etc. Review this list and press **Enter** to continue.

7 The installer prompts you with the following question:

```
Where do you want to install Veritas OpsCenter? </opt>
```

Type a directory path where you want to install the OpsCenter Server packages and press **Enter**.

To accept the default path (`/opt`), press **Enter** without typing a directory path.

8 Type **y** to confirm the directory path and press **Enter**.

9 The installer prompts you with the following question:

```
Participate in the NetBackup Product Improvement Program? [y,n,q] (y)
```

If you type **y** and press **Enter**, the installer uploads installation deployment and product usage information to Veritas automatically and in a secured manner. This data helps Veritas to guide future product development and also analyze issues.

10 OpsCenter Server is installed on the system.

The installer prompts for the following information:

```
Specify a local directory for the Veritas OpsCenter database.
A directory named 'OpsCenterServer' will be created within the
directory that you specify. (/var/symantec/)
```

Type a directory path under which to install the OpsCenter database and press **Enter**.

If you create an alternate database directory, the script creates the folder `OpsCenterServer` below your directory.

To accept the default database installation directory `(/var/Symantec)`, press **Enter** without typing a directory path.

In case the database installation directory (`/var/symantec`) does not exist on the host, the following information is displayed:

```
Directory "/var/symantec" does not exist. Do
you want to create the directory? [y,n,q] y
```

Type **y** to confirm and press **Enter**.

The following information is displayed:

```
The OpsCenter database server may require up to
1 GB of temporary space at runtime. By default, temporary files
will be created in the database installation directory
/var/Symantec/OpsCenterServer
```

11 You are prompted with the following message:

```
Would you like to use an alternate directory for
database server temporary space? [y,n,q] (n)
```

To use the database installation directory for database server temporary space, press **Enter** without typing a directory path.

To specify an alternate directory, type **y** and press **Enter**.

Type a directory path for the database server temporary space and press **Enter**.

12 Review the installation options you selected. The location of database directory and the database temp directory is also displayed.

13 Type `y` and press **Enter** to confirm the selection and continue.

Type `n` and press **Enter** to repeat the configuration steps and revise your selection.

Configuration changes are made to the system.

14 You are prompted for license information. The installer prompts you with the following:

```
Please enter a Veritas OpsCenter Analytics license key
or press <Return>:
```

Enter a valid demo or permanent key that you have received with the purchase of OpsCenter and press **Enter**.

If you do not enter a key, you get an unlicensed version. With the unlicensed OpsCenter version, you cannot access the licensed features.

See "OpsCenter Analytics license keys" on page 74.

You can also add the license keys later from the OpsCenter console.

See "About managing licenses" on page 212.

Note: After successful installation, OpsCenter database password is set to an auto-generated string. Veritas recommends that you change the database password after the installation.

See "Changing the OpsCenter database administrator password" on page 172.

About installing OpsCenter silently on Windows

This section explains how you can install the OpsCenter components silently on Windows platform. It also covers how you can track the progress of silent installation and some troubleshooting tips.

See "Installing OpsCenter Server software silently" on page 97.

See "About editing the response file" on page 110.

See "About tracking the progress of silent installation" on page 112.

Installing OpsCenter Server software silently

A silent installation avoids the need for interactive input. A silent installation uses a response file to automate OpsCenter installation. Use a silent installation when you need to perform an identical installation on several servers.

You must create a response file first and then use the file to perform a silent installation. The procedure for creating a response file requires that you run through the Installation Wizard. The values that you specify in the Wizard pages are saved to the response file.

You can also edit the response file if required.

See "About editing the response file" on page 110.

Note the following points about silent installation:

- Silent installation of OpsCenter is only supported on Windows platforms.
- Silent installation of OpsCenter is not supported on clusters.

To install OpsCenter server software silently

1. Log on as administrator to the system where you want to install OpsCenter server software.
2. Insert the appropriate OpsCenter product DVD in the DVD drive.
3. Open the command prompt on your system.

   Navigate to `<DVD Drive>\<Architecture>\Server` directory.
4. Enter the following command:

   ```
   SETUP.EXE -NoInstall
   ```

   Note that the switch `-NoInstall` is case-sensitive .

   This command starts the Installation Wizard where you can specify your preferences. Note that the Installation Wizard creates the response file based on your inputs and does not install the product.

5 The **Welcome** panel of the OpsCenter Installation Wizard appears. Click **Next**.

6 Read the license agreement, check **I accept the terms of the license agreement** and click **Next**.

You may opt to check or uncheck **Participate in the NetBackup Product Improvement Program**. This option is checked by default.

If you check this option, the installer uploads installation deployment and product usage information to Veritas automatically and in a secured manner. This data helps Veritas to guide future product development and also analyze issues.

7 Select **Install to this computer only** on the **Installation Choice** panel.

In the **Installation Method** section, click **Typical** to use the default settings, installation location, or port numbers. Also compare the space that is required by the installation with the actual space available in the installation directory.

Note: Click **Custom** if you want to change the default settings, locations, or port numbers.

Click **Next**.

8 On the **License Keys** panel, enter your demo or permanent key that you have received with the purchase of OpsCenter and click **Add Key**.

If you do not enter a key, you get an unlicensed version. With the unlicensed version (OpsCenter), you cannot access the licensed features.

See *OpsCenter Administrator's Guide* for licensing details.

Click **Next**.

9 The installer shows the summary of the settings that you have selected for installation. Check **Save Summary to** field to save the installation summary. Click **Browse** to save the installation summary in your preferred location.

Click **Install**. Note that clicking Install does not install the product.

10 The **Installation Status** panel is displayed. Click **Finish**.

11 A response file named `Server-<DD-MM-YY-HH-MIN-SS>.XML` is created at the following location:

Drive`:\windows\temp\Symantec\OpsCenter`

For example: `C:\windows\temp\Symantec`

This XML file can be used to install OpsCenter Server software on multiple computers.

12 On the command prompt, ensure that you are in the directory where `SETUP.EXE` is located.

13 Enter the following command to run the silent installation:

`SETUP -Silent -RespFile` *<path of the response file>*

Example: `Setup -Silent -RespFile C:\Server-07-12-09-06-11-31.xml`

Note that the switches `-Silent` and `-RespFile` are case-sensitive .

14 The installation logs are generated in the following location:

`%ALLUSERSPROFILE%\Symantec\OpsCenter\INSTALLLOGS\OpsCenterServerInstallLog.htm`.

If you run the installer in a maintenance mode later,`OpsCenterServerMaintenanceInstallLog.htm` is also generated in the same location.

See the following section to track the progress of the installation.

See "About tracking the progress of silent installation" on page 112.

After successful installation, you can see OpsCenter Server in **Add/Remove Programs**.

To install OpsCenter Agent silently

1 Log on as administrator to the system where you want to install OpsCenter Agent software.

2 Insert the appropriate OpsCenter product DVD in the DVD drive.

3 Open the command prompt on your system.

Navigate to `<DVD Drive>\<Architecture>\Agent` directory.

Example: `D:\x86\Agent`

4 Enter the following command:

`SETUP.EXE -NoInstall`

Note that the switch `-NoInstall` is case-sensitive .

This command starts the Installation Wizard where you can specify your preferences. Note that the Installation Wizard creates the response file based on your inputs and does not install the product.

5 The OpsCenter Installation Wizard appears. Click **Next**.

6. Read the license agreement, check **I accept the terms of the license agreement** and click **Next**.

   You may opt to check or uncheck **Participate in the NetBackup Product Improvement Program**. This option is checked by default.

   If you check this option, the installer uploads installation deployment and product usage information to automatically and in a secured manner. This data helps Veritas to guide future product development and also analyze issues.

7. The default installation location is `C:\Program Files\Symantec`. To install OpsCenter to a different directory, click **Browse**.

   Click **Next**.

8. The installer shows the summary of the settings that you have selected for Agent installation. Check **Save Summary to** field to save the installation summary. Click **Browse** to save the installation summary in your preferred location.

9. Click **Install**. Note that clicking **Install** does not install the product.

10. The **Installation Status** panel is displayed. Click **Finish**.

11. A response file named `Agent-<DD-MM-YY-HH-MIN-SS>.XML` is created at the following location:

    `C:\windows\temp\Symantec\OpsCenter`

    This XML file can be used to install OpsCenter Agent software on multiple computers.

12. On the command prompt, ensure that you are in the directory where `SETUP.EXE` is located.

13 Enter the following command to run the silent installation:

`SETUP -Silent -RespFile` *<path of the response file>*

Example: `Setup -Silent -RespFile C:\Agent-07-12-09-06-11-31.xml`

Note that the switches `-Silent` and `-RespFile` are case-sensitive .

14 The installation logs are generated in the following location:

`%ALLUSERSPROFILE%\Symantec\OpsCenter\INSTALLLOGS\OpsCenterAgentInstallLog.htm`.

If you run the installer in a maintenance mode later,`OpsCenterAgentMaintenanceInstallLog.htm` is also generated in the same location.

See the following section to track the progress of the installation.

See "About tracking the progress of silent installation" on page 112.

After successful installation, you can see OpsCenter Agent in **Add/Remove Programs**.

To install View Builder silently

1 Log on as administrator to the system where you want to install OpsCenter View Builder software.

2 Insert the appropriate OpsCenter product DVD in the DVD drive.

3 Open the command prompt on your system.

Navigate to `<DVD Drive>\<Architecture>\ViewBuilder` directory.

Example: `D:\x86\ViewBuilder`

4 Enter the following command:

`SETUP.EXE -NoInstall`

Note that the `-NoInstall` switch is case-sensitive .

This command starts the Installation Wizard where you can specify your preferences. Note that the Installation Wizard creates the response file based on your inputs and does not install the product.

5 The OpsCenter Installation Wizard appears. Click **Next**.

6. Read the license agreement, check **I accept the terms of the license agreement** and click **Next**.

   You may opt to check or uncheck **Participate in the NetBackup Product Improvement Program**. This option is checked by default.

   If you check this option, the installer uploads installation deployment and product usage information to automatically and in a secured manner. This data helps Veritas to guide future product development and also analyze issues.

7. The default installation location is `C:\Program Files\Symantec`. To install OpsCenter View Builder to a different directory, click **Browse**.

   Note: The default installation location on a Windows 64-bit computer is C:\Program Files (x86)\Symantec.

   Click **Next**.

8. The installer shows the summary of the settings that you have selected for OpsCenter View Builder installation.

   Check **Save Summary to** field to save the installation summary. Click **Browse** to save the installation summary in your preferred location.

9. Click **Install**. Note that clicking **Install** does not install the product.

10. The **Installation Status** panel is displayed. Click **Finish**.

11. A response file named `ViewBuilder-<DD-MM-YY-HH-MIN-SS>.XML` is created at the following location:

    `C:\windows\temp\Symantec\OpsCenter`

    This XML file can be used to install OpsCenter View Builder software on multiple computers.

12. On the command prompt, ensure that you are in the directory where `SETUP.EXE` is located.

13 Enter the following command to run the silent installation:

`SETUP -Silent -RespFile` *<path of the response file>*

Example: `Setup -Silent -RespFile C:\ViewBuilder-07-12-09-06-11-31.xml`

Note that the switches `-Silent` and `-RespFile` are case-sensitive .

14 The installation logs are generated in the following location:

`%ALLUSERSPROFILE%\Symantec\OpsCenter\INSTALLLOGS\OpsCenterViewBuilderInstallLog.htm`.

If you run the installer in a maintenance mode later,`OpsCenterViewBuilderMaintenanceInstallLog.htm` is also generated in the same location.

See the following section to track the progress of the installation.

See "About tracking the progress of silent installation" on page 112.

After successful installation, you can see OpsCenter View Builder in **Add/Remove Programs**.

Upgrading OpsCenter silently

Use the following procedures to upgrade to OpsCenter components silently.

To upgrade OpsCenter

1 If you are using OpsCenter to monitor NetBackup, ensure that you upgrade OpsCenter before upgrading NetBackup.

2 Log on as administrator to the OpsCenter system that you want to upgrade.

3 Insert the appropriate OpsCenter DVD in the DVD drive.

4 Open the command prompt on your system.

Navigate to `<DVD Drive>\<Architecture>\Server` directory.

5 Enter the following command:

`SETUP.EXE -NoInstall`

Note that the `-NoInstall` switch is case-sensitive .

This command starts the Installation Wizard where you can specify your preferences. Note that the Installation Wizard creates the response file based on your inputs and does not install the product.

6. The Installation Wizard detects an existing installation of OpsCenter on the system. For example, the following message may be displayed on the Welcome screen:

   `The installer has detected that Veritas OpsCenter Server is already installed on your system that will now be upgraded to` *`version`*`.`

   Click **Next**.

7. Read the license agreement, check **I accept the terms of the license agreement** and click **Next**.

   You may opt to check or uncheck **Participate in the NetBackup Product Improvement Program**. This option is checked by default.

   If you check this option, the installer uploads installation deployment and product usage information to Veritas automatically and in a secured manner. This data helps Veritas to guide future product development and also analyze issues.

8. In the **Installation Method** section, click **Typical** to use the default settings, installation location, or port numbers. **Typical** is selected by default.

   Also compare the space that is required for installing OpsCenter server and the actual space that is available.

   Click **Next**.

Note: The **Custom** option is disabled when you upgrade from to OpsCenter. You cannot customize the default settings, locations, or port numbers while upgrading to OpsCenter.

---

9 Specify a location for saving the old OpsCenter database. The default location is `C:\Program Files\Symantec\OpsCenter_SavedData`.

Warning: In case of sequential OpsCenter upgrades (for example, version 1 > version 2 > version 3), the old `OpsCenter_SavedData` folder may already exist. If the `OpsCenter_SavedData` folder is overwritten during upgrade, the OpsCenter GUI may not start properly. To avoid this problem, you should rename the old `OpsCenter_SavedData` folder before upgrading to OpsCenter.

Click **Browse** to specify a different location.

In case the directory `C:\Program Files\Symantec\OpsCenter_SavedData` does not exist, you are prompted to create it. Click **Yes** to create the directory.

Note: Ensure that the database location has adequate space by going through the **Disk space requirements** section on this page. A green checkmark appears in the **Required** column if there is adequate disk space.

---

10 On the **License Keys** panel, enter your demo or permanent key that you have received with the purchase of OpsCenter and click **Add Key**.

See "OpsCenter Analytics license keys" on page 74.

Click **Next**.

11 The installer shows a summary of the installation settings.

Check **Save Summary to** option to save the installation summary. Click **Browse** to save the installation summary in your preferred location.

Click **Install**. Note that clicking **Install** does not install the product.

12 The **Installation Status** panel is displayed. Click **Finish**.

13 A response file named `Server-<DD-MM-YY-HH-MIN-SS>.XML` is created at the following location:

```
C:\windows\temp\Symantec\OpsCenter
```

This XML file can be used to upgrade OpsCenter Server software on multiple computers.

14 On the command prompt, ensure that you are in the directory where `SETUP.EXE` is located.

15 Enter the following command to run the silent installation:

`SETUP -Silent -RespFile` *<path of the response file>*

Example: `Setup -Silent -RespFile C:\Server-07-12-10-06-11-31.xml`

Note that the switches `-Silent` and `-RespFile` are case-sensitive .

16 The installation logs are generated in the following location:

`%ALLUSERSPROFILE%\Symantec\OpsCenter\INSTALLLOGS\OpsCenterServerInstallLog.htm`.

If you run the installer in a maintenance mode later,`OpsCenterServerMaintenanceInstallLog.htm` is also generated in the same location.

See the following section to track the progress of the installation.

See "About tracking the progress of silent installation" on page 112.

After successful installation, you can see the OpsCenter Server entry in **Add/Remove Programs**.

To upgrade OpsCenter agent silently

1 If you are using OpsCenter to monitor NetBackup, ensure that you upgrade OpsCenter first before upgrading NetBackup.

2 Log on as administrator to the OpsCenter Agent system that you want to upgrade.

3 Insert the appropriate OpsCenter DVD in the DVD drive.

4 Open the command prompt on your system.

Navigate to *<<DVD Drive>\Architecture>*`\Agent` directory.

Example: `D:\x86\Agent`

5 Enter the following command:

`SETUP.EXE -NoInstall`

Note that the `-NoInstall` switch is case-sensitive.

This command starts the Installation Wizard where you can specify your preferences. Note that the Installation Wizard creates the response file based on your inputs and does not install the product.

6. The OpsCenter Installation Wizard appears. The Installation Wizard detects an existing installation of OpsCenter Agent on the system. Based on your installed OpsCenter Agent version, the following message may be displayed on the Welcome screen:

   `The installer has detected that Veritas OpsCenter Agent old_version is already installed on your system that will now be upgraded to current_version.`

   Click **Next** to continue.

7. Read the license agreement, check **I accept the terms of the license agreement** and click **Next**.

   You may opt to check or uncheck **Participate in the NetBackup Product Improvement Program**. This option is checked by default.

   If you check this option, the installer uploads installation deployment and product usage information to Veritas automatically and in a secured manner. This data would help Veritas to guide future product development and also analyze issues.

8. The installer shows a summary of the settings that you have selected for OpsCenter Agent installation. Check **Save Summary to** field to save the installation summary. Click **Browse** to save the installation summary in your preferred location.

   Click **Install**. Note that clicking Install does not install the product.

9. The **Installation Status** panel is displayed. Click **Finish**.

10. A response file named `Agent-<DD-MM-YY-HH-MIN-SS>.XML` is created at the following location:

    `C:\windows\temp\Symantec\OpsCenter`

    This XML file can be used to upgrade OpsCenter Agent software on multiple computers.

11. On the command prompt, ensure that you are in the directory where `SETUP.EXE` is located.

12 Enter the following command to run the silent installation:

`SETUP -Silent -RespFile` *<path of the response file>*

Example: `Setup -Silent -RespFile C:\Agent-07-12-09-06-11-31.xml`

Note that the switches `-Silent` and `-RespFile` are case-sensitive .

13 The installation logs are generated in the following location:

`%ALLUSERSPROFILE%\Symantec\OpsCenter\INSTALLLOGS\OpsCenterAgentInstallLog.htm`.

If you run the installer in a maintenance mode later,`OpsCenterAgentMaintenanceInstallLog.htm` is also generated in the same location.

See the following section to track the progress of the installation.

See "About tracking the progress of silent installation" on page 112.

After successful installation, you can see the OpsCenterAgent entry in **Add/Remove Programs**.

To upgrade OpsCenter View Builder silently

1 Log on as administrator to the OpsCenter View Builder system that you want to upgrade.

2 Insert the appropriate OpsCenter DVD in the DVD drive.

3 Open the command prompt on your system.

Navigate to `<DVD Drive>\<Architecture>\ViewBuilder` directory.

Example: `D:\x86\ViewBuilder`

4 Enter the following command:

`SETUP.EXE -NoInstall`

Note that the `-NoInstall` switch is case-sensitive .

This command starts the Installation Wizard where you can specify your preferences. Note that the Installation Wizard creates the response file based on your inputs and does not install the product.

5. The OpsCenter Installation Wizard appears. The Installation Wizard detects an existing OpsCenter View Builder and shows the following message on the **Welcome** panel:

   `The installer has detected that Veritas OpsCenter View Builder old_version is already installed on your system that will now be upgraded to current_version.`

   Click **Next** to continue.

6. Read the license agreement, check **I accept the terms of the license agreement** and click **Next**.

   You may opt to check or uncheck **Participate in the NetBackup Product Improvement Program**. This option is checked by default.

   If you check this option, the installer uploads installation deployment and product usage information to Veritas automatically and in a secured manner. This data helps Veritas to guide future product development and also analyze issues.

7. The installer shows a summary of the settings that you have selected for OpsCenter View Builder installation. Check **Save Summary to** field to save the installation summary. Click **Browse** to save the installation summary in your preferred location.

   Click **Install**.

8. A response file named `ViewBuilder-<DD-MM-YY-HH-MIN-SS>.XML` is created at the following location:

   `C:\windows\temp\Symantec\OpsCenter`

   This XML file can be used to upgrade OpsCenter View Builder software on multiple computers.

9. On the command prompt, ensure that you are in the directory where `SETUP.EXE` is located.

10 Enter the following command to run silent installation:

```
Setup -Silent -RespFile <path of the response file>
```

Example: `Setup -Silent -RespFile C:\ViewBuilder-07-12-10-06-11-31.xml`

Note that the switches `-Silent` and `-RespFile` are case-sensitive .

11 The installation logs are generated in the following location:

`%ALLUSERSPROFILE%\Symantec\OpsCenter\INSTALLLOGS\OpsCenterViewBuilderInstallLog.htm`.

If you run the installer in a maintenance mode later,`OpsCenterViewBuilderMaintenanceInstallLog.htm` is also generated in the same location.

See the following section to track the progress of the installation.

See "About tracking the progress of silent installation" on page 112.

After successful installation, you can see OpsCenter View Builder in **Add/Remove Programs**.

About editing the response file

You can edit the response file to modify any inputs that you provided to the Installation Wizard. The silent installation is based on these inputs. To edit the response file, open it from `C:\Windows\Temp\Symantec\OpsCenter` and modify the **Value** field of the applicable install property. For example, you can edit the response file to modify the OpsCenter installation location, license key information, or database directory.

The following are the contents of a sample response file:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
- <XML_Install>
- HYPERLINK  \l ""- <OpsCenter_Server>
<InstallProperty Name="RAN_SETUP" Value="1" />
<InstallProperty Name="SYMTMPPATH" Value="C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\
1\Symantec\OpsCenter\" />
<InstallProperty Name="TELEMETRY_UPLOAD" Value="YES" />
<InstallProperty Name="INSTALLHTMLLOGPATH" Value="C:\Documents and Settings\
All Users\Symantec\OpsCenter\InstallLogs\OpsCenterServerInstallLog.htm" />
<InstallProperty Name="BUSINESS_REP_LIC_KEYS" Value="0" />
<InstallProperty Name="SCMSTARTTYPE" Value="auto" />
<Installproperty Name="INSTALLPBX" Value="YES" />
<Installproperty Name="STARTSERVICE" Value="YES" />
```

```
<InstallProperty Name="INSTALLDIR" Value="C:\Program Files\Symantec\" />
<Installproperty Name="DATABASE_DATA_DIR" Value="C:\Program Files\Symantec\
OpsCenter\DB\Data" />
</OpsCenter_Server>
</XML_Install>
```

For example, you can modify the OpsCenter installation location in this response file by changing the value of INSTALLDIR property from `C:\Program Files\Symantec` to `D:\Symantec`. You can also modify the database directory by modifying the value of the DATABASE_DATA_DIR property.

Similarly you can edit the license key by changing the value in the **<TagValue> *LicenseKey* </TagValue>** element under the BUSINESS_REP_LIC_KEYS install property.

If you do not have the license key, you must enter 0 (zero) as the value for the BUSINESS_REP_LIC_KEYS install property. For example, <InstallProperty Name="BUSINESS_REP_LIC_KEYS" Value="0" />

Zero indicates that the license key was not provided during the installation. In this case, you can use the features that are available only with the free or unlicensed version of OpsCenter.

For more information about the features of OpsCenter (unlicensed version), see the "About OpsCenter functions" section in the *Veritas NetBackup OpsCenter Administrator's Guide*.

If you have the license key to use with the installation, you must pass it in the response file by using the **<TagValue>*LicenseKey* </TagValue>** element under the BUSINESS_REP_LIC_KEYS install property.

You can also add multiple license keys in the response file. To add multiple license keys in the response file, add the license keys in the **<TagValue>*LicenseKey* </TagValue>** element under the BUSINESS_REP_LIC_KEYS install property on separate lines. You may enter the license keys in any order.

For example,

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
- <XML_Install>
- HYPERLINK  \l ""- <OpsCenter_Server>
<InstallProperty Name="RAN_SETUP" Value="1" />
<InstallProperty Name="SYMTMPPATH" Value="C:\DOCUME~1\ADMINI~1\LOCALS~1\
Temp\1\Symantec\OpsCenter\" />
<InstallProperty Name="TELEMETRY_UPLOAD" Value="YES" />
<InstallProperty Name="INSTALLHTMLLOGPATH" Value="C:\Documents and Settings\
All Users\Symantec\OpsCenter\InstallLogs\OpsCenterServerInstallLog.htm" />
<InstallProperty Name="BUSINESS_REP_LIC_KEYS"/>
```

```
        <TagValue>ORZDD-XYZU-BBBB-CCCC-TTTT-DRTR-UPUP-ININ-HJHJ-P</TagValue>
        <TagValue>XYZU-ORZF-UPUP-YHYH-KIOP-BUSA-LIIP-UBSI-VNGR-K</TagValue>
        <TagValue>SDHA-JNRA-UJUJ-BRDR-DEWS-HPYL-NINC-MBRI-AVXO-W</TagValue>
<InstallProperty Name="SCMSTARTTYPE" Value="auto" />
<Installproperty Name="INSTALLPBX" Value="YES" />
<Installproperty Name="STARTSERVICE" Value="YES" />
<InstallProperty Name="INSTALLDIR" Value="C:\Program Files\Symantec\" />
<Installproperty Name="DATABASE_DATA_DIR" Value="C:\Program Files\Symantec\
OpsCenter\DB\Data" />
</OpsCenter_Server>
</XML_Install>
```

For more details about the features of OpsCenter Analytics (licensed version), see the "About OpsCenter Analytics functions" section in the *Veritas NetBackup OpsCenter Administrator's Guide*.

- Veritas recommends that you do not change the value of RAN_SETUP, SCMSTARTTYPE, INSTALLPBX, and STARTSERVICE install properties.
  You must save the response file after you modify it.
  The text that you enter or modify in the response file is case-sensitive.

Note: By default, in OpsCenter, the database is upgraded in the beginning. If you want the OpsCenter software to be upgraded first in case of silent installation, you need to add the following in the response file: `<InstallProperty Name="ENABLEPREDBUPGRADE" Value="FALSE" />`

See "About OpsCenter upgrade failure scenarios" on page 133.

About tracking the progress of silent installation

When a silent installation is in progress, you can see `SETUP.EXE` process running in the **Processes** tab of the Windows Task Manager. In addition, you will also find multiple `msiexec.exe` processes running in the Task Manager.

You can also track, if a silent installation is in progress by checking the size of `bkuptemp.log` file. The size of `bkuptemp.log` file increases as silent installation progresses. The `bkuptemp.log` file is generated in `%ALLUSERSPROFILE%\SYMANTEC\OPSCENTER\INSTALLLOGS`.

Once the installation is complete, the installer converts `bkuptemp.log` to an HTML file.

See "Troubleshooting silent installation issues" on page 113.

Troubleshooting silent installation issues

Use the following procedure to troubleshoot silent installation issues. This procedure must be performed after the silent installation ends.

To troubleshoot silent installation issues

1. After the silent installation ends, navigate to the following location:

   `%ALLUSERSPROFILE%\SYMANTEC\OPSCENTER\INSTALLLOGS`.

2. Check if a file named `OpsCenterInstallLog.htm` is present. If `OpsCenterInstallLog.htm` is not present, see 7.

3. Open `OpsCenterInstallLog.htm` and check the timestamp and the OpsCenter component it is for to ensure that it is the appropriate log file.

   You must check the timestamp because `OpsCenterInstallLog.htm` may have been generated as a result of previous silent installations.

   In addition, the same `OpsCenterInstallLog.htm` file is generated when you install OpsCenter server, Agent, or View Builder. Hence you must check the specific OpsCenter component that is associated with `OpsCenterInstallLog.htm`.

4. You can check the timestamp by opening `OpsCenterInstallLog.htm` and seeing the first line in the file. For example, the following is the first line from a sample `OpsCenterInstallLog.htm` file:

   ```
   01-19-2010,13:35:30: -Silent _RespFile "C:\Documents and
   Settings\Administrator\Agent-19-01-10-13-04-21.xml"
   ```

   In this example, the timestamp is 01-19-2010, 13:35:30.

5 To know the OpsCenter component the log file is associated with, search for the following keywords in the `OpsCenterInstallLog.htm` file:

OpsCenter Server	You will find matches when you search for **OpsCenter Server** in the file. This means that the log file is for OpsCenter server.
OpsCenter Agent	You will find matches when you search for **OpsCenter Agent** in the file. This means that the log file is for OpsCenter Agent.
OpsCenter View Builder	You will find matches when you search for **OpsCenter View Builder** in the file. This means that the log file is for OpsCenter View Builder.

Note: If you have checked the timestamp and the OpsCenter component associated with all present `OpsCenterInstallLog.htm` files and do not find a valid `OpsCenterInstallLog.htm` file, see 7.

---

6 Use the `OpsCenterInstallLog.htm` file to troubleshoot silent installation issues. Open the `OpsCenterInstallLog.htm` file to see if the installation was successful or to understand why the installation failed. This file shows the installation status at the end. Installation errors are flagged in this file in red color. You may also see a description about why the error occurred and troubleshoot accordingly.

Ignore the subsequent steps of this procedure.

7 If `OpsCenterInstallLog.htm` is not present or you cannot find a valid `OpsCenterInstallLog.htm` file, check if `OpsCenter<Product>InstallLog.htm` file is present. In `OpsCenter<Product>InstallLog.htm`, *<Product>* can be Server, Agent, or View Builder depending on the OpsCenter component that you are installing.

8 Always ensure that the `OpsCenter<Product>InstallLog.htm` file is appropriate by checking the timestamp. You can check the timestamp by opening the `OpsCenter<Product>InstallLog.htm` file and seeing the first line of the file. For example, the following is the first line from a sample `OpsCenter<Product>InstallLog.htm` file:

```
01-19-2010,13:35:30: -Silent _RespFile "C:\Documents and
Settings\Administrator\Agent-19-01-10-13-04-21.xml"
```

In this example, the timestamp is 01-19-2010, 13:35:30.

9 Use the `OpsCenter<Product>InstallLog.htm` file to troubleshoot silent installation issues. You can open the OpsCenter`<Product>InstallLog.htm` file to see if the installation was successful or to understand why the installation failed. This file shows the installation status at the end. Installation errors are flagged in this file in red color. You may also see a description about why the error occurred and troubleshoot accordingly.

See "About tracking the progress of silent installation" on page 112.

About OpsCenter upgrade on Windows and UNIX

This section describes how you can upgrade OpsCenter on Windows and UNIX platforms.

Note: NetBackup OpsCenter does not support Search & Hold functionality. However, OpsCenter continues to show certain hold-related information. You cannot perform a search for backup images. The existing saved searches of backup images and corresponding results are deleted. The legal holds are converted to user holds. You can manage the holds by using the nbholdutil command of NetBackup. For more information about the command, see the *NetBackup Commands Reference Guide*. The Hold reports are deleted after you upgrade to version 7.7. If you have saved custom reports containing the filters related to indexing, those filters are automatically deleted from the report.

See "Upgrading OpsCenter on UNIX" on page 129.

Review the following procedures before you upgrade to OpsCenter:

See "About importing authentication settings during OpsCenter upgrade" on page 116.

See "About OpsCenter upgrade scenarios with respect to OpsCenter AT" on page 116.

See "Exporting authentication settings" on page 119.

See "Important notes regarding OpsCenter upgrade " on page 120.

About importing authentication settings during OpsCenter upgrade

This section provides the information that you may require before OpsCenter upgrade. While upgrading to latest version of OpsCenter from a version that is older than 7.6, you need to do a few tasks because of a few changes in the AT (Veritas Product Authentication Service) service.

AT is used for user authentication. For example, AT is used while importing authentication settings from a previous OpsCenter setup.

Starting from OpsCenter 7.6, authentication service (formerly it was known as Veritas Product Authentication Service or AT) is embedded with the OpsCenter Server. Each OpsCenter 7.6 setup has its own AT configuration, which is called OpsCenter AT. Depending on the various installation and upgrade scenarios, the tasks vary that you need to carry out before and after the installation.

See “About OpsCenter AT” on page 27.

See “About OpsCenter upgrade scenarios with respect to OpsCenter AT” on page 116.

See “Exporting authentication settings” on page 119.

See “Important notes regarding OpsCenter upgrade ” on page 120.

About OpsCenter upgrade scenarios with respect to OpsCenter AT

Table 2-9 describes various scenarios of OpsCenter upgrade:

Table 2-9 OpsCenter upgrade scenarios

Which installation scenario?	Which additional tasks are required?	What happens after the installation?
Fresh OpsCenter installation	None	The installer installs OpsCenter AT on the OpsCenter server host OpsCenter uses its own OpsCenter AT for user authentication **Note:** If OpsCenter is deployed in a clustered mode, each OpsCenter node has OpsCenter AT configuration of its own. Each cluster node has embedded AT binary and all nodes share the same AT configuration and authentication data exists on a shared disk.
Upgrade to OpsCenter: Non-clustered setup and shared AT in previous OpsCenter version	None	The installer installs OpsCenter AT on the OpsCenter server host OpsCenter uses its own OpsCenter AT for user authentication The shared AT broker's data store is imported to OpsCenter AT broker's data store Only OpsCenterUsers(vx) domain users are imported to OpsCenter AT All credentials of PureDisk and NBAC-enabled NetBackup are imported from remote AT to OpsCenter AT All imported OpsCenterUsers(vx) users can logon to OpsCenter after the installation.

Table 2-9 OpsCenter upgrade scenarios *(continued)*

Which installation scenario?	Which additional tasks are required?	What happens after the installation?
Upgrade to OpsCenter: Non-clustered setup and remote AT in previous OpsCenter version	Pre-upgrade tasks: Export the shared AT broker's data to an XML file using the atutil utility See "Exporting authentication settings" on page 119. **Note:** While copying the exported xml file, the DOS to UNIX conversion may be improper that may result in garbage characters in the xml file. This may cause failure of import. To avoid this, copy the xml file through FTP and with binary format. Upgrade tasks: During OpsCenter upgrade, when prompted, import this XML file to add the authentication settings from the shared AT to OpsCenter AT See "About importing authentication settings during OpsCenter upgrade" on page 116. Post-upgrade tasks: If the import is not successful, the default OpsCenter user needs to reset the passwords of OpsCenterUsers(vx) domain users that you have imported from the earlier OpsCenter version. Trust between NBAC-enabled NetBackup / PureDisk servers and OpsCenter server need to be established again. See "Setting up trust between OpsCenter and NBAC-enabled NetBackup or PureDisk" on page 135.	The installer installs OpsCenter AT on the OpsCenter server host OpsCenter uses its own OpsCenter AT for user authentication All credentials of PureDisk and NBAC-enabled NetBackup are imported from remote AT to OpsCenter AT Only OpsCenterUsers(vx) domain users are imported to OpsCenter AT All imported OpsCenterUsers(vx) users can logon to OpsCenter after the installation.

Table 2-9 OpsCenter upgrade scenarios *(continued)*

Which installation scenario?	Which additional tasks are required?	What happens after the installation?
Upgrade to OpsCenter: Clustered setup and remote AT in previous OpsCenter version	Pre-upgrade tasks: Export the shared AT broker's data to an XML file using the atutil utility See "Exporting authentication settings" on page 119. **Note:** While copying the exported xml file, the DOS to UNIX conversion may be improper that may result in garbage characters in the xml file. This may cause failure of import. To avoid this, copy the xml file through FTP and with binary format. Upgrade tasks: During OpsCenter upgrade, when prompted, import this XML file to add the authentication settings from the shared AT to OpsCenter AT See "About importing authentication settings during OpsCenter upgrade" on page 116. Post-upgrade tasks: If the import is not successful, the default OpsCenter user needs to reset the passwords of OpsCenterUsers(vx) domain users that you have imported from the earlier OpsCenter version. Trust between NBAC-enabled NetBackup / PureDisk servers and OpsCenter server need to be established again. See "Setting up trust between OpsCenter and NBAC-enabled NetBackup or PureDisk" on page 135.	The installer installs OpsCenter AT on the OpsCenter server host OpsCenter uses its own OpsCenter AT for user authentication All credentials of PureDisk and NBAC-enabled NetBackup are imported from remote AT to OpsCenter AT Only OpsCenterUsers(vx) domain users are imported to OpsCenter AT All imported OpsCenterUsers(vx) users can logon to OpsCenter after the installation.

Exporting authentication settings

Export OpsCenterUsers(vx) users and certificates using the `atutil` utility.

Refer to the following procedures to export the authentication settings from the earlier OpsCenter versions:

On Windows, to export the authentication settings

1. Logon to the remote AT host.
2. Copy `atutil.exe` from the DVD to the local machine (that is the remote AT host).

DVD location for `atutil` on Windows	OpsCenter_*version*_Win/bin/atutil

3. Run the following commands from the command prompt:
   - *INSTALL_PATH*\OpsCenter\server\authbroker>set EAT_DATA_DIR=*INSTALL_PATH*\OpsCenter\server\authbroker\data
     INSTALL_PATH is the location where you have installed OpsCenter.
   - *local_atutil_location*\atutil.exe export -f *filename*.xml -p *password* -b
     For Example: `atutil.exe export -f E:\userdata.xml -p pass -b`

On Unix, to export the authentication settings

1. Logon to the remote AT host.
2. Copy `atutil` from the DVD to the local machine (that is the remote AT host).

DVD location for `atutil` on UNIX	OpsCenter_*version*_Unix/bin/atutil

3. Run the following command from the command prompt:

   local_atutil_location/atutil export -f *filename*.xml -p *password* -b

   For example: `atutil export -f /temp/userdata.xml -p pass -b`

Note: On RHEL platform, run the following command:

```
/opt/SYMCOpsCenterServer/authbroker/bin/atutil export -p password
-f /tmp/at.xml -b -z /opt/SYMCOpsCenterServer/authbroker/data/
```

Important notes regarding OpsCenter upgrade

- During OpsCenter upgrade, NT users (on Windows) and PWD, NIS, or NIS+ users (on UNIX) from the previous OpsCenter version are transferred to LDAP users. You cannot logon to OpsCenter using the LDAP user credentials until you configure LDAP.

See "Adding AD / LDAP domain in OpsCenter" on page 228.

- OpsCenter upgrade does not retain the LDAP configuration that you had done in an older version. You need to reconfigure LDAP after you upgrade to OpsCenter.
  See "Adding AD / LDAP domain in OpsCenter" on page 228.
- After OpsCenter upgrade, PWD, NIS, or NIS+ users (on UNIX) cannot be accessed from OpsCenter server that is installed on Windows. This is because in OpsCenter, remote AT is not supported. It also does not support multibroker.

Upgrading OpsCenter on Windows

Use the following procedure to upgrade OpsCenter components on a Windows host.

Review the following considerations before installing OpsCenter components on Windows:

- If you plan to upgrade both the backup product like NetBackup, Backup Exec, or PureDisk and the OpsCenter components, it is recommended that you upgrade OpsCenter components first. By upgrading OpsCenter components before the backup product, OpsCenter can start collecting data from the backup product once it is added to the console.
  You must perform upgrades in the following order:

Serial No.	Steps to upgrade	Reference
1.	Upgrade the OpsCenter Server	See "To upgrade OpsCenter Server on Windows" on page 122.
2.	Upgrade the OpsCenter Agent	See "To upgrade OpsCenter Agent on Windows" on page 125.
3.	Upgrade the OpsCenter View Builder	See "To upgrade OpsCenter View Builder on Windows" on page 127.
4.	Upgrade the backup product that you are using like NetBackup, Backup Exec, or PureDisk.	Refer to the appropriate product manuals.

The above order also holds true if you plan to upgrade only OpsCenter and not the backup product. Always upgrade the OpsCenter Server first followed by the Agent and the View Builder.

- Veritas recommends that you enable 8.3 file name creation before installing OpsCenter components. If 8.3 file name creation is disabled, enable it and restart the Windows host before installing or upgrading to OpsCenter components.
- You must not run any other installation while installing OpsCenter components. Additionally after an installation is complete, you should wait for some time before installing other OpsCenter components.
- Veritas recommends that you do not cancel or interrupt the installation process once it is started.
- If you try to install OpsCenter components on a system where OpsCenter is already installed, the installer runs in a Maintenance mode. The Maintenance mode lets you repair or remove the OpsCenter component that is installed on your system.

To upgrade OpsCenter Server on Windows

1. If you plan to upgrade your backup product and OpsCenter, ensure that you upgrade OpsCenter first. When upgrading OpsCenter, always upgrade the OpsCenter Server first followed by the Agent and then the View Builder.
2. On a Windows host where you want to install OpsCenter Server, insert the appropriate OpsCenter product DVD in the DVD drive.
3. - If auto-run is enabled, the Veritas DVD Browser appears.
   - If auto-run is not enabled, click **Start > Run**. On the **Run** dialog box, in the **Open** text box, type '*D*`:\Browser.exe`' and press **Enter**:
     Where *D* is the DVD drive.
     The Veritas DVD Browser appears.
4. On the Veritas DVD Browser, click the **Installation** link.
5. Click the **OpsCenter Server Installation** link to install Veritas NetBackup OpsCenter Server.
6. The **Welcome** panel of the Installation Wizard appears. The Installation Wizard detects an existing installation of OpsCenter Server on the system. Depending on the installed version, the following message may be displayed on the **Welcome** panel:

   `The installer has detected that Veritas OpsCenter Server` *`current version`* `is already installed on your system that will now be upgraded to` *`new version`*`.`

   Click **Next** to continue.

7 Read the license agreement, check **I accept the terms of the license agreement**.

You may opt to check or uncheck **Participate in the NetBackup Product Improvement Program**. This option is checked by default.

If you check this option, the installer uploads installation deployment and product usage information to Veritas automatically and in a secured manner. This data helps Veritas to guide future product development and also analyze issues.

Click **Next**.

8 On the **Installation Choice** panel, click **Typical** to use the default settings, installation location, or port numbers. **Typical** is selected by default.

Also compare the space that is required for installing OpsCenter Server and the actual space that is available.

Note: The **Custom** option is disabled when you upgrade to OpsCenter. You cannot customize the default settings, locations, or port numbers while upgrading to OpsCenter.

Click **Next**.

9 Specify a location for saving the old OpsCenter database. The default location is `C:\Program Files\Symantec\OpsCenter_SavedData`.

Warning: In case of sequential OpsCenter upgrades (for example, version 1 > version 2 > version 3), the old `OpsCenter_SavedData` folder may already exist. If the `OpsCenter_SavedData` folder is overwritten during upgrade, the OpsCenter user interface may not start properly. To avoid this problem, you should rename the old `OpsCenter_SavedData` folder before upgrading to OpsCenter.

Click **Browse** to specify a different location.

In case the directory `C:\Program Files\Symantec\OpsCenter_SavedData` does not exist, you are prompted to create it. Click **Yes** to create the directory.

Note: Ensure that the database location has adequate space by going through the **Disk space requirements** section on this page. A green checkmark appears in the **Required** column if there is adequate disk space.

---

10 Click **Next**.

11 On the Import Authentication Settings panel, select one of the following options:

Do not import users	Select this option if you do not want to import users from the earlier OpsCeOpsCenter versions into OpsCenter database. Only default OpsCenter user is created who can logon to OpsCenter and reset passwords for all other existing passwords.
Import users	Select this option if you want to import users from earlier OpsCenter versions into OpsCenter database.

For more details, refer to the About Importing Authentication Settings section.

See "About importing authentication settings during OpsCenter upgrade" on page 116.

If import of authentication settings and users from the older OpsCenter version fails, you need to reset passwords of all OpsCenter(vx) users using the default OpsCenter user credentials.

See "Resetting an OpsCenter user password" on page 238.

12 On the **License Keys** panel, enter your demo or permanent key that you have received with the purchase of OpsCenter and click **Add Key**.

See "OpsCenter Analytics license keys" on page 74.

13 The installer shows the summary of the installation settings. Check **Save summary to** option to save the installation summary. Click **Browse** to save the installation summary in your preferred location.

Click **Install** to begin the installation. The installer installs OpsCenter Server software and also migrates data to the OpsCenter database. The database migration may take some time based on the size of your database.

14 After successful installation, you can view the installation logs or view the Readme.

Click **Finish**.

The installation logs are generated in the following location:

```
%ALLUSERSPROFILE%\Symantec\OpsCenter\
INSTALLLOGS\OpsCenterServerInstallLog.htm
```

Note: If you run the installer in a maintenance mode later, `OpsCenterServerMaintenanceInstallLog.htm` is also generated in the same location.

In OpsCenter, the database upgrade logs are stored at the following location:

```
%ALLUSERSPROFILE%\Symantec\OpsCenter\INSTALLLOGS\pre-install-config\db\log
```

See "About OpsCenter upgrade failure scenarios" on page 133.

Note: After successful upgrade, OpsCenter database password is set to an auto-generated string, if the earlier password is still the default one, that is 'SQL'. Veritas recommends that you change the database password after the installation.

See "Changing the OpsCenter database administrator password" on page 172.

If you had changed the default password in the earlier version, you do not need to change it again. The installer retains the old password that you can use in the current version.

To upgrade OpsCenter Agent on Windows

1 If you plan to upgrade your backup product and OpsCenter, ensure that you upgrade OpsCenter first. When upgrading OpsCenter, always upgrade the OpsCenter Server first followed by the OpsCenter Agent and then the View Builder.

2 On a Windows host where you want to install OpsCenter Agent, insert the OpsCenter product DVD in the DVD drive.

3
- If auto-run is enabled, the Veritas DVD Browser appears.
- If auto-run is not enabled, click **Start > Run**. On the **Run** dialog box, in the **Open** text box, type ***D*:\Browser.exe** and press **Enter**:
  Where *D* is the DVD drive.
  The Veritas DVD Browser appears.

4 On the Veritas DVD Browser, click the **Installation** link.

5 Click the **OpsCenter Agent Installation** link to install Veritas NetBackup OpsCenter Agent.

6 The **Welcome** panel of the Installation Wizard appears. The Installation Wizard detects an existing installation of OpsCenter Agent on the system. Depending on the installed version, the following message may be displayed on the Welcome screen:

```
The installer has detected that Veritas OpsCenter Agent
old_version is already installed on your system that will now be
upgraded to new_version.
```

Click **Next** to continue.

Note: The Installation Wizard automatically detects and installs 32-bit Agent software on 32-bit Windows platforms and 64-bit Agent software on 64-bit Windows platforms. 32-bit Agent software is not supported on 64-bit Windows platforms.

If you have an existing 32-bit Agent installation on a 64-bit system and you install OpsCenter Agent, the Installer automatically uninstalls the older 32-bit software and installs 64-bit Agent software. You need to perform the following tasks after you upgrade to 64-bit OpsCenter Agent:

- If 32-bit Agent software is upgraded to 64-bit, all Agent tuning configurations in `OpsCenterAgentService.xml` file that you may have made earlier should be performed again manually. The `OpsCenterAgentService.xml` file is used to specify how much memory is allocated for the Agent Java process and can be located in <INSTALL_PATH>\agent\bin.
- If 32-bit Agent software is upgraded to 64-bit software and the Agent is not installed on the OpsCenter Server, any Agent configurations in the `log.conf` file that you may have made earlier must be performed manually again after you upgrade. Possible Agent configuration in `log.conf` can be changing the Agent logging level etc. The `log.conf` file is located in *<INSTALL_PATH>*\agent.

7 Read the license agreement, check **I accept the terms of the license agreement**.

You may opt to check or uncheck **Participate in the NetBackup Product Improvement Program**. This option is checked by default.

If you check this option, the installer uploads installation deployment and product usage information to Veritas automatically and in a secured manner. This data helps Veritas to guide future product development and also analyze issues.

Click **Next**.

8 The installer shows the summary of the installation settings. Check **Save summary to** option to save the installation summary. Click **Browse** to save the installation summary in your preferred location.

Click **Install** to begin the installation. The installer installs OpsCenter Agent software.

9 After successful installation, you can view the installation logs or view the Readme.

Click **Finish**.

The installation logs are generated in the following location:

`%ALLUSERSPROFILE%\Symantec\OpsCenter\INSTALLLOGS\OpsCenterAgentInstallLog.htm`

Note: If you run the installer in a maintenance mode later, `OpsCenterAgentMaintenanceInstallLog.htm` is also generated in the same location.

To upgrade OpsCenter View Builder on Windows

1 If you plan to upgrade your backup product and OpsCenter, ensure that you upgrade OpsCenter first. When upgrading OpsCenter, always upgrade the OpsCenter Server first followed by the Agent and then the View Builder.

2 On a Windows host where you want to install OpsCenter View Builder, insert the OpsCenter product DVD in the DVD drive.

3
- If auto-run is enabled, the Veritas DVD Browser appears.
- If autorun is not enabled, click **Start > Run**. On the **Run** dialog box, in the **Open** text box, type ***D*:\Browser.exe** and press **Enter**:
  Where *D* is the DVD drive.
  The Veritas DVD Browser appears.

4 On the Veritas DVD Browser, click the **Installation** link.

5 Click the **OpsCenter View Builder Installation** link to install Veritas NetBackup OpsCenter View Builder.

6 The **Welcome** panel of the Installation Wizard appears. The Installation Wizard detects an existing installation of OpsCenter View Builder on the system. Depending on the installed version, the following message is displayed on the **Welcome** panel:

```
The installer has detected that Veritas OpsCenter View Builder
old_version is already installed on your system that will now be
upgraded to new_version.
```

Click **Next** to continue.

7 Read the license agreement, check **I accept the terms of the license agreement**.

You may opt to check or uncheck **Participate in the NetBackup Product Improvement Program**. This option is checked by default.

If you check this option, the installer uploads installation deployment and product usage information to Veritas automatically and in a secured manner. This data helps Veritas to guide future product development and also analyze issues.

Click **Next**.

8 The installer shows the summary of the installation settings. Check **Save summary to** option to save the installation summary. Click **Browse** to save the installation summary in your preferred location.

Click **Install** to begin the installation. The installer installs OpsCenter View Builder software.

9 After successful installation, you can view the installation logs or view the Readme.

Click **Finish**.

The installation logs are generated in the following location:

```
%ALLUSERSPROFILE%\Symantec\OpsCenter\
INSTALLLOGS\OpsCenterViewBuilderInstallLog.htm
```

Note: If you run the installer in a maintenance mode later, `OpsCenterViewBuilderMaintenanceInstallLog.htm` is also generated in the same location.

Upgrading OpsCenter on UNIX

Use the following procedure to upgrade to OpsCenter software on UNIX hosts.

Note: Veritas recommends that you do not cancel or interrupt the installation process once it is started.

To upgrade OpsCenter Server on UNIX

1. If you plan to upgrade your backup product and OpsCenter, ensure that you upgrade OpsCenter first. When upgrading OpsCenter, always upgrade the OpsCenter Server first followed by the Agent and then the View Builder.
2. Open a UNIX console and log on as `root` on the target host.
3. Mount the OpsCenter product DVD on the OpsCenter Server that you want to upgrade.
4. Type the following command: **`./install`**. Press **Enter**.
5. The Welcome message is displayed. Press **Enter** to continue.
6. The installer then checks if OpsCenter Server is installed on the system or not. It prompts you in case OpsCenter Server is already installed. The installer also examines the system for existing packages.
7. The following prompt is displayed:

   ```
   Where should the existing OpsCenter
   database and configuration files be backed up?
   An 'OpsCenterServer_backup' directory will be created within
   the directory that you specify to store these
   files. (/var/symantec/)
   ```

   Type the directory name in which the existing OpsCenter database and configuration files can be saved and then press **Enter**.

   To accept the default directory path (`/var/symantec`), press **Enter**.
8. The installer displays a list of components that will be installed or upgraded like PBX, OpsCenter Server, OpsCenter user interface and so on. Review this list and press **Enter** to continue.
9. The installer prompts you with the following question:

   ```
   installOpsCenterServer is now ready to
   upgrade OPSCENTERSERVER.
   Are you sure you want to upgrade OPSCENTERSERVER? [y,n,q] (y)
   ```

   Press **Enter** to continue OpsCenter upgrade.

10 The installer prompts you with the following question:

```
Participate in the NetBackup Product Improvement program? [y,n,q] (y)
```

Press **Enter** if you want to participate in the NetBackup Product Improvement program or press **n** if you do not want to participate.

11 The installer prompts you with the following question:

```
Do you want to import users from <remote AT host name> to OpsCenter AT?
```

Press **Enter** to import users from the earlier OpsCenter versions.

For more details, refer to the About Importing Authentication Settings section.

If the import fails, you need to reset password of all OpsCenter(vx) users.

See "Resetting an OpsCenter user password" on page 238.

12 By default, in OpsCenter, the database is upgraded in the beginning. However, you can choose to first upgrade the OpsCenter software.

See "About OpsCenter upgrade failure scenarios" on page 133.

The database upgrade process starts. In this process, the OpsCenter data is migrated to the new OpsCenter database version. The database process may take time depending on your database size.

The following message is displayed:

```
The database upgrade is in progress.
This may take some time based on the database size.
You can see the progress and current status in

/var/tmp/(directory)/db/log/dbManager_<timestamp>_.log file.
```

After complete installation, the logs are copied to the following location:`/var/VRTS/install/logs/`*`LogDirectory`*`/db/log`

LogDirectory is generated during the upgrade progress.

13 The installer displays the OpsCenter packages that are installed. Depending on the installed packages, the following message may be displayed:

```
The following packages were found on the system. However the package
versions are older than the ones required by OpsCenter.

VRTSOpsCenterServer existing version was found on the system,
but OpsCenter requires VRTSOpsCenterServer new version
VRTSOpsCenterGUI existing version was found on the system,
but OpsCenter requires VRTSOpsCenterGUI new version
VRTSOpsCenterLegacyServer existing version was found on the system,
but OpsCenter requires VRTSOpsCenterLegacyServer new version
```

The installer then uninstalls the older packages and installs new version of OpsCenter Server.

14 OpsCenter Server is installed. Configuration changes are made to the system.

15 All the OpsCenter processes are started. The following information is also displayed:

- Web URL to access OpsCenter console
- Location of install log and summary files.

Note: After successful upgrade, OpsCenter database password is set to an auto-generated string, if the earlier password is still the default one, that is 'SQL'. Veritas recommends that you change the database password after the installation.

See "Changing the OpsCenter database administrator password" on page 172.

If you had changed the default password in the earlier version, you do not need to change it again. The installer retains the old password that you can use in the current version.

About files and folders that are protected during OpsCenter upgrade

This section provides a list of files and folders that are protected during OpsCenter upgrade.

Note: The locations of all files and folders that are listed here are default locations.

For UNIX, following is the list of files and folders that are protected during upgrade:

For OpsCenter Server

- /opt/SYMCOpsCenterGUI/webserver/conf/server.xml
- /opt/SYMCOpsCenterServer/db/data/vxpmdb.log
- /opt/SYMCOpsCenterServer/db/data/vxpmdb.db
- /opt/SYMCOpsCenterServer/db/data/symcOpscache.db
- /opt/SYMCOpsCenterServer/db/data/symcopsscratchdb.db
- /opt/SYMCOpsCenterServer/db/data/symcsearchdb.db
- /opt/SYMCOpsCenterServer/config
- /opt/SYMCOpsCenterServer/bin/startserver
- /opt/SYMCOpsCenterServer/db/conf
- /opt/SYMCOpsCenterGUI/config/
- /opt/SYMCOpsCenterServer/authbroker/data/

For Windows, following is the list of files and folders that are protected during upgrade:

For OpsCenter Server

- C:\Program Files\OpsCenter\gui\webserver\conf\server.xml
- C:\Program Files\OpsCenter\gui\bin\WebUI_Login.url
- C:\Program Files\OpsCenter\gui\bin\OpsCenterGUIService.xml
- C:\Program Files\OpsCenter\server\bin\OpsCenterServerService.xml
- C:\Program Files\OpsCenter\server\db\data\vxpmdb.db
- C:\Program Files\OpsCenter\server\db\data\symcOpscache.db
- C:\Program Files\OpsCenter\server\db\data\symcopsscratchdb.db
- C:\Program Files\OpsCenter\server\db\data\symcsearchdb.db
- C:\Program Files\OpsCenter\server\db\data\vxpmdb.log
- C:\Program Files\OpsCenter\gui\config
- C:\Program Files\OpsCenter\server\db\CONF
- C:\Program Files\OpsCenter\server\authbroker\data

For OpsCenter Agent

- C:\Program Files\OpsCenter\agent\bin\OpsCenterAgentService.xml

- C:\Program Files\OpsCenter\agent\config

For OpsCenter View Builder

- C:\Program Files\OpsCenter\jvb\bin\OpsCenterViewBuilder.xml

About OpsCenter upgrade failure scenarios

In the versions prior to OpsCenter 7.6, the upgrade process first upgrades the OpsCenter software and then the database. If the upgrade fails, the database can become inconsistent and you cannot get it back to the original state.

Starting from OpsCenter 7.6, the database is upgraded in the beginning that is during the pre-installation process. In case of upgrade failure, the older OpsCenter setup is still available for use.

By default, the OpsCenter database is upgraded in the beginning. If you want the OpsCenter software to be upgraded first, you need to do the following:

To change the default upgrade sequence to upgrade database in the end

◆ Make the following ENABLEPREDBUPGRADE registry entry on the OpsCenter Server host:

Windows	■ Create a registry value `ENABLEPREDBUPGRADE=FALSE` at the following location: `HKLM\\SOFTWARE\\Symantec\\OpsCenter\\Server`
UNIX	■ Before starting the upgrade, run the following command: `EXPORT ENABLEPREDBUPGRADE=FALSE`

Note: In case of Windows silent installation, you need to add the following in the response file: `<InstallProperty Name="ENABLEPREDBUPGRADE" Value="FALSE" />`

See “About editing the response file” on page 110.

Table 2-10 describes the possible upgrade failure scenarios and how you can recover the database in OpsCenter even though the upgrade has failed.

Table 2-10 Upgrade failure scenarios

Database upgrade	OpsCenter software upgrade	Required action
Successful	Failed	To use the upgraded database **1** Remove the failed installation. **2** Install OpsCenter as a fresh installation. **3** Stop all OpsCenter services. **4** Copy the upgraded OpsCenter database that was stored at the following location during the database upgrade to the new setup: On Windows - *OpsCenter_SavedData*\OpsCenter\server\db\data*new_version* For example: OpsDBBackup\OpsCenter\server\db\data\7.7 On UNIX - *OpsCenterServer_backup*/new_version/SYMCOpsCenterServer/db/data For example:OpsDBBackup/7.7/SYMCOpsCenterServer/db/data **5** Start all services. To revert to the previous OpsCenter setup after the software upgrade failure **1** Remove the failed installation. **2** Install the previous base OpsCenter version and maintenance packs that were in place prior to upgrade. **3** Stop all OpsCenter services. **4** Copy the previous OpsCenter database that was saved at the following location during the database upgrade. On Windows - *OpsCenter_SavedData*\OpsCenter\server\db\data On Unix - *OpsCenterServer_backup*/SYMCOpsCenterServer/db/data **5** Start all OpsCenter services.
Failed	Failed because the database upgrade was failed	■ Use the previous OpsCenter setup that is still intact. ■ Check the database upgrade logs at the following location for errors to learn more about the root cause for the database upgrade failure: On Windows - %ALLUSERSPROFILE%\Symantec\OpsCenter\INSTALLLOGS\pre-install-config\db\log On UNIX - /var/VRTS/install/logs/*LogDirectory*/db/log *LogDirectory* is generated during the upgrade process.

About post-installation tasks

The following sections explain how to start using OpsCenter and includes some performance tuning tips for OpsCenter.

See "Setting up trust between OpsCenter and NBAC-enabled NetBackup or PureDisk" on page 135.

See "Verifying that OpsCenter is running properly" on page 135.

See "About starting to use OpsCenter" on page 136.

See "About the start up tasks that OpsCenter performs" on page 137.

For performance and tuning information, refer to the new *OpsCenter Performance and Tuning Guide* at the following location:

http://www.veritas.com/docs/000003387

Setting up trust between OpsCenter and NBAC-enabled NetBackup or PureDisk

Use the following procedure to setup the trust between the OpsCenter server and NBAC-enabled NetBackup Master Server or PureDisk Server.

To setup trust

1. Logon to the NetBackup Master Server or PureDisk Server host.
2. `vssat setuptrust --broker` *`OpsCenter hostname`*`:1556:OPSCENTER_PBXSSLServiceID --securitylevel high`

Verifying that OpsCenter is running properly

After installing OpsCenter on either Windows or UNIX, perform a check to verify that OpsCenter is running properly.

To verify that OpsCenter is running properly

1. Use the URL that is presented at the end of the OpsCenter Server installation to access the OpsCenter console.

   Alternately type the following in the Web browser address bar:
   https://<server-host>/opscenter

   Note: By default, OpsCenter tries to run on port 443 (HTTPS). If port 443 is not available, OpsCenter can use a different port. To learn more about the HTTPS ports that OpsCenter uses, run the `configurePorts` utility. Run the following command:

   On Windows:
   `<INSTALL_PATH>\OpsCenter\gui\bin\goodies\configurePorts.bat -status`

   On UNIX:
   `<INSTALL_PATH>/SYMCOpsCenterWebGUI/bin/goodies/configurePorts.sh -status`

   If OpsCenter uses HTTPS port 8443, then use https://host.domain:8443/opscenter.

   If the OpsCenter login screen appears, the OpsCenter Server, the Web server, and the authentication service are running.

   The first time you log on , it takes longer than usual time for the GUI to load.

2. Log on as an administrator. Select the following private domain:
   OpsCenterUsers(vx)

About starting to use OpsCenter

After you complete the OpsCenter installation, you are ready to start using the OpsCenter console.

Table 2-11 lists the common tasks in OpsCenter and contains links to the corresponding topics and descriptions.

Table 2-11 Links to get you started with OpsCenter

Task	Topic	Topic Description
To access and log on to the OpsCenter console.	See "About accessing the OpsCenter console" on page 34.	This topic provides instructions on how to access the console and log on, and provides solutions to possible issues.

Table 2-11 Links to get you started with OpsCenter *(continued)*

Task	Topic	Topic Description
To change the password for the administrator logon.	See "Changing your OpsCenter password" on page 211.	For administrator initial logon, the user name is `admin` and the password is `password` if you have chosen to keep the default password during installation. After initial logon, it is recommended that you change the user name and password.
To learn about the OpsCenter console components.	See "About OpsCenter console components" on page 48.	This topic provides an overview of the console components.
To learn more about using the OpsCenter console.	See "About using the OpsCenter console" on page 30.	For instructions on understanding and using the various OpsCenter monitoring, managing, reporting, and settings views and related tasks, use the OpsCenter online Help .

About the start up tasks that OpsCenter performs

OpsCenter performs the following tasks when it starts for the first time.

When OpsCenter starts, it performs the following tasks:

- Creates and initializes the security domain that the authentication broker requires. If these security domains are present, OpsCenter uses them. When OpsCenter server is installed, the following domains are created: OpsCenterUsers, OpsCenterServices, and NOM_MACHINES.
- Creates the OpsCenter admin user in the OpsCenterUsers domain with the default password as 'password'.

About uninstalling OpsCenter on Windows and UNIX

This section describes uninstallation procedures for OpsCenter on Windows and UNIX.

See "Uninstalling OpsCenter on Windows" on page 137.

See "Uninstalling OpsCenter on UNIX " on page 138.

Uninstalling OpsCenter on Windows

Before uninstalling OpsCenter components, ensure that the NetBackup Administration Console is closed.

Note: After a rollback, the keys are not recreated to display an entry in the **Add or Remove Programs** dialog box. If a rollback occurs during an uninstall of OpsCenter, the keys are not removed from the **Add or Remove Programs** dialog box. You must remove OpsCenter. Use `setup.exe` to remove OpsCenter.

Use the Windows Add/Remove Programs utility to uninstall OpsCenter on a Windows host.

Note: To uninstall OpsCenter, you must log on as the official administrator. Users that are assigned to the Administrators Group but are not the official administrator cannot uninstall OpsCenter from UAC-enabled environments. To allow users in the Administrators Group to uninstall OpsCenter, disable UAC.

To uninstall OpsCenter Server on Windows

1. Log on to the target host as a user with administrator privileges.
2. In the Windows Control Panel, click **Add/Remove Programs**.
3. Click **Veritas OpsCenter Server** and click **Remove**.

   For Windows 64-bit systems, click **Veritas OpsCenter Server (64bit)** and click **Remove**.
4. Click **Next** to continue and remove OpsCenter Server from your computer.

To uninstall OpsCenter Agent on Windows

1. Log on to the target host as a user with administrator privileges.
2. In the Windows Control Panel, click **Add/Remove Programs**.
3. Click **Veritas OpsCenter Agent** and click **Remove**.
4. Click **Next** to continue and remove OpsCenter Agent from your computer.

To uninstall OpsCenter View Builder on Windows

1. Log on to the target host as a user with administrator privileges.
2. In the Windows Control Panel, click **Add/Remove Programs**.
3. Click **Veritas OpsCenter View Builder** and click **Remove**.
4. Click **Next** to continue and remove OpsCenter View Builder from your computer.

Uninstalling OpsCenter on UNIX

Use the Uninstall Script, which resides in the root directory of the product DVD and also in `opt/VRTS/install` directory, to uninstall OpsCenter on a UNIX host.

Note: If you want to reinstall OpsCenter components, use the product DVD. You cannot reinstall OpsCenter components using the `install` scripts in the `opt/VRTS/install` directory.

Note: Veritas recommends that you do not cancel or interrupt the uninstallation process once it is started.

To uninstall OpsCenter Server on UNIX

1. Open a UNIX console and log on as **`root`** on the target host.
2. Change to the following directory:

   `opt/VRTS/install`
3. Type the following command and press **Enter**:

   `./uninstallOpsCenterServer`

   The Uninstall Script checks the components that are installed on the system.
4. When asked to confirm if you want to uninstall OpsCenter Server, do one of the following:
   - Type **`y`**.
     Press **Enter** to start the uninstall process.
     The Uninstall Script stops all processes and then uninstalls the component packages. When the uninstall is complete, it displays a summary of the uninstall, including the location of the uninstall log files.
   - Type **`n`**.
     Press **Enter** to cancel the uninstall procedure.

About clustering OpsCenter

The following sections describe how you can cluster OpsCenter.

About OpsCenter clusters

Clusters provide high availability of applications and data to users. In a cluster, two or more nodes are linked in a network and work collectively as a single system. Each node can access the shared disks with the help of cluster software. All nodes in a cluster are constantly aware of the status of resources on the other nodes. If a node becomes unavailable, resources running on that node migrate to an available node.

OpsCenter operates in an active or a passive failover configuration. OpsCenter Server must be installed on the active node and the passive (or failover nodes). When a failover occurs in an OpsCenter cluster, OpsCenter is shut down on the active node and starts on one of the failover nodes in the cluster. During failover, users experience only a short interruption in service. This failover provides high availability for OpsCenter. You can cluster only the OpsCenter Server. Installing OpsCenter in a clustered environment makes OpsCenter a highly available application.

About database defragmentation in a cluster

Use the `dbdefrag` utility to defragment the database in an OpsCenter cluster.

See dbdefrag on page 633.

Note: Before you run the `dbdefrag` command, you need to freeze the cluster nodes.

Supported platforms for cluster solutions

An OpsCenter cluster is supported on Windows platform. You can install an OpsCenter cluster on the following platforms:

- Windows 2012 R2 Datacenter (x64)
- Windows 2008 R2 x64
- Windows 2008 x64

For OpsCenter to be clustered, you must have Cluster Server (VCS) installed.

Table 2-12 lists the supported versions of Cluster Server (VCS).

Table 2-12 OpsCenter cluster support matrix

Platform	Latest supported version	Start of support
VCS Windows	6.1	4.2 RP2

Cluster Server (VCS) is a high-availability solution for cluster configurations. With VCS you can monitor systems and application services, and restart services on a different system when hardware or software fails.

For more information about VCS, see the *Veritas Cluster Server User's Guide*.

Note: Clustered OpsCenter is not supported on Windows Server Failover Clustering (WSFC). WSFC was earlier referred to as MSCS (Microsoft Cluster Server).

About running commands on the active node

For a clustered OpsCenter server, you must run commands on the active node. You may get unexpected results if you run a command on an inactive node. The command may fail to run and may sometimes result in an unexpected behavior.

For example, running the `dbbackup` command on an inactive node may result in the following unexpected result:

Command: `E:\OpsCenter\server\bin>dbbackup.bat E:\temp`

Result: `"Could not find Z:\OpsCenter\server\config\db.conf file"`

In addition, the OpsCenter service group may failover if the command requires restarting the OpsCenter services. Some OpsCenter commands or utilities like the support utility require restarting the services.

Connecting Authentication Service and Veritas Private Branch Exchange

An OpsCenter cluster requires that the authentication service (OpsCenter AT) and PBX components that are installed on the remote host are connected. To check if AT and PBX are connected, verify whether `pbxexchflag` of the authentication service is set or not. When `pbxexchflag` is set, its value is equal to 1 and this means that PBX and AT are connected.

Note: The information in this section applies to OpsCenter clusters only.

Before setting the value of `pbxexchflag`, you must stop all OpsCenter Server services, Authentication Service and Veritas Private Branch Exchange. After setting the value of `pbxexchflag` to 1, you must restart these services.

Use the following procedure to connect the authentication service and PBX components.

To connect Authentication Service and Veritas Private Branch Exchange on Windows

1. Open the command prompt and enter the following command:

   ```
   <INSTALL_PATH>\Security\Authentication\bin\vssat.exe  showispbxexchflag
   ```

   This command gives the value of *pbxexchflag*. If the value of `pbxexchflag` is 0, you need to set it to 1.

   In case the value of `pbxexchflag` is 1, you do not need to follow the remaining steps.

2. Navigate to `<INSTALL_PATH>\Security\Authentication\bin` directory. Enter the following command at the bin directory to set the value of `pbxexchflag`:

   ```
   vssat.exe setispbxexchflag --enable
   ```

   The value of `pbxexchflag` is set to 1.

   Verify if the value of `pbxexchflag` is 1.

   See step 1.

3. Stop all the OpsCenter Server services by executing the following command:

   ```
   <INSTALL_PATH>\OpsCenter\server\bin\opsadmin.bat stop
   ```

4. Stop Authentication Service by performing either of the following steps:
   - Use the stop option in the **Windows Service** pane, or
   - Execute the following command in a command console:

     ```
     net stop ops_atd
     ```

5. Restart Authentication Service by performing either of the following steps:
   - Use the start option in the **Windows Service** pane, or
   - Execute the following command in a command console:

     ```
     net start ops_atd
     ```

6. Restart all the OpsCenter Server services by performing the following steps:
   - Navigate to `<INSTALL_PATH>\OpsCenter\server\bin` directory.
   - Restart all the OpsCenter Server services by executing the following command:

     ```
     opsadmin.bat start
     ```

Clustering OpsCenter on Windows

This section provides information about installing OpsCenter in a clustered mode, on a Windows host.

Table 2-13 provides the Windows clustering steps.

Table 2-13 OpsCenter clustering steps

Step	Description	Reference topic
1	Understand the limitations of an OpsCenter cluster	See "Limitations of OpsCenter cluster on Windows" on page 143.
2	Make sure that you have met all prerequisites.	See "Prerequisites for OpsCenter cluster on Windows" on page 143.
3	Install OpsCenter.	See "About installing OpsCenter on Windows" on page 88.

Limitations of OpsCenter cluster on Windows

An OpsCenter cluster has the following limitations:

- Only the OpsCenter Server can be clustered.OpsCenter Agent and the OpsCenter View Builder cannot be clustered.
- OpsCenter cluster cannot co-exist with any other Veritas product running in secure mode using the Veritas Product Authentication Service.
- OpsCenter does not support clustered AT.

Prerequisites for OpsCenter cluster on Windows

This section contains information about the requirements that must be met before you install and configure OpsCenter in a clustered mode, on a Windows host.

Prerequisites:

- Verify that VCS and OpsCenter support your hardware. For a list of supported storage devices, visit the following Web site:
  http://www.veritas.com/support
- Verify that the supported version of VCS is correctly installed and configured. Follow the steps in the *Veritas Cluster Server Installation Guide*.
- For VCS Windows 4.2 versions, ensure that the patch is installed before installing OpsCenter. For OpsCenter, the supported VCS version starts from 4.2 RP2. The patch is available at the following URL:
  http://www.veritas.com/docs/000029739

This Technote is applicable to OpsCenter.

- Verify that no VCS resource group and resource exist with the same name as that which you intend to use for OpsCenter.
- The SharedDisk must be configured and accessible to all cluster nodes where you want to install OpsCenter.
- Verify that you have an IP address and host name (virtual host name) to be assigned to the OpsCenter resource in VCS. Only use these for the OpsCenter resource. The virtual host name must be the short name and less than 15 characters.
  Also, ping the IP address and verify that the IP address is not plumbed.
- Verify that you can mount the disk.
- Verify that you have the OpsCenter installation program and a valid license key.
- For a Windows cluster, verify that the cluster disk groups and dynamic volumes for OpsCenter are created on the shared storage. Refer to the *Veritas Storage Foundation Administrator's Guide* for details.
- Verify that all VCS services are up and running on all the nodes in the cluster.
- Verify that OpsCenter installation is carried out with the domain admin account.
- PBX is installed when you install OpsCenter Agent.
- Verify that PBX on the remote host is connected.
  See "Connecting Authentication Service and Veritas Private Branch Exchange" on page 141.

Installing OpsCenter Server on a Windows cluster

To cluster OpsCenter and make it highly available, you must install and configure OpsCenter in a clustered mode.

Note: To install OpsCenter Server in clustered mode, first install the OpsCenter Server on the active node and then on the passive nodes. Also, you need to install OpsCenter Server manually on all the nodes.

To install OpsCenter Server on a Windows cluster

1. On an active cluster node where you want to install OpsCenter server, insert the OpsCenter DVD in the DVD drive.
2. - If auto-run is enabled, the Veritas OpsCenter Installation Wizard appears.
   - If auto-run is not enabled, click **Start > Run**. On the **Run** dialog box, in the **Open** text box, type ***D***`:\Browser.exe` and press **Enter**:

Where *D* is the DVD drive.

The Veritas NetBackup OpsCenter Installation Wizard appears.

3 On the Veritas NetBackup OpsCenter Installation Wizard, click the **Installation** link.

4 Click the **OpsCenter Server Installation** link to install Veritas NetBackup OpsCenter server.

5 Click **Next**.

6 Read the license agreement, check **I accept the terms of the license agreement** and click **Next**.

You may opt to check or uncheck **Participate in the NetBackup Product Improvement Program**. This option is checked by default.

If you check this option, the installer uploads installation deployment and product usage information to Veritas automatically and in a secured manner. This data helps Veritas to guide future product development and also analyze issues.

7 Select **Install a clustered OpsCenter Server** to install OpsCenter Server in clustered mode. You need to install OpsCenter Server manually on each node of the cluster.

This option is enabled if you have VCS installed.

8 In the Installation Method section, click **Typical** to use the default settings and installation location.

Also compare the space that is required for installation with the actual space available in the installation directory.

Note: Click **Custom** if you want to change the default settings and locations.

Click **Next**.

9 On the **License Keys** panel, enter the demo or permanent key that you have received with the purchase of OpsCenter and click **Add Key**.

Note: You can also add the license keys from the OpsCenter console.

See "About managing licenses" on page 212.

The license keys that are already installed on the system are also displayed in the box that is shown on this panel. The license type information is also shown along with the key.

More information about licenses is available.

See "About the OpsCenter licensing model" on page 73.

10 Click **Next**. The **Cluster Settings** panel is displayed.

11 On the **Cluster Settings** panel, enter the following information:

Cluster Group Name	Enter the name for the OpsCenter cluster. For example: OpsCenter_Server
Virtual host Name	Enter the virtual host name that is assigned to the OpsCenter cluster. For example: Oc_cluster. The virtual host name must be the short name and less than 15 characters.
Virtual IP address	Enter the IP address that assigned to the OpsCenter cluster
Subnet mask	Enter the subnet mask . For example: 255.255.252.0
Path to Shared data	Select the shared drive path that you have configured in VxVM. For example, Z:\
Public Network	Select LAN as a public network. You can select different public network for passive nodes.

Note: While installing OpsCenter on a passive node, only Public Network option is enabled.

---

12 Click **Next**. The installer shows the summary of the settings that you have selected for OpsCenter Server installation.

Check **Save Summary to** field to save the installation summary. Click **Browse** to save the installation summary in your preferred location.

13 Click **Install**.

The installer starts installing the OpsCenter Server software.

In a clustered mode, the default OpsCenter database location on Windows is the following location on the shared drive:

`OpsCenter\Server\db`

14 After successful installation, you can view the OpsCenter console or view installation logs.

15 Click **Finish**. Repeat this procedure for all the cluster nodes.

Note: After installing an OpsCenter cluster on Windows 2008 R2 x64 system, you need to manually bring the `NetBackupOpsCenterVCS` resource online. You can bring the `NetBackupOpsCenterVCS` resource online from the CLI or by using the cluster GUI. Use the following command:

`hares -online <resource name> -sys <Name of the active node>`

Example: `hares -online newonelatest-OpsCenter -sys OPS-CLUSTER-1`

Upgrading OpsCenter cluster on Windows

Use the following procedure to upgrade OpsCenter cluster on Windows.

Note: To upgrade to OpsCenter Server in a clustered mode, first install the OpsCenter Server on the active node and then on the passive nodes. Also, you need to install OpsCenter Server manually on all the nodes.

To upgrade OpsCenter cluster on Windows

1 From the active node of the OpsCenter cluster that you want to upgrade, insert the OpsCenter DVD in the DVD drive.

2
- If auto-run is enabled, the Veritas OpsCenter Installation Wizard appears.
- If auto-run is not enabled, click **Start > Run**. On the **Run** dialog box, in the **Open** text box, type ***D*:\Browser.exe** and press **Enter**:
  Where *D* is the DVD drive.
  The Veritas NetBackup OpsCenter Installation Wizard appears.

3 On the OpsCenter Installation Wizard, click the **Installation** link.

4 Click the **OpsCenter Server Installation** link to install Veritas NetBackup OpsCenter server.

5 Click **Next**.

6 The **Welcome** panel of the Installation Wizard appears. The Installation Wizard detects an existing installation of OpsCenter Server on the system. Depending on the installed version, the following message may be displayed on the **Welcome** panel:

```
The installer has detected that Veritas OpsCenter Server
old_version is already installed on your system that will now be
upgraded to new_version.
```

Click **Next** to continue.

7 Read the license agreement, check **I accept the terms of the license agreement** and click **Next**.

You may opt to check or uncheck **Participate in the NetBackup Product Improvement Program**. This option is checked by default.

If you check this option, the installer uploads installation deployment and product usage information to Veritas automatically and in a secured manner. This data would help Veritas to guide future product development and also analyze issues.

8 Select **Install a clustered OpsCenter Server** to install OpsCenter Server in clustered mode. You need to install OpsCenter Server manually on each node of the cluster.

This option is enabled if you have VCS installed.

9 In the Installation Method section, click **Typical** to use the default settings and installation location. **Typical** is selected by default.

Also compare the space that is required for installation with the actual space available in the installation directory.

Note: The **Custom** option is disabled when you upgrade OpsCenter . You cannot customize the default settings, locations, or port numbers while upgrading from OpsCenter.

Click **Next**.

10 Specify a location for saving the old OpsCenter database. The default location is `C:\Program Files\Symantec\OpsCenter_SavedData`. Click **Browse** to specify a different location.

In case the directory `C:\Program Files\Symantec\OpsCenter_SavedData` does not exist, you are prompted to create it. Click **Yes** to create the directory.

Note: Ensure that the database location has adequate space by going through the **Disk space requirements** section on this page. A green checkmark appears in the **Required** column if there is adequate disk space.

---

11 On the **License Keys** panel, enter the demo or permanent key that you have received with the purchase of OpsCenter and click **Add Key**.

Note: You can also add the license keys from the OpsCenter console.

See "About managing licenses" on page 212.

The license keys that are already installed on the system are also displayed in the box that is shown on this panel. The license type information is also shown along with the key.

More information about licenses is available.

See "About the OpsCenter licensing model" on page 73.

12 Click **Next**. The **Import Authentication Settings** panel is displayed.

13 On the **Import Authentication Settings** panel.

Do not import users	Select this option if you do not want to import users from the earlier OpsCenter versions into OpsCenter database. Only default OpsCenter user is created who can logon to OpsCenter and reset passwords for all other existing passwords. **Note:** Starting from OpsCenter 7.6, Veritas Product Authentication Service is not a shared component and is local to each Veritas product. The authentication service (Root Broker and Authentication Root Broker) that is installed with OpsCenter is called OpsCenter AT.
Import users	Select this option if you want to import users from earlier OpsCenter versions into OpsCenter database.

See "About importing authentication settings during OpsCenter upgrade" on page 116., for more details.

14 Click **Next**. The **Cluster Settings** panel is displayed.

15 On the **Cluster Settings** panel, enter the following information:

Cluster Group Name	This option is disabled.
Virtual host Name	This option is disabled.
Virtual IP address	This option is disabled.
Subnet mask	This option is disabled.
Path to Shared data	This option is disabled.
Public Network	Select LAN as a public network. You can select different public network for active and passive nodes.

16 Click **Next**. The installer shows the summary of the settings that you have selected for OpsCenter Server installation.

Check **Save Summary to** field to save the installation summary. Click **Browse** to save the installation summary in your preferred location.

17 Click **Install**.

The installer starts installing the OpsCenter Server software.

Note: In clustered mode, the default OpsCenter database location on Windows is the following location on the shared drive:

`OpsCenter\Server\db`

---

18 After successful installation, you can view the OpsCenter console or view installation logs.

19 Click **Finish**. Repeat this procedure for the passive nodes.

Known issue in upgrading OpsCenter cluster setup

While upgrading from OpsCenter cluster, there may be a problem in getting shared drive access during installation or upgrade. Due to a configuration issue, installer may not get access of shared drive which in turn causes an issue in creating the domain.

To create domain again in cluster,

1 Freeze the cluster setup.

2 Stop the OpsCenter services.

3 Open **security.conf** file on the path **Shared_Drive\OpsCenter\Server\config**.

4 Change the value of parameter **vxss.initialized** from **False** to **True** (vxss.initialized = True).

5 Restart the OpsCenter services again.

6 Unfreeze the cluster setup.

7 Access OpsCenter.

Uninstalling OpsCenter from the Windows cluster

Use the Windows **Add/Remove Programs** utility to uninstall OpsCenter Server from a Windows cluster. Use the following procedure to uninstall OpsCenter from all the cluster nodes.

To uninstall Veritas NetBackup OpsCenter Server completely from the cluster

1 Log on to the active node as a user with administrator privileges.

2 Log on to the cluster web user interface.

3 Right-click the selected cluster monitor panel and click **Explorer View** from the menu to access Cluster Explorer.

4 Click the **Service Groups** tab in the Cluster Explorer configuration tree.

5 Right-click the OpsCenter resource group and select **Offline > All Systems**.

6 Click **Yes** to forcefully take the resource group offline.

7 In the Windows Control Panel, click **Add/Remove Programs**.

8 Click **Veritas OpsCenter Server** and click **Remove**.

9 Click **Next** to continue and remove Veritas OpsCenter Server from your computer.

10 Uninstall OpsCenter software from all the nodes. Repeat steps 7 through 9 for all the passive nodes.

11 Delete the OpsCenter resource groups manually. Note that the installer does not remove the OpsCenter resource groups. These must be removed manually.

See "Deleting OpsCenter resource group from the cluster" on page 152.

Deleting OpsCenter resource group from the cluster

Use the following procedure to delete OpsCenter resource group from the cluster.

To delete OpsCenter resource group from the cluster

1 Log on to the cluster web user interface.

2 Right-click the selected cluster monitor panel and click **Explorer View** from the menu to access Cluster Explorer.

3 Click the **Service Groups** tab in the Cluster Explorer configuration tree.

4 Right-click the OpsCenter resource group and select **Offline > All Systems**.

5 Click **Yes** to forcefully take the resource group offline.

6 Right-click the OpsCenter resource group and select **Delete**.

7 Click **Yes** to delete the OpsCenter resource group.

See "Uninstalling OpsCenter from the Windows cluster" on page 151.

Chapter 3

OpsCenter Getting Started feature

This chapter includes the following topics:

- About the OpsCenter Getting Started feature
- OpsCenter user roles
- Learn more about adding NetBackup Master Servers
- Learn more about OpsCenter Views
- Add Users
- Edit User
- Reset password
- Add NetBackup Master Server
- Add OpsCenter Agent
- Add OpsCenter Views/Groups
- Configure SMTP Server

About the OpsCenter Getting Started feature

OpsCenter provides you with the Getting Started feature that assists you in the initial OpsCenter configuration. When you logon to OpsCenter for the first time, you need to do a few initial configurations in the following recommended sequence to start monitoring NetBackup:

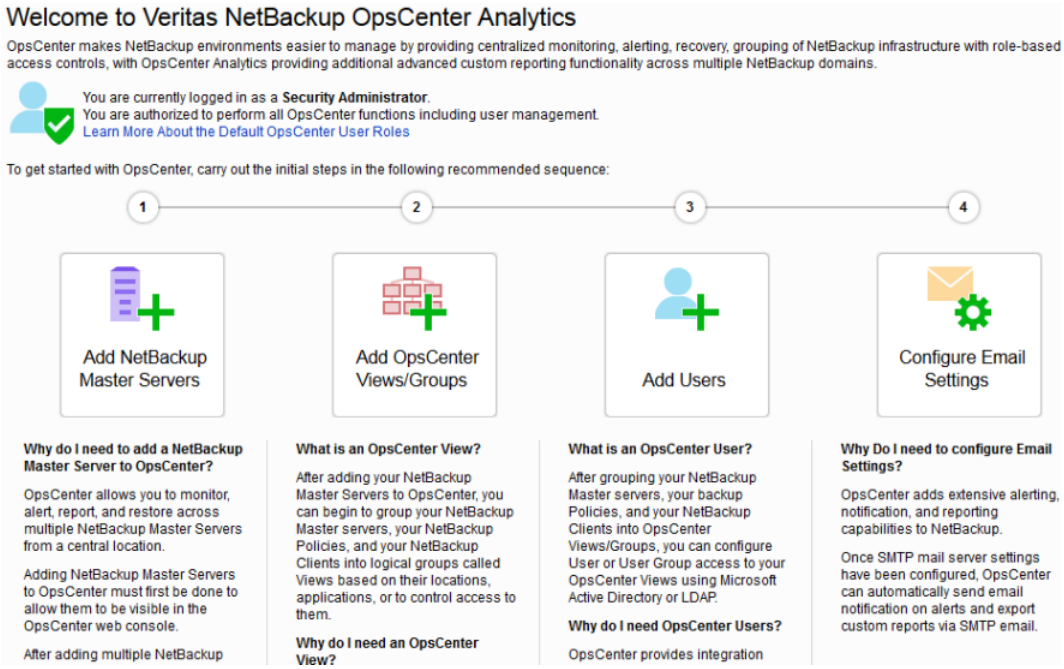
Step	Task	Details
Step 1	Add NetBackup Master Servers	Adding NetBackup Master Servers in the OpsCenter console is the first step of the NetBackup data collection. You can add multiple NetBackup master servers in the OpsCenter console.
Step 2	Add OpsCenter views / groups	After adding NetBackup master servers, you can group them (or NetBackup policies or clients) into logical groups called OpsCenter views based on their locations or applications. You can group master servers, policies, or clients to restrict their access to the OpsCenter users.
Step 3	Add users into OpsCenter	Once the master servers, policies, or clients are grouped, you can add users in OpsCenter who can access OpsCenter views depending on their roles. OpsCenter provides integration with Microsoft Active Directory (AD) and LDAP. You can add AD / LDAP users and user groups in OpsCenter.
Step 4	Configure email settings	OpsCenter provides alerting and reporting functionality. Once you configure SMTP email server, OpsCenter can automatically send email notifications on alerts and export reports.

You can carry out these tasks using other tabs and screens across the OpsCenter user interface. However, the OpsCenter Getting Started feature provides four simple set of wizards and user interface screens that help you do all the required configurations in one go. Once you do all these configurations, NetBackup data collection begins. You can then generate the required reports using the Reports tab.

After the initial configuration, if you want to access the OpsCenter Getting Started feature, click **Home** on the OpsCenter user interface.

Figure 3-1 displays the OpsCenter Getting Started feature GUI.

Figure 3-1 OpsCenter Getting Started GUI



OpsCenter user roles

OpsCenter users are categorized as follows:

Table 3-1

User	Description
Security Administrator	A Security Administrator is a super admin user who can perform all OpsCenter functions including user management. The OpsCenter Security Administrator can create, edit, or delete users.
Administrator	This user can perform all OpsCenter functions except for user management.
Operator	This user is not involved in the activities that are related to managing users, OpsCenter Server, and NetBackup configuration.

Table 3-1 *(continued)*

User	Description
Restore Operator	The role of this user is to mainly perform restore operations. The Restore Operator can monitor, perform alert operations and run standard or custom reports.
Reporter	The role of this user is to mainly generate the operational and business-level reports for further analysis. A Reporter would be able to view only those schedules that they themselves create. The Security Administrator, Administrator, and Operator would however be able to access all the schedules.

Note: You can assign a user role to a user group of an authorized AD / LDAP domain. The same user role is assigned to each user of the authorized domain group.

See "About adding AD / LDAP user groups in OpsCenter" on page 227.

Table 3-2 lists the OpsCenter user roles and the OpsCenter UI functions that these users can perform.

Table 3-2 User roles

OpsCenter function	Security Administrator	Administrator	Operator	Restore Operator	Reporter
User Management	Y	N	N	N	N
OpsCenter Management	Y	Y	N	N	N
NetBackup Operations	Y	Y	Y	Partial (Only perform operations on Restore Jobs)	N
Backup and Recovery	Y	Y	Y	Y	N
Views Management	Y	Y	N	N	N
All Views Read	Y	Y	P	P	P
Report Execution	Y	Y	Y	Y	Y
Custom Reports	Y	Y	Y	Y	Y

Table 3-2 User roles *(continued)*

OpsCenter function	Security Administrator	Administrator	Operator	Restore Operator	Reporter
Custom SQL Reports	Y	Y	N	N	N
Monitoring	Y	Y	Y	Y	Y
Alert Management	Y	Y	Y	Y	Y

“Y” represents “Yes”, which means that the users of this role can perform this particular OpsCenter function.

“N” represents “No”, which means that the users of this role cannot perform this particular OpsCenter function.

P represents "Permission based", which means that users of this role need permission to perform the particular function.

Learn more about adding NetBackup Master Servers

OpsCenter monitors and manages NetBackup master and media servers, clients, and policies. It also generates reports. To perform the monitoring, management, and reporting functions, OpsCenter collects data from the NetBackup master servers. The NetBackup data collection and management logic that OpsCenter uses is built into NetBackup master servers. This logic is included in the NetBackup Service Layer (NBSL).

OpsCenter uses the bpjava protocol to collect capacity and traditional license data.

Learn more about OpsCenter Views

OpsCenter views are logical groups of IT assets (master servers or clients) organized in a hierarchical manner. A Security Administrator or an Administrator can create views either from OpsCenter console or the OpsCenter View Builder (formerly called Java View Builder) and make them available in the OpsCenter console.

In an OpsCenter view, IT assets that are scattered across organization can be arranged according to their locations, business units, or applications. You can generate various OpsCenter reports that are filtered by views. With these reports, you can identify the locations or departments with hosts storing business critical data. After you install and run the OpsCenter Server and the OpsCenter Agent,

OpsCenter detects the IT assets, which are then stored in the database. The OpsCenter View Builder makes these IT assets available when a view is created.

Add Users

You can either add the existing users that are discovered from various domains to OpsCenter or create users in the private “OpsCenterUsers” domain.

You can add AD / LDAP domain groups to OpsCenter to authorize all users from that group to access OpsCenter.

All users from the authorized domain group can logon to OpsCenter with their AD / LDAP credentials. Any changes like addition or removal of a user from an authorized AD / LDAP domain group are automatically reflected in OpsCenter.

Note: Only a Security Administrator can add or modify user profiles by using the OpsCenter console.

To add a new user to OpsCenter

1. On the Add User screen, select the user creation type: **New User**, **Existing Domain User**, or **Existing Domain Group**.

   By selecting the Existing Domain Group creation type you can add AD / LDAP domain groups to OpsCenter. Once a domain user group is authorized to access OpsCenter, all users from that group can logon to OpsCenter with their AD / LDAP credentials.

   If you have selected the **New User** option, specify the password, and enter it once again for confirmation.

   If you have selected the **Existing Domain User** option, you need to select the domain to which the user belongs.

   If you have selected the **Existing Domain Group** option, you need to provide the AD/LDAP group name that you want to add and authorize.

2. Enter the following general and demographic details of the user, which change depending on the user creation type that you have selected:

   User name, user role, and domain name.

   If you have selected **Operator**, **Reporter**, or **Restore Operator** as the **User Role**, you can see the Granted Views list box. Select one or more views from the Granted Views list box to grant access of the specific views to the specific user.

3. Select status of the user or user group: Enabled or Disabled

   If you want to temporarily revoke a user's permission to access OpsCenter, set the user status to 'Disabled'. User with the 'Disabled' user status cannot logon to OpsCenter. However, the user-specific data such as reports or schedules is retained.

4. Save the information.

Edit User

Only a Security Administrator can add or modify user profiles by using the OpsCenter console.

On the Edit User screen, you can view the following user information:

Option	Description
Domain Name	You cannot modify the domain name of the user or the user group.
User Name	You cannot modify the name of the user or the user group.
Reset Password	You can see the 'Reset Password' link, if the user is from the OpsCenterUsers(vx) domain. Click the link to reset the password of this user account.
User Role	Modify the user role, if required. If you change the user role to Operator, Reporter, or Restore Operator, you also need to assign appropriate OpsCenter views to this user.
User Status	Select status of the user or user group: Enabled or Disabled **Note:** If you want to temporarily revoke a user's permission to access OpsCenter, set the user status to 'Disabled'. User with the 'Disabled' user status cannot logon to OpsCenter. However, the user-specific data such as reports or schedules is retained.
Assign Views	You can see this field if the user role is Operator, Reporter, or Restore Operator. Assign appropriate OpsCenter views to this user. Select a view from the Available Views list box and click the right-arrow button.

Reset password

If you are OpsCenter Security Administrator, you can reset the password of an OpsCenterUsers(vx) domain user while you modify the user information. NT or LDAP domain users should contact the System Administrator to reset their passwords.

For security reasons, OpsCenter user should change the password after it was reset by the OpsCenter Security Administrator. OpsCenter displays the Change Password page when you try to log in after your password was reset.

To reset an OpsCenterUsers(vx) domain user password

1. Log on to the OpsCenter console as a Security Administrator.
2. On the OpsCenter user interface, click **Settings > Users**.
3. Select the user to edit the user profile.
4. Click **Edit**.
5. On the Edit User screen, click **Reset Password**.
6. On the Reset Password screen, enter the new password.
7. Enter the same password again for confirmation.

   Note: You must set your new password according to the password rules or guidelines: Password must be at least 8 characters long and should contain at least one upper case letter, one lower case letter, and one numeric digit. The new password must be different than the current password.

   The password rules are also provided on the Reset Password page.

8. Click **OK**.

Add NetBackup Master Server

Add a NetBackup Master Server from which you want to collect data.

See "About configuring data collection for NetBackup" on page 271.

Enter the following details on the Add NetBackup Master Server page:

Option	Description
NetBackup Master Server Name	Enter a host name or an IP address of the master server.

Option	Description
Display Name	Enter an alternate name for the master server or appliance master server. The display name is used for the master server on all views of the OpsCenter console.
NetBackup User Name	Enter a valid NetBackup user name.
NetBackup Password	Enter the NetBackup password. **Note:** OpsCenter uses the bpjava protocol to collect some of the data types from NetBackup. The bpjava protocol requires NetBackup credentials.

Click the **Test Connection** button to validate the NetBackup credentials.

Click the **Save and Add More** button to add more master servers. Click the **Save and Close** button to save the settings. Click the **Cancel** button to cancel the settings.

Add OpsCenter Agent

On the Agent screen, specify the following details:

Option	Description
Agent Host	Enter the name of the Agent that you want to add on the base screen for selection.
Agent Operating System Type	Select the required operating system from the drop down-list.
OpsCenter Server Network Address	The OpsCenter Server may have multiple network interface cards (NIC). You can select a preferred network address from the drop-down list. OpsCenter uses the address that you select to connect to the master server.

Click the **Locate** button to locate the agent. Click **Save** to create the agent or click **Cancel** to exit.

Add OpsCenter Views/Groups

On the Add OpsCenter Views screen, enter the following information:

Option	Description
View Name	Enter the name of the view that you want to create.
View Type	Select the view type: Client, Master Server, or Policy
Description	Provide the description of the view, like which type of assets it comprises.
+ (Plus sign)	Click the plus sign (+) to add one more view.

Configure SMTP Server

On the Configure SMTP Server screen, specify the following details:

Option	Description
SMTP Server Name	Enter the SMTP (Simple Mail Transfer Protocol) Server host name. Notifications of the alerts that are generated in OpsCenter are sent using this SMTP server.
SMTP Server Port	Enter the SMTP (Simple Mail Transfer Protocol) Server port number.
Sender Display Name	Enter the name that is associated with the Email ID. For example, Backup Reporting Department.
Sender Email Address	Specify the Email ID to receive any replies to the alerts or the reports that were sent by OpsCenter.
SMTP Server User Name	Some SMTP servers may require user name and password credentials to send email. Enter the user name.
SMTP Server Password	Some SMTP servers may require user name and password credentials to send email. Enter the password for this user account.

See “About storing the SMTP Server configurations in OpsCenter” on page 216.

Chapter 4

Administering OpsCenter

This chapter includes the following topics:

- About the services and processes used by OpsCenter
- OpsCenter server scripts on Windows and UNIX
- About OpsCenter database administration
- About backup and restore of OpsCenter and OpsCenter Analytics
- About communication ports and firewall considerations in OpsCenter
- Gathering troubleshooting data with the support script
- About OpsCenter log files

About the services and processes used by OpsCenter

This section provides information about OpsCenter services and processes and how you can control these services.

These topics assume you already installed OpsCenter on a server.

If you have not installed OpsCenter, review the installation chapter.

See "Services used by OpsCenter on Windows" on page 164.

See "Controlling the OpsCenter services" on page 164.

See "Processes used by OpsCenter on UNIX" on page 165.

Services used by OpsCenter on Windows

After you install OpsCenter server and Agent on Windows, the following services should be active. OpsCenter depends on these services. If any of these services fail to start, OpsCenter does not start.

Table 4-1 contains information about the services that OpsCenter uses on Windows.

Table 4-1 Services used by OpsCenter on Windows

Service Name	Process	Description
OpsCenter Agent Service	java.exe	This service is for the OpsCenter Agent. By default, the OpsCenter Agent Service starts whenever you boot your Agent host.
OpsCenter Server Service	java.exe	The OpsCenter server interacts with the OpsCenter GUI and provides the data that is requested by the GUI from the OpsCenter database. It also interacts with NetBackup through NBSL to get data regularly.
OpsCenter Database Server	dbsrv11.exe	This service manages the OpsCenter databases. This process must be running on the OpsCenter server during all normal operations like viewing reports, running reports and so on.
OpsCenter Web server Service	java.exe	This service is not an OpsCenter service. OpsCenter uses this service to host the OpsCenter Console.
Veritas Private Branch Exchange	pbx_exchange.exe	This service is not an OpsCenter service, but it is a component used by OpsCenter. Veritas Private Branch Exchange allows all socket communication to take place through a single port.
OpsCenter Authentication Service (AT)	ops_atd.exe	This is an OpsCenter service.

Note: The processes that are listed in this table show the actual memory that is consumed by the respective OpsCenter service.

Controlling the OpsCenter services

Use the following procedure to verify if these services are running or not.

To control these services

1. Use **Start > Settings > Control Panel > Administrative Tools > Services**.
2. Check the **Status** column for each service. From the **Status** column, you can verify if a service is running or not.
3. The Services panel can also be used to stop, start, and restart the OpsCenter services and Veritas shared services.

Processes used by OpsCenter on UNIX

After you install OpsCenter server on UNIX, the following processes should be active.

Table 4-2 describes the processes that OpsCenter uses on UNIX.

Table 4-2 Processes used by OpsCenter on UNIX

Process Description	Process	Detailed Description
OpsCenter Server	<INSTALL_PATH>/SYMCOpsCenterServer/bin/.OpsCenterServerd	The OpsCenter server interacts with the OpsCenter user interface and provides the data that the user interface requests from the OpsCenter database. It also interacts with NetBackup to get data regularly.
OpsCenter Database Server	<INSTALL_PATH>/SYMCOpsCenterServer/db/bin/OpsCenterDBd	This process manages the OpsCenter databases. This process must be running on the OpsCenter server during all normal operations like viewing reports, running reports and so on.
OpsCenter Web Server	java	This process is not an OpsCenter process. OpsCenter uses this process to host the OpsCenter Console. Many Veritas Web consoles share this component.

Table 4-2 Processes used by OpsCenter on UNIX *(continued)*

Process Description	Process	Detailed Description
Veritas Private Branch Exchange	<INSTALL_PATH>/VRTSpbx/bin/pbx_exchange	This process is not an OpsCenter process, but it is a component used by OpsCenter. PBX allows all socket communication to take place through a single port.
OpsCenter Authentication Service (AT)	<INSTALL_PATH>/SYMCOpsCenterServer/authbroker/bin/ops_atd	This is an OpsCenter process.

Note: The processes that are listed in this table show the actual memory consumed by the respective OpsCenter process.

OpsCenter server scripts on Windows and UNIX

The following scripts are used within OpsCenter. The OpsCenter administrator may use many of these scripts. Use the -h option for help about these scripts.

Table 4-3 lists the OpsCenter server scripts on Windows.

Table 4-3 OpsCenter server scripts on Windows

Script	Location	Function	Invokes or Is Invoked by
startserver.bat and stopserver.bat	*INSTALL_PATH*\OpsCenter\server\bin	Starts or stops the OpsCenter Server service that is OpsCenterServerd.	OpsCenter Administrator
startat.bat and stopat.bat	*INSTALL_PATH*\OpsCenter\server\bin	Starts or stops the OpsCenter AT service that is ops_atd.	OpsCenter Administrator
dbbackup.bat	*INSTALL_PATH*\OpsCenter\server\bin	Backs up the OpsCenter database	OpsCenter Administrator
startdb.bat and stopdb.bat	*INSTALL_PATH*\OpsCenter\server\bin	Starts or stops the OpsCenter database	OpsCenter Administrator

Table 4-3 OpsCenter server scripts on Windows *(continued)*

Script	Location	Function	Invokes or Is Invoked by
opsadmin.bat	*INSTALL_PATH*\OpsCenter\server\bin	Starts and stops all OpsCenter Server services	OpsCenter Administrator
dbdefrag.bat	*INSTALL_PATH*\OpsCenter\server\bin	Defragments the OpsCenter database	OpsCenter Administrator
changedbpassword.bat	*INSTALL_PATH*\OpsCenter\server\bin	Changes the OpsCenter database password	OpsCenter Administrator
runStoredQuery.bat	*INSTALL_PATH*\OpsCenter\server\bin	Runs saved custom SQL and generates output in the desired format.	OpsCenter Administrator

Table 4-4 lists the OpsCenter server scripts on UNIX.

Table 4-4 OpsCenter server scripts on UNIX

Script	Location	Function	Invokes or Is Invoked by
startserver and stopserver	*INSTALL_PATH*/SYMCOpsCenterServer/bin	Starts or stops OpsCenterServerd.	OpsCenter Server
startat.sh and stopat.sh	*INSTALL_PATH*/SYMCOpsCenterServer/bin	Starts or stops the OpsCenter AT service that is ops_atd.	OpsCenter Server
startdb and stopdb	*INSTALL_PATH*/SYMCOpsCenterServer/bin	Starts or stops the OpsCenter database	OpsCenter Administrator
opsadmin.sh	*INSTALL_PATH*/SYMCOpsCenterServer/bin	Starts, stops, and monitors all OpsCenter Server processes	OpsCenter Administrator
dbbackup.sh	*INSTALL_PATH*>/SYMCOpsCenterServer/bin	Backs up the OpsCenter database	OpsCenter Administrator
dbdefrag	*INSTALL_PATH*>/SYMCOpsCenterServer	Defragments the OpsCenter database	OpsCenter Administrator

Table 4-4 OpsCenter server scripts on UNIX *(continued)*

Script	Location	Function	Invokes or Is Invoked by
changeDbPassword.sh	*INSTALL_PATH*>/SYMCOpsCenterServer	Changes the OpsCenter database password	OpsCenter Administrator
runStoredQuery.sh	*INSTALL_PATH*/SYMCOpsCenterServer	Runs saved custom SQL and generates output in the desired format.	OpsCenter Administrator

Commands to control OpsCenter services and processes

This section provides information on how you can control the OpsCenter server services and OpsCenter Agent service.

Table 4-5 Start and stop commands on Windows

Service	Commands or Steps

All OpsCenter server services	To start all OpsCenter server services:
	`INSTALL_PATH\OpsCenter\server\bin\opsadmin.bat start`
	To stop all Veritas NetBackup OpsCenter server services:
	`INSTALL_PATH\OpsCenter\server\bin\opsadmin.bat stop`

OpsCenter database server service	Select **Control Panel > Administrative Tools > Services** and start or stop the **Veritas OpsCenter Database Server** service.
OpsCenter Server Service	Select **Control Panel > Administrative Tools > Services** and start or stop the **Veritas OpsCenter Server Service**.
OpsCenter Web server Service	Select **Control Panel > Administrative Tools > Services** and start or stop the **Veritas OpsCenter Web Server Service**.
OpsCenter Agent Service	Select **Control Panel > Administrative Tools > Services** and start or stop the **Veritas OpsCenter Agent Service**.

Table 4-6 Start and stop commands on UNIX

Process	Commands or Steps

All OpsCenter server processes	To start all OpsCenter server processes:
	`<INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh start`
	To stop all OpsCenter server processes:
	`<INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh stop`
	To monitor all processes:
	`<INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh monitor`

OpsCenter database server process	`<INSTALL_PATH>/SYMCOpsCenterServer/bin/startdb` `<INSTALL_PATH>/SYMCOpsCenterServer/bin/stopdb`
OpsCenter server process	`<INSTALL_PATH>/SYMCOpsCenterServer/bin/startserver` `<INSTALL_PATH>/SYMCOpsCenterServer/bin/stopserver`
OpsCenter Web server process	`<INSTALL_PATH>/SYMCOpsCenterGUI/bin/startgui.sh` `<INSTALL_PATH>/SYMCOpsCenterGUI/bin/stopgui.sh`

About dependency of services

The OpsCenter server service requires that the following OpsCenter services (processes) are running:

- OpsCenter Database Server
- OpsCenter Authentication Service
- Veritas Private Branch Exchange

If you stop any of these services, then the OpsCenter server also stops.

Note: After a reboot, the OpsCenter processes do not start automatically on SUSE Linux systems. Veritas recommends that you start the OpsCenter processes after you perform a reboot.

Also after you reboot a SUSE 11 Server, and even though OpsCenter Server services are running, an attempt to logon may not succeed. Occasionally, OpsCenter services may not start on reboot in case of SUSE 11. This issue may happen because of the PBX taking time to start.

About nbproxy processes on NetBackup master servers

When OpsCenter is connected to a master server, you may find one or more `nbproxy` processes running on the master server. You may also see `nbproxy` processes when NetBackup-Java GUI or NetBackup-Windows GUI request certain data from NetBackup (like LiveUpdate , storage lifecycle policies).

Most of the `nbproxy` processes are started, managed, and removed by NBSL. This section talks about the `nbproxy` processes that NBSL manages.

Note: Not all `nbproxy` processes on the master server are managed by NBSL. For example, some of the `nbproxy` processes are managed by `nbjm` and `nbpem`.

An `nbproxy` process runs to retrieve the following NetBackup data for OpsCenter:

- Policies
- Catalogs
- Storage lifecycle policies
- LiveUpdate
- Client details

Note the following points about the NBSL-managed `nbproxy` processes:

- If the data collection for a master server is disabled or a master server is removed from the OpsCenter console, all `nbproxy` processes are stopped immediately.
- If OpsCenter crashes (or is abruptly closed), the `nbproxy` process is removed within an hour.
- If NetBackup is stopped (and NBSL is already killed), all `nbproxy` processes are stopped immediately.
- If NBSL crashes (or is abruptly closed), all `nbproxy` processes exit within 10 minutes.

About OpsCenter database administration

The Sybase database that OpsCenter uses is installed as part of the OpsCenter installation. The database is located on the OpsCenter server.

More information about the Sybase database is available.

See `http://www.sybase.com/support/manuals`.

Note: Starting from OpsCenter 8.0, the database password is set to an auto-generated string during installation.

During OpsCenter upgrade, the installer retains the old password, if you had changed it from the default value. During upgrade, if the password is still the default one, that is 'SQL', the installer changes it to an auto-generated string. You can change the database password using the `changeDbPassword` utility.

See "Changing the OpsCenter database administrator password" on page 172.

OpsCenter database commands

OpsCenter provides some useful commands to help manage the OpsCenter database.

Table 4-7 lists some of the commands that are available.

Table 4-7 Commands available with OpsCenter

Command	Reference
`changeDbPassword`	See "Changing the OpsCenter database administrator password" on page 172.
`startdb` and `stopdb`	See "Starting and stopping the OpsCenter database" on page 173.
`dbdefrag`	For information on OpsCenter database defragmentation, refer to the *OpsCenter Performance and Tuning Guide* at the following location: http://www.veritas.com/docs/DOC5808
`dbbackup`	See "Backing up the OpsCenter database" on page 184. See "Restoring the OpsCenter database" on page 186.

Note: For a clustered OpsCenter server, you must run commands on the active node.See "About running commands on the active node" on page 141.

http://www.veritas.com/docs/DOC5808

Changing the OpsCenter database administrator password

The `changeDbPassword` utility lets you change the password that is used to connect to the OpsCenter database.

OpsCenter uses the Sybase SQL Anywhere to store data.

The database administrator user ID is `DBA`.

- After fresh OpsCenter installation, the database password is set to an auto-generated string. You can change the password using the following procedure.
- After OpsCenter upgrade, the database password is set to an auto-generated string, if it is still the default one, which is 'SQL'.
  You can change the password using the following procedure.
  However, if you had changed the password from the default one in the earlier version, OpsCenter retains that password.

Review the rules for forming a new database password.

The OpsCenter database administrator password has the following constraints:

- It should contain 7 or more characters, but should not exceed 30 characters.
- It should not contain consecutive black slash characters.
- It should not contain any bracket characters.
- It should not contain any of the following characters (these characters have special meaning in Windows or in shell scripts):
  ‘ ! $ % & . ; ^ | < > , { } $ " ~ [ ] \\
- It should not contain the ASCII characters that are less than 32 or greater than 127.
- It should not begin with a white space or a single quote character.
- It should not end with a white space.

Note: Information about role-based access in OpsCenter is available.

See "User access rights and functions in OpsCenter user interface" on page 231.

To change the database administrator password on Windows and UNIX

1. Enter the following command on Windows:

   `INSTALL_PATH\OpsCenter\server\bin\changeDbPassword.bat`

   Enter the following command on UNIX:

   `<INSTALL_PATH>/SYMCOpsCenterServer/bin/changeDbPassword.sh`

2. Enter the OpsCenter Administrator's password. OpsCenter Administrator is authorized to change the database password.
3. Enter the new password for the database that you want to set.
4. Restart the OpsCenter services and processes on Windows and UNIX platforms.

Windows	Enter the following commands to stop and then start the OpsCenter services: INSTALL_PATH\OpsCenter\server\bin\opsadmin.bat stop INSTALL_PATH\OpsCenter\server\bin\opsadmin.bat stop
UNIX	Enter the following commands to stop and then start the OpsCenter processes: <INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh stop <INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh start

Starting and stopping the OpsCenter database

The `startdb` script is used to start the OpsCenter database. The `stopdb` script is used to stop the OpsCenter database.

To start the database server on Windows and UNIX

- To start the OpsCenter database on Windows, run the following command:

  `INSTALL_PATH\OpsCenter\server\bin\startdb.bat`

  To start the OpsCenter database on UNIX, run the following command:

  `<INSTALL_PATH>/SYMCOpsCenterServer/bin/startdb`

To stop the database server on Windows and UNIX

- To stop the OpsCenter database on Windows, run the following command:

  ```
  INSTALL_PATH\OpsCenter\server\bin\stopdb.bat
  ```

  To stop the OpsCenter database on UNIX, run the following command:

  ```
  <INSTALL_PATH>/SYMCOpsCenterServer/bin/stopdb
  ```

Moving the OpsCenter database and database logs to a different hard disk

To improve OpsCenter performance, OpsCenter database files and the log files that are associated with the OpsCenter database should be stored on separate hard disks. You can store the OpsCenter database files on one hard disk and the log files on another hard disk.

Veritas recommends you not to store the database files on the hard disk that contains your operating system files.

You can specify a custom location (non-default location) for the OpsCenter database during OpsCenter installation. The default location for the OpsCenter database can also be changed after OpsCenter has been installed.

Use the following procedures to move the OpsCenter database and log files to a different hard disk. The first two procedures are for moving the OpsCenter database files on Windows or UNIX. The last two procedures are for moving the database log files.

To move the OpsCenter database to a different hard disk on Windows

1. Stop all OpsCenter services. Enter the following command:

   ```
   INSTALL_PATH\OpsCenter\server\bin\opsadmin.bat stop
   ```

2. Open the `databases.conf` file with a text editor like notepad from the following directory:

   ```
   INSTALL_PATH\OpsCenter\server\db\conf
   ```

   This file has the following contents:

   ```
   "INSTALL_PATH\OpsCenter\server\db\data\vxpmdb.db"
   ```

   This path specifies the default location of the OpsCenter database.

3 To move the database to a custom location like `E:\Database`, replace the contents of the file with the following:

```
"E:\Database\vxpmdb.db"
```

Caution: Make sure that you specify the database path in double quotes. The directories in the specified path and also the `databases.conf` file should not contain any special characters like %, ~, !, @, $, &, ^, #, and so on. For example, do not specify a path like `E:\Database%`. Commenting out the path is also not allowed. For example, the following string is not allowed in the `databases.conf` file: `#"E:\Database\vxpmdb.db"`

If you want to change the database path, you should replace the original path with the new one instead of commenting out the original path.

If the `databases.conf` file contains characters or strings other than the database location, the database upgrade will not succeed.

If you need a reference, you can create a backup copy of the original `databases.conf` file with a different file name.

Save the `databases.conf` file.

4 Copy the database files to the new location. Copy `vxpmdb.db`, `symcOpscache.db`, `symcopsscratchdb.db`, and `symcsearchdb.db` from `INSTALL_PATH\OpsCenter\server\db\data` to a location like E:\Database.

5 Restart all OpsCenter server services.

To restart all OpsCenter services, enter the following command:

```
INSTALL_PATH\OpsCenter\server\bin\opsadmin.bat start
```

You should run and monitor OpsCenter for a certain period after moving the database. If OpsCenter works as expected, you can delete `vxpmdb.db`, `symcOpscache.db`, `symcopsscratchdb.db`, and `symcsearchdb.db` from the default location (`INSTALL_PATH\OpsCenter\server\db\data`).

To move the OpsCenter database to a different hard disk on UNIX

1. Stop all OpsCenter server processes. Enter the following command:

   ```
   <INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh stop
   ```

2. The default location of the OpsCenter database is `<INSTALL_PATH>/SYMCOpsCenterServer/db/data`.

   Back up the OpsCenter database (`<INSTALL_PATH>/SYMCOpsCenterServer/db/data`) to some other location. Enter the following command:

   ```
   cp -R <INSTALL_PATH>/SYMCOpsCenterServer/db/data /backup/data
   ```

3. To move the database to a custom location like `/usr/mydata`, always create a new directory named OpsCenterServer inside `/usr/mydata` by entering the following command:

   ```
   mkdir -p /usr/mydata/OpsCenterServer
   ```

   Veritas recommends that when you move the OpsCenter database to a custom location on UNIX, the database must be saved in a directory named OpsCenterServer inside the custom location: /*CUSTOM_LOCATION*/OpsCenterServer.

4. To move the database to a custom location like `/usr/mydata/OpsCenterServer`, enter the following command:

   ```
   mv <INSTALL_PATH>/SYMCOpsCenterServer/db/data/*
   /usr/mydata/OpsCenterServer
   ```

5. Remove the symbolic link that exists for the OpsCenter database. Enter the following command:

   ```
   unlink <INSTALL_PATH>/SYMCOpsCenterServer/db/data
   ```

6. Create a symbolic link to `/usr/mydata/OpsCenterServer` in `<INSTALL_PATH>/SYMCOpsCenterServer/db/data`. To create a symbolic link, enter the following command:

   ```
   ln -s /usr/mydata/OpsCenterServer
   <INSTALL_PATH>/SYMCOpsCenterServer/db/data
   ```

7. Restart all OpsCenter server processes by entering the following command:

   ```
   <INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh start
   ```

   You should run and monitor OpsCenter for a certain period after moving the database. If OpsCenter works as expected, you can delete `vxpmdb.db` and `symcOpscache.db` from `/backup/data`.

To move the database log files to a different hard disk on Windows

1. Stop all OpsCenter server services. Enter the following command:

   ```
   INSTALL_PATH\OpsCenter\server\bin\opsadmin.bat stop
   ```

2. Navigate to the following location for 32-bit and 64-bit systems respectively:

   ```
   INSTALL_PATH\OpsCenter\server\db\WIN32
   ```

   ```
   INSTALL_PATH\OpsCenter\server\db\WIN64
   ```

   Enter the following commands:

   ```
   dblog -t directory_path\vxpmdb.log database_path\vxpmdb.db
   ```

   where *directory_path* is the path where you want to store the database logs and *database_path* is the path where your database is located.

   This command moves the log file that is associated with the OpsCenter database to the new directory (*directory_path*). It is recommended to use `vxpmdb.log` as the name of the log file.

3. Restart all OpsCenter server services.

   To restart all OpsCenter services, enter the following command:

   ```
   INSTALL_PATH\OpsCenter\server\bin\opsadmin.bat start
   ```

To move the database log files to a different hard disk on UNIX

1. Stop all OpsCenter server processes. Enter the following command:

   ```
   <INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh stop
   ```

2. Set the path of the LD_LIBRARY_PATH variable in the following manner:

   ```
   LD_LIBRARY_PATH=<INSTALL_PATH>/SYMCOpsCenterServer/db/
   lib:$LD_LIBRARY_PATH export LD_LIBRARY_PATH
   ```

3 Navigate to the following location:

```
<INSTALL_PATH>/SYMCOpsCenterServer/db/bin
```

Enter the following commands:

```
./dblog -t directory_path/vxpmdb.log database_path/vxpmdb.db
```

where *directory_path* is the path where you want to store your database log file and *database_path* is the path where the OpsCenter database is located.

This command moves the log file that is associated with the OpsCenter database to the new directory (*directory_path*). It is recommended to use `vxpmdb.log` as the name of the log file.

4 Restart all OpsCenter server processes by entering the following command:

```
<INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh start
```

Moving OpsCenter server to a different computer

This section talks about the scenarios in which you need to move OpsCenter server to a different machine.

Consider the following scenarios:

- Scenario 1: You have OpsCenter setup that you want to upgrade and because of certain constraints with the new version, you need to move the OpsCenter server to a different machine.
  For example: If your existing version of OpsCenter is installed on a platform that is unsupported.
  See "Moving OpsCenter server because of constraints in upgrade" on page 178.
- Scenario 2: You want to move OpsCenter server to a different machine. For example, if the hardware of the existing machine is faulty.
  See "Moving OpsCenter server because of issues in the existing setup" on page 181.

Moving OpsCenter server because of constraints in upgrade

This section provides the procedure to move the existing OpsCenter server to a different machine where you want to install the latest version of OpsCenter. The following example explains the scenario in detail:

You have OpsCenter setup that you want to upgrade to the latest version. If OpsCenter is installed on a platform that is not supported by the latest version of

OpsCenter, you need to move the existing OpsCenter server to a different machine that has a supported platform.

You need to carry out a few steps on the existing OpsCenter server host and a few on the new host.

To move the existing OpsCenter server to a different machine

1. **Steps to be carried out on the existing OpsCenter server host**

   Stop all OpsCenter services.

   See "OpsCenter server scripts on Windows and UNIX" on page 166.

2. Take a hot backup of the OpsCenter database using the `dbbackup` script. You can run this script when you need to back up your OpsCenter database and database password file (`db.conf`).

   See "Backing up the OpsCenter database" on page 184.

3. Existing OpsCenter server host may have AT (Veritas Product Authentication Service) data that you want to import into the new OpsCenter. You need to first export the AT data on the existing OpsCenter server host, which you can import into the new OpsCenter setup.

   Export the shared or remote AT broker's data to an XML file using the `atutil` utility. AT data comprises OpsCenterUsers(vx) users and certificates.

   See "Exporting authentication settings" on page 119.

   See "About OpsCenter AT" on page 27.

   See "About OpsCenter upgrade scenarios with respect to OpsCenter AT" on page 116.

4. Copy the XML file that you have created in the earlier step to the new host.

   Note: While copying the exported XML file, the DOS to UNIX conversion may result into garbage characters in the xml file that can cause import failure. To avoid this problem, copy the XML file through FTP and with binary format.

5. **Steps to be carried out on the new host where you want to install the latest version of OpsCenter**

   Install the latest version of OpsCenter on the new host.

   See "Installing OpsCenter on Windows and UNIX" on page 87.

6. Stop all OpsCenter services on the new host.

   See "OpsCenter server scripts on Windows and UNIX" on page 166.

7 Carry out the performance tuning steps that you had done earlier.

The new OpsCenter Performance and Tuning Guide provides information on how to tune OpsCenter for improved performance. The online version of the OpsCenter Performance and Tuning Guide can be found at:

http://www.veritas.com/docs/DOC5808

8 Restore the database that you have backed up earlier.

See "Restoring the OpsCenter database" on page 186.

9 Update the following information from the `db.conf` file:

- If you are using the port that is different than the default one, update the value of the `db.port` parameter as follows:

  `db.port=13786`

- Set the `db.serviceName` parameter to the name of the target host as follows:

  `db.serviceName=`*`TargetHostName`*

10 Upgrade the database using `dbUpgrade` command.

Run the following command:

Windows `dbUpgrade.bat install <old_version_number> <new_version_number>`

For example:
`<OpsCenterInstallLocation>\OpsCenter\server\bin\dbUpgrade.bat install 8.0 8.1`

UNIX `dbUpgrade.sh install <old_version_number> <new_version_number>`

For example:
`<OpsCenterInstallLocation>/SYMCOpsCenterServer/bin/dbUpgrade.sh install 8.0 8.1`

11 Check the progress of database upgrade in the upgrade logs at the following location:

Windows `<OpsCenterInstallLocation>\ OpsCenter\server\db\log`

Unix `<OpsCenterInstallLocation>/SYMCOpsCenterServer/db/log`

12 Import old authentication or AT data into the new OpsCenter server host.

Make sure that you have copied the export XML file that you have created on the existing OpsCenter server host to the new OpsCenter server host.

Run the following command:

Windows
```
<OpsCenterInstallLocation>\OpsCenter\server\authbroker\bin\atutil
import -p <password of exported xml file> -f <location
of xml file that contains old AT data> -z <location of
AT data folder> -overwrite
```

For example:
```
atutil import -p "password" -f
\temp\userdata.xml -z C:Program
Files\Symantec\OpsCenter\server\authbroker\data
-overwrite
```

UNIX
```
<OpsCenterInstallLocation>/SYMCOpsCenterServer/authbroker/bin/atutil
import -p <password of exported xml file> -f <location
of xml file that contains old AT data> -z <location of
AT data folder> -overwrite
```

For example:
```
atutil import -p "password" -f
/temp/userdata.xml -z
/opt/SYMCOpsCenterServer/authbroker/data -overwrite
```

Note: If the import is not successful, the default OpsCenter user needs to reset the passwords of OpsCenterUsers(vx) domain users that you have imported from the earlier OpsCenter version. Trust between NBAC-enabled NetBackup / PureDisk server and OpsCenter server need to be established again.

See "About OpsCenter upgrade failure scenarios" on page 133.

---

13 Start OpsCenter services.

See "OpsCenter server scripts on Windows and UNIX" on page 166.

Moving OpsCenter server because of issues in the existing setup

This section provides the procedure to move OpsCenter server to a different machine. You need to move OpsCenter server to a different machine in certain scenarios for example:

- Faulty hardware
- Hardware upgrade

- Operating System upgrade
- Moving from physical machine to virtual machine (or from virtual machine to physical machine)

To move OpsCenter server to a different machine

1. **Steps to be carried out on the OpsCenter source host**

   Stop all OpsCenter services.

2. Take a hot backup of the OpsCenter database using the `dbbackup` script. You can run this script when you need to back up your OpsCenter database and database password file (`db.conf`).

   See "Backing up the OpsCenter database" on page 184.

3. OpsCenter source host may have authentication (AT) data that you want to import into OpsCenter target host. You need to first export the AT data on the OpsCenter source host, which you can import into OpsCenter target host.

   Export the AT data to an xml file using the `atutil` utility. AT data comprises OpsCenterUsers(vx) users and certificates.

   See "Exporting authentication settings" on page 119.

4. Copy the XML file to the OpsCenter target host.

   Note: While copying the exported xml file, the DOS to UNIX conversion may result into garbage characters in the xml file that can cause import failure. To avoid this problem, copy the xml file through FTP and with binary format.

   ---

5. **Steps to be carried out on the OpsCenter target host**

   Install OpsCenter on the new host that is target host.

   See "Installing OpsCenter on Windows and UNIX" on page 87.

6. Stop all OpsCenter services.

7. Carry out the performance tuning steps that you had done earlier.

   The new OpsCenter Performance and Tuning Guide provides information on how to tune OpsCenter for improved performance. The online version of the OpsCenter Performance and Tuning Guide can be found at:

   http://www.veritas.com/docs/DOC5808

8. Restore the database that you have backed up earlier.

   See "Restoring the OpsCenter database" on page 186.

9. Update the following information from the `db.conf` file:

- If you are using the port that is different than the default one, update the value of the `db.port` as follows:

  `db.port=13786`

- Set the `db.serviceName` parameter to the name of the target host as follows:

  `db.serviceName=TargetHostName`

10 Import old authentication or AT data into OpsCenter target host.

Make sure that you have copied the export xml file that you have created on the OpsCenter source host to OpsCenter target host.

Run the following command for import:

Windows
```
<OpsCenterInstallLocation>\OpsCenter\server\authbroker\bin\atutil
import -p <password of exported xml file> -f <location
of xml file that contains old AT data> -z <location
of AT data folder> -overwrite
```

UNIX
```
<OpsCenterInstallLocation>/SYMCOpsCenterServer/authbroker/bin/atutil
import -p <password of exported xml file> -f <location
of xml file that contains old AT data> -z <location
of AT data folder> -overwrite
```

Note: If the import is not successful, the default OpsCenter user needs to reset the passwords of OpsCenterUsers(vx) domain users that you have imported from the earlier OpsCenter version. Trust between NBAC-enabled NetBackup / PureDisk server and OpsCenter server need to be established again.

---

11 Start OpsCenter services.

About database troubleshooting

Security information about the OpsCenter database is available.

See "About communication between OpsCenter and Sybase database" on page 193.

Information about the log files on Windows and UNIX servers is available.

See "About OpsCenter log files on Windows servers" on page 200.

See "About OpsCenter log files on UNIX servers" on page 202.

About backup and restore of OpsCenter and OpsCenter Analytics

The procedures in this section explain how you can back up and restore OpsCenter and OpsCenter Analytics in case of a disaster.

See "Backing up OpsCenter in case of a disaster" on page 184.

See "Restoring OpsCenter" on page 186.

Backing up OpsCenter in case of a disaster

The sequence of steps gives an overview about the steps that need to be followed to back up OpsCenter.

To back up OpsCenter in case of a disaster

1. Take a hot backup of the OpsCenter database files using the `dbbackup` script. This script can be run whenever you need to back up your OpsCenter database, database password file (`db.conf`), and database password encryption key file.

   See "Backing up the OpsCenter database" on page 184.

2. Along with the OpsCenter database, the user information that Veritas Product Authentication Service manages must be saved in a directory or by using a NetBackup backup policy.

   See "Saving the OpsCenter user profiles managed by OpsCenter Authentication Service" on page 185.

Note: You can also create schedules for taking regular database and authentication profile backups. In this case, NetBackup policies can be created to back up the specified directories that contain OpsCenter database snapshots and the authentication service user configuration files.

See the *NetBackup Administrator's Guide, Volume I* for more information on how to configure a policy and schedule.

http://www.veritas.com/docs/DOC5332

Backing up the OpsCenter database

OpsCenter is shipped with a database backup script that performs backup of the database , the corresponding database password file, and the encryption key file without interrupting its operations, which is referred to as hot backup. On UNIX as

well as Windows platforms, the script overwrites the existing database files before backing up or restoring them.

Note: Regular file system backups are not sufficient for backing up the OpsCenter database. You must schedule periodic hot backups for the OpsCenter database to avoid losing any important data.

To back up the OpsCenter database

1. Log on to the OpsCenter database server host in one of the following ways:

Windows	As an administrator or user in the Administrator group
UNIX	`root`

2. Open the Windows command prompt or the UNIX console.
3. Run the backup script that is appropriate for your platform. Specify one of the following backup directories depending on your platform:

Windows	`INSTALL_PATH\OpsCenter\server\bin\dbbackup.bat C:\MyDbBackupFolder`
UNIX	`<INSTALL_PATH>/SYMCOpsCenterServer/bin/dbbackup.sh /my_db_backup_dir`

   The backup script backs up the database files, database password files, and encryption key file in the backup directory that you specified.

Saving the OpsCenter user profiles managed by OpsCenter Authentication Service

Use the following procedures to save the authentication service profiles on Windows and UNIX servers.

To save authentication service profiles on Windows servers

- Do one of the following to save the user profiles:
  - Copy the folder `INSTALL_PATH\VERITAS\Security\Authentication\systemprofile` to another folder.
  - Create a NetBackup job policy to back up the authentication service `systemprofile` folder.

To save authentication service profiles on UNIX servers

- Do one of the following to save the user profiles:
  - Copy the folder `/var/VRTSat` to another folder.
  - Create a NetBackup job policy to back up the authentication service profile folder.

Restoring OpsCenter

This section provides the procedure to restore OpsCenter in the case of a disaster.

Note: The following procedures assume that you have OpsCenter database snapshots, db.conf file, and the authentication service user profiles saved in folders.

The sequence of steps gives an overview about the steps that need to be followed to restore OpsCenter.

To restore OpsCenter in case of a disaster

1. Install OpsCenter on a server with the same name as the server where problems happened.
2. Stop all OpsCenter server services.
3. Restore the OpsCenter database snapshot files and authentication service user profiles from the backup image.

   See "Restoring the OpsCenter database" on page 186.

   See "Restoring the OpsCenter user profiles managed by OpsCenter Authentication Service" on page 187.
4. Restart all OpsCenter server services.

Restoring the OpsCenter database

You can restore the database that you have backed up earlier. On Windows and UNIX hosts, the restore operation automatically stops the database, restores the backup database files along with the database password file and encryption key file, and restarts the database. The `dbbackup` script overwrites existing database (db) files before backing up or restoring the database or the database password file.

Note: Veritas strongly recommends that you change the password for the admin user account after you restore the OpsCenter database.

To restore a backed up OpsCenter database

1. On the OpsCenter server with backup data you want to restore, open a UNIX console or a Windows command prompt and log on as `root` (on UNIX) or as an administrator or user in the Administrators group (on Windows).

Windows	Open a Windows command prompt and log on as an administrator or user in the Administrators group.
UNIX	Open a UNIX console and then log on as `root`.

   All the paths that are shown in the steps that follow are the default database install paths. These paths may different for your site if the database was installed anywhere other than the default location.

2. To restore the backed up database, do one of the following:

Windows	Type the following command and press **Enter**. `INSTALL_PATH\OpsCenter\server\bin\dbbackup.bat` *`backupDir`* `-restore`
UNIX	Type the following command and press **Enter**. *`INSTALL_PATH`*`/SYMCOpsCenterServer/bin/dbbackup.sh` *`backupDir`* `-restore`

   backupDir is the directory where the backed up database files, database password file, and encryption key file reside.

   The script prompts you with a message similar to the following:

   ```
   WARNING: this operation will overwrite the active
   OpsCenter data on this host.
   Do you wish to continue ? [y/n] (n)
   ```

3. To continue with the restore, press **Enter** on Windows hosts.

   To continue with the restore, type **y** on UNIX hosts.

   The `dbbackup` script automatically stops and restarts the database.

Restoring the OpsCenter user profiles managed by OpsCenter Authentication Service

Use the following procedures to save the authentication service profiles on Windows and UNIX servers.

To restore the authentication user profiles on Windows

1. Stop all OpsCenter server services. Enter the following command:

   ```
   INSTALL_PATH\OpsCenter\server\bin\opsadmin.bat stop
   ```

2. Copy or overwrite the folder containing the authentication service user profiles to INSTALL_PATH\VERITAS\Security\Authentication\systemprofile.
3. Start all OpsCenter server services. Enter the following command:

   ```
   INSTALL_PATH\OpsCenter\server\bin\opsadmin.bat start
   ```

To restore the authentication user profiles on UNIX

1. Stop all OpsCenter server processes. Enter the following command:

   ```
   <INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh stop
   ```

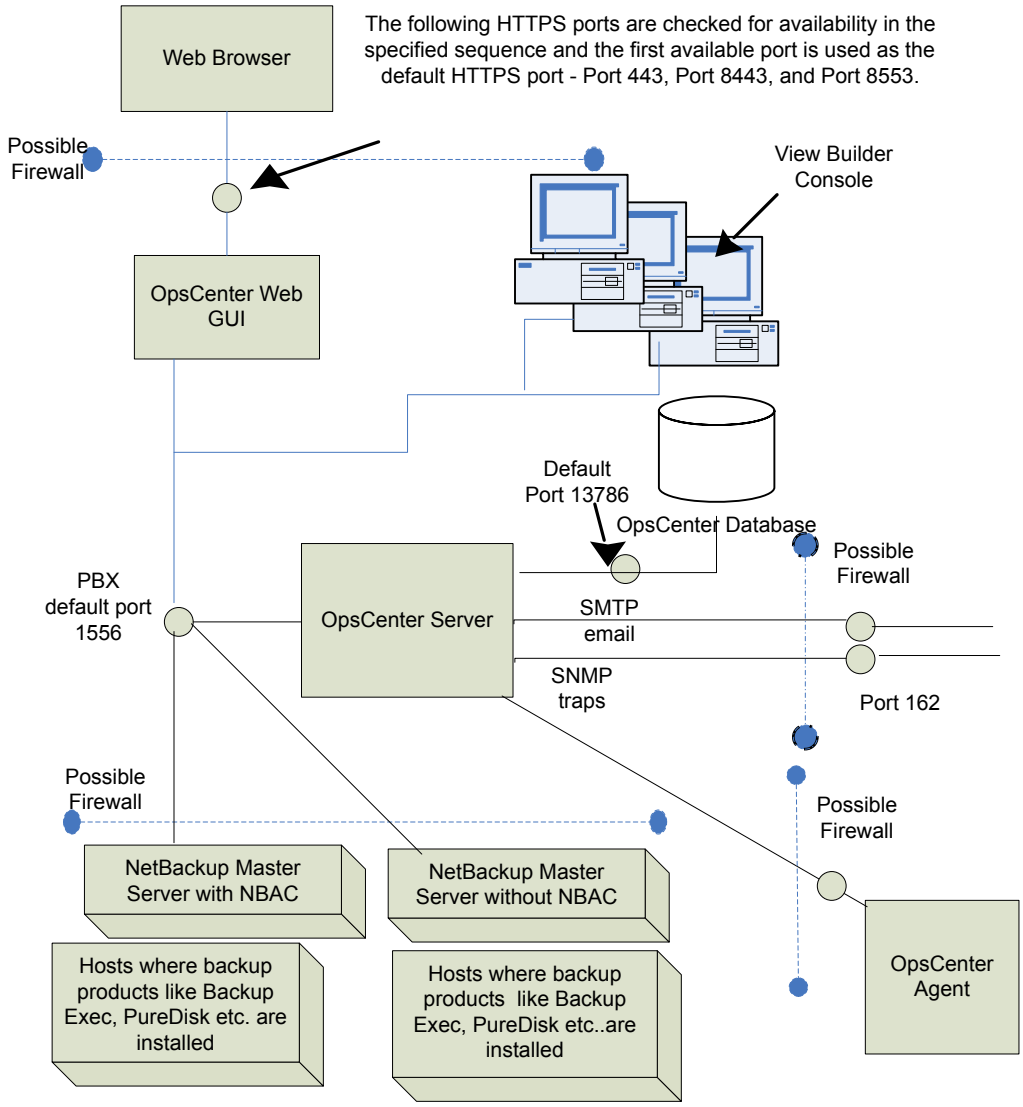
2. Copy or overwrite the folder containing the authentication service user profiles to /var/VRTSat
3. Start all OpsCenter server processes. Enter the following command:

   ```
   <INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh start
   ```

About communication ports and firewall considerations in OpsCenter

Figure 4-1 shows the key OpsCenter components and the communication ports that are used.

Figure 4-1 Key OpsCenter components and how they communicate



See "Communication ports used by key OpsCenter components" on page 189.

Communication ports used by key OpsCenter components

The following table shows the default port settings for OpsCenter.

SMTP recipient ports can be configured from the OpsCenter console (using **Settings > Configuration > SMTP Server**). The SNMP trap recipient ports can also be configured from the OpsCenter console (using **Settings > Recipients > SNMP**).

If these ports are changed then the appropriate hardware ports have to be opened.

Table 4-8 lists the communication ports that are used by key OpsCenter components.

Table 4-8 Communication ports used by key OpsCenter components

Source Host	Destination Host	Port Number	Usage (Process Name)	Port Configuration
OpsCenter Server	Mail server	25	SMTP	Allow from source to destination.
OpsCenter Server	SNMP Server	162	SNMP trap recipient	Allow from source to destination.
OpsCenter Server	NetBackup Master Server(s)	1556	PBX (pbx_exchange)	Allow between source and destination (bi-directional). PBX port number configuration is not supported. See "About OpsCenter user interface and OpsCenter server software communication" on page 192.
OpsCenter Client	OpsCenter Server	1556	PBX (pbx_exchange)	Allow between source and destination. Some hardened servers and firewall configurations may block this port. PBX port number configuration is not supported. See "About OpsCenter user interface and OpsCenter server software communication" on page 192.

Table 4-8 Communication ports used by key OpsCenter components *(continued)*

Source Host	Destination Host	Port Number	Usage (Process Name)	Port Configuration
Web browser	OpsCenter Server	The following HTTPS ports are checked for availability in the specified sequence and the first available port is used by default: **1** 443 (HTTPS) **2** 8443 (HTTPS) **3** 8553 (HTTPS)	HTTPS	Allow from all hosts on network.
OpsCenter Server	OpsCenter Server	13786	Sybase database (`dbsrv16`)	Allow between source and destination. Some hardened servers and firewall configurations may block this port.
OpsCenter Server	OpsCenter Server	1556	OpsCenter Product Authentication Service (`ops_atd`)	Allow between source and destination in case NBAC is enabled on NetBackup master server.

Ports required to communicate with backup products

This section provides information about the ports that OpsCenter Agent uses to communicate with backup products like Backup Exec and PureDisk.

Table 4-9 lists the ports that must be opened on OpsCenter Agent to collect data from various backup products.

Table 4-9 Ports required to communicate with backup products

Backup product	Communication	Port number
Backup Exec	OpsCenter (Backup Exec data collector) communicates with Backup Exec Server using Backup Exec API	6106
PureDisk	OpsCenter (PureDisk data collector) communicates with PureDisk SPA using `atssl`	443 (HTTPS) 2821 (AT)

Web browser to launch OpsCenter user interface

Web browsers use Secure hypertext transfer protocol (HTTPS) to communicate with the OpsCenter web graphical user interface. These protocols use TCP/IP.

Table 4-10 lists how the default HTTPS ports are selected.

Table 4-10 Default HTTPS ports

Sr. No.	HTTPS port number	Description
1.	443	Port 443 is checked for availability. ■ If port 443 is available, it is used as the default HTTPS port. ■ In case, some other application like a web server uses this port, then the next port is checked for availability.
2.	8443	Port 8443 is checked for availability. ■ If port 8443 is available, port 8443 is used as the default HTTPS port. ■ In case another application like VRTSWeb installed with VCS or any other product uses one or both ports, then the next port combination is checked for availability.
3.	8553	Port 8553 is checked for availability.

These HTTPS ports are opened only for input and are configurable using the command lines.

See configurePorts on page 630.

About OpsCenter user interface and OpsCenter server software communication

The OpsCenter web graphical user interface uses Veritas Private Branch Exchange (PBX) to communicate with the OpsCenter server software. The default port is 1556. The PBX port is opened for input and output traffic.

About OpsCenter server to NetBackup master server (NBSL) communication

OpsCenter requires the NetBackup Service Layer (NBSL) to be present on all managed master servers.

The OpsCenter server software collects data from NBSL in the following ways:

- Initial data load
- Listening for change notifications or events

Whenever OpsCenter server software starts, when data collection for a master server is enabled or when a master server is added in OpsCenter, the OpsCenter server starts collecting all the available data from NetBackup master server into the OpsCenter database using NBSL. The initial data load happens serially for each data type. As soon as the initial data load is complete, the OpsCenter server software listens to the notifications that are sent by NBSL for any change in NetBackup data. Then OpsCenter updates the OpsCenter database.

Veritas Private Branch Exchange (PBX) is used for communication and requires a port opened on the OpsCenter server and the NetBackup master server for input and output. The default PBX port is 1556.

About SNMP traps

SNMP trap protocol is used for outbound UDP traffic and requires a port that opens for output. The port number is 162.

About communication between OpsCenter and Sybase database

The OpsCenter web graphical user interface communicates with the OpsCenter Sybase SQL Anywhere database server by using the default port 13786.

The Sybase database server port is closed to all inbound connections. The database is available only to resident OpsCenter components on the OpsCenter server.

About email communication in OpsCenter

SMTP email server protocol is used for outgoing mail. The port number is defined when the user specifies the SMTP server port (see **Settings > Configuration > SMTP Server** in the OpsCenter console to specify this port). The port is opened for output only.

Gathering troubleshooting data with the support script

If you are running OpsCenter on UNIX or Windows, you can use the `support` script to gather troubleshooting information for OpsCenter Server and OpsCenter Agent. The script collects Server and Agent logs, collects information about any data collection problems, captures the current Agent configuration, and compresses the

results into a `zip` file. This file can serve as a first-level information for the Support team in case of an issue with OpsCenter.

To gather troubleshooting data for OpsCenter Server on Windows

1. Run the following command to execute the support script for OpsCenter Server:

   ```
   INSTALL_PATH\OpsCenter\server\bin\opsCenterSupport.bat
   ```

   Note: The following is the default directory location on Windows computers.

2. The script then prompts the following questions:

   ```
   Do you want to collect configuration files? [y/n] y

   Do you want to collect application log files? [y/n] y

   Do you want to collect OpsCenter GUI <147> log files? [y/n] y

   Do you want to collect OpsCenter Server <148> log files? [y/n] y

   Do you want to collect db log files? [y/n] y

   Do you want to collect WebServer log files? [y/n] y

   Do you want to collect setEnv file? [y/n] y

   Do you want to collect database files? [y/n] y

   If this is an upgrade scenario, do you want to collect
   old database and log files? [y/n]  y

   If this is an install scenario, do you want to collect
   installation lzgs? [y/n]  y
   ```

   Answer **y** or **n** based on your preferences.

3 This script collects system information and OpsCenter configuration information based on your preferences. It then compresses all this information in a file that is called `Support.zip`. You can use OpsCenter and run the support script in the background.

Note: Adding log files and OpsCenter database files can increase the file size of the resulting `Support.zip` file.

---

4 The `Support.zip` file is stored in the following directory:

```
INSTALL_PATH\OpsCenter\server\temp\support
```

To gather troubleshooting data for OpsCenter Agent on Windows

1 Run the following command to execute the support script for OpsCenter Agent:

```
INSTALL_PATH\OpsCenter\Agent\bin\opsCenterAgentSupport.bat
```

Note: This is the default directory location on Windows computers.

---

2 The script stops the OpsCenter Agent service and then collects the OpsCenter Agent logs. It then collates this information in a `Support.zip` file.

3 This `zip` file is stored in the following directory:

```
INSTALL_PATH\OpsCenter\Agent\temp\support
```

4 After the `Support.zip` file is created, the script starts the OpsCenter Agent service.

To gather troubleshooting data for the OpsCenter Server on UNIX

1. Run the following commands to execute the support scripts for OpsCenter Server:

   ```
   <INSTALL_PATH>/SYMCOpsCenterServer/bin/opsCenterSupport.sh
   ```

2. The script then prompts the following questions:

   ```
   Do you want to collect configuration files? [y/n] y

   Do you want to collect application log files? [y/n] y

   Do you want to collect OpsCenter GUI <147> log files? [y/n] y

   Do you want to collect OpsCenter Server <148> log files? [y/n] y

   Do you want to collect db log files? [y/n] y

   Do you want to collect WebServer log files? [y/n] y

   Do you want to collect setEnv file? [y/n] y

   Do you want to collect database files? [y/n] y

   If this is an upgrade scenario, do you want to collect old
   database and log files? [y/n]  y

   If this is an install scenario, do you want to collect
   installation logs? [y/n]  y
   ```

   Answer **y** or **n** based on your preferences.

3. This script collects system information and OpsCenter configuration information based on your preferences. It then collates all this information in a `support.zip` file. You can use OpsCenter and run the support script in the background.

   Note: Adding log files and OpsCenter database files can increase the file size of the resulting `support.zip`.

4. The `support.zip` file is stored in the following directory:

   ```
   <INSTALL_PATH>/SYMCOpsCenterServer/temp/support
   ```

About OpsCenter log files

OpsCenter creates log files that you can use to troubleshoot installation, performance, and other issues. OpsCenter writes log files using Veritas Unified Logging (VxUL), legacy, and other log file formats.

See "About OpsCenter log files on Windows servers" on page 200.

See "About OpsCenter log files on UNIX servers" on page 202.

VxUL log files

The VxUL log file creates log file names and messages in a format that is standardized across all Veritas components. These messages use VxUL IDs (a product ID and an originator ID) that identify the component that wrote the log message.

OpsCenter components create most log messages in VxUL format.

Table 4-11 shows the originator IDs used by OpsCenter and key shared components.

Table 4-11 VxUL IDs used by OpsCenter components

VxUL originator ID	Originator name
103	Veritas Private Branch Exchange service (PBX)
132	NetBackup Service Layer (NBSL)
146	OpsCenter Agent
147	OpsCenter Web GUI
148	OpsCenter Server
423	Application log file
18	OpsCenter AT

In Windows, OpsCenter writes VxUL logs to the following directory:

```
INSTALL_PATH\OpsCenter\server\logs
```

In UNIX, OpsCenter writes VxUL logs to the following directory:

```
INSTALL_PATH/SYMCOpsCenterServer/logs
```

You can control how OpsCenter writes log files for OpsCenter Server, OpsCenter Agent, OpsCenter Web GUI, and also application log files.

The following OID values must be used for OpsCenter Server, OpsCenter Agent, OpsCenter Web GUI, and application logging.

OpsCenter Server	148
OpsCenter Agent	146
OpsCenter Web GUI	147
Application logging	423

Table 4-12 lists the commands by which you can control logging on Windows.

Table 4-12 Control logging on Windows

Control Logging	Command
To change the log directory destination (default value is *<INSTALL_PATH>*\OpsCenter\server\logs)	INSTALL_PATH\OpsCenter\server\bin\vxlogcfg.exe -a -p 58330 -o <OID> -s LogDirectory="<New log directory location>" **Note:** 58330 is the OpsCenter product ID.
To configure the verbosity level (default value is 1)	INSTALL_PATH\OpsCenter\server\bin\vxlogcfg.exe -a -p 58330 -o <OID> -s DebugLevel=1
To configure the diagnostic level (default value is 1)	INSTALL_PATH\OpsCenter\server\bin\vxlogcfg.exe -a -p 58330 -o <OID> -s DiagnosticLevel=1
To configure the number of log files that are created (default value is 100)	INSTALL_PATH\OpsCenter\server\bin\vxlogcfg.exe -a -p 58330 -o <OID> -s NumberOfLogFiles=100

Table 4-13 lists the commands by which you can control logging on UNIX.

Table 4-13 Control logging on UNIX

Control logging	Command
To change the log directory destination (default value is *<INSTALL_PATH>*/SYMCOpsCenterServer/logs)	<INSTALL_PATH>/SYMCOpsCenterServer/bin/vxlogcfg -a -p 58330 -o <OID> -s LogDirectory="<New log directory location>" **Note:** 58330 is the OpsCenter product ID.
To configure the debug level (default value is 1)	<INSTALL_PATH>/SYMCOpsCenterServer/bin/vxlogcfg -a -p 58330 -o <OID> -s DebugLevel=<New debug level>

Table 4-13 Control logging on UNIX *(continued)*

Control logging	Command
To configure the diagnostic level (default value is 1)	<INSTALL_PATH>/SYMCOpsCenterServer/bin/vxlogcfg -a -p 58330 -o <OID> -s DiagnosticLevel=<New diagnostic level>
To configure the number of log files that are created (default value is 100)	<INSTALL_PATH>/SYMCOpsCenterServer/bin/vxlogcfg -a -p 58330 -o <OID> -s NumberOfLogFiles=<New number>

OpsCenter application log files

Table 4-14 shows details about the application log files.

Table 4-14 OpsCenter application log files

Log file directory	Log file	Troubleshooting purpose
INSTALL_PATH\OpsCenter\server\logs or <INSTALL_PATH>/SYMCOpsCenterServer/logs	58330-423-*.log	This log file has minimal information that helps in understanding the flow of each use case. Unlike *148* logs, this log file does not have detailed log information. This log file can be mainly used by Support to diagnose the problem if a particular use case has failed. An example of a failed use case is when you run a report and any of the pre-defined steps like fetching report definition , building query, converting result etc. fail. Each failed use case will have error code and the message. Currently, data collection and reporting component has well defined error code and messages. This log file also has a detailed stack trace for failed use case. By default, the application logging is enabled. You can disable it by configuring the `log.conf` file. To disable application logging, set the debug level as 0 in `log.conf` file using the following command: Windows: <*INSTALL_PATH*>\OpsCenter\server\bin\vxlogcfg.exe -a -p 58330 -o <OID> -s DebugLevel=0 UNIX: /<*INSTALL_PATH*>/SYMCOpsCenterServer/bin/vxlogcfg -a -p 58330 -o <OID> -s DebugLevel=0 To enable application logging later, you can give any value greater than 0. For example, DebugLevel=1 enables application logging. To disable application logging later, modify the value of DebugLevel to 0.

About OpsCenter log files on Windows servers

OpsCenter creates the following log files using VxUL and legacy formats.

OpsCenter installation log files

Table 4-15 shows details about the installation log files for OpsCenter components. These log files can be used to troubleshoot installation issues of the respective OpsCenter component.

Table 4-15 OpsCenter installation log files

OpsCenter component	Log file
OpsCenter Server	%ALLUSERSPROFILE%\Symantec\OpsCenter\INSTALLLOGS\OpsCenterServerInstallLog.html
OpsCenter Agent	%ALLUSERSPROFILE%\Symantec\OpsCenter\INSTALLLOGS\OpsCenterAgentInstallLog.html
OpsCenter View Builder	%ALLUSERSPROFILE%\Symantec\OpsCenter\INSTALLLOGS\OpsCenterViewBuilderInstallLog.html

OpsCenter log files

Table 4-16 shows details about the OpsCenter log files.

Table 4-16 OpsCenter log files

Log file directory	Log file	Troubleshooting purpose
INSTALL_PATH\OpsCenter\server\logs\	ServerService_*timestamp*.log	These log files for system.err and system.out of OpsCenter server service.

Log files associated with Authentication Service

Table 4-17 lists the log files that are associated with Authentication Service.

Table 4-17 Log files for Authentication Service

Log file directory	Log file	Troubleshooting purpose
On Windows platforms: INSTALL_PATH\OpsCenter\server\authbroker\bin	vxatd.log	User authentication activity

OpsCenter database log files

Table 4-18 lists the log files that are associated with the OpsCenter database.

Table 4-18 Log files associated with the OpsCenter database

Log file directory	Log file	Troubleshooting purpose
INSTALL_PATH\OpsCenter\server\db\log\	server.log	OpsCenter Sybase database activity.

Table 4-18 Log files associated with the OpsCenter database *(continued)*

Log file directory	Log file	Troubleshooting purpose
INSTALL_PATH\OpsCenter\server\db\data\	vxpmdb.log	OpsCenter Sybase database transaction files. **Note:** Do not change this log file.

OpsCenter Web server log files

The log files that are associated with the OpsCenter Web server are present in the `INSTALL_PATH\OpsCenter\gui\webserver\logs` directory.

VxUL log files for OpsCenter and the components that OpsCenter uses

Table 4-19 lists the log files that are associated with VxUL and other components that OpsCenter uses.

Table 4-19 Log files associated with VxUL and other components

Log file directory	Log file	Troubleshooting purpose
INSTALL_PATH\VERITAS\VxPBX\bin\	50936-103-*.log	PBX activity
INSTALL_PATH\VERITAS\NetBackup\logs\	51216-132-*.log	NBSL activity
INSTALL_PATH\OpsCenter\Agent\logs	51216-146-*.log	OpsCenter Agent activity
INSTALL_PATH\OpsCenter\gui\logs\	51216-147-*.log	OpsCenter Web GUI activity
INSTALL_PATH\OpsCenter\server\logs	58330-148*.log	OpsCenter server activity
INSTALL_PATH\OpsCenter\server\logs	58330-423-*.log	OpsCenter application logging
INSTALL_PATH\OpsCenter\server\logs	58330-18-*.log	OpsCenter authentication activity

About OpsCenter log files on UNIX servers

OpsCenter creates the following log files by using VxUL and legacy formats.

Log files on UNIX servers associated with OpsCenter

Table 4-20 lists the log files for OpsCenter.

Table 4-20 Log files for OpsCenter

OpsCenter log file	Troubleshooting purpose
INSTALL_PATH/SYMCOpsCenterServer/logs/OpsCenterServer_out.log	stdout and stderr for the OpsCenterServer daemon
INSTALL_PATH/SYMCOpsCenterServer/logs/purge-status.log	Shows the details of purge operations
/var/VRTS/install/logs/ (directory)	Provides a trace for any installation issues

Log files on UNIX servers for Authentication Service

Table 4-21 lists the log files that are associated with Veritas Product Authentication Service.

Table 4-21 Log files for Authentication Service

Log file	Troubleshooting purpose
INSTALL_PATH/SYMCOpsCenterServer/authbroker/bin/vxatd.log	OpsCenter authentication activity

Log files on UNIX servers associated with OpsCenter database

Table 4-22 lists the log files that are associated with the OpsCenter database.

Table 4-22 Log files associated with OpsCenter database

OpsCenter log file	Troubleshooting purpose
INSTALL_PATH/ SYMCOpsCenterServer/db/log/ dbserver.log	OpsCenter Sybase database activity.
INSTALL_PATH/SYMCOpsCenterServer/ db/data/vxpmdb.log	OpsCenter Sybase database transaction files. **Note:** Do not change this log file.

Log files on UNIX servers associated with OpsCenter Web server

Table 4-23 lists the log files that are associated with the OpsCenter Web server.

Table 4-23 Log files associated with the OpsCenter Web server

OpsCenter log directory	Troubleshooting purpose
<INSTALL_PATH>/SYMCOpsCenterGUI/webserver/logs	OpsCenter Web GUI application activity (stdout).

Log files on UNIX associated with VxUL and other components

Table 4-24 lists the log files that are associated with VxUL and other components.

Table 4-24 Log files associated with VxUL and other components

OpsCenter log file	Troubleshooting purpose
INSTALL_PATH/VRTSpbx/log/50936-103-*.log	PBX activity
INSTALL_PATH/openv/logs/51216-132-*.log	NBSL activity
INSTALL_PATH/SYMCOpsCenterGUI/logs/51216-147-*.log	OpsCenter Web GUI activity
INSTALL_PATH/SYMCOpsCenterServer/logs/558330-148*.log	OpsCenter server activity
INSTALL_PATH/SYMCOpsCenterServer/logs/58330-423-*.log	OpsCenter application logging
INSTALL_PATH/SYMCOpsCenterServer/logs/58330-18-*.log	OpsCenter authentication activity

Chapter 5

Understanding OpsCenter settings

This chapter includes the following topics:

- OpsCenter settings
- Setting user preferences
- About managing licenses
- Configuring the data purge period on the OpsCenter Server
- About storing the SMTP Server configurations in OpsCenter
- Configuring SMTP server settings for OpsCenter
- Adding host aliases in OpsCenter
- Merging objects (hosts) in OpsCenter
- Modifying tape library information in OpsCenter
- Copying a user profile in OpsCenter
- Setting report export location in OpsCenter
- About managing Object Types in OpsCenter
- About managing OpsCenter users
- About managing recipients in OpsCenter
- About managing cost analysis and chargeback for OpsCenter Analytics

OpsCenter settings

This topic describes the various OpsCenter settings. An OpsCenter Admin can configure these settings using the OpsCenter console. The normal users can view or access the information that is relevant only to their profiles, which the OpsCenter Administrator has set.

You can configure the following settings in OpsCenter.

Table 5-1 Settings in OpsCenter

Setting	Lets you...	Reference topic
User Preferences	Add user-specific details and create user profiles.	See "Setting user preferences" on page 207.
Configuration > NetBackup	Add NetBackup master servers and their properties to collect data from it.	See "About configuring data collection for NetBackup" on page 271.
Configuration > Agent	Create Agent and Data Collectors to collect data from non-NetBackup products.	See "About managing OpsCenter Agents" on page 264.
Configuration > License	Manage permanent or demo license keys.	See " Adding OpsCenter license keys" on page 213.
Configuration > Data Purge	Specify when you want to purge the data that is collected from various products.	See "Configuring the data purge period on the OpsCenter Server" on page 214.
Configuration > SMTP Server	Configure the SMTP server details that you need while sending reports or alerts through emails.	See "Configuring SMTP server settings for OpsCenter" on page 216.
Configuration > Host Alias	Add aliases for hosts.	See "Adding host aliases in OpsCenter" on page 218.
Configuration > Object Merger	Configure OpsCenter to merge the objects that represent the same backup client, but registered as separate objects	See "Merging objects (hosts) in OpsCenter" on page 219.
Configuration > Tape Library	Modify tape library information	See "Merging objects (hosts) in OpsCenter" on page 219.
Configuration > Copy User Profile	Configure OpsCenter to copy a user's profile to another user.	See "Copying a user profile in OpsCenter" on page 221.

Table 5-1 Settings in OpsCenter *(continued)*

Setting	Lets you...	Reference topic
Configuration > Report Export Location	Specify the location where the exported reports are stored.	See "Setting report export location in OpsCenter" on page 222.
Configuration > Object Type	Add new object types and attributes.	See "About managing Object Types in OpsCenter" on page 223.
Views	Create and manage OpsCenter views.	See "About managing OpsCenter views" on page 306.
Users	Manage users and user groups.	See "About managing OpsCenter users " on page 226.
Recipients	Manage Email and SNMP recipients.	See "About managing recipients in OpsCenter" on page 242.
Chargeback > Currency Settings	Manage the currency settings that appear in cost reports. You can select a currency from the global currency list and set it as default.	See "Setting the default currency for OpsCenter cost reports" on page 249.
Chargeback > Cost Variables	Create cost variables.	See "Settings > Chargeback > Cost Variable options" on page 251.
Chargeback > Cost Formulae	Create cost formulae.	See "Settings > Chargeback > Cost Formulae options" on page 255.
Chargeback > Cost Estimation	Manage cost estimation.	See "Estimating chargeback costs using the OpsCenter Formula Modeling Tool" on page 256.

Setting user preferences

In OpsCenter, you can set your preferences, such as default locale or time zone and personal details, such as email ID or name. You can also change your password using the **User Preferences** tab, if your user account belongs to the OpsCenterUsers domain.

To set user preferences

1. In the OpsCenter console, click **Settings > User Preferences**. The user preferences options are organized in the **General** and **My Profile** tabs.
2. Click the **General** tab to set **Default Locale**, **Data Display Time Zone**, **Start 24 Hour Day at**, **Disable Auto Refresh**, **Auto Refresh Interval (Minutes)**, and **Allow Multiple Selection in View Pane**.
3. Click **Save**.
4. Click the **My Profile** tab to see or modify **User Name**, **Password**, **User Role**, and **Domain Name**

Settings > User Preferences options

Use the **General** tab options as follows:

Table 5-2 General options

Option	Description
Default Locale	Select a locale of your choice from the drop-down list. For example, if you select English as a default locale, all OpsCenter GUI screens use English as a default language.
Data Display Time Zone	Select a preferred time zone - either OpsCenter Server time zone or any other time zone from the Other drop-down list. OpsCenter displays time on the GUI screens according to the selected time zone.
Start 24 Hour Day at	Enter the time that is used as the start time of a day in reports. Report data is grouped depending on this start time.
Disable Auto Refresh	Select this check box if you do not want to automatically refresh the OpsCenter GUI. By default, the auto-refresh option is enabled.
Auto Refresh Interval (Minutes)	Enter auto-refresh interval in minutes. For example, if you want to refresh the OpsCenter GUI to show updated data after every 5 minutes, enter five in the **Auto Refresh Interval** text box.
View Preferences	

Table 5-2 General options *(continued)*

Option	Description
Default View	This drop-down list shows the views for which you have permission. Select one of these views as the default view for the Monitor and Manage tabs in the OpsCenter console. By default, data for the selected view is shown in the Monitor and Manage tabs of the OpsCenter console.
Report Template Default View	This drop-down list shows the views for which you have permission. Select one of these views as the default view for report templates. By default, data for the selected view is shown when you run a report based on any of the report templates.

Table 5-2 General options *(continued)*

Option	Description
Allow Multiple Selection in View Pane	Select this check box if you want to select multiple nodes or view objects in the View Pane. When you check this option, you can see a check box next to each master server or node in the View Pane. To view data for multiple master servers and nodes, you check the corresponding check boxes and then click **Apply Selection**. By default, the multiple-selection option is enabled. When you uncheck the multiple-selection option, you can only select a single node or view object from the View Pane at a given time. Each node or a view object is a link. You can click a node or a view object to view data for the respective node or view object. For example, you can click a master server in the View Pane to view data for the specific master server. See "About making multiple or single-click selections in the View pane" on page 53. When you uncheck the multiple-selection option, a **Group Component Summary** table is displayed when you click **Monitor > Jobs** and select **Summary View** from the drop-down list. The **Group Component Summary** table at the bottom of the view displays job summary information. It shows the immediate NetBackup constituents of the selected view or node (group) in the **View** pane. For example if you select the ALL MASTER SERVERS view, the Group Component Summary table displays job summary for each master server. More details about the Group Component Summary table are available. See "About the Group Component Summary table" on page 341.
Report Export Layouts	

Table 5-2 General options *(continued)*

Option	Description
PDF Tabular Report Export Layout	You can export a tabular report in various PDF formats. These preferences apply to standard reports only. Select one of the following PDF formats in which you want to export the tabular reports: ■ Portrait Displays a maximum of seven columns of data per page. ■ Landscape Displays a maximum of ten columns of data per page. ■ Portrait for less than eight headers Displays data in the Portrait format for data up to seven headers and Landscape format for more than seven headers. ■ Expand to fit Displays the entire data across a single page.

Read and use the **My Profile** tab options as follows:

Table 5-3 My Profile options

Option	Description
User Name	Displays the user name.
Password	The OpsCenter security admin sets a default password for each user when it creates the profiles. The users that belong to the OpsCenterUsers domain can change their passwords after logging on . To change password, click the **Change Password** link. See "Changing your OpsCenter password" on page 211. The users from other domains cannot change their passwords using this option.
User Role	The role of this user.
Domain Name	The name of the domain to which this user belongs.

Changing your OpsCenter password

Change the administrator-assigned password the first time you logon to OpsCenter console. Change the password at regular intervals thereafter.

For security reasons, you should change your password after it was reset by the OpsCenter Security Administrator. OpsCenter displays the **Change Password** page when you try to log in after your password was reset.

To change your OpsCenter password

1. In the OpsCenter console, click **Settings > My Profile**.
2. In the **My Profile** dialog box, click **Change Password**.
3. In the **Change Password** dialog box, do the following:
   - Type the old password in the **Old Password** field.
   - Type the new password in the **New Password** field.

     You must set your new password according to the password rules or guidelines: Password must be at least 8 characters long and should contain at least one upper case letter, one lower case letter, and one numeric digit. The new password must be different than the current password.

     The password rules are also provided on the Change Password page.

   - Type your new password again in the **Confirm New Password** text box.
4. Click **Save**.

About managing licenses

To use the advanced features that are not available in OpsCenter, you need to use a license key and enable Veritas NetBackup OpsCenter Analytics.

See "About OpsCenter" on page 19.

See " Adding OpsCenter license keys" on page 213.

See " Viewing OpsCenter license keys" on page 213.

See " Deleting OpsCenter license keys" on page 214.

Settings > Configuration > License options

The **License** tab shows the current state of the following options:

Table 5-4 License options

Option	Description
Key	License keys associated with OpsCenter.
Type	Type of license key like PERMANENT, EVALUATION etc.
Expiry Date	Expiry date that is associated with the license key.
Licensed Features	Licensed features that are associated with the key.
Enabled	This column tells whether the licensed feature is enabled or not.
Current Usage	Actual current usage of the licensed feature.
License Limit	Total licensed value that is associated for the specific licensed feature.

Adding OpsCenter license keys

An OpsCenter administrator can install OpsCenter license keys to activate additional product features or delete the license keys that are no longer needed.

You can add one or more OpsCenter license keys.

To add OpsCenter license keys

1. Log on to the OpsCenter console as admin.
2. In the OpsCenter console, click **Settings > Configuration**.
3. Click the **License** tab.
4. Click **Add**.
5. On the **Add License Key** pop-up screen, enter a license key and click **OK**.

Viewing OpsCenter license keys

You can view the license keys that are installed on the OpsCenter server host.

To view OpsCenter license keys

1. Log on to the OpsCenter console as admin.
2. In the OpsCenter console, click **Settings > Configuration**.
3. Click the **License** tab.

Deleting OpsCenter license keys

You can remove one or more OpsCenter Analytics license keys from the OpsCenter Server, on which you are connected as an administrator.

To delete OpsCenter Analytics license keys

1. Log on to the OpsCenter console as admin.
2. In the OpsCenter console, click **Settings > Configuration**.
3. Click the **License** tab.
4. Select the check box in front of the license key that you want to delete.
5. Click **Delete**.

Configuring the data purge period on the OpsCenter Server

You can configure the OpsCenter Server retention periods for the data types that are logged, such as Job, Policy, and Skipped Files.

Note: The details of the purged data are stored in the `purge-status.log` file, which is located in the OpsCenter server logs directory.

To configure the data purge period on the OpsCenter Server

1. Log on to the OpsCenter console as admin.
2. In the OpsCenter click **Settings > Configuration**.
3. Click the **Data Purge** tab.

   By default, data purge is enabled.
4. Edit the default data purge settings as necessary.

   See "Settings > Configuration > Data Purge options" on page 214.
5. In the **Time of Purge** text box, enter the time of day (in 24-hour clock format) when you want to purge the data.
6. Click **Save**.

Settings > Configuration > Data Purge options

By default, data purge is enabled.

Data purge settings help you manage the retention of the data that you have collected from NetBackup. For each data type, you can set the data retention in days. After the specified number of days, the corresponding data is purged from the OpsCenter database. Once the data is purged, you cannot retrieve it. For each data type, you can either use the default setting or change it as required.

Edit the default data purge options as follows:

Table 5-5 Data Purge options

Option	Description
Enable Data Purge	To change the default data purge settings, select the Enable Data Purge option.
Enable Expired Image Purge	Select this option to purge the images that have expired in the NetBackup catalog.
Backup Job	Set the number of days after which you want to purge the backup jobs (default is 220 days). The number of days set for backup logs should be less than or equal to the number of days set for backup jobs. In other words, logs can be purged earlier than their respective jobs, or they can be purged at the same time.
Backup Log	Set the number of days after which you want to purge the Backup logs (default is 3 days).
Tape Drive History	Set the number of days to retain Tape Drive History logs (default is 31 days).
Media History	Set the number of days to retain Media History logs (default is 31 days).
Alert	Enter the number of days for which you want to retain the Alert data (default is 31 days). Alert data older than this number is purged from the OpsCenter database.
SLP Images	Number of days for which the SLP data should be retained (default is 90 days).
Audit Trail	Number of days for which you want to retain the Audit Trail records. **Note:** By default, data purge for Audit Trail is set to 420 days.

Table 5-5 Data Purge options *(continued)*

Option	Description
Time of Purge	Enter the time of day (in 24-hour clock format) when you want to purge the data.

About storing the SMTP Server configurations in OpsCenter

The SMTP Server settings are stored in the OpsCenter database in the **nm_SmtpSettings** table.

Note the following points:

- When you upgrade OpsCenter, all SMTP-related configuration details (if they are already present in the `nm.conf` file from the previous version) are saved in the OpsCenter database in the nm_SmtpSettings table. The SMTP-related configuration details are subsequently removed from the `nm.conf` file.
- You should specify the SMTP-related configuration details through the OpsCenter GUI and not in the `nm.conf` file. If you specify any SMTP details manually in the `nm.conf` file and they are already present in the nm_SmtpSettings database table, the configuration details from the `nm.conf` file will be ignored. On the next OpsCenter Server service start up, these SMTP details are removed from the `nm.conf` file. However, if the nm_SmtpSettings database table is empty, the SMTP details from the `nm.conf` file are inserted in the table on the next OpsCenter Server service start up. The SMTP-related configuration details are subsequently removed from the `nm.conf` file.

Note: SNMP trap configuration details continue to remain in the `nm.conf` file as before.

Configuring SMTP server settings for OpsCenter

This section provides the procedure to configure the SMTP server that you can use for sending emails and alerts.

See “About storing the SMTP Server configurations in OpsCenter” on page 216.

To configure SMTP server settings for OpsCenter

1. Log on to the OpsCenter console as admin.
2. In the OpsCenter console, click **Settings > Configuration**.
3. Click **SMTP Server**.

   OpsCenter uses these global server settings to send email notifications using the SMTP server that you specify.
4. Enter the required information.

   See "Settings > Configuration > SMTP server options" on page 217.
5. Click **Save**.

Settings > Configuration > SMTP server options

A description of the **Settings > Configuration > SMTP Server** options follows in the table.

Table 5-6 SMTP server options

Option	Description
SMTP Server Name	Enter the SMTP (Simple Mail Transfer Protocol) Server host name. Notifications of the alerts that are generated in OpsCenter are sent using this SMTP server.
SMTP Server port	Enter the SMTP (Simple Mail Transfer Protocol) Server port number.
Sender Display Name	Enter the name that is associated with the Email ID. For example, Backup Reporting Department.
Sender Email Address	Specify the Email ID to receive any replies to the alerts or the reports that were sent by OpsCenter.
Server User Name	Some SMTP servers may require user name and password credentials to send email. Enter the user name.
Server User Password	Some SMTP servers may require user name and password credentials to send email. Enter the password for this user account.

See "About storing the SMTP Server configurations in OpsCenter" on page 216.

Adding host aliases in OpsCenter

This section provides the procedures to add aliases for hosts.

The host's primary alias is displayed in all console functions and reports. Other host aliases are used when you search in OpsCenter or gather and collate data.

Warning: Your alias names must be compatible with your hosts' DNS names or with the names by which they are known to applications such as NetBackup and Backup Exec. For example, if you use an alias that is unknown to OpsCenter, the explorer stops collecting information from the OpsCenter host. Instead the explorer attempts to collect data from a host with the alias name.

To add a host alias

1. In the OpsCenter console, click **Settings > Configuration > Host Alias**.
2. From the drop-down list select a host name or type a host name and click **Show Alias**.

   All the existing aliases are displayed.
3. Click **Add Alias**.
4. Enter the alias name for the host that you have selected from the drop-down list.
5. Click **Save**.

Settings > Configuration > Host Alias options

A description of the **Settings > Configuration > Host Alias** options follows in the table.

Table 5-7 Host Alias options

Option	Description
Select Host	From the drop-down list select a host name or type a host name.
Show Alias	Click **Show Alias** to display the aliases associated with the selected host.
Alias 1, 2, 3, etc.	A selected host can have one or more alias associated with it. You can clear and save the alias for removing the particular alias.

Table 5-7 Host Alias options *(continued)*

Option	Description
Add Alias	Click **Add Alias** to add aliases for the selected host.

Merging objects (hosts) in OpsCenter

OpsCenter provides a facility to merge objects (hosts) that represent the same media server, backup client, but registered as separate objects (hosts). Using the OpsCenter UI, you can merge only one object into other, at a time.

In OpsCenter, you can merge objects (hosts) representing the same backup client.

Caution: Merging objects is not reversible.

Veritas recommends that you do not merge a host that is a master server, a media server and a client (that is, a source that is of entity type 14) with any other host. If you merge a host of entity type 14 with another host, it would result in deleting the master server and all of its related data from OpsCenter. This is applicable only when you try to merge objects by using the view_exportimport utility or OpsCenter ViewBuilder.

To merge two objects

1. Log on to the OpsCenter console with administrator privileges.
2. In the OpsCenter console, click **Settings > Configuration > Object merger**.
3. Select the **Host Type**: Media Server, or Client.

   See "Settings > Configuration > Object Merger options" on page 220.
4. Select the **Source Host** from the drop-down list. An auto-suggest feature is available.
5. Select the **Target Host** from the drop-down list. An auto-suggest feature is available.
6. Click **Validate Object Merging**.
7. You can view the snapshot of the selection that you have made earlier. To modify the **Source Host** or **Target Host** click **Back**. To begin the merge, click **Start Merge**.

   Repeat these steps if you want to merge more objects.

Settings > Configuration > Object Merger options

A description of the **Settings > Configuration > Object Merger** options follows in the table.

Table 5-8 Object Merger options

Option	Description
Host Type	Select the **Media Server**, or **Client** radio button to indicate **Host Type**.
Source Host	Select a source host from the drop-down list. An auto-suggest feature is available. Source host is the host that you want to merge.
Target Host	Select a target host from the drop-down list. An auto-suggest feature is available. Target host is the host to which you want to merge the source host. Target host is the resultant host after the object merger.
Validate Object Merging	Click **Validate Object Merging** to view a snapshot of the selection that you have made.

Modifying tape library information in OpsCenter

OpsCenter provides a facility to monitor all the tapes that the data collector uses. Using the OpsCenter user interface, you can edit the serial number, type, manufacturer, alias, slot count of the tape drives the data collector uses.

OpsCenter receives information from NBSL about specific SCSI robots. Veritas recommends that you do not edit **Slot Count** information for the following SCSI robots:

- TLD
- TL4
- TL8

To modify tape library information in OpsCenter

1. Log on to the OpsCenter console with administrator privileges.
2. In the OpsCenter console, click **Settings > Configuration**.
3. Click **Tape Library**.

4 You can view the list of the tape libraries in OpsCenter. Select the check box next to tape library, for which you want to edit the information.

5 Edit the information.

See "Settings > Configuration > Tape Library options" on page 221.

6 Click **Save**.

Settings > Configuration > Tape Library options

The following table provides a description of the **Settings > Configuration > Tape Library** options.

Table 5-9 Tape Library options

Option	Description
ID	Displays the unique ID that is associated with the tape library.
Host Name	Displays the media server to which the tape library is attached.
Type	Select the type of tape library from the drop-down list.
Serial Number	Enter the serial number of the tape library.
Manufacturer	Enter the manufacturer of the tape library.
Alias	Enter the alias for the tape library.
Slot Count	Enter the slot count for the tape library.

Copying a user profile in OpsCenter

Most user-definable content, such as reports, cost variables, and cost formulas, is accessible only by the user who has created it. Using the copy user profile functionality, you can copy information from one user account to another.

To copy a user profile

1 Log on to the OpsCenter console with administrator privileges.

2 In the OpsCenter console, click **Settings > Configuration > Copy User Profile**.

3 Select the source user account from the **From User** drop-down list.

See "Settings > Configuration > Copy User Profile options" on page 222.

4 Select the target user account from the **To User** drop-down list.

5 In the **Copy Items** options, select the items you want to copy, for example reports or cost rates or formulae.

6 Click **Next**.

7 Select reports or cost rates or formulae to be copied to this user profile.

If you copy a cost formula, the associated cost variables are implicitly copied.

If you copy a cost report, the associated cost formula and variables are implicitly copied.

8 Click **Copy**.

Settings > Configuration > Copy User Profile options

A description of the **Settings > Configuration > Copy User Profile** options follows in the table.

Table 5-10 Copy User Profile options

Option	Description
From User	Select the source user account from the **From User** drop-down list.
To User	Select the target user account from the **To User** drop-down list.
Copy Items	Select the items you want to copy: **Reports** or **Cost Rates and Formulae**.
Reports	Select reports to be copied to this user profile.
Cost Rates and Formulae	Select cost rates and formulae to be copied to this user profile.

Setting report export location in OpsCenter

In OpsCenter you can configure exporting of reports to a predefined location. Data from exported reports is stored in a default directory, if you have not defined any location.

To set report export location

1 Log on to the OpsCenter console with administrator privileges.

2 In the OpsCenter console, click **Settings > Configuration > Report Export Location**.

3 In the **Report Export Location** box type the directory where you want to save the reports.

4 Click **Save**.

Settings > Configuration > Report Export Location options

A description of the **Settings > Configuration > Report Export Location** options follows in the table.

Table 5-11 Report Export Location options

Option	Description
Report Export Location	Type the directory path where you want to save the reports.

About managing Object Types in OpsCenter

See the following sections for the procedures related to managing object types and their attributes in OpsCenter.

See "Adding object types in OpsCenter" on page 224.

See "Modifying object types in OpsCenter" on page 225.

See "Deleting object types in OpsCenter" on page 224.

See "Adding attributes to object types in OpsCenter" on page 225.

See "Deleting attributes from object types in OpsCenter" on page 225.

Settings > Configuration > Object Type options

A description of the **Settings > Configuration > Object Type** options follows in the table.

Table 5-12 Object Type options

Option	Description
Object Types	Click the list box to select an object type that you want to configure.

Table 5-12 Object Type options *(continued)*

Option	Description
Add/Edit/Delete	Located to the right of the **Object Types** drop-down list. Click to add, edit, or delete object types. **Note:** You can edit or delete only user-defined objects.
Add/Delete	Located above the **Attributes** check box. Click to add or delete attributes.
Attributes	Attributes associated with the selected object type.

Adding object types in OpsCenter

In OpsCenter you can add or edit attributes of predefined object types. You can also add new object types and attributes for those new object types.

To add an object type

1. Log on to the OpsCenter console with administrator privileges.
2. In the OpsCenter console, click **Settings > Configuration > Object Types**.
3. Click **Add**.
4. Enter the name in the **Add Object Type** dialog box..
5. Click **OK**.

Deleting object types in OpsCenter

You can only delete an object type that you have created. You cannot delete the predefined objects in the drop-down list.

To delete object types

1. Log on to the OpsCenter console with administrator privileges.
2. In the OpsCenter console, click **Settings > Configuration > Object Types**.
3. Select the object type from the drop-down list. You can delete the object types that you have created. You cannot delete predefined object types.
4. Click **Delete**.

See “Adding object types in OpsCenter” on page 224.

Modifying object types in OpsCenter

You can only modify the name of an object type that you have created. You cannot modify the name of the predefined objects in the drop-down list.

To modify an object type name

1. Log on to the OpsCenter console with administrator privileges.
2. In the OpsCenter console, click **Settings > Configuration > Object Type**.
3. Select the object type that you want to modify from the drop-down list.

   You can rename the object types that you have created. You cannot rename the predefined object types.
4. Click **Edit**.
5. On the **Edit Object Type** pop-up screen, modify the object type name and click **OK**.

Adding attributes to object types in OpsCenter

You can add attributes to all object types.

To add attributes to an object type

1. Log on to the OpsCenter console with administrator privileges.
2. In the OpsCenter console, click **Settings > Configuration > Object Types**.
3. Select the object type from the drop-down list and in **Attributes** section, click **Add**.
4. Enter the name of the attribute and click **OK**.

See "Adding object types in OpsCenter" on page 224.

Deleting attributes from object types in OpsCenter

You can delete the attributes that are added to an object type.

To delete attributes from an object type

1. Log on to the OpsCenter console with administrator privileges.
2. In the OpsCenter console, click **Settings > Configuration > Object Types**.
3. Select the object type from the drop-down list. In the **Attributes** section, select the check box in front of the attribute you want to delete.
4. Click **Delete**.

About managing OpsCenter users

After you install OpsCenter, you need to create user accounts. The OpsCenter Authentication Service (AT) validates credentials of OpsCenter users based on Windows, NIS, or private domains.

See "User access rights and functions in OpsCenter user interface" on page 231.

See " Adding new users to OpsCenter" on page 236.

See "Resetting an OpsCenter user password" on page 238.

See " Viewing OpsCenter user account information" on page 235.

See " Adding new users to OpsCenter" on page 236.

See " Editing OpsCenter user information" on page 238.

See " Deleting OpsCenter users" on page 240.

About managing user password

This section provides the information on how you can manage your passwords using the OpsCenter GUI.

You can change your default password at the time of first login using the Change Password UI. If you want to change your password while you are logged in, go to **Settings > User preferences > My Profile > Change Password**.

See "Changing your OpsCenter password" on page 211.

Note: If you are an OpsCenter(vx) domain user and have forgotten the password, contact the OpsCenter Security Administrator to reset your password. OpsCenter Security Administrator can reset passwords only for OpsCenter(vx) domain users. NT or LDAP domain users should contact the System Administrator to reset their passwords.

If you are an OpsCenter Security Administrator and you need to reset the password of an OpsCenter(vx) domain user, go to **Settings > Users > Edit User > Reset Password**.

See "Resetting an OpsCenter user password" on page 238.

If you are a Security Administrator and you have forgotten the OpsCenter user account password, you can manually reset your password.

See "Resetting password of the OpsCenter Security Admin" on page 239.

About adding AD / LDAP user groups in OpsCenter

You can add AD / LDAP domain user groups in OpsCenter and assign user roles to them. All users in the group inherit the same user role and they can access OpsCenter using their AD / LDAP credentials. With this enhancement, you do not need to add and authenticate each user of the group in OpsCenter. Any changes to the user group like addition or removal of a user is automatically reflected in OpsCenter.

Active Directory (AD) is a directory service created by Microsoft for Windows domain networks. It is included in most Windows Server operating systems.

Active Directory provides a central location for network administration and security. Server computers that run Active Directory are called domain controllers. An AD domain controller authenticates and authorizes all users and computers in a Windows domain type network - assigning and enforcing security policies for all computers and installing or updating software. For example, when a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a system administrator or a normal user.

Active Directory uses Lightweight Directory Access Protocol (LDAP), which is an application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.

The AD / LDAP user groups that you have added in OpsCenter are listed on the OpsCenter GUI on the **Settings > Users > Users** tab.

Some important notes and considerations about adding AD / LDAP user groups in OpsCenter:

- In OpsCenter, an AD / LDAP user group and a single user can be differentiated with the help of the User column in the Users table.
- A single user is indicated as ‘Individual’ and an AD / LDAP user group is indicated as ‘Group’.
- If an individual OpsCenter user is a part of an AD / LDAP user group, the user inherits the role that was individually assigned, irrespective of the role of the user group. For example: UserA is added as an OpsCenter individual user. UserA is also part of an AD / LDAP user group called GroupA. The role of UserA is ‘Administrator’ and the role of GroupA is ‘Reporter’. In this scenario, the user role of UserA is always ‘Administrator’.
- If a user is part of multiple AD / LDAP user groups, the user inherits the highest role in the hierarchy out of all user group roles. For example: UserA is part of three AD / LDAP user groups: GroupA, GroupB, and GroupC. User role of GroupA is ‘Administrator’, of GroupB is ‘Security Administrator’, and of GroupC is ‘Reporter’. In this scenario, UserA inherits the role ‘Security Administrator’.

- Subgroups of a user group that you have added to OpsCenter should not contain special characters in their names. Subgroups cannot contain special characters like: ',' , '\', '&', '#', '%', or '*'

  For example: You have created two groups called 'ValidGroup' and 'Invalid%Group'. 'Invalid%Group' is added to 'ValidGroup'. 'Invalid%Group' is now a subgroup of 'ValidGroup'. 'ValidGroup' is added to OpsCenter. As 'Invalid%Group' contains special characters in its name, users of this group cannot log on to OpsCenter.

  However, if 'Invalid%Group' is directly added to OpsCenter, all of its users can log on to OpsCenter.

  User groups with names containing special characters cannot be used as subgroups in OpsCenter.

See " Adding new users to OpsCenter" on page 236.

Adding AD / LDAP domain in OpsCenter

You can add existing AD / LDAP domains in OpsCenter and authenticate the domain group users to access OpsCenter.

To add an AD / LDAP domain

1. Logon to OpsCenter Server.
2. On the command prompt, navigate to the following directory: `Installation Directory\OpsCenter\server\authbroker\bin`.

3 Run the following command to create an AD or LDAP domain on the OpsCenter Server:

AD

```
vssat addldapdomain -d domain_name -s ldap://AD server name -u user based DN --g group based DN -t msad -m admin user DN -w admin user password -b BOB | FLAT
```

For example:

```
vssat addldapdomain -d OpsADDomain -s ldap://dc.virtual.lab -u DC=virtual,DC=lab -g DC=virtual,DC=lab -t msad -m CN=Administrator,CN=Users,DC=virtual,DC=lab -w password -b BOB
```

LDAP

```
vssat addldapdomain -d LDAPDomainName -s LADPServerName -u ou=People,dc=domainName1,dc=domainname2 -g ou=Group,dc=domainName1,dc=domainName2 -t LDAPSchema
```

For example:

```
vssat addldapdomain -d OpsLDAPDomain -s ldap://opscenter-win.veritas.com -u ou=People,dc=OpsLDAPDomain,dc=veritas,dc=com -g ou=Group,dc=OpsLDAPDomain,dc=veritas,dc=com -t rfc2307
```

4 Run the following command to add the OpsCenter Server as authentication broker: `vssat addbrokerdomain -b OpsCenterServerName:1556 -d ldap:LDAPDomain`

Settings > Users > Users options

The following table provides the descriptions of the **Settings > Users > Users** options.

Table 5-13 Users options

Option	Description
Add/Edit/Delete options	Click **Add/Edit/Delete** to add, edit, or delete users.
Name	Login name of the user.
User Role	Role that is associated with the user. See "User access rights and functions in OpsCenter user interface" on page 231.

Table 5-13 Users options *(continued)*

Option	Description
User	Type of the user: Individual User or Group User. You can add AD / LDAP domain groups to OpsCenter to authorize all users from that group to access OpsCenter. All users from the authorized domain group can logon to OpsCenter with their AD / LDAP credentials. Any changes like addition or removal of a user from an authorized AD / LDAP domain group are automatically reflected in OpsCenter.
User Status	Status of the user: Enabled or Disabled If you want to temporarily revoke a user's permission to access OpsCenter, set the user status to 'Disabled'. User with the 'Disabled' user status cannot logon to OpsCenter. However, the user-specific data such as reports or schedules is retained.
Domain Type	Domain type (like vx) that the user is a member of and also specified while adding the user.
Domain Name	Domain name (like OpsCenterUsers) that the user is a member of and also specified while adding the user .

The Security Administrator can view the list of views that each user can access under the Assigned Views tab at the bottom. The Assigned Views tab is only visible if you log on as a Security Administrator (like `admin`).

The following columns are shown in the table:

Name This column lists the views to which a user is permitted.

Type This column lists the type of the specific view like Client, Master Server, or Policy.

Permission Type The Security Administrator can assign a view directly to a user using the OpsCenter console. A Security Administrator or Administrator can also assign a view directly to a user group using the OpsCenter View Builder.

This column lists if the view was assigned directly to the selected user or via a user group.

Created On This column lists the date and time when the view was created.

Owner This column lists the name of the user who owns the specific view.

User access rights and functions in OpsCenter user interface

The following tables provide information on OpsCenter users and the functions that they can perform in the OpsCenter user interface.

You can add AD / LDAP domain groups to OpsCenter to authorize all users from that group to access OpsCenter.

Table 5-14 provides details of the OpsCenter user interface functions that authorized users or user groups can perform.

Table 5-14 OpsCenter user interface functions

OpsCenter functions	Tasks	Go to this topic
User Management	The User Management function includes the following tasks: ■ Create, update, delete users. ■ Create, update, delete user groups. ■ Add, remove users from user groups. ■ Assign, remove roles to users and user groups.	See "About managing OpsCenter users " on page 226.
OpsCenter Management	The OpsCenter Management function includes the following tasks: ■ Add, Update, Delete Master Server ■ Add, Update, Delete OpsCenter Agents ■ Set default currency, SNMP, SMTP server	See "Adding a master server or appliance in OpsCenter" on page 285. See "Editing a master server or an appliance master server in OpsCenter" on page 292. See "Deleting a master server or an appliance master server in OpsCenter" on page 292. See "About managing OpsCenter Agents" on page 264. See "About managing cost analysis and chargeback for OpsCenter Analytics" on page 249. See "About managing recipients in OpsCenter" on page 242. See "Configuring SMTP server settings for OpsCenter" on page 216.

Table 5-14 OpsCenter user interface functions *(continued)*

OpsCenter functions	Tasks	Go to this topic
NetBackup Operations	The NetBackup Operations function includes the following tasks: Change states of the NetBackup entities as follows: ■ Policy (Activate/De-active) ■ Job (Stop/Start/Suspend/Resume) ■ Media (Assign, Freeze, unfreeze) ■ Drives (Up/Down) ■ Others	See "Activating or deactivating a job policy" on page 355. See "Controlling NetBackup jobs" on page 335. See "Controlling media" on page 364. See "Controlling drives" on page 373.
Backup and Recovery	The Backup and the Recovery function includes the following tasks: ■ Execute manual backups. ■ Search and restore files, folders, application (Oracle, SQL Server, and Exchange Server)	See "Starting a manual backup" on page 356.
Views Management	The Views Management function includes the following tasks: ■ Create, update, or delete OpsCenter views and nodes. The ALL MASTER SERVERS view cannot be modified. ■ Assign Read permission to users on OpsCenter views and nodes.	See "About managing OpsCenter views" on page 306. See "User access rights and functions in OpsCenter user interface" on page 231.
All Views Read	The All Views Read function includes the following tasks: ■ View OpsCenter views and nodes.	See "About managing OpsCenter views" on page 306.

Table 5-14 OpsCenter user interface functions *(continued)*

OpsCenter functions	Tasks	Go to this topic
Report Execution	This function includes the following tasks: ■ Execute report templates and public custom reports. ■ Schedule canned and public custom reports. ■ Create, update Dashboard.	See "Creating an OpsCenter report using a Report Template" on page 550. See "Creating a custom report in OpsCenter" on page 559. See "About managing report schedules in OpsCenter" on page 585. See "About managing My Dashboard" on page 578.
Custom Reports **Note:** This feature is available with the licensed (OpsCenter Analytics) version of the product.	This function includes the following tasks: ■ Create, update, delete custom reports. ■ Make custom reports public, private, or both.	See "Creating a custom report in OpsCenter" on page 559.
Custom SQL Reports **Note:** This feature is available with the licensed (OpsCenter Analytics version) of the product.	This function includes the following tasks: ■ Create, update, delete custom SQL reports.	See "Creating an OpsCenter report using SQL query" on page 573.
Monitoring	Monitoring includes the following tasks: ■ View entities (Dashboards, Summary, Details): Job, Policy, Media, Alerts, Drives, Others.	See chapter Monitoring NetBackup using OpsCenter
Alert Management	The Alert Management function includes the following tasks: ■ .Create, update, delete alert policies. ■ Assign, acknowledge, clear alerts.	See "About creating (or changing) an alert policy" on page 420. See "Managing an alert policy " on page 436.

OpsCenter users are categorized as follows:

Table 5-15 User categories

User	Description
Security Administrator	A Security Administrator is a super admin user who can perform all OpsCenter functions including user management. The OpsCenter Security Administrator can create, edit, or delete users.
Administrator	This user can perform all OpsCenter functions except for user management. The OpsCenter Administrator cannot create, edit, or delete users.
Operator	This user is not involved in the activities that are related to managing users, OpsCenter Server, and NetBackup configuration.
Restore Operator	The role of this user is to mainly perform restore operations. The Restore Operator can monitor, perform alert operations and run standard or custom reports.
Reporter	The role of this user is to mainly generate the operational and business-level reports for further analysis. A Reporter would be able to view only those schedules that they themselves create. The Security Administrator, Administrator, and Operator would however be able to access all the schedules.

Note: You can also assign a user role to a user group of an authorized AD / LDAP domain. The same user role is assigned to each user of the authorized domain group.

Table 5-16 lists the OpsCenter user roles and the OpsCenter UI functions that these users can perform.

Table 5-16 User roles

OpsCenter function	Security Administrator	Administrator	Operator	Restore Operator	Reporter
User Management	Y	N	N	N	N

Table 5-16 User roles *(continued)*

OpsCenter function	Security Administrator	Administrator	Operator	Restore Operator	Reporter
OpsCenter Management	Y	Y	N	N	N
NetBackup Operations	Y	Y	Y	Partial (Only perform operations on Restore Jobs)	N
Backup and Recovery	Y	Y	Y	Y	N
Views Management	Y	Y	N	N	N
All Views Read	Y	Y	P	P	P
Report Execution	Y	Y	Y	Y	Y
Custom Reports	Y	Y	Y	Y	Y
Custom SQL Reports	Y	Y	Y	N	N
Monitoring	Y	Y	Y	Y	Y
Alert Management	Y	Y	Y	Y	Y

“Y” represents “Yes”, which means that the users of this role can perform this particular OpsCenter function.

“N” represents “No”, which means that the users of this role cannot perform this particular OpsCenter function.

P represents "Permission based", which means that users of this role need permission to perform the particular function.

See “About managing OpsCenter users ” on page 226.

Viewing OpsCenter user account information

You can view a list of OpsCenter users and their information that is arranged in a tabular format. You can sort the table by user attributes.

In OpsCenter, you can view the following information in addition to user name, user role, domain name, and domain type.

User	Type of the user: Individual User or Group User. All users from the authorized domain group can logon to OpsCenter with their AD / LDAP credentials. Any changes like addition or removal of a user from an authorized AD / LDAP domain group are automatically reflected in OpsCenter. **Note:** You can add AD / LDAP domain groups to OpsCenter to authorize all users from that group to access OpsCenter.
User Status	Status of the user: Enabled or Disabled If you want to temporarily revoke a user's permission to access OpsCenter, set the user status to 'Disabled'. User with the 'Disabled' user status cannot logon to OpsCenter. However, the user-specific data such as reports or schedules is retained.

To view OpsCenter user account information

1. Log on to the OpsCenter console with administrator privileges.
2. In the Veritas NetBackup OpsCenter console, click **Settings > Users**.
3. Click **Users** to view the list of users.

Adding new users to OpsCenter

You can either add the existing users that are discovered from various domains to OpsCenter or create users in the private “OpsCenterUsers” domain.

You can also add AD / LDAP domain groups to OpsCenter to authorize all users from that group to access OpsCenter.

Individual users or domain user groups that you add in OpsCenter are listed on the **Settings > Users > Users** tab.

All users from the authorized domain group can logon to OpsCenter with their AD / LDAP credentials. Any changes like addition or removal of a user from an authorized AD / LDAP domain group are automatically reflected in OpsCenter.

Note: Only a Security Administrator can add or modify user profiles by using the OpsCenter console.

To add a new user to OpsCenter

1. Log on to the OpsCenter console as a Security Administrator.
2. In the OpsCenter console, click **Settings > Users**.
3. On the **Users** tab, click **Add**.
4. Select the user creation type: **New User**, **Existing Domain User**, or **Existing Domain Group**.

   In OpsCenter, by selecting the Existing Domain Group creation type you can add AD / LDAP domain groups to OpsCenter. Once a domain user group is authorized to access OpsCenter, all users from that group can logon to OpsCenter with their AD / LDAP credentials.

   If you have selected the **New User** option, specify the password, and enter it once again for confirmation.

   If you have selected the **Existing Domain User** option, you need to select the domain to which the user belongs.

   If you have selected the **Existing Domain Group** option, you need to provide the AD/LDAP group name that you want to add and authorize.
5. Enter the following general and demographic details of the user, which change depending on the user creation type that you have selected:

   User name, user role, domain name, email ID, first name, last name, department, cost center, work number, mobile number, and contact details.

   See "User access rights and functions in OpsCenter user interface" on page 231.

   If you have selected **Operator**, **Reporter**, or **Restore Operator** as the **User Role**, you can see the Granted Views list box. Select one or more views from the Granted Views list box to grant access of the specific views to the specific user.
6. Select status of the user or user group: Enabled or Disabled

   If you want to temporarily revoke a user's permission to access OpsCenter, set the user status to 'Disabled'. User with the 'Disabled' user status cannot logon to OpsCenter. However, the user-specific data such as reports or schedules is retained.
7. Click **Save**.

Editing OpsCenter user information

Only a Security Administrator can edit the existing users.

To edit an existing user in OpsCenter

1. Log on to the OpsCenter console as a Security Administrator.
2. In the OpsCenter console, click **Settings > Users**.
3. On the **Users** tab, click the check box in front of the user that you want to edit.
4. Click **Edit**.
5. Modify the user information.

   You cannot modify the domain of the user.

   You can also reset passwords of the OpsCenter users using this page.

   You can modify the views that you want a user to access. You can modify the views for user roles like Operator, Restore Operator, or Reporter. Select one or more views from the Granted Views list to grant access of the specific views to the user.

   See "Resetting an OpsCenter user password" on page 238.
6. Click **Save**.

Resetting an OpsCenter user password

If you are OpsCenter Security Administrator, you can reset the password of an OpsCenterUsers(vx) domain user while you modify the user information. NT or LDAP domain users should contact the System Administrator to reset their passwords.

For security reasons, OpsCenter user should change the password after it was reset by the OpsCenter Security Administrator. OpsCenter displays the Change Password page when you try to log in after your password was reset.

To reset an OpsCenterUsers(vx) domain user password

1. Log on to the OpsCenter console as a Security Administrator.
2. In the OpsCenter console, click **Settings > Users**.
3. On the **Users** tab, click the check box in front of the user for whom you want to reset the password.
4. Click **Edit**.
5. On the Edit User page, click **Reset Password**.

6 On the Reset Password page, enter the new password and confirm password for the selected user.

Note: You must set your new password according to the password rules or guidelines: Password must be at least 8 characters long and should contain at least one upper case letter, one lower case letter, and one numeric digit. The new password must be different than the current password.

The password rules are also provided on the Reset Password page.

---

7 Click **OK**.

See "About managing OpsCenter users " on page 226.

Resetting password of the OpsCenter Security Admin

This section provides the procedure to reset password for the OpsCenter Security Administrator (Security Admin). For security purposes, password reset function for the Security Admin is not provided on the OpsCenter GUI. The Security Admin can reset his or her password manually through OpsCenter Authentication Service (OpsCenter AT).

For security reasons, the OpsCenter Security Administrator should change the password after it was reset. OpsCenter displays the Change Password page when you try to log in after your password was reset.

Note: If an OpsCenter user forgets the password, the OpsCenter Security Administrator can reset it using the Reset Password page on the OpsCenter GUI. Navigation to the Reset Password page:**Settings > Users > Edit User > Reset Password**

See "Resetting an OpsCenter user password" on page 238.

To reset Security Admin password on Windows

1 Logon to OpsCenter Server host with the Administrator's credentials.

2 On the Command Prompt, run the following command:
`OpsCenterInstallPath\Symantec\OpsCenter\server\bin\setEnv.bat`.

3 Once the environment is set, run the reset password command as follows:

```
OpsCenterInstallPath\Symantec\OpsCenter\server\authbroker\bin\vssat
resetpasswd --pdrtype <root|ab|cluster> --domain <domain name>
--prplname <principal name>
```

For example: `C:\Program Files\Symantec\OpsCenter\server\authbroker\bin\vssat resetpasswd --pdrtype ab --domain OpsCenterUsers --prplname admin`

4 When prompted, enter the new password.

5 Re-enter the new password.

To reset Security Admin password on UNIX

1 Logon to OpsCenter Server host with the Administrator's credentials.

2 On the Command Prompt, run the following command:.
`/OpsCenterInstallPath/SYMCOpsCenterServer/bin/setEnv.sh`

3 Once the environment is set, run the reset password command as follows:

```
OpsCenterInstallPath/SYMCOpsCenterServer/authbroker/bin/vssat
resetpasswd -t <root|ab|cluster> -d <domain name> -p <principal
name>
```

For example: `opt/SYMCOpsCenterServer/authbroker/bin/vssat resetpasswd --pdrtype ab --domain OpsCenterUsers --prplname admin`

4 When prompted, enter the new password.

5 Re-enter the new password.

Deleting OpsCenter users

You can delete the user accounts that do not need to be maintained.

Note: The default OpsCenter user admin cannot be deleted.

Warning: Do not inadvertently delete all your administrator accounts.

To delete a OpsCenter user

1 Log on to the OpsCenter console as a Security Administrator.

2 In the OpsCenter console, click **Settings > Users**.

3 Click **Users**.

4 Check the box next to the user account you want to delete.

5 Click **Delete**.

Viewing OpsCenter user groups

This section provides the procedure to view the existing user groups.

To view a user group

1 Log on to the OpsCenter console as a Security Administrator.

2 In the OpsCenter console, click **Settings > Users**.

3 Click **User Groups** to view the list of user groups.

Settings > Users > User Groups options

A description of the **Settings > Users > User Groups** options follows in the table. Only a Security Administrator can access this view.

Table 5-17 User Groups options

Option	Description
Add/Edit/Delete options	Click **Add** to add user groups. Click **Edit** to add or delete users to the existing user group. Click **Delete** to delete the user groups.
Name	Enter a name for the user group that you add.
Description	Enter a description for the user group that you add.

Adding OpsCenter user groups

If you want to give the same privileges to multiple users, add them to a single user group. The same access rights on views are attributed to all users in the user group.

To create an OpsCenter user group

1 Log on to the OpsCenter console as a Security Administrator.

2 In the OpsCenter console, click **Settings > Users.**

3 Click **User Groups**.

4 Click **Add**.

5 On the **User Groups** tab, enter the name of the group and description.

6 In the **List of Users** pane, click **Add** to open the **Add Users** pop-up screens.

7 On the Add Users dialog box, select the users that you want to add to this user group.

8 Click **OK**.

9 On the **User Group** tab, click **Save**.

Editing OpsCenter user groups

You can modify an existing user group.

To edit a OpsCenter user group

1 Log on to the OpsCenter console as a Security Administrator.

2 In the OpsCenter console, click **Settings > Users**.

3 Click **User Groups**.

4 Select the check box in front of the user group that you want to edit.

5 Click **Edit**.

6 Modify the user group name or description.

7 Add or delete the users using the **List of Users** pane and **Add Users** pop-up screens.

8 Click **Save**.

Deleting OpsCenter user groups

You can delete a user group that you no longer need.

To delete a Veritas NetBackup OpsCenter user group

1 Log on to the OpsCenter console as a Security Administrator.

2 In the OpsCenter console, click **Settings > Users**.

3 Click **User Groups**.

4 Select the check box next to the user groups that you want to delete.

5 Click **Delete**.

About managing recipients in OpsCenter

You can specify the recipients to whom you want to send alert notifications or email reports.

Note: Make sure that the mail server is configured to send emails.

See "Configuring SMTP server settings for OpsCenter" on page 216.

The following sections provide procedures for viewing, creating, modifying, and deleting email and SNMP trap recipient information.

See "Viewing email recipients in OpsCenter" on page 243.

See "Viewing SNMP trap recipients in OpsCenter" on page 244.

See "Creating OpsCenter email recipients" on page 245.

See "Creating OpsCenter SNMP trap recipients" on page 246.

See "Modifying OpsCenter Email or SNMP recipient information" on page 248.

See "Deleting OpsCenter Email or SNMP trap recipient" on page 248.

Viewing email recipients in OpsCenter

This section provides the procedure to view the available email recipients.

To view the email recipients

1. Log on to the OpsCenter console.
2. In the OpsCenter console, click **Settings > Recipients**.

   By default, the **Email** tab is selected. All email recipients are displayed on this tab.
3. Modify recipients and recipient details as needed.

See "Settings > Recipients > Email options" on page 243.

See "About managing recipients in OpsCenter" on page 242.

Settings > Recipients > Email options

A description of the **Settings > Recipients > Email** options follows in the table.

Table 5-18 Email recipient options

Option	Description
Recipient Name	Name of the email recipient
Email Address	Email ID of the recipient

Table 5-18 Email recipient options *(continued)*

Option	Description
Active	The status of the email recipient that states whether it is active or not If a recipient is not active, it is not available for selection on the Adding Email Recipients pop-up screen, when emails are sent.
Description	Description about the email recipient

Viewing SNMP trap recipients in OpsCenter

This section provides the procedure to view the available SNMP trap recipients.

To view the SNMP trap recipients

1. Log on to the OpsCenter console.
2. In the OpsCenter console, click **Settings > Recipients**.
3. Click **SNMP**.
4. Modify recipients and recipient details as needed.

Settings > Recipients > SNMP trap recipient options

A description of the **Settings > Recipients > SNMP trap recipient** options follows in the table.

Table 5-19 SNMP trap recipient options

Option	Description
Recipient Name	Name of the SNMP trap recipient.
SNMP Host	Name of the SNMP host.
Port	Port number on the SNMP host where you want to send traps.
Active	The status of the trap recipient that states whether it is active or not. If a recipient is not active, it is not available for selection on the Adding Trap Recipients pop-up screen, when alert policies are configured.
Description	Description about the trap recipient.

Creating OpsCenter email recipients

This section describes how to create email recipients.

To create email recipients

1. Log on to the OpsCenter console with administrator privileges.
2. In the OpsCenter console, click **Settings > Recipients**.
3. In the **Email** tab, click **Add** to create new email recipients.
4. Enter the required information.

   See " Settings > Recipients > Email > Add Email Recipient options" on page 245.
5. Click **Save**.

Settings > Recipients > Email > Add Email Recipient options

A description of the **Settings > Recipients > Email > Add Email Recipient** options follows in the table.

Table 5-20 Add Email Recipient options

Option	Description
Email Recipient Name	Enter the name of the official whom you want to notify about an alert or send reports.
Email Address	Enter the email ID of the official, to which alert notifications or reports are sent.
Active	Select this check box if you want the recipient to receive alert notifications and reports by emails.
Description	Enter a short description about the alert or report so that recipients can understand.
Activate Delivery Limit	Select this check box to activate the **Alert Notification Delivery Limit** settings. If you do not select this check box, **Maximum Number of Messages**, **Delivery Time Span**, and **Reset Message Count After Time** are not taken into account when notifications are sent.
Maximum Number of Messages	Enter the maximum number of notifications that you want to receive within the specified **Delivery Time Span**.

Table 5-20 Add Email Recipient options *(continued)*

Option	Description
Delivery Time Span	Enter the time duration in hours, minutes, or seconds, during which notifications are sent. Once the message count reaches **Maximum Number of Messages**, the Notification Manager blocks the delivery of any new notifications to the associated recipient for the time period that is specified for **Reset Message Count After Time**.
Reset Message Count After Time	Enter the time period in hours, minutes, or seconds, during which notifications are blocked if the message count has reached **Maximum Number of Messages**. Once this time period is over, **Maximum Number of Messages** is reset and the Notification Manager starts sending notifications for the specified **Delivery Time Span**. **Note:** For example, assume **Maximum Number of Messages** = 10, **Delivery Time Span** = 30 Minutes, and **Reset Message Count After Time** = 2 Hours. In this case, Alert Manager sends messages until message count reaches 10 in 30 Minutes. Once it has sent 10 messages, it blocks the delivery of new messages for next two Hours. After two hours, Alert Manager once again starts sending messages until message count reaches 10.

Creating OpsCenter SNMP trap recipients

Traps or interrupts are signals sent to inform the programs that an event has occurred. In OpsCenter, traps are the notifications that are sent to a specified SNMP host or group of hosts when a condition is met.

A trap recipient is a host that receives notifications in the form of SNMP traps when an alert condition is met. For example, a trap is sent after an alert was generated as a result of failure of communication between the OpsCenter Agent and Server.

For more details, refer to the About using SNMP with OpsCenter section.

To create SNMP recipients

1. Log on to the OpsCenter Server host with administrator privileges.
2. In the OpsCenter console, click **Settings > Recipients**.
3. Click **SNMP**.
4. Click **Add**.

5 In the **SNMP Attributes** page enter the required information.

See "Settings > Recipients > SNMP > Add SNMP trap recipient options" on page 247.

6 Click **Save**.

Settings > Recipients > SNMP > Add SNMP trap recipient options

A description of the **Settings > Recipients > SNMP > Add SNMP trap recipient** options follows in the table.

Table 5-21 Add SNMP trap recipient options

Option	Description
Recipient Name	Enter the name of the SNMP trap recipient.
SNMP Host	Enter an SNMP host, to which you want to send traps.
SNMP Port	Enter the port number on the SNMP host where you want to send traps.
Active	Select this check box if you want the recipient to receive notifications by SNMP traps.
Description	Enter a short description about the traps.
Activate Delivery Limit	Select this check box to activate the **Alert Notification Delivery Limit Settings**. If you do not select this check box, **Maximum Number of Messages**, **Delivery Time Span**, and **Reset Message Count After Time** are not taken into account when notifications are sent. The notifications are sent as soon as alerts are generated.
Maximum Number of Messages	Enter a maximum number of notifications that can be sent within the specified **Delivery Time Span**.
Delivery Time Span	Enter the time duration in hours, minutes, or seconds, during which notifications are sent. Once the message count reaches **Maximum Number of Messages**, Alert Manager blocks the delivery of any new notifications to the associated recipient for the time period that is specified for **Reset Message Count After Time**.

Table 5-21 Add SNMP trap recipient options *(continued)*

Option	Description
Reset Message Count After Time	Enter the time period in hours, minutes, or seconds, during which notifications are blocked if the message count has reached **Maximum Number of Messages**. Once this time period is over, **Maximum Number of Messages** is reset and Alert Manager starts sending notifications for the specified **Delivery Time Span**.

Modifying OpsCenter Email or SNMP recipient information

Only OpsCenter administrators can modify email or trap recipient information.

See "Creating OpsCenter email recipients" on page 245.

See "Creating OpsCenter SNMP trap recipients" on page 246.

To modify email or SNMP trap recipient information

1. In the OpsCenter console, click **Settings > Recipients**.
2. In the **Email Recipients** tab or **SNMP Recipients** tab, select the email or trap recipient that you want to edit.
3. Click **Edit**.
4. On the modify email or trap recipient page, change **Email Recipient** or **SNMP Trap Recipient** attributes and **Alert Notification Delivery Limit Settings**.
5. Click **Save**.

Deleting OpsCenter Email or SNMP trap recipient

Only OpsCenter administrator can delete email or trap recipient.

See "Creating OpsCenter email recipients" on page 245.

To delete Email or SNMP trap recipient

1. In the OpsCenter console, click **Settings > Recipients**.
2. In the **Email Recipients** tab or **SNMP Recipients** tab, select the email or trap recipient(s) from the table that you want to delete.
3. Click **Delete**.
4. Click **Save**.

About managing cost analysis and chargeback for OpsCenter Analytics

This feature is accessible only to OpsCenter Analytics users.

In OpsCenter Analytics, you can choose the currency that you want to be displayed on cost reports. If you have OpsCenter administrator privilege, you can set multiple global currencies, one of which can be set as default currency. You can set the cost variable, cost formulae, and cost estimation that you want to run the cost reports.

You cannot access the **Settings > Chargeback** feature if you do not have OpsCenter Analytics. This feature is disabled for unlicensed OpsCenter version.

The following sections provide procedures for managing cost analysis and chargeback.

See "Setting the default currency for OpsCenter cost reports" on page 249.

See "Editing the OpsCenter global currency list" on page 250.

See "Settings > Chargeback > Cost Variable options" on page 251.

See "Settings > Chargeback > Cost Formulae options" on page 255.

Setting the default currency for OpsCenter cost reports

This section provides the procedure to set the default currency that you want to be displayed on OpsCenter cost reports.

Note: Setting the default currency gives you the flexibility of displaying cost report values in the currency of your choice. However, OpsCenter does not support conversion of currencies.

To set the default currency for cost reports

1. Log on to the OpsCenter console with administrator privileges.
2. In the OpsCenter console, click **Settings > Chargeback**.

   You cannot access the **Settings > Chargeback** feature if you do not have OpsCenter Analytics. This feature is disabled for unlicensed OpsCenter version.
3. On the **Currency Settings** tab, in the **Default Currency** drop-down list, all global currencies that are set by the administrator are available for selection. Select a currency from the drop-down list.

   See "Editing the OpsCenter global currency list" on page 250.

4 Select the **Currency Display Mode**: **Currency Code** or **Currency Symbol**. For example, for US dollar currency you can either select a currency code USD or symbol $, which appears on chargeback reports.

5 Select the **Display Currency Option in Cost Reports** check box to show the default currency on the cost reports.

6 Click **Save**.

Settings > Chargeback > Currency Settings options

A description of the **Settings > Chargeback > Currency Settings** options follows in the table.

Table 5-22 Currency Settings options

Option	Description
Default Currency	Select a currency from the drop-down list. All global currencies that are set by the administrator are available for selection.
Edit Currency List	Click this option to change the list of currencies available for selection.
Currency Display Mode	Select the **Currency Display Mode**: **Currency Code** or **Currency Symbol**. For example, for US dollar currency you can either select a currency code USD or symbol $, which appears on chargeback reports.
Display Currency Option in Cost Reports	Select the **Display Currency Option in Cost Reports** check box to show the default currency on the cost reports.

Editing the OpsCenter global currency list

This section provides the procedure to edit the global currency list. This list is available when a default currency is selected to be displayed on OpsCenter cost reports.

To edit the global currency list

1 Log on to the OpsCenter console with administrator privileges.

2 In the OpsCenter console, click **Settings > Chargeback**.

If you have not entered the OpsCenter Analytics license key, you cannot access the **Settings > Chargeback** feature. This feature is disabled for unlicensed OpsCenter version.

3 On the **Currency Settings** tab, click **Edit Currency List**.

4 On the **Edit Currency List** pop-up screen, select currencies from the **Global Currency** list which you want to make available for selection in the **Currency Settings > Default Currency** drop-down list.

   See "Setting the default currency for OpsCenter cost reports" on page 249.

5 Click **Add** to add the selected currencies to the **User Currency** list.

   You can use **Add**, **Remove**, **Add All**, and **Remove All** options to alter the **User Currency** list.

6 Click **OK**.

Settings > Chargeback > Currency Settings > Edit Currency List options

A description of the **Settings > Chargeback > Currency Settings > Edit Currency List** options follows in the table.

Table 5-23 Edit Currency List options

Option	Description
Global Currency	Lists the available global currencies.
User Currency	It is the default currency list and lists the currencies that you select.
Add/Remove/Add All/Remove All	You can use these options to alter the **User Currency** list.

Settings > Chargeback > Cost Variable options

You can create cost variables based on various parameters to determine cost of various services.

A description of the **Settings > Chargeback > Cost Variable** options follows in the table.

Table 5-24 Cost Variable options

Option	Description
Name	Displays the name of the cost variable that you add.
Metric	Displays the metric that you select for the cost variable.
Total Date Ranges and Rates	Displays the date ranges and rate in units for the date range that you select.

And if you click the **Add** option, a page with the following settings appears.

Table 5-25 Add Cost Variable options

Option	Description
Variable Name	Enter a name for the cost variable that you want to add.
Variable Metric	Select a variable metric from the drop-down list for the cost variable that you add.
Job Type	Measure costs for a specific type of job, for example Backup or Restore. The default option is All.
Job Policy Type	Measure costs for the jobs that use a specific policy type. In NetBackup, the policy type determines the type of clients that can be part of the policy and, in some cases, the types of backups that can be performed on the clients. Examples include DB2, Sybase, and MS Exchange Server. The default policy type is All.
Job Transport Type	Measure cost for a specific transport type for example, LAN (local area network) or FT (Fibre Transport). The default option is All.
Job Storage Type	Measure cost for a specific storage type for example, tape or disk. OpsCenter supports NetBackup's disk-based data protection feature, which enables you to select disk as a storage type, when a cost variable is created. The default option is All.
Date Range Starts	Select to add a start date to the cost variable.
Date Range Ends	Select to add a end date to the cost variable. You can also select Never as the end date.
Rate	Add an associated rate to the cost variable.
Add New Range	Select to add more date ranges.

Creating cost variables in OpsCenter

Cost reports in OpsCenter Analytics are based on the user-defined variables that define the cost of various services.

Typically, each service is represented by one variable that reflects the cost of the service, for example $1.00 per backup job. However, you can account for rate changes in one of two ways: by creating two variables for the same service (which you can include in a single cost formula later) or by incorporating both rates into a

single variable. For example, a single variable can incorporate the rate of $1.00 per backup job until 31 December 2004 and the rate of $1.25 per backup job starting on 1 January 2005.

Note: To generate deduplication savings reports, you must create a cost variable with the Protected Job Size (GB) metric.

To set up OpsCenter to run cost reports, you need to create the variables that define the cost of various services.

To create a cost variable

1. Log on to the OpsCenter console with administrator privileges.
2. In the OpsCenter console, click **Settings > Chargeback**.

   Click **Cost Variable**.
3. On the **Cost Variable** tab, click **Add**.
4. Enter the variable name.
5. Select any of the following variable metrics from the drop-down list:
   - **Daily Occupancy**
   - **Job Count**
   - **Job Size**
   - **Protected Job Size**
   - **Storage Size**
6. If necessary, select additional parameters to refine the metric you selected. For **Job Count**, **Job Size**, and **Protected Job Size** select the **Job Type**, **Job Policy Type**, **Job Transport Type**, and **Job Storage Type**.

   Note: These fields are not applicable for the Daily Occupancy and Storage Size variable metrics. For Storage Size, Cloud Provider field is available.

   See "Settings > Chargeback > Cost Variable options" on page 251.
7. Add one or more date ranges using the drop-down lists for Month, Day, Year, and Time. Add an associated rate by typing a cost per service unit (such as backup jobs or backed-up GB) in the **Rate** field.

   Add at least one date range.

8 Optionally, to add more date ranges, click **Add New Range**.

This can be useful for defining multiple date ranges to represent historical or future changes in service costs. You can also modify the variable later to add or delete date ranges as costs change.

9 Click **OK** .

You can now use the variable you created to build the formulas that form the basis for cost reports.

See "Creating cost formulae in OpsCenter" on page 255.

Modifying cost variables in OpsCenter

You can update cost variables and formulas without having to recreate the reports that rely on them. For example, you can modify the name, date ranges and rates of a variable to reflect changing conditions in your enterprise.

To modify a cost variable

1 Log on to the OpsCenter console with administrator privileges.

2 In the OpsCenter console, click **Settings > Chargeback**.

Click **Cost Variables**.

3 Select the check box in front of the variable name that you want to modify.

4 Click **Edit**.

5 Modify the cost variable details.

6 Click **OK**.

Deleting cost variables in OpsCenter

You can variables you no longer need. Deleting a cost variable removes it permanently from the database, and you must update any formulas that use the variable. To restore a deleted variable, you must recreate the variable manually.

To delete a cost variable

1 Log on to the OpsCenter console with administrator privileges.

2 In the OpsCenter console, click **Settings > Chargeback**.

3 Click **Cost Variables**.

4 Select the check box in front of the cost variable that you want to delete.

5 Click **Delete**.

Settings > Chargeback > Cost Formulae options

Based on cost variables you can create the cost formulas that you can use to generate cost reports.

A description of the **Settings > Chargeback > Cost Formulae** options follows in the table.

Table 5-26 Cost Formulae options

Option	Description
Name	Displays the name of the cost formulae added.
Total Cost Variables	Displays the number of cost variables added to the cost formulae.

Creating cost formulae in OpsCenter

After you create cost variables, create the formula that define the cost of various services to run cost reports.

To create a cost formula

1. Log on to the OpsCenter console with administrator privileges.
2. In the OpsCenter console, click **Settings > Chargeback**.

   Click **Cost Formulae**.
3. On the **Cost Formulae** tab, click **Add**.
4. Enter the name of the formula.
5. Select a cost variable from the drop-down list.

   You need to select at least one cost variable.
6. Optionally, to define formulae containing more than one variable, click **Add new cost variable**. Select a different variable from the drop-down list.

   You can also modify the formulae later to add or delete variables.
7. Click **OK**.

   You now can use the formula to create cost reports. These reports help you evaluate the cost of services and make decisions about what to charge for performing those services.

Modifying cost formulae in OpsCenter

You can modify the name and variables of a cost formula that you have created.

You can update chargeback formulas without having to recreate the reports that rely on them. For example, you might want to update a formula that is called RecoveryRate to reflect a change in the hourly rate that is charged for recovery operations.

To modify a cost formulae

1. Log on to the OpsCenter console with administrator privileges.
2. In the OpsCenter console, click **Settings > Chargeback**.

   Click **Cost Formulae**.
3. On the **Cost Formulae** tab, select the cost formulae that you want to modify.
4. Click **Edit**.
5. Modify the details of the cost formula.
6. Click **OK**.

Deleting a cost formulae in OpsCenter

You can also delete formulae that you no longer need. Deleting a cost formula removes it permanently from the database.

To delete cost formulae

1. Log on to the OpsCenter console with administrator privileges.
2. In the OpsCenter console, click **Settings > Chargeback**.

   Click **Cost Formulae**.
3. On the **Cost Formulae** tab, select the cost formulae that you want to delete.
4. Click **Delete**.
5. On the confirmation dialog box, click **OK**.

Estimating chargeback costs using the OpsCenter Formula Modeling Tool

The Formula Modeling Tool offers an easy way to estimate baseline rates for the IT services you provide. Using historical data, it provides you with an estimate of how much it costs your organization to provide a specific kind of service.

For example, suppose you anticipate spending $500,000 over the next year to provide backup services throughout your enterprise. By inserting the metric Daily Occupancy into the tool, along with the amount $500,000, you can obtain an estimate per kilobyte that is based on the backup activity you performed last year.

See “Creating cost variables in OpsCenter” on page 252.

See "Creating cost formulae in OpsCenter" on page 255.

To estimate baseline (chargeback) costs using the Formula Modeling Tool

1. Log on to the OpsCenter console with administrator privileges.
2. In the OpsCenter console, click **Settings > Chargeback**.

   Click **Cost Estimation**.
3. Select a **Report Grouping** parameter to define the model's scope.
4. Use the **Metric Selection** parameters to specify the metric whose rate you want to estimate:

   See "Settings > Chargeback > Cost Estimation options" on page 257.
5. Use the following **Time Frame** parameters to define the time intervals for which data is modeled.
6. Click **Run Model** to input different values into the model, or to run a new model.

Settings > Chargeback > Cost Estimation options

A description of the **Settings > Chargeback > Cost Estimation** options follows in the table.

Table 5-27 Cost Estimation options

Option	Description
Report Grouping	Select a report grouping parameter to define the model's scope. Examples: All Master Servers or User
Metric	Select a metric or category of service. Example: Daily Occupancy
Amount	Specify the total amount of money, in dollars, you expect to charge for service within that category in a given time frame. Examples: $50000, $10000, or $10000.00

Table 5-27 Cost Estimation options *(continued)*

Option	Description
Time Frame	Defines the beginning and end of the time interval the estimate must cover. You can choose either absolute or relative dates. Choose absolute dates if you want the estimate's contents to remain static whenever you display it. Choose relative dates if you want the estimate to reflect data that was collected over the most recent time interval. Select one of the following: ■ Click **Absolute** to configure an absolute time frame. Select a start time (month, day, year, and time of day) using the **From** drop-down lists, and a stop time using the **To** drop-down lists. The estimate reflects data from the time period between the start and the end dates. Example: From MAR 1 2004 12:00 A.M. to APR 30 2004 12:00 A.M. ■ Click **Relative** to configure a relative time frame. Then select a time interval using the Last drop-down lists. The estimate reflects the data that is collected within the specified time period, up to the current time. Examples: Last 21 Days or Last two Quarters The **Relative** setting is especially useful for the estimates that you plan to generate on a regular basis. Such estimates always reflect the data that is collected over the most recent time interval.

Chapter 6

Understanding data collection

This chapter includes the following topics:

- About data collection in OpsCenter
- About managing OpsCenter Agents
- About managing OpsCenter Data Collectors
- About configuring data collection for NetBackup
- Configuring Backup Exec data collector
- Collecting data from PureDisk

About data collection in OpsCenter

OpsCenter provides extensive reporting on the data that is collected from backup products. An OpsCenter Agent comprises the product-specific data collectors that collect data from point products and return it to the OpsCenter Server.

Note: Only one OpsCenter Agent can be installed on a single host.

An OpsCenter Agent consists of the data collectors that can collect data from the following backup products:

- Backup Exec (Windows only)

  Note: To collect data from Backup Exec server host, you need to install the OpsCenter Agent on a Windows host.

- NetBackup PureDisk

See "About configuring data collection for NetBackup" on page 271.

See "About OpsCenter Agents" on page 260.

See "OpsCenter Data Collector types" on page 260.

About OpsCenter Agents

The OpsCenter Agent collects data from various Veritas backup products. These products can reside on the OpsCenter Agent host or on remote hosts.

For more details on OpsCenter Agent installation and deployment scenarios, refer to the Installing OpsCenter chapter.

Note: When you install the OpsCenter Server, OpsCenter Integrated Agent is also installed and configured, which you can use to collect only PureDisk data. To collect PureDisk data, you do not need to manually install or configure OpsCenter Agent.

You cannot delete the Integrated Agent.

You can collect PureDisk data only through the OpsCenter Integrated Agent.

About OpsCenter Agent logs

OpsCenter Agent logs are stored at the following location:

InstallPath`\Symantec\OpsCenter\Agent\logs`

Where *InstallPath* is the location where you have installed the OpsCenter Agent.

By default the *InstallPath* is: `C:\Program Files`

Naming convention for the OpsCenter Agent log file:

`5*-146-*.log`

An example of the OpsCenter Agent log file name:

`58330-146-2567491850-091129-0000000000.log`

OpsCenter Data Collector types

The OpsCenter data collectors, collect data from backup product hosts. Each data collector collects data from a single product host. You can configure multiple data collectors on a single OpsCenter Agent host.

You can create data collectors to communicate with the various products, such as Backup Exec. These data collectors collect the specified data type as specified in

the configuration. You can specify to collect all or some of the data types for that product. For example, Backup Exec data collector can collect Tape Drive information, Media, Policy and Schedule, Job, or Image.

Note: Error logs and skipped files are collected as part of job data.

You can enable or disable a data collector.

Table 6-1 lists the data collectors that you can configure in OpsCenter.

Table 6-1 Data collector types

Data Collector type	Description
Veritas Backup Exec Data Collector (Windows only)	Create this data collector to collect data from Backup Exec. See "Configuring Backup Exec data collector" on page 293.
NetBackup PureDisk Data Collector	Create this data collector to collect data from NetBackup PureDisk. See "Collecting data from PureDisk" on page 295. **Note:** You can collect the PureDisk data only through the OpsCenter Integrated Agent that is installed with the OpsCenter server. To collect PureDisk data, you need to create a data collector for the Integrated Agent.

Table 6-2 lists the data types that OpsCenter collects from different NetBackup versions (including NetBackup Appliance).

Table 6-2 Data Types collected for different NetBackup versions

Data Type	NetBackup versions 7.5, 7.6, 7.6.1, 7.7	7.1.x	7.0.1	7.0	NetBackup Appliance
					(Appliance 2.0, 2.0.1, or 2.0.2 master server or NetBackup 7.1.0.3 master server and later)

Table 6-2 Data Types collected for different NetBackup versions *(continued)*

Data Type	NetBackup versions 7.5, 7.6, 7.6.1, 7.7	7.1.x	7.0.1	7.0	NetBackup Appliance
Appliance Hardware	Y	Collected only for 7.1.0.3 and later versions	N.A.	N.A.	Y
Audit	Y	Y	N.A.	N.A.	Y
BMR, Skipped Files and Job Throughput	Y	Y	Y	Y	Y
Catalog	N.A.	N.A.	N.A.	N.A.	N.A.
Client	Y	Y	Y	Y	Y
Disk	Y	Y	Y	Y	Y
Error Logs	Y	Y	Y	Y	Y
FT	Y	Y	Y	Y	Y
Host Properties	Y	Y	N.A.	N.A.	Y
Images	Y	Y	Y	Y	Y
Job	Y	Y	Y	Y	Y
Media server	Y	Y	Y	Y	Y
Policy and Schedule	Y	Y	Y	Y	Y
Retention Level	Y	Y	Y	Y	Y
Robot	Y	Y	Y	Y	Y
Scheduled jobs	Y	Y	Y	Y	Y
Service	Y	Y	Y	Y	Y

Table 6-2 Data Types collected for different NetBackup versions *(continued)*

Data Type	NetBackup versions 7.5, 7.6, 7.6.1, 7.7	7.1.x	7.0.1	7.0	NetBackup Appliance
SLP Image	Y	Y	N.A.	N.A.	Y
Storage service	Y	Y	Y	Y	Y
Storage unit	Y	Y	Y	Y	Y
Storage unit Group	Y	Y	Y	Y	Y
SubJobs	Y	Y	bpjava protocol	bpjava protocol	Y
Tape drive Information	Y	Y	Y	Y	Y
Throughput	N.A.	N.A.	N.A.	N.A.	N.A.
Virtual machine	Y	Y	Y	Y	Y
Volume/Media	Y	Y	Y	Y	Y
Volume group	Y	Y	Y	Y	Y
Volume Pool	Y	Y	Y	Y	Y

Table 6-3 lists the data types that OpsCenter collects from various Veritas backup products other than NetBackup.

Table 6-3 Data types collected from products other backup products

Data Types	Backup Exec	PureDisk
	(11.x, 12.x, 2010, 2010 R2, 2010 R3)	(6.2.x, 6.5.x, 6.6, 6.6.0.1, 6.6.0.2, 6.6.0.3, 6.6.1, 6.6.1.2)
Job	Y	Y
Policy and Schedules	Y	Y
Tape drive Information	Y	N
Media	Y	N

About managing OpsCenter Agents

The following topics provide more information about viewing, modifying, creating, and deleting an OpsCenter Agent configuration.

See "About the OpsCenter Agent" on page 27.

See "Viewing OpsCenter Agent status" on page 265.

See "Configuring an OpsCenter Agent" on page 265.

See "Modifying an OpsCenter Agent" on page 266.

See "Deleting OpsCenter Agents" on page 266.

Settings > Configuration > Agent options

A description of the **Settings > Configuration > Agent** options follows in the table.

Table 6-4 Settings > Configuration > Agent options

Option	Description
Create/Edit/Delete Agent	Select the **Create Agent** or **Edit Agent** option to create an agent or modify the details of an agent. Select **Delete Agent** to delete the selected agent. See "Settings > Configuration > Agent > Create Agent or Edit Agent options" on page 265.
Create/Edit/Delete Data Collector	Select the **Create Data Collector** or **Edit Data Collector** option to create an agent or modify the details of an agent using the Data Collector Wizard. Select **Delete Data Collector** to delete the selected agent. See "Data Collector Wizard settings" on page 269.
Name	Name of the Agent host.
Product Host	Host from where the Agent collects the data such as Backup Exec server or PureDisk server.
Policy and Schedule	Data collection status for policy and schedule on the product host.
Tape Drive Information	Data collection status for tapes on the product host.
Media	Data collection status for media on the product host.

Table 6-4 Settings > Configuration > Agent options *(continued)*

Option	Description
Job	Data collection status for jobs on the product host.
Appliance Hardware	Appliance hardware details that are associated with NetBackup Appliance Master Server.

Viewing OpsCenter Agent status

Use this section to view general details and status of an OpsCenter Agent that you have configured in OpsCenter.

To view Agent status

1. In the OpsCenter console, click **Settings > Configuration > Agent**.
2. On the Agent list, select an Agent to view its status at the bottom of the page.

   By default the **General** tab is selected. The tab displays the parameters which you have specified when you created this Agent.

   See "Settings > Configuration > Agent options" on page 264.

   See "Configuring an OpsCenter Agent" on page 265.
3. Click the **Agent Summary by Data Collector Status**, **Agent Summary by Data Type Status**, or **Agent Summary by Data Collector Count** tab to view the relevant details.

Configuring an OpsCenter Agent

This section provides the procedure to configure an OpsCenter Agent.

To configure an OpsCenter Agent

1. In the OpsCenter console, click **Settings > Configuration > Agent**.
2. Click **Create Agent** and complete the fields.

   See "Settings > Configuration > Agent > Create Agent or Edit Agent options" on page 265.
3. Click **Save**.

Settings > Configuration > Agent > Create Agent or Edit Agent options

To create an Agent, the **Create Agent** pane options must be completed as follows:

Table 6-5 Settings > Configuration > Agent > Create Agent or Edit Agent options

Option	Description
Agent Host	Enter the host name where you want to configure the agent
Agent Operating System Type	Select the operating system of the host where you want to install Agent. For example: Windows For Windows hosts, you can configure an Agent for all supported backup products.
OpsCenter Server Network Address	Select the network address from the drop-down list, using which you want to connect to the OpsCenter Server
Locate option	Click **Locate** to check if OpsCenter can connect to the Agent host that you entered, validate the OS, and Network address. An error appears if OpsCenter cannot connect to the Agent.

Note: Changing the port number that the OpsCenter Agent requires to connect to the PBX on the OpsCenter Server is not supported in OpsCenter 7.5. If you add or edit a new OpsCenter Agent, the PBX port value is taken as 1556 by default. If you had configured a PBX port other than 1556 and upgrade to OpsCenter 7.5, then when you edit and save the Agent in OpsCenter 7.5 the PBX port value is changed to 1556.

Modifying an OpsCenter Agent

This section provides the procedure to modify an OpsCenter Agent information.

To modify an OpsCenter Agent

1. In the OpsCenter console, click **Settings > Configuration > Agent**.
2. From the list of agents, select the check box in front of the Agent that you want to modify.
3. Click **Edit Agent**.
4. On the **Edit Agent** page, modify **OpsCenter Server Network Address**.
5. Click **Save**.

Deleting OpsCenter Agents

This section provides the procedure to delete an OpsCenter Agent.

To delete an OpsCenter Agent

1. In the OpsCenter console, click **Settings > Configuration > Agent**.
2. From the list of agents, select the check box in front of the Agent that you want to delete.
3. Click **Delete**.

About managing OpsCenter Data Collectors

The following topics provide more information about viewing, configuring, modifying, or deleting a data collector.

See "Viewing OpsCenter Data Collector status" on page 267.

See " Configuring an OpsCenter Data Collector" on page 268.

See " Modifying an OpsCenter Data Collector configuration" on page 270.

See " Deleting OpsCenter Data Collectors" on page 271.

Viewing OpsCenter Data Collector status

Use this section to view general details and status of a Data Collector that you have configured for an Agent.

To view data collector status

1. In the OpsCenter console, click **Settings > Configuration > Agent**.
2. On the **Agent** list, expand an Agent to view the Data Collectors that are configured for this Agent.

3 Select a Data Collector to view its details and status at the bottom of the page.

By default the **General** tab is selected displaying the following Data Collector details, which you have specified when you created this Data Collector.

See " Configuring an OpsCenter Data Collector" on page 268.

Product	Displays the name of the product type, for which this Data Collector is configured. For example: Veritas Backup Exec
Product Host	Displays the name of the target host, which this Data Collector collects data from.
Status	Displays the status of the Data Collector as Enabled or Disabled that you have set. If the Data Collector status is disabled, the data is not collected from the target host.

4 Select the **Data Collection Status** tab.

More information is available about the parameters that are displayed on this tab.

See "Data collection status of a master server" on page 283.

Configuring an OpsCenter Data Collector

OpsCenter is designed to provide extensive reporting on the data that is received from backup products. OpsCenter consists of Server, Agent, OpsCenter View Builder, and a console. The OpsCenter Agent contains product-specific data collectors collecting data from the products and returning it to the OpsCenter Server. You can generate various business reports on this backup data.

After you install and configure an OpsCenter Agent, configure the data collectors.

See "Configuring an OpsCenter Agent" on page 265.

To configure a data collector

1 In the OpsCenter console, click **Settings > Configuration > Agent**.

2 On the **Agent** list, select a check box in front of the Agent, for which you want to configure a Data Collector.

3 Click **Create Data Collector**.

4 Complete the fields on the **Create Data Collector: Product Selection** page.

5 Click **Next**.

On the **Create Data Collector: Details** page, the **Target Details, Configuration Settings** and **Data Collection Settings** are displayed.

6 Verify or modify the default **Target Details**:

See "Data Collector Wizard settings" on page 269.

7 Enter the data collector **Configuration Settings**. These settings vary depending on the data collector type you configure. For product-specific configuration settings, refer to the respective data collector settings.

See "Configuring Backup Exec data collector" on page 293.

8 Enter the **Data Collection Settings**.

9 Click **Save**.

Data Collector Wizard settings

Complete the **Product Selection** fields as follows:

Table 6-6 Product Selection settings

Setting	Description
Select Product	Select the name of the product from which you want to collect data. For example, Veritas Backup Exec. The options available in the **Select Product** drop-down list depends on the Agent operating system family that you have selected while creating the respective Agent. For Backup Exec, only Windows option is available, as it supports only Windows operating system.
Target host name	Enter the name of the product host from which you want to collect backup data.

Complete the **Data Collector: Details** fields as follows:

Table 6-7 Data Collector: Details settings

Setting	Description
Select Product	Displays the name of the product from which this data collector collects data. You need to specify the product name when you create the data collector. For example: Veritas Backup Exec.

Table 6-7 Data Collector: Details settings *(continued)*

Setting	Description
Target Host Name	Displays the name of the product host from which this data collector collects data. You need to specify the product name when you create the data collector.
Data Collection Status	By default, the data collector status is Enabled. You can disable the data collection by changing the status.
User Name	Enter the user name.
Password	Enter the user password.
Product Version	Select the product version.
Blackout Period Start Time	Select the start time of a blackout period. The data is not collected during the time that is specified in **Blackout Period Start Time** and **Blackout Period End Time**.
Blackout Period End Time	Select the end time of a blackout period. The data is not collected during the time that is specified in **Blackout Period Start Time** and **Blackout Period End Time**.
Configuration Status	Select this check box to collect the associated data type.
Collectible Data Type	Lists the data types that can be collected from a product host. The data types vary depending on the product that you are collect data from. See "OpsCenter Data Collector types" on page 260.
Collection Interval (sec)	Enter the **Collection Interval** in minutes, hours, and days. **Collection interval** is the time interval that you want to set between the two consecutive data collections. For example: You have set the **Collection Interval** to 15 Minutes. The first data collection starts at say 9:00 A.M. till all backup records are collected and ends at 11:00 A.M. The next data collection starts at 11:15 A.M. after 15-minutes interval .
Last Successful Data Load	States whether last data load was successful or not. See "Viewing OpsCenter Agent status" on page 265.

Modifying an OpsCenter Data Collector configuration

This section provides procedure to modify configuration of a Data Collector.

To modify a Data Collector configuration

1. Log on to the OpsCenter console.
2. In the OpsCenter console, click **Settings > Configuration > Agent.**.
3. On the **Agent** list, expand an Agent to view Data Collectors that are configured for this Agent.
4. Select a check box in front of the Data Collector that you want to modify.
5. Click **Edit Data Collector**.
6. On the **Edit Data Collector: Details** page, modify the **Target Details**.
7. Modify Data Collection or Configuration Settings. These settings vary depending on the product, which this data collector collects data from.
8. Modify blackout period settings.
9. Modify collection interval.
10. Click **Save**.

Deleting OpsCenter Data Collectors

This section provides procedure for deleting Data Collector configurations from an Agent.

To delete a Data Collector configuration

1. Log on to the OpsCenter Server.
2. In the OpsCenter console, click **Settings > Configuration > Agent**.
3. On the **Agent** list, expand an Agent to view Data Collectors that are configured for this Agent.
4. Select check boxes in front of the Data Collectors that you want to delete.
5. Click **Delete Data Collector**.

About configuring data collection for NetBackup

This section describes how OpsCenter collects data from NetBackup. It also describes how you can add, edit, delete, and control data collection for a master server.

Review the following notes before you add or configure a NetBackup master server in OpsCenter:

- OpsCenter does not support monitoring NetBackup master servers that are configured only in IPv6 environment.

If you have added a master server that is configured only with IPv6 in OpsCenter, the following error message is displayed during data collection, which may be misleading:

```
The specified NetBackup Master Server could not be found. Make
sure that you have entered the correct server name, the server is
reachable, and the NetBackup services are running.
```

- To collect data from a NetBackup 8.1 master server, ensure that the OpsCenter server name is configured against the `OPS_CENTER_SERVER_NAME` option in the NetBackup configuration file (the `bp.conf` file on UNIX or the Windows registry). If the OpsCenter server name is configured against the `SERVER` option, the connection between the NetBackup master server and the OpsCenter server may not be established and data collection from the master server may fail.
- To collect data from a NetBackup 8.1 or later master server, ensure that insecure communication is allowed in NetBackup. Check if one of the following is true:
  - In the NetBackup Administration Console on the master server host, the Security Management > Global Security > Secure Communication > Enable insecure communication with NetBackup 8.0 and earlier hosts option is selected.
  - On the master server host, the `nbseccmd -setsecurityconfig -insecurecommunication` command-line option is set to ‘on’.
- In an OpsCenter cluster setup, to collect data from NetBackup, you need to add the host names of all nodes and the virtual name in the **NetBackup Administration Console**. Do the following:

1. Expand **NetBackup Management > Host Properties > Master Servers**.
2. Right-click **Servers** and then click **Properties**.
3. In the **Properties** pane, click **Servers**.
4. In the **OpsCenter Servers** tab, click **Add**.
5. In the **New Server** dialog box, specify the following:
   - Add the virtual name of the OpsCenter cluster and click **Add**.
   - Add the host name of an OpsCenter cluster node and click **Add**. Repeat the step for all OpsCenter cluster nodes.

The following sections describe the NetBackup data collection in detail:

- See “NetBackup data collection view” on page 274.
- See “How OpsCenter collects data from NetBackup” on page 275.
- See “About the Breakup Jobs option” on page 276.

- See "Viewing master server details and data collection status" on page 281.
- See "Adding a master server or appliance in OpsCenter" on page 285.
- See "Editing a master server or an appliance master server in OpsCenter" on page 292.
- See "Deleting a master server or an appliance master server in OpsCenter" on page 292.
- See "Controlling data collection for a master server in OpsCenter" on page 293.

Settings > Configuration > NetBackup options

A description of the **Settings > Configuration > NetBackup** options follows in the table.

Table 6-8 NetBackup options

Option	Description
Add/Edit/Delete	Select **Add** to add a NetBackup Master Server to the OpsCenter console. Note that you must first configure the master server to allow server access and data collection by OpsCenter. After configuring the master server, you must add this server to the OpsCenter console so that it can be monitored. See "Adding a master server or appliance in OpsCenter" on page 285. Select **Edit** to edit the properties of a master server. The master server name cannot be edited. Select **Delete** to delete one or more master servers from the OpsCenter console. Deleting a master server removes all the data that is associated with the master server from the OpsCenter database.
Disable/Enable Data Collection	Select **Disable Data Collection** or **Enable Data Collection** to disable or enable data collection from one or more NetBackup master servers.
Master Server Name	Name or IP address of the master server that is configured.
Display Name	The display name that you have chosen for the master server.
Operating System	Operating system of the master server.
Product	Backup product and version from where the data is collected.

Table 6-8 NetBackup options *(continued)*

Option	Description
Server Status	The master server can show any of the following states: ■ **Connected** ■ **Not Connected** ■ **Disabled** If the server status is 'Connected', the time since when the OpsCenter Server and the and master server are connected is also displayed. This does not necessarily represent the last time that OpsCenter collected information from the master server. See "NetBackup Master Server states in OpsCenter" on page 285.
Reason	Reason if any for the current server status.

NetBackup data collection view

This view is displayed when you select **Settings > Configuration > NetBackup** from the OpsCenter console. This view shows details of master servers.

The table that appears in this view shows the following columns:

Master Server Name Name or IP address of the master server that is configured.

Display Name The display name that you have chosen for the master server.

Operating System Operating system of the master server.

Product Backup product and version from where the data is collected.

Server Status The master server can show any of the following states:

- **Connected**
- **Not Connected**
- **Disabled**

If the server status is 'Connected', the time since when the OpsCenter Server and the NetBackup Master Server are connected is also displayed. This does not necessarily represent the last time that OpsCenter collected information from the master server.

See "NetBackup Master Server states in OpsCenter" on page 285.

Reason Reason if any for the current state.

How OpsCenter collects data from NetBackup

OpsCenter is used to monitor, manage, and report on NetBackup master and media servers, clients, and policies. To perform the monitoring, management, and reporting functions, OpsCenter collects data from the NetBackup master servers. The NetBackup data collection and management logic that OpsCenter uses is built into NetBackup master servers. This logic is included in the NetBackup Service Layer (NBSL).

Note: OpsCenter only uses the NBSL on master servers for data collection. Though NBSL is also included on media servers, OpsCenter does not use it. You must add only master servers to the OpsCenter console. You must not add any media servers to the OpsCenter console.

NBSL provides a single point of access to key NetBackup data, objects, and change events. The NetBackup UI also uses NBSL. NBSL runs as a service or daemon and has local configuration information, but no local database.

OpsCenter uses NBSL for all NetBackup monitoring, managing, and control functions. If NBSL service stops running on a managed NetBackup server, OpsCenter gets affected.

If NBSL stops, OpsCenter may not capture any changes that were made to the NetBackup configuration. When NBSL restarts, OpsCenter correctly recaptures the latest state.

See "Data collection status of a master server" on page 283.

The OpsCenter Server software collects data from NBSL in the following ways:

- Initial data load
- Listening for change notifications

Whenever OpsCenter server software starts, when data collection for a master server is enabled or when a master server is added to OpsCenter, the OpsCenter server starts collecting all the available data from NetBackup master server into the OpsCenter database using NBSL. The initial data load happens serially for each data type. As soon as the initial data load is complete, OpsCenter server software listens to the notifications from NBSL for any change in NetBackup data, and updates the OpsCenter database.

Note: Consider a scenario when you add a master server or when OpsCenter Server software starts after a long time, or when the data collection for a master server is enabled after a long time. In this case, it may take some time for the OpsCenter server to collect all data (such as media, jobs, images, drives etc.) from the NetBackup master server and insert it into the OpsCenter database.

Consider a scenario where a master server is already added on the OpsCenter console, and you uninstall and then reinstall NetBackup on the master server. In this case, you should disable the data collection (**Settings > Configuration > NetBackup**) before you uninstall NetBackup. Once NetBackup installation completes, you must enable the master server. Enabling the master server marks the existing master server as retired and also create a new master server with the freshly installed NetBackup.

See "Adding a master server or an appliance master server in the OpsCenter console" on page 291.

Note: After you install a NetBackup Master Server, you should enter the OpsCenter Server name in the NetBackup Host Properties.

See "Configuring a master server or appliance master server for server access and data collection by OpsCenter" on page 288.

Veritas Private Branch Exchange (PBX) is used for communication and requires a port to be opened on the OpsCenter server and the NetBackup master server for input and output. The default PBX port that is used is 1556. You cannot configure the PBX port in OpsCenter.

About the Breakup Jobs option

This section describes the NetBackup-specific Breakup Jobs option that you can set in OpsCenter while adding a master server. With the Breakup Jobs option, detailed file-level information like size and backup file count for each backup selection (associated with a NetBackup job) is collected and displayed as a part of custom reports in OpsCenter. The Breakup Jobs functionality is most effective if you have multiple backup selection lists in the NetBackup policy.

You can either enable or disable the breakup job option for master servers. When the Breakup Jobs option is enabled, OpsCenter collects a greater level of job detail at a file-system level. In addition to other job attributes, OpsCenter collects job attributes like size, file count, and directory name from the master server. For example, when the Breakup Jobs option is enabled, you can see how much data was backed up per file system.

See "Settings > Configuration > NetBackup > Add Master Server options" on page 290.

The Breakup Jobs functionality is disabled by default for master servers. To enable the Breakup Jobs functionality for master servers, you must configure the `scl.conf` file.

See "Configuring the Breakup Jobs option for master servers" on page 278.

Note: Enabling the Breakup Jobs option increases the load on the master server, the load on the Agent, and the time it takes to gather and load data in OpsCenter.

You can also configure the jobs for which you want to collect breakup job information. The job selection is based on the maximum number of files that a job backs up. By default, breakup job information is not collected for the jobs whose file count is greater than 1000000. This applies to all master server versions.

See "Configuring the Breakup Jobs option for master servers" on page 278.

Review the following considerations with respect to the Breakup Jobs functionality:

- The Breakup Jobs functionality is specific to NetBackup and does not apply to any other product.
- The Breakup Jobs data collection only happens for the jobs that are collected after you upgrade to OpsCenter. The breakup jobs data is not collected for the jobs that already exist in the OpsCenter database.
- The Breakup Jobs data collection happens through image IDs. Veritas recommends that you enable image data collection for the master server if you want to collect the breakup jobs data. The image data collection happens automatically by NBSL.
  You can enable image data collection while adding a master server.
  See "Adding a master server or an appliance master server in the OpsCenter console" on page 291.
- The Breakup Jobs option is only valid for the backup jobs whose Job State is **Done**.
- The breakup jobs data is collected directly from the master server by NBSL. The OpsCenter Agent is required if you want to collect breakup jobs data for the master server. The OpsCenter Agent uses the `bplist` command to collect data from the NetBackup master server.
  See "About planning an OpsCenter Agent deployment" on page 80.
- Data for the breakup jobs is collected from NetBackup after every 15 minutes.

- The Breakup Jobs functionality applies to OpsCenter Analytics only. The Breakup Jobs functionality cannot be used with Veritas NetBackup OpsCenter (free version).
- If you were using OpsCenter and applied the appropriate license keys for the licensed version (OpsCenter Analytics), breakup jobs may still not be displayed. To display breakup jobs, you must disable and then enable data collection for the master server from **Settings > Configuration**.
  See "Controlling data collection for a master server in OpsCenter" on page 293.

Configuring the Breakup Jobs option for master servers

The Breakup Jobs option for master servers is disabled by default. You can enable the Breakup Jobs option in the scl.conf file.

Note: Enabling the Breakup Jobs option increases the load on the master server and the time it takes to gather and load data in OpsCenter.

You can also configure the jobs for which you want to collect breakup job information. The job selection is based on the maximum number of files that a job backs up. By default, breakup job information is not collected for the jobs whose file count is greater than 1000000. This applies to all master server versions.

To enable the Breakup Jobs option for master servers

1. Log on to the OpsCenter Server host. Stop all OpsCenter Server services on Windows and UNIX:

   Windows INSTALL_PATH\OpsCenter\server\bin\opsadmin.bat stop

   UNIX <INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh stop

2. Open `scl.conf` file from the following directory on Windows and UNIX:

   Windows INSTALL_PATH\OpsCenter\Server\config\scl.conf

   UNIX <INSTALL_PATH>/SYMCOpsCenterServer/config

3 The Breakup Jobs option is disabled by default. To enable the Breakup Jobs option, add the following text to `scl.conf` file:

```
nbu.scl.collector.enableBreakupJobDataCollection=true
```

Note: To disable the Breakup Jobs option, add the following text to scl.conf file:

```
nbu.scl.collector.enableBreakupJobDataCollection=false
```

---

4 Save `scl.conf` file.

5 Restart all OpsCenter Server services on Windows and UNIX:

Windows	INSTALL_PATH\OpsCenter\server\bin\opsadmin.bat start
UNIX	<INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh start

To specify the maximum file size of jobs for Breakup Job data collection

1 Go to the OpsCenter Server host. Stop all OpsCenter Server services on Windows and UNIX:

Windows	INSTALL_PATH\OpsCenter\server\bin\opsadmin.bat stop
UNIX	<INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh stop

2 Open `scl.conf` file from the following directory on Windows and UNIX:

Windows	INSTALL_PATH\OpsCenter\Server\config\scl.conf
UNIX	<INSTALL_PATH>/SYMCOpsCenterServer/config

3 By default, breakup job information is not collected for the jobs that back up more than 1000000 files. However, you can configure the jobs for which you want to collect breakup job information based on the maximum number of files that a job backs up. This applies to all master server versions.

For example, if you do not want to collect breakup job information for the jobs that back up more than 20,000 files, add the following text to the scl.conf file:

nbu.scl.collector.breakupJobMaxFileCountPerJob=20000

Once you complete this procedure, breakup job information is not collected for the jobs whose file count is greater than 20000. This applies to all master servers.

4 Save `scl.conf` file.

5 Restart all OpsCenter Server services on Windows and UNIX:

Windows	INSTALL_PATH\OpsCenter\server\bin\opsadmin.bat start
UNIX	<INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh start

Viewing the data collection status for breakup jobs

You can also view the data collection status for breakup jobs data for a specific master server.

To view the breakup job data collection status for a master server

1 Go to the **Settings > Configuration > NetBackup** view in the OpsCenter console.

2 Click the master server from the **Master Server Name** column and then click the **Data Collection Status** tab.

3 To view the breakup jobs data collection status, check the status for the **SubJobs** data type.

About viewing breakup jobs data in custom reports

The Breakup Jobs option provides more granular-level reporting on the files that are backed up by NetBackup. You can see the breakup jobs data by creating custom reports in OpsCenter Analytics.

To view breakup jobs data in OpsCenter Analytics, ensure that the Breakup Jobs option is enabled in OpsCenter and then create a custom report of category **Backup/Recovery** and subcategory **Job/Image/Media/Disk** in a tabular format.

The custom report shows the following additional columns:

- Backup Sub Job File Count
- Backup Sub Job Size

In this example, you may notice some job directories named Other in addition to the actual job directories from NetBackup. The Other job directory exists in cases when the total backup size that we get from the primary job is different from the summation of the sizes of the individual files in the file list. To keep the total backup size consistent, a new job directory named Other is shown to make up the difference. Hence you see some additional file system objects named “Other” in OpsCenter other than the actual list that comes from NetBackup.

About breakup jobs considerations

Review the following considerations with respect to the Breakup Jobs functionality:

- OpsCenter does not provide the option to purge breakup jobs. In OpsCenter, the breakup jobs are tightly coupled with jobs and are purged along with the jobs.
- For a specific job ID in an OpsCenter custom report, breakup job data (like Backup Sub Job File Count, Backup Sub Job Size) is available only for 50 job directories. When a NetBackup policy or job has more than 50 backup selections, breakup jobs data for only 50 backup selections is available with NetBackup. The NetBackup GUI truncates data for the subsequent backup selections (greater than 50).
- OpsCenter Analytics does not show deduplication or snap duplication data for a specific job directory in the custom reports. OpsCenter Analytics does not show deduplication or snap duplication data because deduplication or snap duplication data for a backup selection is not available with NetBackup.

Viewing master server details and data collection status

Use the following procedure to view the details for a master server. The details for the master server are shown at the bottom of the **Settings > Configuration > NetBackup** view under the following tabs:

General	This tab displays the contents of many of the columns that are displayed in the table. See "About general details of master servers" on page 282.
Data Collection Status	This tab displays the collection status for each of the data types. The **Data Collection Status** tab is shown by default when you select **Settings** > **Configuration** > **NetBackup**. It also lists details like the time when the data load was last successful, when data collection last happened, and the exception message if the data collection failed for any of the data types. See "Data collection status of a master server" on page 283.

To view master server details and data collection status for a master server

1. In the OpsCenter console, select **Settings > Configurations > NetBackup**.
2. Click the name of the master server (link) from the **Master Server Name** column.

   The details for the master server are shown at the bottom of this view.

About general details of master servers

This section describes the general details that are displayed on the NetBackup data collection UI.

Table 6-9 provides general details about data collection for the selected NetBackup Master Server.

Table 6-9

Column	Description
Master Server Name	Name of the master server for which you want to view the collection status
Display Name	Display name of the master server for which you want to view the data collection status
Operating System	Operating system of the selected master server
Product	Version of the NetBackup software For example: Veritas NetBackup 7.7
Server Status	Status of the master server For example: Connected, Not Connected, or Disabled
The following additional fields are displayed when the master server status is Disconnected.	
Last Connection Attempt	The time when the connection between the OpsCenter Server and master server was last attempted.
Next Connection Attempt (Estimated)	The time when the connection between OpsCenter Server and master server is scheduled to establish. **Note:** This is an estimated time. The actual time may vary depending on the existing load on the OpsCenter Server.
Number of Connection Attempts	Number of attempts that are made to establish the connection between the OpsCenter Server and master server.

Data collection status of a master server

This section describes the NetBackup data types that OpsCenter collects and the different states for managed servers.

Table 6-10 gives a description of the contents in the **Data Collection Status** tab.

Table 6-10 Data Collection Status view

Column	Description
Data Type	The type of data that is collected from NetBackup. See "NetBackup data types and collection status" on page 283.
Last Successful Data Load	This column lists the date and time when the last successful data load happened for the specific data type.
Last Run Time	This column lists the date and time when data collection was attempted.
Next Run Time	This column lists the date and time when the data collection of the respective data type is attempted next. This is an estimated time. The actual time may vary depending on the existing load on the OpsCenter Server.
Collection Status	This column provides the status of each data load activity that OpsCenter requests.
Last Exception Message	This column lists the last exception message if data collection failed for a data type.

NetBackup data types and collection status

OpsCenter collects data for many NetBackup data types (such as Appliance Hardware, jobs, policy, media server, service, storage unit etc.) by using NBSL.

For most operations and changes in NetBackup, NBSL sends notifications to OpsCenter. For changes such as job, policy, services, and devices, the notification also contains the changed data. This data is stored in the OpsCenter database.

The following are the collection status for the different data types and their description:

Table 6-11 Collection statuses

Collection status	Description
Not Applicable	This status occurs when the master server version does not support the specific data type. This status also comes when you have not configured data collection for the following data types: ■ Error Logs ■ Image ■ Breakup Jobs You can enable data collection for these data types while adding or editing a master server under Advanced Data Collection Properties section. See "Adding a master server or an appliance master server in the OpsCenter console" on page 291. See "Editing a master server or an appliance master server in OpsCenter" on page 292. See "NetBackup Master Server states in OpsCenter" on page 285.
Not Started	The data collection for the specific data type has not started. This status appears when you initially add a master server or when you start the OpsCenter server.
Queued	The data collection for the specific data type is queued.
Running	The data collection for the specific data type is in progress.
Completed	The data collection for the specific data type is complete.
Failed	The data collection for the specific data type has failed. When the data collection fails, you can see the exception message from the **Last Exception Message** column. **Note:** Data collection can fail, and then start after some time. This is normal behavior. If data collection for a particular data type fails, it should be automatically started again within 10 minutes. All the functionality other than the functionality of the failed data type can be used normally while collection for a data type fails.
Not Licensed	This status is seen when the specific data type like FT is not licensed in NetBackup.

See "Data collection status of a master server" on page 283.

NetBackup Master Server states in OpsCenter

This section lists the different states that can exist for a master server and what they mean.

The master server can have any of the following states:

Table 6-12 Master server states

Master server state	Description
Connected	The master server is **Connected** when the data collection status for all data types is not **Failed**. This means that the collection status for all the data types must be any other status except **Failed**.
Not Connected	The master server is **Not Connected** when the data collection for all data types fails. This may be when there is a network issue because of which OpsCenter is not able to connect and collect data from NetBackup. **Note:** Data collection can fail, and then start after some time. This is normal behavior. If data collection for a particular data type fails, it should be automatically started again within 10 minutes. All the functionality other than the functionality of the failed data type can be used normally while collection for a data type fails.
Disabled	The master server is **Disabled** when the data collection for the selected master server is disabled.

Adding a master server or appliance in OpsCenter

To allow OpsCenter to communicate with a managed NetBackup server and collect data requires some security configuration. OpsCenter can monitor the master servers which have NetBackup Access Control (NBAC) configured and also those servers that do not have NBAC configured.

Note: Veritas recommends that any NetBackup master server or appliance master server is monitored by only one OpsCenter Server.

Use the following steps to add a master server or an appliance master server. Note that you must first configure the master server to allow server access and data collection by OpsCenter. After configuring the master server, you must add this server to the OpsCenter console so that it can be monitored.

Note: You cannot add an appliance media server to the OpsCenter console. To monitor an appliance media server, you can add a master appliance or a regular master server to which it is connected.

To add a master server or an appliance master server

1. Configure your managed master server or appliance master server to allow server access and data collection by OpsCenter.

   See "Configuring a master server or appliance master server for server access and data collection by OpsCenter" on page 288.

2. After configuring the master server or appliance master server, you must add the master server or appliance to the OpsCenter console so that it can be monitored.

   See "Adding a master server or an appliance master server in the OpsCenter console" on page 291.

Note: You can use an alternate procedure to add a NetBackup master server to OpsCenter. This procedure can be used for both NBAC and non-NBAC servers.

See "Adding a NetBackup master server" on page 286.

Adding a NetBackup master server

Use the following procedure to add a NetBackup master server or a NetBackup Appliance master server to the OpsCenter console. This procedure can be used for both NBAC and non-NBAC servers.

In case of a clustered NetBackup setup, use this procedure for each node of the cluster.

To add a NetBackup master server or appliance master server to the OpsCenter console on Windows and UNIX

1. Log on to the managed master server or NetBackup Appliance master server as `Administrator` or `root` for Windows and UNIX respectively.

2. Browse to the following NetBackup installation directory:

Windows	*INSTALL_PATH*/bin/admincmd
UNIX	*INSTALL_PATH*/bin/admincmd

3 Run the following command on the master server or the appliance master server:

```
nbregopsc -add <Name of the OpsCenter Server>
```

The `nbregopsc` command registers OpsCenter with the current master server and adds this master server to OpsCenter. This command also establishes a trust relationship from the authentication broker of NetBackup master server to the authentication broker of OpsCenter server.

4 If OpsCenter is of an earlier version and the master server is NBAC-enabled, a trust relationship must be established from the authentication broker of the OpsCenter server to the authentication broker (AB) of the NetBackup master server. OpsCenter cannot monitor NetBackup servers if the trust relationship has not been set up between OpsCenter and NetBackup server.

To establish the trust relationship, log on as `Administrator` or `root` on the OpsCenter server host and navigate to the following OpsCenter installation directory:

Windows	*INSTALL_PATH*\server\authbroker\bin
UNIX	*INSTALL_PATH*/SYMC/Opscenter/Server/authbroker/bin

On the OpsCenter server host, run the following command depending on your specific master server version:

7.0 and 7.0.1 master server	`vssat setuptrust --broker <MasterServerhost:2821> --securitylevel high`
7.1 or later master server or appliance master server	`vssat setuptrust --broker <MasterServerhost:13783> --securitylevel high`
7.6 or later master server or appliance master server	`vssat setuptrust --broker <MasterServerhost:2821> --securitylevel high` This is an optional step for OpsCenter 7.6 and later versions.

Note that *<MasterServerhost>* is the name of the master server.

5 Restart all the NetBackup services (processes).

In case you add an appliance 2.0 master server, check if OpsCenter can connect to the appliance master server. Restart all appliance services or processes only if OpsCenter cannot connect to the Appliance master server.

Note: In case running the `nbregopsc` command fails, you must manually add the master server or the appliance master server to the OpsCenter console.

See "Adding a master server or an appliance master server in the OpsCenter console" on page 291.

---

6 Once you perform this procedure, the master server is automatically added to the OpsCenter console.

Configuring a master server or appliance master server for server access and data collection by OpsCenter

Use the following procedures to configure a master server or an appliance master server for data collection by OpsCenter on Windows and UNIX. This procedure applies to both NBAC and non-NBAC master servers.

In case of a clustered NetBackup setup, use this procedure on each node of the cluster.

You can use an alternate procedure to configure an appliance master server for data collection by OpsCenter.

See "Adding a master server or an appliance master server in the OpsCenter console" on page 291.

To configure a master server or appliance master server for server access and data collection on Windows and UNIX

1 Log on to the managed master server or the appliance master server as `Administrator` or `root` on Windows and UNIX respectively.

2 Start the **NetBackup Administration Console**.

3 Expand **NetBackup Management** > **Host Properties** > **Master Servers**.

4 Double-click the master server name to view its properties. The **Master Server Properties** dialog box appears.

5 For a NetBackup server, select the **Servers** tab and then the **OpsCenter servers** tab from the **Master Server Properties** dialog box. The **OpsCenter servers** tab displays all of the **OpsCenter** servers that can access the currently selected NetBackup master server.

Note: In a clustered OpsCenter setup, ensure that you add the host names of all clustered OpsCenter nodes and the virtual name in the **OpsCenter Servers** tab.

---

6 To add the OpsCenter server to the server list, click **Add**. The **Add a New Server Entry** dialog box appears.

7 Type the OpsCenter server name in the field and click **Add** to add the server to the list.

Ensure that the OpsCenter server name that you add is reachable from the NetBackup server.

8 Click **Close**.

9 In the **Master Server Properties** dialog box, click **OK**.

10 Ignore this step for master servers on which NBAC is not configured.

If the master server is NBAC-enabled, a bi-directional trust relationship must be established between the authentication broker of the OpsCenter server and the authentication broker(AB) of each managed NetBackup server. OpsCenter cannot monitor NetBackup servers if the trust relationship has not been set up between OpsCenter and NetBackup server (NBAC enabled).

To set up these trust relationships, use the `vssat` command in Veritas Product Authentication Service. Run this command from `%Program Files%\Veritas\Security\Authentication\bin` directory in Windows or *`INSTALL_PATH`*`/VRTSat/bin` in UNIX.

On the NetBackup master server or the appliance master server host, run the following command:

```
vssat setuptrust --broker OpsCenter
hostname:1556:OPSCENTER_PBXSSLServiceID --securitylevel high
```

where <*OpsCenterABhost*> is same as the host where OpsCenter server is installed. However if OpsCenter is installed in a clustered mode, then <*OpscenterAB*> is the host name that is provided as the remote authentication broker host during the OpsCenter installation.

Similarly, log on as `Administrator` or `root` on the OpsCenter server host and run the following command depending on your specific master server version:

In case of NetBackup 7.6 master server and of later versions, this is an optional step.

7.0 and 7.0.1 master server	`vssat setuptrust --broker <MasterServerhost:2821> --securitylevel high`
7.1 or later master server	`vssat setuptrust --broker <MasterServerhost:13783> --securitylevel high`

where <*MasterServerhost*> is the name of the master server.

11 Restart all the NetBackup services.

12 Add this master server to the OpsCenter console, so that it can be monitored.

See "Adding a master server or an appliance master server in the OpsCenter console" on page 291.

Settings > Configuration > NetBackup > Add Master Server options

Enter the details for the master server on the Add NetBackup Master Servers page.

Table 6-13 NetBackup Master Server options

Option	Description
Master Server Name	Enter a host name or an IP address of the master server or appliance master server. This field is required. In case the master server is clustered, enter the virtual name of the master server. **Note:** You cannot add an appliance media server directly to the OpsCenter console.
Display Name	Enter an alternate name for the master server or appliance master server. The display name is used for the master server on all views of the OpsCenter console.
NetBackup User Name	Enter a valid NetBackup user name.
NetBackup Password	Enter the NetBackup password. **Note:** OpsCenter uses the NetBackup bpjava protocol to collect some of the data types from NetBackup. The bpjava protocol requires NetBackup credentials.

Click the **Test Connection** button to validate the NetBackup credentials.

Click the **Save and Add More** button to add more master servers. Click the **Save and Close** button to save the settings. Click the **Cancel** button to cancel the settings.

Note: The data for image, error log, capacity license, traditional license, and breakup jobs is used in OpsCenter reports.

NBSL and bpjava protocol are used to automatically collect NetBackup data.

Adding a master server or an appliance master server in the OpsCenter console

You must add a master server or an appliance master server to the OpsCenter console so that it can be monitored. Use the following procedure to add a master server or an appliance master server.

To add a master server or an appliance master server

1. In the OpsCenter console, select **Settings > Configurations > NetBackup** .
2. Click **Add**.

3 Enter the required details for the master server.

See "Settings > Configuration > NetBackup > Add Master Server options" on page 290.

4 Click the **Test Connection** button to validate the information that you entered. This would validate the credentials for the master server.

5 Click **Save and Add more** to save the master server and to add more master servers.

6 Click **Save and Close** to save the master server.

Alternately, you can click **Cancel** to exit.

7 In case you add an appliance 2.0 master server, restart all appliance services or processes only if OpsCenter cannot connect to the Appliance master server. See the Appliance documentation for details on how to restart services.

Editing a master server or an appliance master server in OpsCenter

Use the following procedure to change the configuration information for a NetBackup master server or an appliance master server.

To edit a master server or an appliance master server

1 In the OpsCenter console, select **Settings > Configurations > NetBackup**.

2 Use the checkbox to select a master server or an appliance master server from the **Master Server Name** column.

3 Click **Edit**.

4 Edit the information that is displayed on the **Edit Master Server** page.

A description of the fields present in these sections is available.

See "Adding a master server or an appliance master server in the OpsCenter console" on page 291.

Note that you cannot edit the **Master Server Name** for the master server. The **Master Server Name** field falls under the **NetBackup Master Server Details** section.

5 Click **Save**.

Deleting a master server or an appliance master server in OpsCenter

You can delete one or more master servers or appliance master servers using the following procedure. Note that deleting a master server deletes all the data that is associated with the master server.

Note: Deleting a master server may take some time.

To delete a master server

1. In the OpsCenter console, select **Settings > Configurations > NetBackup** .
2. Use the checkbox to select one or more master servers from the **Master Server Name** column.
3. Click **Delete**.
4. The following warning message appears:

   ```
   Deletion of the selected master server(s)
   will delete all related data. Do you want to proceed?
   ```

   Click **OK**.

Controlling data collection for a master server in OpsCenter

You can disable or enable OpsCenter data collection for a particular managed NetBackup master server or an appliance master server depending on your needs.

Note: If you disable data collection it may appear to be a loss of data in OpsCenter. For example, a drive may have the same status until you enable OpsCenter data collection again.

To disable data collection for a master server

1. In the OpsCenter console, select **Settings > Configurations > NetBackup**.
2. Use the checkbox to select one or more master servers from the **Master Server Name** column.
3. Click **Disable Data Collection**.

To enable data collection for a master server

1. In the OpsCenter console, select **Settings > Configurations > NetBackup** .
2. Use the checkbox to select one or more master servers from the **Master Server Name** column.
3. Click **Enable Data Collection**.

Configuring Backup Exec data collector

This section describes data collection from Backup Exec.

Caution: The Backup Exec data collector requires the following component to be installed on the OpsCenter Agent host, to collect data properly.

Microsoft Visual C++ 2005 SP1 Redistributable Package (x86) that is vcredist_x86.exe

VC Redistributable Package is available at:

http://www.microsoft.com/downloads/details.aspx?familyid=200B2FD9-AE1A-4A14-984D-389C36F85647&displaylang=en

Once you install this component on the Agent host, configure the Backup Exec data collector as described in the following section.

To configure Backup Exec data collector

1. Click **Settings > Configuration > Agent**.
2. On the **Agent** list, select a check box in front of the Agent, for which you want to configure a Data Collector.
3. Click **Create Data Collector**.
4. On the **Create Data Collector: Product Selection** page, select Veritas Backup Exec from the **Select Product** drop-down list.
5. In the **Target Host Name** text box, enter the Backup Exec server host name, from which you want to collect data.
6. Click **Next**.
7. On the **Create Data Collector: Details** page, specify the following Backup Exec data collector configuration settings:

User name	Enter the name of the user account that is required to connect to the Backup Exec Database .
Password	Enter the password of this user account.
Version	Select the version of the Veritas Backup Exec Server - 11.x or 12.x - from which you want to collect data.

8. Select blackout period details, data types to be collected, and collection interval.

   For more details on collection interval, and other data collector settings, refer to the following section:

   See " Configuring an OpsCenter Data Collector" on page 268.

9. Click **Save**.

Collecting data from PureDisk

OpsCenter supports collection of data from Veritas NetBackup PureDisk. The collected data is stored in the OpsCenter database, based on which you can generate reports. OpsCenter can collect Policy & Schedule and Job data types from PureDisk Storage Pool Authority (PureDisk SPA).

For more details on PureDisk, refer to the *NetBackup PureDisk documentation*.

PureDisk SPA and its components that run on the PureDisk operating system (PDOS). The Single Instance Storage (SIS) or deduplication technology of NetBackup PureDisk is unique in storage and backup industry. PureDisk identifies files and the data segments that contain identical data and treats them as a single instance of a file, which it backs up only once. This lets you save storage space. Attributes of identical files, such as name and date of modification can vary.

While backing up a file, PureDisk determines whether multiple instances of the file are present on hosts across the network, including remote hosts. By using the deduplication technology, PureDisk stores only one instance of the file.

Table 6-14 describes the steps that you need to carry out to collect data from PureDisk.

Table 6-14 Steps to collect data from PureDisk

Step number	Step	Reference topic
Step 1	Install OpsCenter server. **Note:** When you install OpsCenter server,OpsCenter Integrated Agent is also installed and configured, which you can use to collect only PureDisk data. To collect PureDisk data, you do not need to manually install or configure OpsCenter Agent. You cannot delete the Integrated Agent. **Note:** You can collect PureDisk data only through the OpsCenter Integrated Agent.	See "Installing OpsCenter on Windows and UNIX" on page 87.
Step 2	You need to establish trust between the authentication brokers of OpsCenter and PureDisk SPA for secure communication. Setting up trust is a pre-requisite for PureDisk data collection from OpsCenter.	See "Setting up a trust between the PureDisk SPA host and the OpsCenter OpsCenter host" on page 296.

Table 6-14 Steps to collect data from PureDisk *(continued)*

Step number	Step	Reference topic
Step 3	Using the OpsCenter console, configure PureDisk data collector for the Integrated Agent.	See "Configuring PureDisk data collector" on page 297.

See "Setting up a trust between the PureDisk SPA host and the OpsCenter OpsCenter host" on page 296.

See "Configuring PureDisk data collector" on page 297.

Setting up a trust between the PureDisk SPA host and the OpsCenter OpsCenter host

You need to set up trust between the PureDisk SPA host the and OpsCenter host. Establishing trust is a pre-requisite for PureDisk data collection from OpsCenter.

Note: OpsCenter host is the host where the OpsCenter server is installed. However, if OpsCenter is installed in a clustered mode, then the OpsCenter host is the host name that was provided as the remote authentication broker host during the OpsCenter installation.

The OpsCenter host name is stored in the `vxss.hostname` parameter in the following file:

On Windows: *`INSTALL_PATH`*`\server\config\security.conf`

On UNIX: *`INSTALL_PATH`*`/SYMCOpsCenterServer/config/security.conf`

This section provides the manual steps that you need to carry out on the PureDisk SPA host, to setup trust between the PureDisk SPA host and the OpsCenter authentication broker host.

To set up a trust between PureDisk SPA host and OpsCenter host

1 On the PureDisk SPA host, logon as root and run the following command:

```
su www-data
```

2 As a “www-data” user, run the following command:

```
INSTALL_PATH/VRTSat/bin/vssat setuptrust --broker
OpsCenterhost:1556:OPSCENTER_PBXSSLServiceID --securitylevel low
```

After successfully setting up a trust between the PureDisk SPA host and the OpsCenter host, the following message is displayed:

```
setuptrust

----------------------

----------------------

Setup Trust With Broker: OpsCenterhost
```

After setting up the trust between OpsCenter Server host and PureDisk SPA host, logon to the OpsCenter GUI and configure PureDisk data collector to start collecting PureDisk data.

See “Configuring PureDisk data collector” on page 297.

Configuring PureDisk data collector

This section provides the procedure to configure NetBackup PureDisk data collector on the OpsCenter GUI.

To configure NetBackup PureDisk data collector

1 Click **Settings > Configuration > Agent**.

2 On the **Agent** list, select a check box in front of the Integrated Agent.

When you install OpsCenter server,OpsCenter Integrated Agent is also installed and configured, which you can use to collect only PureDisk data. To collect PureDisk data, you do not need to manually install or configure OpsCenter Agent.

You can collect PureDisk data only through the OpsCenter Integrated Agent.

3 Click **Create Data Collector**.

4 On the **Create Data Collector: Product Selection** page, select NetBackup PureDisk from the **Select Product** drop-down list.

5 In the **Target Host Name** text box, enter the PureDisk SPA Server host name, from which you want to collect data.

6 Click **Next**.

7 On the **Create Data Collector: Details** page, specify the following PureDisk configuration settings:

Product Version	Select any of the following NetBackup PureDisk versions from the drop-down list: 6.2, 6.2.1, 6.2.2, 6.5, 6.5.0.1, 6.5.1, 6.6, 6.6.0.1, 6.6.0.2, 6.6.0.3

For more details on collection interval, and other data collector settings, refer to the following section:

See " Configuring an OpsCenter Data Collector" on page 268.

8 Click **Save**.

Setting up a trust between the OpsCenter authentication broker host and PureDisk SPA host is accomplished automatically after PureDisk data collector is configured. If it is not successful, you need to do it manually.

Refer to Setting up a trust between the OpsCenter AB host and PureDisk SPA host in the *OpsCenter Administrator's Guide*.

Chapter 7

Managing OpsCenter views

This chapter includes the following topics:

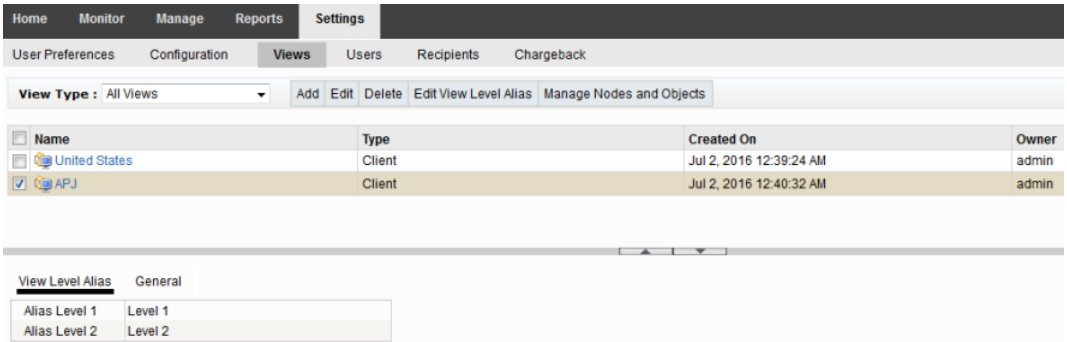
- About OpsCenter views
- About managing OpsCenter views
- About managing nodes and objects in OpsCenter
- Adding nodes to a view in OpsCenter
- Modifying node details in OpsCenter
- Deleting nodes in OpsCenter
- Adding objects to a view node in OpsCenter
- Deleting objects from a view node in OpsCenter
- View filters in OpsCenter
- Setting up logging for OpsCenter View Builder

About OpsCenter views

Veritas NetBackup OpsCenter views are logical groups of IT assets (master servers or clients) organized in a hierarchical manner. A Security Administrator or an Administrator can create views either from OpsCenter console or the OpsCenter View Builder (formerly called Java View Builder) and make them available in the OpsCenter console.

Figure 7-1 shows the details that are displayed on the **Views** tab in the OpsCenter console.

Figure 7-1 The Views tab



Note: Only a Security Administrator or an Administrator can create or modify views.

See "User access rights and functions in OpsCenter user interface" on page 231.

In an OpsCenter view, IT assets that are scattered across organization can be arranged according to their locations, business units, or applications. You can generate various OpsCenter reports that are filtered by views. With these reports, you can identify the locations or departments with hosts storing business critical data.

After you install and run the OpsCenter Server and the OpsCenter Agent, OpsCenter detects the IT assets, which are then stored in the database. The OpsCenter View Builder makes these IT assets available when a view is created.

Note: To run the OpsCenter View Builder, you need Java Runtime Environment (JRE) installed on the host.

In a view hierarchy, between top and bottom levels you can create a number of user-defined levels. An OpsCenter view is a homogeneous one, it cannot have hosts and file systems in the same tree.

Settings > Views options

OpsCenter displays all view types that are supported by OpsCenter View Builder (like File System) on the **Settings > Views** pane. However, you cannot perform operations like add, edit, delete, manage nodes and objects from the OpsCenter GUI on view types like File System. Use the OpsCenter View Builder to add, edit, delete, or manage these view types.

You can manage only the Master Server, Client, and Policy view types using the OpsCenter GUI.

A description of the **Views** tab options follows in the table.

Table 7-1 Views tab options

Option	Description
View Type	Select the type of view from the drop-down list. The options are All Views, Client, Master Server, and Policy. See "OpsCenter view types" on page 302.
Add/Edit/Delete	Select to add new views, or to edit and delete the available views. These options are available only when you log on as a Security Administrator or an Administrator. In addition, you can add, edit, or delete only the Master Server, Client, and Policy view types using the OpsCenter GUI. You can only delete the File System view type. However, you cannot add a new or edit an existing File System view in OpsCenter GUI
Edit View Level Alias	Select to edit the view level aliases. This option is available only when you log on as a Security Administrator or an Administrator. This option is available only for Master Server, Client, and Policy view types. The **Edit View Level Alias** option is disabled if you select any other view type like File System.
Manage Nodes and Objects	Select to view the objects on the node and objects that are not in the selected view. This option is available only when you log on as a Security Administrator or an Administrator. This option is available only for Master Server, Client, and Policy view types. The **Manage Nodes and Objects** option is disabled if you select any other view type like File System.
Name	Displays the names of the views that you can access.
Type	Displays the view type. OpsCenter displays all view types that are supported by OpsCenter View Builder like File System on the **Settings > Views** pane.
Created On	Displays the date and time when the view was created.
Owner	Displays the role of the user who created the view.

Two tabs appear in the **Details** pane of the **Settings > Views** page.

Table 7-2 Settings > Views Details pane tabs

Option	Description
View Level Alias tab	This tab shows the details of view level aliases of the selected view. Default view level aliases are as follows: Level 1, Level 2, and so on. The **View Level Alias** tab does not contain any data, if you have not added any nodes or objects to the selected view. Only a Security Administrator or an Administrator can modify the view level aliases. See "Modifying alias view levels in OpsCenter" on page 309.
General tab	The **General** tab displays the following details: ■ Name of the selected view ■ Description of the view ■ Date and time when the view was created ■ Name of the user who has created this view

See "About OpsCenter views" on page 299.

OpsCenter view types

In OpsCenter, each view is associated with a view type. Depending on the type of the view, objects are made available for assigning to that view.

You can create views of the following types from the OpsCenter console:

Client — If you create a view of type Client, only backup clients are available to be assigned to the view.

Master server — If you create a view of type Master Server, only Master Servers are available to be assigned to the view.

Policy — If you create a view of type Policy, only policies are available to be assigned to the view.

Note: Use the OpsCenter View Builder to create any other view types.

OpsCenter user interface access for specific view types

You may not see data in some tabs or subtabs when you have selected specific views. This is because data for those tabs is not applicable for the specific view types. For example, a Client view should display data that is relevant to Client objects only and not show any unrelated data like media or services.

In such a scenario, you see the following error message:

```
Data is not applicable for the view that you have selected. Click UI
access for specific view types for details about the applicable view
types.
```

Table 7-3 lists if data in specific tabs or subtabs is applicable when you select a view of a specific view type like Master Server, Policy, or Client.

Table 7-3 Tab access for specific view types

Tab	Subtab	Master Server view	Policy view	Client view
Monitor				
	Overview	Yes	Yes	Yes
	Jobs	Yes	Yes	Yes
	Services	Yes	No	No
	Policies	Yes	Yes	Yes
	Media	Yes	No	No
	Devices (all subtabs)	Yes	No	No
	Hosts > Master Server	Yes	No	No
	Hosts > Media Server	Yes	No	No
	Hosts > Client	Yes	No	Yes
	Alerts	Yes	Yes	Yes
	Audit Trails	Yes	No	No
	Cloud	Yes	No	No

Table 7-3 Tab access for specific view types *(continued)*

Tab	Subtab	Master Server view	Policy view	Client view
	Appliance Hardware	Yes	No	No
Manage				
	Alert Policies	Yes	Yes	Yes
	Storage > Storage Unit	Yes	No	No
	Storage > Storage Unit Group	Yes	No	No
	Storage > Storage Lifecycle Policy	Yes	No	No
	Devices (all subtabs)	Yes	No	No
	Hosts	Yes	No	No

Note: Manage > Restore and **Manage > NetBackup Licensing** tabs are not dependent on any view selection. The content in these tabs is shown for all views.

About access rights for a view

While creating an OpsCenter view, a Security Administrator can specify the access rights for that view.

Note: An Administrator can specify the access rights for a view from the OpsCenter View Builder.

See "Creating OpsCenter views" on page 307.

Table 7-4 lists the default access levels for specific OpsCenter or OpsCenter View Builder roles.

Table 7-4 Default access levels

JVB Role	OpsCenter Role	Permitted View	ALL MASTER SERVER View
admin	Security Administrator	RW	R
	Administrator	RW	R
User	Reporter	P	P
	Restore Operator	P	P
	Operator	P	P

In this table, RW stands for Read and Write permission, R stands for Read permission, and P stands for Needs Permission. The Analyst user role is no longer available.

An Operator, Reporter, or Restore Operator cannot create or modify views. They also need permission to access a view.

The concept of public or private views that existed earlier has been removed in OpsCenter 7.5. An Operator or Reporter now only has Read access for all prior public views. An Analyst is upgraded to OpsCenter 7.5 as a Reporter.

The following table describe the permissions available to a user for a public or private view after he or she upgrades.

Table 7-5 Permissions available after upgrade

Role	Public View		Private View	
	Existing	After Upgrade	Existing	After Upgrade
Security Administrator	RW	RW	RW	RW
Administrator	RW	RW	RW	RW
Operator	RW	R	RW	R
Reporter	RW	R	RW	R

About OpsCenter view levels

A newly created view has only one level. You can add multiple nodes to a view at different levels. You can add alias for each of these view levels.

Only a Security Administrator or an Administrator can modify views.

See "Modifying alias view levels in OpsCenter" on page 309.

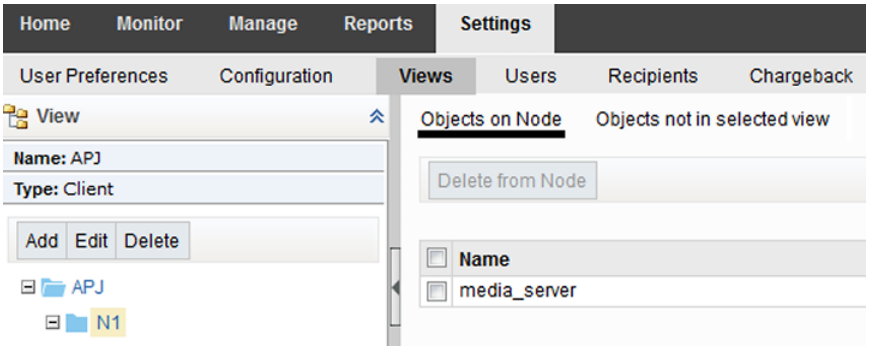
Master server hosts, clients, or policies are always at the lowest levels in a view. Between the top level and the bottom level, you can create multiple intermediate levels to organize view objects into logical groups, creating a hierarchical structure in the view.

About nodes and objects

An OpsCenter view comprises nodes and view objects. A node is a logical entity that you add to create a hierarchical structure of a view. Between the first level (the view name itself) and the last level (actual view object), you can add multiple nodes.

Figure 7-2 shows an example of a view comprising multiple nodes and objects.

Figure 7-2 View nodes and objects



About managing OpsCenter views

The following topics provide procedures to add, edit, or delete OpsCenter views.

See "Looking at OpsCenter views and their details" on page 307.

See "Creating OpsCenter views" on page 307.

See "Modifying OpsCenter views" on page 308.

See "Deleting OpsCenter views" on page 309.

See "Modifying alias view levels in OpsCenter" on page 309.

Settings > Views > Manage Nodes and Objects options

A description of the **Settings > Views > Manage Nodes and Objects** options follows in the table.

Table 7-6 Settings > Views > Manage Nodes and Objects options

Option	Description
Objects on Node tab	The objects that are assigned to the current view or view node are displayed on the **Objects on Node** tab.
Objects not in selected view tab	The **Objects not in selected view** tab shows all host objects that are not a part of the selected view or view node. The available objects list varies depending on the view type. For example: If the view is of type **Client**, only client hosts are available on the **Objects not in selected view** tab for selection.

Looking at OpsCenter views and their details

This topic provides the procedure to see OpsCenter views.

See "About OpsCenter views" on page 299.

To look at OpsCenter views

1. In the OpsCenter console, click **Settings > Views**. A list of views that you are permitted to access is displayed.

   See "Modifying OpsCenter views" on page 308.

   See "Creating OpsCenter views" on page 307.

2. To check the details of a view, select the view from the views list. The **View Level Alias** and **General** details are displayed in the lower section of the page.

   See "Settings > Views options" on page 300.

Creating OpsCenter views

This topic provides the procedure to create a view using OpsCenter. Only a Security Administrator or an Administrator can create views.

Veritas recommends that while creating a view, the lowest level of the view should be an object that is created by a data collector like a master server, policy, client and so on. For example, if you create a view called Geography, the lowest level can be an object like abc.veritas.com or xyz.veritas.com and not any other hypothetical object like Region, Continent and so on.

Example:

```
Geography

 | - US

    |- - Colorado

           |- - - abc.veritas.com
```

In this example, US, and Colorado are hypothetical nodes (which are not associated with any data collector), and the lowest-level of the view is abc.veritas.com which is an object created by a data collector. You can create such views.

You should not create any view like the following where the lowest level of the view is a hypothetical object like Denver:

```
Geography

 | - US

    |- - Colorado

           |- - - xyz.veritas.com

                |- - - - Denver
```

To create an OpsCenter view

1. Log on to the OpsCenter console as a Security Administrator or an Administrator.
2. In the OpsCenter console, click **Settings > Views**.
3. Click **Add**.
4. On the **Add View** dialog box, specify the view details.
5. Click **OK**.

Modifying OpsCenter views

This topic provides the procedure to modify view details. Only a Security Administrator or an Administrator can modify views.

Note: The ALL MASTER SERVERS view cannot be modified.

To modify OpsCenter views

1. Log on to the OpsCenter console as a Security Administrator or an Administrator.
2. In the OpsCenter console, click **Settings > Views**.
3. From the list of views, select a view that you want to modify.
4. Click **Edit**.
5. On the **Edit View** dialog box, you can modify the view details.
6. Click **OK**.

Deleting OpsCenter views

This topic provides the procedure to delete views. Only a Security Administrator or an Administrator can modify views.

Only Master Server, Client, and Policy view types can be deleted using the OpsCenter GUI.

Note: Once you have deleted a view, it cannot be recovered. If you delete a view, all its nodes are deleted and the objects are moved to the unassigned tree.

Note: The ALL MASTER SERVERS view cannot be deleted.

To delete OpsCenter views

1. Log on to the OpsCenter console as a Security Administrator or an Administrator.
2. In the OpsCenter console, click **Settings > Views**.
3. From the list of views, select a view that you want to delete.
4. Click **Delete**.

Modifying alias view levels in OpsCenter

This topic provides the procedure to modify alias of view levels. Only a Security Administrator or an Administrator can modify views.

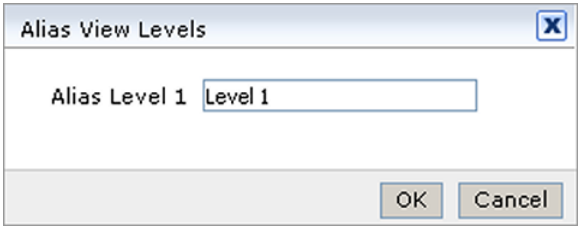
Only Master Server, Client, and Policy view types can be modified using the OpsCenter GUI.

See “Adding nodes to a view in OpsCenter” on page 311.

See “About managing nodes and objects in OpsCenter” on page 310.

To modify alias view levels in OpsCenter

1. Log on to the OpsCenter console as a Security Administrator or an Administrator.
2. In the OpsCenter console, click **Settings > Views**.
3. From the list of views, select a view for which you want to modify view level alias.
4. Click **Edit Alias View Levels**.
5. On the **Alias View Levels** dialog box, text boxes for entering aliases for all available view levels appear. For example, if the selected view has only one level, the **Alias View Levels** dialog box appears as follows:



6. Rename the available levels. For example, if the selected view has three levels, you can rename the levels as follows: rename Alias Level 1 as Geography, Alias Level 2 as Country, and Alias Level 3 as Region.
7. Click **OK**.

About managing nodes and objects in OpsCenter

The following topics provide procedures to create, modify, and delete nodes and objects related to a view.

Only Master Server, Client, and Policy view types can be managed using the OpsCenter GUI.

Note: The ALL MASTER SERVERS view cannot be modified.

See "Adding nodes to a view in OpsCenter" on page 311.

See "Modifying node details in OpsCenter" on page 311.

See "Deleting nodes in OpsCenter" on page 312.

See "Adding objects to a view node in OpsCenter" on page 312.

See "Deleting objects from a view node in OpsCenter" on page 313.

See "View filters in OpsCenter" on page 314.

Adding nodes to a view in OpsCenter

This topic provides the procedure to add a node to a view. Only a Security Administrator or an Administrator can modify views.

See "About nodes and objects" on page 306.

To add nodes to a view

1. Log on to the OpsCenter console as a Security Administrator or an Administrator.
2. In the OpsCenter console, click **Settings > Views**.
3. From the list of views, select a view to which you want to add nodes and objects.
4. Click **Manage Nodes and Objects**.
5. On the view tree, select the view to which you want to add a node.
6. Click **Add**.
7. On the **Add** dialog box, enter the node name.
8. Click **OK**.

Modifying node details in OpsCenter

This topic provides the procedure to modify the information of a view node. Only a Security Administrator or an Administrator can modify views.

See "Adding nodes to a view in OpsCenter" on page 311.

To modify node information

1. Log on to the OpsCenter console as a Security Administrator or an Administrator.
2. In the OpsCenter console, click **Settings > Views**.
3. From the list of views, select a view to modify the information of associated nodes.
4. Click **Manage Nodes and Objects**.
5. On the view tree, expand the view to see the associated nodes.
6. Select the node that you want to modify.
7. Click **Edit**.

8 On the **Edit** dialog box, modify the name of the node.

9 Click **OK**.

Deleting nodes in OpsCenter

This topic provides the procedure to delete the nodes from a view. Only a Security Administrator or an Administrator can modify views.

See "Adding nodes to a view in OpsCenter" on page 311.

To delete a node

1 Log on to the OpsCenter console as a Security Administrator or an Administrator.

2 In the OpsCenter console, click **Settings > Views**.

3 From the list of views, select a view from which you want to delete nodes.

4 Click **Manage Nodes and Objects**.

5 On the view tree, expand the view to see the associated nodes.

6 Select the node that you want to delete.

7 Click **Delete**.

8 On the confirmation dialog box, click **OK**.

Adding objects to a view node in OpsCenter

This topic provides the procedure to add objects to a view or a node within a view. Only a Security Administrator or an Administrator can modify views.

To add an object to a view node

1 Log on to the OpsCenter console as a Security Administrator or an Administrator.

2 In the OpsCenter console, click **Settings > Views**.

3 From the list of views, select the view to which you want to add objects.

4 Click **Manage Nodes and Objects**.

5 On the view tree, select the view name or a view node to which you want to add an object.

6 In the right-hand pane, select the **Objects not in selected view** tab. The available objects list varies depending on the view type.

For example: If the view is of type **Client**, only client hosts are available on the **Objects not in selected view** tab for selection.

The **Objects not in selected view** tab shows all host objects that are not a part of the selected view or view node.

You can filter the objects that are not in the selected view with the help of default filters. Or you can create new filters and apply them to view the required objects on the tab.

See "View filters in OpsCenter" on page 314.

7 Select the check boxes in front of the view objects that you want to add to the selected view or view node.

8 Click **Add to Node**.

The added view objects are removed from the **Objects not in selected view** tab and appear on the **Objects on Node** tab.

Deleting objects from a view node in OpsCenter

This topic provides the procedure to delete the objects from a view or a view node. Only a Security Administrator or an Administrator can modify views.

To delete an object from a view node

1 Log on to the OpsCenter console as a Security Administrator or an Administrator.

2 In the OpsCenter console, click **Settings > Views**.

3 From the list of views, select the view from which you want to delete objects.

4 Click **Manage Nodes and Objects**.

5 On the view tree, select the view name or a view node from which you want to delete an object.

The objects that are assigned to this view or the view node are displayed on the **Objects on Node** tab.

6 Select the check boxes in front of the view objects that you want to delete.

7 Click **Delete from Node**.

8 On the confirmation dialog box, click **OK**.

View filters in OpsCenter

OpsCenter provides a set of default filters using which you can filter the view objects that you need to add to a view. You can also create your own filters and apply them to view the required list of view objects.

The default set of filters varies depending on the view type.

Table 7-7 lists the default filters available for various view types.

Table 7-7 Default filters

View type	Default filters
Client	All Clients, Windows Clients, Solaris Clients, Linux Clients, Other Clients
Master Server	All Servers, Connected Servers, Not Connected Servers, Windows Servers, Solaris Servers, Linux Servers, Other Servers
Policy	All Policies, Active Policies, Inactive Policies, Windows Policies, Catalog Policies, Standard Policies, Other Policies

See the following topics for information about creating, modifying, and deleting view object filters.

Creating a view object filter in OpsCenter

This topic provides the procedure to create user-defined view object filters.

See "View filters in OpsCenter" on page 314.

To create a view object filter

1. Log on to the OpsCenter console as a Security Administrator or an Administrator.
2. In the OpsCenter console, click **Settings > Views**.
3. From the list of views, select the view to which you want to assign objects.
4. Click **Manage Nodes and Objects**.
5. On the view tree, select the view name or the view node to which you want to assign view objects.
6. In the right pane, select the **Objects not in selected view** tab. The list of objects that is displayed varies depending on the view type.

   For example: If the view is of type **Client**, only client hosts are available on the **Objects not in selected view** tab for selection.

7 Click the **Create Filter** icon.

8 In the **Add Filter** dialog box, specify the filter details.

9 Click **OK**.

This user-defined filter is now added in the **Filter** drop-down list on the **Objects not in selected view** tab, which you can modify or delete.

See "Modifying view object filters in OpsCenter" on page 315.

See "Deleting view object filters in OpsCenter" on page 316.

Modifying view object filters in OpsCenter

You can modify definition of user-defined view object filters. You cannot modify the default filters.

Only a Security Administrator or an Administrator can modify view object filters.

See "Creating a view object filter in OpsCenter" on page 314.

To modify view object filters

1 Log on to the OpsCenter console as a Security Administrator or an Administrator.

2 In the OpsCenter console, click **Settings > Views**.

3 From the list of views, select the view to which you want to assign objects.

4 Click **Manage Nodes and Objects**.

5 On the view tree, select the view name or a view node to which you want to assign view objects.

6 In the right pane, select the **Unassigned Objects** tab. The list of objects that is displayed varies depending on the view type.

For example: If the view is of type **Client**, only client hosts are available on the **Unassigned Objects** tab for selection.

7 From the **Filter** drop-down list, select the user-defined filter that you want to modify.

8 Select the **Edit Filter** icon.

If you have selected a default filter, the **Edit Filter** icon is disabled.

9 On the dialog box, modify name or definition of the filter.

10 Click **OK**.

Deleting view object filters in OpsCenter

You can delete user-defined view object filters. You cannot delete the default filters.

Only a Security Administrator or an Administrator can delete user-defined view object filters.

See "Creating a view object filter in OpsCenter" on page 314.

To delete view object filters

1. Log on to the OpsCenter console as a Security Administrator or an Administrator.
2. In the OpsCenter console, click **Settings > Views**.
3. From the list of views, select the view to which you want to assign objects.
4. Click **Manage Nodes and Objects**.
5. On the view tree, select the view name or a view node to which you want to assign view objects.
6. In the right pane, select the **Unassigned Objects** tab. The list of objects that is displayed varies depending on the view type.
7. From the **Filter** drop-down list, select the user-defined filter that you want to delete.

   If you have selected a default filter, the **Delete Filter** icon is disabled.

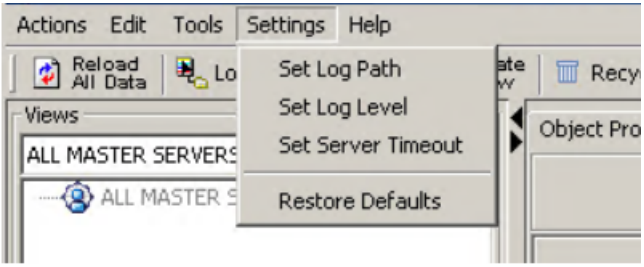
Setting up logging for OpsCenter View Builder

This section includes the procedure to set up logging in OpsCenter View Builder. The OpsCenter View Builder uses its own log file: `admingui.log file.` By default, this log file is stored in the temporary working directory which is `C:\Users\<username>\AppData\Local\Temp\1\`.

To Set up a log path for View Builder log

1 Open the **View Builder** and authenticate using the login credentials.

2 Under the **Settings** menu, click **Set Log Path**.



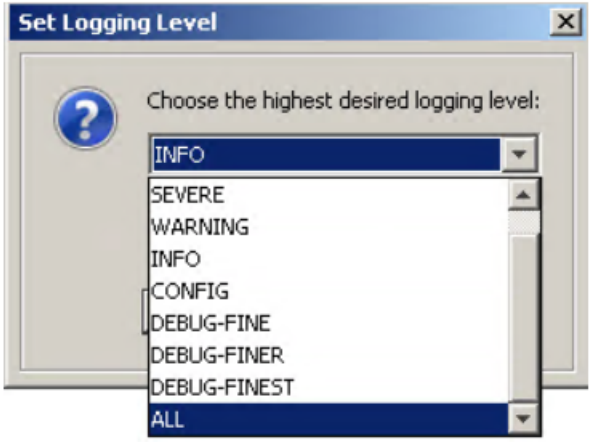
3 Restart the **View Builder** to apply the changes.

To Set up log level for the View Builder log

1 Open the **View Builder** and authenticate using the credentials.

2 To change the log verbosity, under the **Settings** menu, click **Set Log Level**.

3 From the drop-down list select the log level.



Chapter 8

Monitoring NetBackup using OpsCenter

This chapter includes the following topics:

- About the Monitor views
- Controlling the scope of Monitor views
- About monitoring NetBackup using the Overview tab
- About monitoring NetBackup jobs
- Monitor > Services view
- About using the List View to monitor NetBackup media
- Viewing the details for NetBackup media
- Viewing the details for a master server associated with the media
- Filtering on NetBackup media type
- Controlling media
- Monitor > Media Summary View options
- Hierarchical View by Volume Pool for monitoring media
- Viewing the details for volume pool
- Viewing the details for media
- Controlling media
- Hierarchical View by Volume Group for monitoring media

- Viewing the details for a volume group
- Viewing the details for media
- Controlling media in OpsCenter
- Monitoring NetBackup devices
- Monitor > Devices > Drives List View options
- About using the List View for monitoring drives
- Viewing the details for a single drive
- Viewing the details for a master server associated with a drive
- Filtering on NetBackup drive category
- Controlling drives
- Monitor > Devices > Drives Summary View
- Viewing the Drive Summary by Status
- Monitor > Devices > Disk Pools options
- Viewing the details for a single disk pool
- About monitoring NetBackup hosts
- Monitor > Hosts > Master Servers view
- Filtering by NetBackup master server type and status
- Monitor > Hosts > Media Servers view
- Viewing the details of a master server that is associated with a media server
- Monitor > Hosts > Clients view
- Viewing the details for a single master server
- About monitoring NetBackup alerts
- Monitor > Alerts List View
- About using the List View to monitor NetBackup alerts
- Viewing the details for a single alert
- Viewing the details of a single alert for Appliance hardware failure
- Viewing the details of the alert policy associated with an alert

- Filtering by alert type
- Responding to alerts
- Summary View for monitoring NetBackup alerts
- Viewing alerts by severity
- Viewing alerts by NetBackup Master Server
- About monitoring Audit Trails
- Monitor > Appliance Hardware > Master Server
- Monitor > Appliance Hardware > Media Server
- Monitor > Appliance Hardware > NetBackup
- Monitor > Appliance Hardware > Deduplication
- Appliance hardware details
- Monitor > Cloud options

About the Monitor views

From the **Monitor** tab and associated subtabs, you can view detailed information about your NetBackup environment including jobs, services, policies, media, devices, hosts, alerts, audit trails, cloud, and appliance hardware.

Note that OpsCenter or OpsCenter Analytics can only monitor and manage NetBackup or NetBackup appliances. It cannot monitor or manage other products like NetBackup PureDisk or Backup Exec.

Controlling the scope of Monitor views

The content that is shown in the **Monitor** views is based on your current **View** pane selection.

You can select the following default option from the **View** pane:

ALL MASTER SERVERS	Select **ALL MASTER SERVERS** to view information for all the NetBackup servers in your environment.

In addition to using the default view i.e. **ALL MASTER SERVERS**, you can also create your own views from **Settings > Views** or by using OpsCenter View Builder.

For example, you can create a view like Geography to view details about master servers in a particular region like Europe.

More information about how to create views by using the **Settings > Views** control is available.

See "About OpsCenter views" on page 299.

See the online *OpsCenter View Builder Help* to know how you can create views using OpsCenter View Builder.

Use the following procedure to view details of all master servers or specific master servers.

To view details of all master servers

- In the OpsCenter console, select **ALL MASTER SERVERS** from the drop-down list in the **View** pane.

To view details of specific master servers

1. In the OpsCenter console, select **ALL MASTER SERVERS** from the drop-down list in the **View** pane.
2. Deselect the checkbox next to **ALL MASTER SERVERS** and select the specific master servers from the list of master servers. Ensure that other master servers are unchecked.
3. Click **Apply Selection**.

See "About time frame selection" on page 321.

About time frame selection

You can also view data for the last 24, 48, or 72 hours for some of the **Monitor** views. You can also configure an absolute or relative timeframe for specific Monitor views.

Click **Last 24 Hours**, **Last 48 Hours**, or **Last 72 Hours** to view data for the last 24, 48, or 72 hours respectively. These options are located on the top-right corner of specific **Monitor** views. Note that by default, data for the last 24 hours is shown in these views.

You can control time frame selection for the following **Monitor** views:

- **Monitor** > **Overview** (Job Summary by State, Job Summary by Exit Status, Top 7 Policies by Failed Jobs, Top 7 Job Error Log Summary, and Alert Summary by Severity sections)

Note: You cannot control timeframes for Media Summary by Status, Drive Summary by Status, Services Summary, and Master Server Summary sections. These sections show all the data from the OpsCenter database.

- **Monitor** > **Jobs**
- **Monitor** > **Alerts**
- **Monitor** > **Policies** (Summary View)

In addition, you can also customize the time frame selection by clicking **Customize** and specifying an absolute time frame or relative time frame. Using the **Customize** option, you can view data for any time frame. Note that the **Customize** option is located on the top-right corner of specific **Monitor** views.

You can configure an absolute or relative timeframe for the following **Monitor** views:

- **Monitor** > **Jobs** (List View, Summary View, and Hierarchical View)
- **Monitor** > **Alerts** (List View and Summary View)

You can also configure a customize timeframe for: **Monitor** > **Audit Trails**

See "Controlling the scope of Monitor views" on page 320.

About monitoring NetBackup using the Overview tab

This view is displayed when you select **Monitor > Overview** (default view). This view gives an overview of your NetBackup environment. This view contains the different sections which display specific information about your NetBackup environment.

From this view, you can use links to drill down and access detailed information about many aspects of your NetBackup environment. Pie charts for most monitoring categories appear. The pie segments are also links to more details for the monitoring category.

The following sections describe the **Overview** subtab in detail:

- See "Viewing the Job Summary by State " on page 323.
- See "Viewing the Media Summary by Status " on page 323.
- See "About Top 7 Job Error Log Summary" on page 324.
- See "Viewing the Services Summary" on page 325.
- See "Viewing the Master Server Summary" on page 325.

- See "Viewing the Job Summary by Job Status" on page 326.
- See "Viewing the Drive Summary by Status" on page 327.
- See "Top 7 Policies by Failed Jobs" on page 328.
- See "Viewing the Alert Summary by Severity" on page 328.

Viewing the Job Summary by State

The **Job Summary by State** section shows an overall distribution of jobs by job state for the current selection in the **View** pane and time frame selection.

This information is shown in a pie chart as well as a table. Data for the last 24 hours is shown by default. You can also view data for the last 48 hours or 72 hours.

See "Controlling the scope of Monitor views" on page 320.

A pie chart with different colors represents the job distribution. Each color of the pie chart represents how jobs are distributed in your environment as per the job state in the selected time frame. You can also view the color code summary in this section to know the colors that represent different job states. Pointing on the pie chart gives the number and percentage of jobs in a particular job state in your NetBackup environment. For example, pointing on the yellow color in the pie chart shows that in the last 24 hours, 22 jobs, or 42% jobs in your environment are in a queued state.

You can drill down from this section to see details for failed, incomplete, queued, active jobs etc.

To view the Job Summary by job state

1. In the OpsCenter console, select **Monitor > Overview**.
2. In the **Job Summary by State** section, do either of the following:
   - Click the number of jobs (link) for a particular job state from the table. For example, click the number that is shown for **Done** jobs.
     Or
   - Click a colored section of the pie chart that corresponds to a particular job state. For example, click the yellow section of the pie chart to view details for **Queued** jobs.

Viewing the Media Summary by Status

The **Media Summary by Status** section shows an overall distribution of media by media status for the current selection in the **View** pane. This information is shown in a pie chart as well as a table.

Note: The timeframe selection does not affect this section. All the data from the OpsCenter database is displayed in this section irrespective of the timeframe that you select.

A pie chart with different colors represents media distribution in this section. Each color of the pie chart represents how media are distributed in your environment as per the media status. You can also view the color code summary in this section to know the colors that represent different media status. Moving your pointer over the pie chart triggers the appearance of the number and percentage of media with a particular media status in your NetBackup environment. For example, pointing on the red color in the pie chart shows that four media or 2% media in your environment are frozen.

You can drill down from this section to see details for media with different status like details for frozen and active media.

To view media by media status

1. In the OpsCenter console, select **Monitor > Overview**.
2. In the **Media Summary by Status** section, do either of the following:
   - Click the number of media (link) for a particular media status from the table. For example, click the number for **Frozen** media.
     Or
   - Click a colored section of the pie chart that corresponds to a particular media status. For example, click the red section of the pie chart to view details for **Frozen** media.

About Top 7 Job Error Log Summary

The **Top 7 Job Error Log Summary** section lists seven exit status codes responsible for maximum failed jobs in your environment. The content that is shown in this section is based on the current **View** pane selection. Data for the last 24 hours is shown by default. You can also view data for the last 48 hours or 72 hours.

See "Controlling the scope of Monitor views" on page 320.

The table that appears in the section lists the top seven exit status codes responsible for maximum job failure. The table also lists the number of failed jobs for each exit status in the selected time frame. Note that the failed jobs that are shown in the **Failed Job Count** column are arranged in descending order in the table. By viewing this section, you can quickly analyze the reasons behind maximum job failures in your environment.

Viewing the Services Summary

The Services Summary section provides a high-level view that shows the total number of running and stopped NetBackup services for the current **View** pane selection.

The total number of running and stopped NetBackup services are shown in a table. You can drill down from the links in this table to see details for running or stopped services.

Note: The timeframe selection does not affect this section. All the data from the OpsCenter database is displayed in this section irrespective of the timeframe that you select.

To view running or stopped services

1. In the OpsCenter console, select **Monitor > Overview**.
2. In the **Service Summary** section, click the number that is shown in the **Service Count** column of the table. For example, click the number that is shown for Running services to view details for the services that are running.

Viewing the Master Server Summary

The **Master Server Summary** section provides the specific information about the master servers based on the current **View** pane selection.

Note: The timeframe selection does not affect this section. All the data from the OpsCenter database is displayed in this section irrespective of the timeframe that you select.

The following information is shown in the **Master Server Summary** section:

- Total number of master servers in your environment
- Number of the master servers that appear as **Connected** in the OpsCenter console
- Number of the master servers that appear as **Not Connected** in the OpsCenter console
- Number of the master servers that appear as **Disabled** in the OpsCenter console

You can drill down from this section to see details for all the master servers in your environment or the master servers that appear as connected, not connected, or disabled.

To view all master servers

1. In the OpsCenter console, select **Monitor > Overview**.
2. In the **Master Server Summary** section, click the number that is shown in the **Total** column.

To view the master servers that are connected

1. In the OpsCenter console, select **Monitor > Overview**.
2. In the **Master Server Summary** section, click the number that is shown in the **Connected** column.

To view details of the master servers that are not connected

1. In the OpsCenter console, select **Monitor > Overview**.
2. In the **Master Server Summary** section, click the number that is shown in the **Not Connected** column.

To view the master servers that are disabled

1. In the OpsCenter console, select **Monitor > Overview**.
2. In the **Master Server Summary** section, click the number that is shown in the **Disabled** column.

Viewing the Job Summary by Job Status

The **Job Summary by Job Status** section shows an overall distribution of jobs by job status or exit status based on the current **View** pane and time frame selection.

This information is shown in a pie chart as well as a table. Data for the last 24 hours is shown by default. You can also view data for the last 48 hours or 72 hours.

See "Controlling the scope of Monitor views" on page 320.

A pie chart with different colors represents the job distribution by exit status in the selected time frame. Each color of the pie chart represents how jobs are distributed in your environment as per the exit status. You can also view the color code summary in this section to know the colors that represent different exit status. Putting your pointer over the pie chart shows the total number and percentage of successful, partially successful, and failed jobs in your NetBackup environment. For example, pointing to the red color in the pie chart shows that in the last 24 hours, 72 jobs, or 42% jobs in your environment failed. This information is also listed in a tabular format. In addition, a table also shows the amount of data that has been backed up for the selected view and time frame.

You can drill down from this section to see details for failed, successful, or partially successful jobs.

To view jobs by job status

1. In the OpsCenter console, select **Monitor > Overview**.
2. In the **Job Summary by Job Status** section, do either of the following:
   - Click the number of jobs (link) corresponding to a particular exit status from the table.
     Or
   - Click a colored section of the pie chart that corresponds to a particular exit status. For example, click the red section of the pie chart to view details for failed jobs.

Viewing the Drive Summary by Status

The **Drive Summary by Status** section shows an overall distribution of drives by drive status for the current **View** pane selection. This information is shown in a pie chart as well as a table.

Note: For 7.0.1 and later master servers, the **Drive Summary by Status** section does not show the drives that are disabled or unreachable.

Note: The timeframe selection does not affect this section. All the data from the OpsCenter database is displayed in this section irrespective of the timeframe that you select.

A pie chart with different colors represents the distribution of drives by drive status in the selected time frame. Each color of the pie chart represents how drives are distributed in your environment as per the drive status. You can also view the color code summary in this section to know the colors that represent different exit status. Putting your pointer over the pie chart shows the number and percentage of drives with up or down status in your NetBackup environment. For example, pointing to the green color in the pie chart shows that 5 drives or 100% drives in your environment are up.

You can drill down from this section to see details of all drives including up, down, or mixed drives.

To view drives by drive status

1. In the OpsCenter console, select **Monitor > Overview**.
2. In the **Drive Summary by Status** section, do either of the following:
   - Click the number of drives (link) for a particular drive status from the table. For example, click the number for Up drives

Or

- Click a colored section of the pie chart that corresponds to a particular drive status. For example, click the green section of the pie chart to view details for the drives that are up.

Top 7 Policies by Failed Jobs

For information about the **Top 7 Policies by Failed Jobs** section, see the following topic.

See "About Top 7 Policies by Failed Jobs" on page 357.

Viewing the Alert Summary by Severity

The **Alert Summary by Severity** section shows an overall distribution of alerts by severity for the current **View** pane and time frame selection.

This information is shown in a pie chart as well as a table. Data for the last 24 hours is shown by default. You can also view data for the last 48 hours or 72 hours.

See "Controlling the scope of Monitor views" on page 320.

A pie chart with different colors represents the alert distribution by severity in this section. Each color of the pie chart represents how alerts are distributed in your environment as per the alert severity. You can also view the color code summary in this section to know the colors that represent different severity.

Moving your pointer over the pie chart gives the number and percentage of alerts with a particular severity in your NetBackup environment. For example, pointing to the green color in the pie chart shows that in the last 24 hours, 200 alerts, or 17% alerts in your environment are critical.

You can drill down from this section to see details for alert categories.

To view alerts by severity

1. In the OpsCenter console, select **Monitor > Overview**.
2. In the **Alert Summary by Severity** section, do either of the following:
   - Click the number of alerts (link) for a particular alert severity from the table. For example, click the number that is shown for Critical alerts.
     Or
   - Click a colored section of the pie chart that corresponds to a particular alert severity. For example, click the red section of the pie chart to view details for Critical alerts.

About monitoring NetBackup jobs

The **Monitor > Jobs** view provides details of NetBackup jobs. You can use the following views to see NetBackup job information:

List View	This view is shown by default when you select **Monitor > Jobs**. This view displays detailed information about jobs based on the current **View** pane and time frame selection. **Note:** You can only view jobs data for the last 30 days from the **List View**. See "Monitor > Jobs List View options" on page 329.
Summary View	The **Summary View** contains the different sections which show the NetBackup job distribution by exit status, job state, and job type based on the current **View** pane and time frame selection. This information is shown in pie charts and tables. See "About using the Summary View for monitoring jobs" on page 338.
Hierarchical View	The **Hierarchical View** shows all parent-child jobs in a hierarchical fashion based on the current **View** pane and time frame selection. **Note:** You can only view jobs data for the last 30 days from the Hierarchical View. See "About using the Hierarchical View for monitoring jobs" on page 343.

Note: You can select these views from the drop-down list. The drop-down list is located at the top-right corner of the page.

Monitor > Jobs List View options

This view is displayed when you select **Monitor > Jobs**. The **List View** is shown by default. This view displays detailed information for jobs for the current **View Pane** and time frame selection. Data for the last 24 hours is shown by default. You can also view data for the last 48 hours or 72 hours.

See "Controlling the scope of Monitor views" on page 320.

The table that appears in this view shows the following columns by default:

Table 8-1 Monitor > Jobs List View options

Option	Description
Job ID	This column shows the unique ID associated with the job (link).
Master Server	This column shows the name of the master server (link) associated with the job. You can click the link to view details for the master server.
Type	This column lists the job type like whether the job is a DB Backup or an Image Cleanup job.
State	This column lists the current NetBackup job state like whether the job is Queued, Waiting for Retry, Done etc.
Status	Exit status of the job. The link provides status description and details on troubleshooting in case it failed.
Policy	This column lists the name of the policy that is associated with the job.
Client	This column lists the name of the client on which the job is run.
Start Time	This column lists the date, time, and year when the job started.
Elapsed Time	This column lists the time that is taken by the job. The Elapsed Time is the difference between End Time and Start Time values. For a running job, Elapsed Time is the difference between the current time and Start time. **Note:** The contents of the Elapsed Time column cannot be sorted in ascending or descending order (when you click the column name.)
End Time	This column lists the date, time, and year when the job ended.
Job Size	This column lists the size of the job.
Files	This column lists the number of files that have been backed up by this job.
% Complete	This column lists the percentage of job that has been completed.

Not all columns are displayed in the table by default. More columns can be added to your view by clicking the **Table Settings** icon. The **Table Settings** icon is located on the top-right corner of the table.

The following columns are not displayed in the table by default:.

- **Schedule**
- **Source Media Server**
- **Destination Media Server**
- **Destination Storage Unit**
- **Attempt**
- **Operation**
- **Data Reduction Savings Job Size**
- **PID**
- **Owner**
- **Parent**
- **KB per sec**
- **Session ID**
- **Data Movement**
- **Submittal Type**
- **Schedule Type**
- **Policy Type**
- **Compression**
- **Current File**
- **Robot**
- **Vault**
- **Media to Eject**
- **Copy**
- **Profile**
- **Active Start**
- **Reconciliation Status**
- **Reconciliation Reason**

- **Data Reduction Savings (%)**
- **Priority**
- **State Details**

See the online *NetBackup Administration Console Help* for a detailed description of these fields.

More information about how to customize tables and view specific columns is available.

See "About using tables" on page 61.

All the details that are associated with a job can be viewed from the Details pane. The Details pane is located at the bottom of the **Monitor > Jobs** view.

The Details pane has the following tabs:

Table 8-2 Monitor > Jobs Details pane tabs

Tab	Description
General	The **General** tab of the Details pane displays all information available for the job. It also includes the contents of all the available columns that can be viewed from the table.
Attempts	The **Attempts** tab shows details of the attempts that have been made to complete a job.
File List	The **File List** tab shows the files that have been backed up by the job and also their location.

About monitoring jobs using the List View

The following topics provide more information about monitoring jobs using the **List View**.

Viewing the details for a single NetBackup job

All the details that are associated with a job can be viewed from the Details pane. The Details pane is located at the bottom of the **Monitor > Jobs** view.

The Details pane has the following tabs:

General	The **General** tab of the Details pane displays all information available for the job. It also includes the contents of all the available columns that can be viewed from the table.
Attempts	The **Attempts** tab shows details of the attempts that have been made to complete a job.
File List	The **File List** tab shows the files that have been backed up by the job and also their location.

To view details for a single NetBackup job

1. In the OpsCenter console, select **Monitor > Jobs**.
2. The job details can be viewed from either **List View** or **Hierarchical View**. Select **List View** or **Hierarchical View** from the drop-down list. The drop-down list is located at the top-right corner of the view.
3. Click the ID (link) for a job from the **Job ID** column of the table.
4. View the job details in the Details pane.

Viewing the details for a master server associated with a job

Use the following procedure to view the details for a master server that is associated with a job.

To view details for the master server that is associated with a job

1. In the OpsCenter console, select **Monitor > Jobs**.
2. These details can be viewed from either **List View** or **Hierarchical View**. Select **List View** or **Hierarchical View** from the drop-down list. The drop-down list is located at the top-right corner of the view.
3. Click the server name (link) associated with the job in the **Master Server** column of the table. The **Monitor > Hosts** page is displayed. The details of the master server are shown this page.

Viewing policy information for a job

Use the following procedure to view the details for the policy that is associated with a job.

To view policy information for a job

1. In the OpsCenter console, select **Monitor > Jobs**.
2. Select **List View** or **Hierarchical View** from the drop-down list. The drop-down list is located at the top-right corner of the view.
3. Click the policy name (link) for the job in the **Policy** column of the table.
4. A separate page appears that shows policy information on four tabs.

   See "Monitor > Policies page" on page 354.

Filtering on NetBackup job type and state

You can filter by using any of the built-in job filters. These filters are available from the drop-down list, which is present on top of the table.

Many job filters exist. This section lists some of the built-in job filters as follows:

All Jobs (default filter)	Select this filter to view details of all the jobs.
Active Jobs	Select this filter to view only active jobs
Queued Jobs	Select this filter to view only queued jobs.
Done Jobs	Select this filter to view only Done jobs.
Suspended Jobs	Select this filter to view the jobs that have been suspended.
Waiting for Retry Jobs	Select this filter to view the jobs that are waiting for retry.
Incomplete Jobs	Select this filter to view the jobs that are incomplete.
Canceled Jobs	Select this filter to view the jobs that have been canceled.
Undefined Jobs	Select this filter to view the jobs that are undefined.
Successful Jobs	Select this filter to view the jobs that are successful.
Partially Successful Jobs	Select this filter to view the jobs that are partially successful.
Failed Jobs	Select this filter to view the jobs that failed.
Index for Search	Select this filter to filter indexing related jobs.

Index Cleanup for Search	Select this filter to filter the index cleanup jobs.

In addition to using the built-in filters, you can also create your own custom filters.

See "Creating, applying, editing, and removing custom view filters" on page 64.

To filter details by job state

1. Select **Monitor > Jobs**.
2. Select **List View** or **Hierarchical View** from the drop-down list. The drop-down list is located at the top-right corner of the view.
3. Select a filter from the drop-down list. Note that the drop-down list is located on top of the table.

Controlling NetBackup jobs

Use the following procedure to cancel, suspend, resume, or restart a job. Before you perform these tasks, manually refresh your Web browser to obtain an updated view for all jobs.

Note: These tasks are not visible if you log on with an Analyst or a Reporter role.

To control a job

1. In the OpsCenter console, select **Monitor > Jobs**.
2. Select **List View** or **Hierarchical View** from the drop-down list. The drop-down list is located at the top-right corner of the view.
3. Select a job from the table. You may select one or more jobs.
4. Click **Cancel**, **Restart**, **Resume**, **Suspend**. These options are located on top of the table.

   The OpsCenter console may take some time to show the updated status once you perform the tasks.

Reconciling NetBackup jobs

You can use the **Reconcile** option to prevent the jobs that failed due to reasons like user terminating a job, host cannot be reached etc. from being billed. By using the **Reconcile** option and selecting a reason, you can let your service provider know not to bill you for these jobs as these jobs failed due to specific issues at your end.

Note: The **Reconcile** option is disabled in the unlicensed version (OpsCenter).

Before you perform this task, manually refresh your Web browser to obtain an updated view for all jobs

To reconcile NetBackup jobs

1. In the OpsCenter console, select **Monitor > Jobs**.
2. Select **List View** or **Hierarchical View** from the drop-down list. The drop-down list is located at the top-right corner of the view.
3. Select a job from the table. You can select one or more jobs.
4. From the **More** drop-down list, select **Reconcile**.
5. In the **Reconcile Jobs** dialog box, select a reason for reconciling the job from the drop-down list.

   Note that you can select **Un-Reconcile** from the drop-down list to undo a reconciliation.
6. Click **OK**.

Changing the job priority

You can change the priority that is associated with a job.

Priority can be changed only for the jobs that are in Active or Queued state.

To change the job priority

1. In the OpsCenter console, select **Monitor > Jobs**.
2. Select **List View** or **Hierarchical View** from the drop-down list. The drop-down list is located at the top-right corner of the view.
3. Select an active job or a queued job from the table.
4. From the **More** drop-down list, select **Change Job Priority**.
5. In the **Change Priority** dialog box, set the job priority to a particular value. You can also increment or decrement the job priority.
6. Click **OK**.
7. Click **Finish**.

   The OpsCenter console may take some time to show the updated status once you perform this task.

Change Job Priority dialog box options

A description of the Change Job Priority dialog box options follows in the table.

Table 8-3 Change Job Priority dialog box options

Option	Description
Set the job priority to	Enter a value to set the job priority.
Increment the job priority by	Select a value from the drop down list to increment the job priority.
Decrement the job priority by	Select a value from the drop down list to decrement the job priority.

See "Changing the job priority" on page 336.

Exporting NetBackup job logs

You can export the log files that are associated with a job. You can view or save the exported log files in an Excel format.

Note: The **Export Job Logs** option is not visible if you log on with an Analyst or a Reporter role.

Note: Logs are not available for all job types. Before exporting a log file, ensure that the NetBackup master server is Connected and the selected job logs are enabled.

To export the NetBackup log files for a job

1. In the OpsCenter console, select **Monitor > Jobs**.
2. Select **List View** or **Hierarchical View** from the drop-down list. The drop-down list is located at the top-right corner of the view.
3. Select a job from the table.

   You can export only one job log at a time.
4. From the **More** drop-down list, select **Export Job Logs**.
5. Click **Open** or **Save** from the dialog box to view or save the log file in an Excel format.

About using the Summary View for monitoring jobs

This view is displayed when you select **Monitor > Jobs** and then select **Summary View** from the drop-down list. The drop-down list is located at the top-right corner of the page.

The content that is shown in the **Summary View** is based on the current **View Pane** and time frame selection. Data for the last 24 hours is shown by default. You can also view data for the last 48 hours or 72 hours.

See "Controlling the scope of Monitor views" on page 320.

The **Summary View** contains the different sections which display specific information about NetBackup jobs. These sections show NetBackup job information in a table as well as a pie chart. The table and the pie charts include links to filtered detail views. You can use these links to drill down and access detailed information about NetBackup jobs.

Note: If you uncheck the **Allow Multiple Selection In View Pane** option, a **Group Component Summary** table is displayed when you access the **Summary View** for **Monitor > Jobs**. The **Group Component Summary** table displays information about immediate NetBackup constituents of the view or node (group) that you selected in the **View** pane. You can uncheck the **Allow Multiple Selection in View Pane** option from **Settings > User Preferences > General**.

The following sections describe this view in detail:

- See "Viewing the Job Summary by Job Status" on page 338.
- See "Viewing the Job Summary by State" on page 339.
- See "Viewing the Job Summary by Type" on page 340.
- See "About the Group Component Summary table" on page 341.

Viewing the Job Summary by Job Status

The **Job Summary by Job Status** section shows an overall distribution of jobs by job status or exit status.

The data that is shown in this view is based on the current **View** pane and time frame selection. This information is shown in a pie chart as well as a table. Data for the last 24 hours is shown by default. You can also view data for the last 48 hours or 72 hours.

See "Controlling the scope of Monitor views" on page 320.

A pie chart with different colors represents the job distribution by exit status in this section. Each color of the pie chart represents how jobs are distributed in your environment as per the exit status. You can also view the color code summary in this section to know the colors that represent different exit status. Moving your pointer over the pie chart gives the number and percentage of jobs with a particular exit status in your NetBackup environment. For example, pointing your cursor to the red color in the pie chart shows that in the last 24 hours, 72 jobs, or 42% jobs in your environment failed.

You can drill down from this section to see details for successful, partially successful, and failed jobs.

To view jobs by job status

1. In the OpsCenter console, select **Monitor > Jobs**.
2. Select **Summary View** from the drop-down list. Note that the drop-down list is located on the top-right corner of the page.
3. In the **Job Summary by Job Status** section, do either of the following:
   - Click the number of jobs (link) corresponding to a particular exit status from the table.

     Or
   - Click a colored section of the pie chart that corresponds to a particular exit status. For example, click the red section of the pie chart to view details for failed jobs.

Viewing the Job Summary by State

The **Job Summary by State** section shows an overall distribution of jobs by the NetBackup job state based on the current **View** pane and time frame selection. This information is shown in a pie chart as well as a table. Data for the last 24 hours is shown by default. You can also view data for the last 48 hours or 72 hours.

See "Controlling the scope of Monitor views" on page 320.

A pie chart with different colors represents the job distribution by job state. Each color of the pie chart represents how jobs are distributed in your environment as per the job state. You can also view the color code summary in this section to know the colors that represent different job states. Moving your cursor over the pie chart gives the number and percentage of jobs in a particular job state in your NetBackup environment. For example, pointing to the yellow color in the pie chart shows that in the last 24 hours, 22 jobs, or 42% jobs in your environment are in a queued state.

You can drill down from this section to see details for the jobs that failed, the jobs that are waiting for retry, queued or active jobs, and so on.

To view jobs by job state

1. In the OpsCenter console, select **Monitor > Jobs**.
2. Select **Summary View** from the drop-down list. Note that the drop-down list is located on the top-right corner of the page.
3. In the **Job Summary by State** section, do either of the following:
   - Click the number of jobs (link) in a particular job state from the table. For example, click the number that is shown for **Done** jobs.
     Or
   - Click a colored section of the pie chart that corresponds to a particular job state. For example, click the yellow section of the pie chart to view details for Queued jobs.

Viewing the Job Summary by Type

The **Job Summary by Type** section shows an overall distribution of jobs by the job type based on the current **View** pane and time frame selection. This information is shown in a pie chart as well as a table. Data for the last 24 hours is shown by default. You can also view data for the last 48 hours or 72 hours.

See "Controlling the scope of Monitor views" on page 320.

A pie chart with different colors represents the job distribution by job type in this section. Each color of the pie chart represents how jobs are distributed in your environment as per the job type. You can also view the color code summary in this section to know the colors that represent different job types. Moving your cursor over the pie chart gives the number and percentage of jobs of a particular job type in your NetBackup environment. For example, pointing to the red color in the pie chart shows that in the last 24 hours, 22 jobs, or 42% jobs in your environment are **DBBackup** jobs.

You can drill down from this section to see details for different job types like **DBBackup**, Image Cleanup etc.

To view jobs by job type

1. In the OpsCenter console, select **Monitor > Jobs**.
2. Select **Summary View** from the drop-down list. Note that the drop-down list is located on the top-right corner of the page.
3. In the **Job Summary by Type** section, do either of the following:
   - Click the number of jobs (link) corresponding to a particular job type from the table. For example, click the number that is shown for **DBBackup** jobs.
     Or

- Click a colored section of the pie chart that corresponds to a particular job type. For example, click the red section of the pie chart to view details for **DBBackup** jobs.

About the Group Component Summary table

When you uncheck the **Allow Multiple Selection In View Pane** option under **Settings > User Preferences > General** view in the OpsCenter console, you can view the Group Component Summary table in the Summary View for **Monitor > Jobs**. The Group Component Summary table is displayed at the bottom of the **Summary View** for **Monitor > Jobs**.

You must select a group (view or node) from the **View** pane to see data in the Group Component Summary table. You do not see any data in the Group Component Summary table if you select a specific view object (master server) in the **View** pane.

More details about nodes and view objects is available.

See "About nodes and objects" on page 306.

The Group Component Summary table displays job summary information about the immediate NetBackup constituents of the selected view or node (group) in the **View** pane. For example if you select the **ALL MASTER SERVERS** view, the Group Component Summary table displays job summary for each master server. If you select a view that contains multiple nodes, a job summary of the nodes (and not the view objects for each node) is displayed.

Note: OpsCenter or OpsCenter Analytics monitors only NetBackup. Hence any other servers (like BE or PD) do not appear in the Group Component Summary table.

The information that is displayed in the Group Component Summary table is based on the current View pane and time frame selection. Data for the last 24 hours is shown by default. You can also view data for the last 48 hours or 72 hours.

See "Controlling the scope of Monitor views" on page 320.

Table 8-4 explains the information that is displayed in the Group Component Summary table.

Table 8-4 Columns and descriptions in the Group Component Summary table

Column	Description
Name	Name of the node or view object.

Table 8-4 Columns and descriptions in the Group Component Summary table *(continued)*

Column	Description
Total	Total number of jobs (link) for the specific node or view object in the selected time frame. Click the link to view detailed information about all the jobs.
Successful	Number of successful jobs (link) for the specific node or view object in the selected time frame. Click the link to view detailed information about successful jobs.
Partially Successful	Number of partially successful jobs (link) for the specific node or view object in the selected time frame. Click the link to view detailed information about the partially successful jobs.
Failed	Number of failed jobs (link) for the specific node or view object in the selected time frame. Click the link to view detailed information about the failed jobs.
Data Backup up	Data that is backed up for the specific node or view object in the selected time frame.
Active	Number of active jobs (link) for the specific node or view object in the selected time frame. Click the link to view detailed information about the active jobs.
Queued	Number of queued jobs (link) for the specific node or view object in the selected time frame. Click the link to view detailed information about the queued jobs.
Suspended	Number of suspended jobs (link) for the specific node or view object in the selected time frame. Click the link to view detailed information about the suspended jobs.
Incomplete	Number of incomplete jobs (link) for the specific node or view object in the selected time frame. Click the link to view detailed information about the incomplete jobs.

Table 8-4 Columns and descriptions in the Group Component Summary table *(continued)*

Column	Description
Undefined	Number of undefined jobs (link) for the specific node or view object in the selected time frame. Click the link to view detailed information about the undefined jobs.
Waiting for Retry	Number of the jobs that are waiting for retry (link) for the specific node or view object in the selected time frame. Click the link to view detailed information about the jobs that are waiting for retry.

About using the Hierarchical View for monitoring jobs

This view is displayed when you select **Monitor > Jobs** and then select **Hierarchical View** from the drop-down list. The data that is shown in this view is based on the current **View** pane and time frame selection. Data for the last 24 hours is shown by default. You can also view data for the last 48 hours or 72 hours.

Note: You can only view jobs data for the last 30 days from the **Hierarchical View**.

See "Controlling the scope of Monitor views" on page 320.

In the **Hierarchical View**, all related jobs can be grouped and you can see all parent-child jobs in a hierarchical fashion. You can view details of only the top level, parent job in this view with the ability to expand and drill into the details of child jobs if there are failures.

The **Hierarchical View** shows details of all jobs and also highlights the parent-child relationship between jobs wherever applicable. All parent jobs have a +sign before the job ID. You can click the + sign to see all child jobs. A child job is indented to the right-hand side in the Job ID column. If some of the child jobs are parent jobs, then + sign also appears before the job ID of the child job. However, if a job does not have a relationship with any other job (it is neither a parent nor a child job), it is represented only by its job ID in the Job ID column. Neither is there a + sign before the job ID of such a job nor this job is indented to the right-hand side.

Note the following things about the related jobs that are shown in the **Hierarchical View**:

- The filters are applied only to parent jobs. The filters are not applied to child jobs. For example, if you apply the Partially Successful Jobs filter, child jobs are

not considered at all. Only parent jobs or unrelated jobs (jobs that are not related to any other job) with partially successful status are considered.

- The sorting feature in the **Hierarchical View** applies to both parent jobs and child jobs. When you expand a parent job, the current selected sort order is applied to child jobs.
- All tasks that apply to the parent job are also applicable to its child jobs.

The following tasks can be performed from the **Hierarchical View**:

Table 8-5 Tasks from the Hierarchical View

Task	Reference topic
View the details for a single master server	See "Viewing the details for a single NetBackup job" on page 332.
View the details for a master server that is associated with a job	See "Viewing the details for a master server associated with a job" on page 333.
View policy information for a job	See "Viewing policy information for a job" on page 333.
Filter on NetBackup job state	See "Filtering on NetBackup job type and state" on page 334.
Control NetBackup jobs	See "Controlling NetBackup jobs" on page 335.
Reconcile NetBackup jobs	See "Reconciling NetBackup jobs" on page 335.
Change job priority	See "Changing the job priority" on page 336.
Export job logs	See "Exporting NetBackup job logs" on page 337.

Viewing the details for a single NetBackup job

All the details that are associated with a job can be viewed from the Details pane. The Details pane is located at the bottom of the **Monitor > Jobs** view.

The Details pane has the following tabs:

General

The **General** tab of the Details pane displays all information available for the job. It also includes the contents of all the available columns that can be viewed from the table.

Attempts	The **Attempts** tab shows details of the attempts that have been made to complete a job.
File List	The **File List** tab shows the files that have been backed up by the job and also their location.

To view details for a single NetBackup job

1. In the OpsCenter console, select **Monitor > Jobs**.
2. Select **Hierarchical View** from the drop-down list. The drop-down list is located at the top-right corner of the view.
3. Click the ID (link) for a job from the **Job ID** column of the table.
4. View the job details in the **Details** pane.

Viewing the details for a master server associated with a job

Use the following procedure to view the details for a master server that is associated with a job.

To view the details for the master server that is associated with a job

1. In the OpsCenter console, select **Monitor > Jobs**.
2. Select **Hierarchical View** from the drop-down list. The drop-down list is located at the top-right corner of the view.
3. Click the server name (link) associated with the job in the **Master Server** column of the table. The **Monitor > Hosts** page is displayed. The details of the master server are shown this page.

Viewing policy information for a job

Use the following procedure to view the details for the policy that is associated with a job.

Note: You can also view policy information from the List View.

To view policy information for a job

1. In the OpsCenter console, select **Monitor > Jobs**.
2. Select **Hierarchical View** from the drop-down list. The drop-down list is located at the top-right corner of the view.

3 Click the policy name (link) for the job in the **Policy** column of the table.

4 A separate page appears that shows policy information on four tabs.

See "Monitor > Policies page" on page 354.

Filtering on NetBackup job state

You can filter by using any of the following built-in job filters. These filters are available from the drop-down list which is present on top of the table.

Some of the built-in job filters are the following:

All Jobs (default filter)	Select this filter to view details of all the jobs.
Active Jobs	Select this filter to view only active jobs
Queued Jobs	Select this filter to view only queued jobs.
Done Jobs	Select this filter to view only Done jobs.
Suspended Jobs	Select this filter to view the jobs that have been suspended.
Waiting for Retry Jobs	Select this filter to view the jobs that are waiting for retry.
Incomplete Jobs	Select this filter to view the jobs that are incomplete.
Undefined Jobs	Select this filter to view the jobs that are undefined.
Canceled Jobs	Select this filter to view the jobs that have been canceled.
Successful Jobs	Select this filter to view the jobs that are successful.
Partially Successful Jobs	Select this filter to view the jobs that are partially successful.
Failed Jobs	Select this filter to view the jobs that failed.

In addition to using the built-in filters, you can also create your own custom filters.

See "Creating, applying, editing, and removing custom view filters" on page 64.

To filter details by job state

1. In the OpsCenter console, select **Monitor > Jobs**.
2. Select **Hierarchical View** from the drop-down list. The drop-down list is located at the top-right corner of the view.
3. Select a filter from the drop-down list. Note that the drop-down list is located on top of the table.

Monitor > Services view

This view is displayed when you select **Monitor > Services**. This view contains detailed information for services.

The data that is shown in this view is based on the current **View** pane selection.

See "Controlling the scope of Monitor views" on page 320.

The table that appears in this view has the following columns:

Name	This column lists the name of the service.
Host Name	This column lists the name of the master server or media server where the service or daemon is present.
Service Type	This column lists the NetBackup service type. Example: **Vault Manager**, **Device Manager**, or **Service Layer**.
Status	The operational status of the service or daemon. This status can be **Stopped**, **Running**, or **Other**. Other can be **Not Installed**, **Not Licensed**, **Start Pending**, **Stop Pending**, **Restart Pending**, **Failed**, or **Unknown**. **Note:** The status for some services may show as **Stopped** on the **Monitor > Services** page in the OpsCenter console. The license for these services is either not installed or configured for a specific media or master server.

You can perform the following tasks from this view:

Use filters to view specific services	See "Filtering on NetBackup service type" on page 348.
Control NetBackup services	See "Controlling NetBackup services" on page 348.

Filtering on NetBackup service type

You can filter by using any of the four built-in filters. These filters are available from the drop-down list which is present on top of the table.

The built-in filters are the following:

All Services (default filter)	Select this filter to view details of all the services.
Stopped Services	Select this filter to view details of the services that have been stopped.
Running Services	Select this filter to view details of running services.
Other Services	Select this filter to view details of all other services like Not Licensed, Unknown (not recognized by OpsCenter), or Not Applicable (some services may not be applicable to earlier versions).

In addition to using the built-in filters, you can also create your own custom filters.

See "Creating, applying, editing, and removing custom view filters" on page 64.

Use the following procedure to view details by type of service.

To filter on service type

1. In the OpsCenter console, select **Monitor > Services**.
2. Select a filter from the drop-down list. Note that the drop-down list is located on top of the table.

Controlling NetBackup services

Under certain circumstances there may be issues among multiple OpsCenter users. For instance, one OpsCenter user stops a service while another user tries to start the same service.

Note: NetBackup service layer (`nbsl`) cannot be controlled from OpsCenter.

To control a service

1. Refresh your Web browser to obtain an updated state for all services.
2. In the OpsCenter console, select **Monitor > Services**.
3. Select a service from the table. You can select one or more services.
4. Click **Start**, **Stop**, or **Restart**. Note that these tasks are located on top of the table.

   Note: These tasks are not visible if you log on with an Analyst or a Reporter role.

   The OpsCenter console may take some time to show the updated status once you perform these tasks. **Stop**, **Running**, or **Restart Pending** appears in the **Status** column until the selected action completes.

   If you start or stop a service that has a dependency on another service, NetBackup ensures that any dependent services are also started or stopped.

About monitoring NetBackup policies

The **Monitor > Policies** view provides details of NetBackup policies. You can use the following views to see NetBackup policy information:

List View

The **List View** is shown by default when you select **Monitor > Policies**. This view shows detailed information about NetBackup policies based on the current **View** pane selection.

See "Monitor > Policies List View" on page 350.

Summary View

The **Summary View** contains the different sections that display specific information about NetBackup policies based on the current **View** pane and time frame selection. These sections show specific policy information in a table as well as a pie chart.

See "Monitor > Policies Summary View" on page 357.

Note: You can select these views from the drop-down list. The drop-down list is located at the top-right corner of the page.

See "About using the List View to monitor NetBackup policies" on page 352.

See "Filtering on NetBackup policy type" on page 353.

See "Viewing details for a single NetBackup policy" on page 354.

See "Viewing details for a single NetBackup policy" on page 354.

See "Viewing details for a single NetBackup policy" on page 354.

See "Viewing details for a single NetBackup policy" on page 354.

See "Viewing details for a single NetBackup policy" on page 354.

See "Viewing details for a single NetBackup policy" on page 354.

Monitor > Policies List View

This view is displayed when you select **Monitor > Policies**. This view contains detailed information about policies. The data that is shown in this view is based on the current **View** pane selection.

See "Controlling the scope of Monitor views" on page 320.

The table that appears in this view has the following columns:

Name	Name of the policy. Click the link to view details about the policy.
Master Server	Name of the master server that is associated with the policy. Click the link to view details of master server.
Type	This column is the policy type. Usually, the Policy type determines the type of clients that can be backed up by this policy. Example: DB2, NBU-Catalog, Oracle, Sybase, Vault etc.
Storage	Storage that is associated with the policy. Click the link to view details for storage.
Volume Pool	Volume pool that is associated with the policy. Click the link to view details of volume pool.
CheckPoint Interval	Interval (in minutes) between two checkpoints in NetBackup.

Jobs/Policy	The total number of jobs that are associated with the policy.
Priority	Priority that you have defined for the policy. Zero means the lowest priority.
Active	This column determines whether the policy is Active or not.

Not all of the available columns appear initially in this view. The following columns do not appear, but can be added to your view by clicking the **Table Settings** icon:

- **Data Classification**
- **Effective Date**
- **Compression**
- **Encryption**
- **Block Level Increments**
- **Allow Multiple Data Streams**
- **Offhost**
- **Follow NFS**
- **Cross Mount Points**
- **Individual File Restore From Raw**
- **True Image Recovery**
- **Collect Disaster Recovery Information**
- **Collect Bare Metal Restore Information**
- **Snapshot Backups**
- **Alternate Client**
- **Data Mover**
- **Virtual Machine Proxy**
- **Snapshot Method**
- **Keyword Phrase**
- **Policy Domain Name**
- **Application Discovery**
- **Indexing (DEPRECATED)**

- **Index Server Name (DEPRECATED)**
- **Use Accelerator**

See the *NetBackup Administration Console Help* for a detailed description of these fields.

More information about how to customize tables and view specific columns is available.

See "About using tables" on page 61.

All the details that are associated with a policy can be viewed from the Details pane. The Details pane is located at the bottom of the **Monitor > Jobs** view.

The **Details** pane has the following tabs:

Table 8-6 Monitor > Policies Details pane tabs

Tab	Description
General	The **General** tab of the Details pane displays all information available for the policy. It also includes the contents of all the available columns that can be viewed from the table.
Schedules	The **Schedules** tab shows details of the schedules that are associated with the policy.
Clients	The **Clients** tab shows the clients that have been backed up by the policy and also their location.
Selections	The **Selections** tab shows the files that were backed up by the policy.

About using the List View to monitor NetBackup policies

You can perform the following tasks from this view:

Use filters to view specific policies	See "Filtering on NetBackup policy type" on page 353.
View the details for a single NetBackup policy	See "Viewing details for a single NetBackup policy" on page 354.
View the details for a master server associated with a policy	See "Viewing the details for a master server associated with a policy" on page 355.

View the details for a volume pool that is associated with a policy	See "Viewing the details for a volume pool associated with a policy" on page 355.
Manage a job policy	See "Activating or deactivating a job policy" on page 355.
Start a manual backup	See "Starting a manual backup" on page 356.
View the history for a job policy	See "Viewing the history for a single job policy " on page 356.

See "Monitor > Policies Summary View" on page 357.

Filtering on NetBackup policy type

You can filter by using any of the seven built-in filters. These filters are available from the drop-down list which is present on top of the table.

The built-in filters are the following:

All Policies (default filter)	Select this filter to view details of all NetBackup policies.
Active Policies	Select this filter to view details of the policies that are active.
Inactive Policies	Select this filter to view details of the policies that are inactive.
Windows Policies	Select this filter to view details of all policies that apply to Windows clients.
Catalog Policies	Select this filter to view details of catalog policies.
Standard Policies	Select this filter to view details of Standard policies.
Other Policies	Select this filter to view details of all other policies like DB2 policies, SAP policies, OS2 policies etc.

In addition to using the built-in filters, you can also create your own custom filters.

See "Creating, applying, editing, and removing custom view filters" on page 64.

Use the following procedure to view details by type of policy.

To filters details by type of policy

1. In the OpsCenter console, select **Monitor > Policies**.
2. Select a filter from the drop-down list. Note that the drop-down list is located on top of the table.

Monitor > Policies page

There are four tabs in the **Details** pane on the **Monitor > Policies** page.

Table 8-7 Monitor > Policies page tabs

Tab	Description
General	The **General** tab of the Details pane displays all information available for the policy. It also includes contents of all the columns that can be viewed from the table. You can also click the master server name (link) to get details of the master server.
Schedules	The **Schedules** tab displays details of the schedules that are associated with the policy.
Clients	The **Clients** tab shows details of clients to be backed up by the policy.
Selections	The **Selections** tab shows the files that have been backed up by the policy and also their location.

Viewing details for a single NetBackup policy

All the details that are associated with a policy can be viewed from the Details pane. The Details pane is located at the bottom of the **Monitor** > **Jobs** view.

The Details pane has four tabs.

See "Monitor > Policies page" on page 354.

To view details for a single NetBackup policy

1. In the OpsCenter console, select **Monitor > Policies**.
2. Click the name (link) for a policy from the **Name** column of the table.
3. View the policy details in the **Details** pane.

Viewing the details for a master server associated with a policy

Use the following procedure to view the details for a master server that is associated with a policy.

To view the details for a master server that is associated with a policy

1. In the OpsCenter console, select **Monitor > Policies**.
2. Click the server name (link) associated with the policy from the **Master Server** column of the table. The **Monitor** > **Hosts** page is displayed. The details of the master server are shown this page.

Viewing the details for a volume pool associated with a policy

Use the following procedure to view the details for a volume pool that is associated with a policy.

To view the details for a volume pool that is associated with a policy

1. In the OpsCenter console, select **Monitor > Policies**.
2. Click the volume pool name (link) associated with the policy from the **Volume Pool** column in the table. The details of the volume pool are shown on a separate page.

Activating or deactivating a job policy

Use the following procedure to activate or deactivate a policy. Before you perform these tasks, manually refresh your Web browser to obtain an updated view of all policies.

Note: These tasks are not visible if you log on with an Analyst or a Reporter role.

To activate or deactivate a policy

1. In the OpsCenter console, select **Monitor > Policies**.
2. Select a job policy from the table.
3. Click **Activate** or **Deactivate**. Note that these options are located on top of the table.

   The OpsCenter console may take some time to show the updated status once you perform these tasks.

Starting a manual backup

Use the following procedure to start a manual backup. Before you perform this task, manually refresh your Web browser to obtain an updated view of all policies.

The OpsCenter console may take some time to show the updated status once you perform this task.

Note: This task is not visible if you log on with an Analyst or a Reporter role.

To start a manual backup

1. In the OpsCenter console, select **Monitor > Policies**.
2. Select a policy from the table. You can select only one policy and it must be an active policy.
3. Click **Manual Backup**. Note that this option is located on top of the table.
4. You can select a schedule and a client from the drop-down lists for the backup, or only select a schedule or a client.

   If you do not select a schedule, NetBackup uses the schedule with the highest retention level.

   If you do not select a client, NetBackup backs up all scheduled clients.

Viewing the history for a single job policy

Use the following procedure to view the history for a policy.

Note: This task is not visible if you log on with an Analyst or a Reporter role.

To view the history for a policy

1. In the OpsCenter console, select **Monitor > Policies**.
2. Select a job policy from the table.
3. Click **View History**. Note that this option is located on top of the table.
4. The **Compare Policies** tab displays the policy versions. You must select two versions from the **Policy Versions** column to compare versions. The changes are highlighted in red color.

   To view only the differences between the versions, click the **View Differences** tab.

Monitor > Policies Summary View

This view is displayed when you select **Monitor > Policies** and then select **Summary View** from the drop-down list. The drop-down list is located at the top-right corner of the page. This view contains detailed information about policies.

The content that is shown in the **Summary View** is based on the current **View** pane and time frame selection. Data for the last 24 hours is shown by default. You can also view data for the last 48 hours or 72 hours.

See "Controlling the scope of Monitor views" on page 320.

The **Summary View** contains the different sections which display specific information about NetBackup policies. These sections show specific policy information in a table.

The following sections describe this view in detail:

- See "About Top 5 Policies by Data Backed up" on page 357.
- See "About Top 7 Policies by Failed Jobs" on page 357.
- See "About Top 7 Policies by No. of Jobs" on page 358.

About Top 5 Policies by Data Backed up

The **Top 5 Policies by Data Backed up** section lists the top five policies which have the maximum data backed up for the current **View** pane and time frame selection. Data for the last 24 hours is shown by default. You can also view data for the last 48 hours or 72 hours.

See "Controlling the scope of Monitor views" on page 320.

The table that is shown in the section lists the top five policies which have maximum data backed up. The table also shows the data that is backed up for each policy. Note that the data that is backed up (shown in Volume (Bytes) column) is arranged in descending order in the table. From this section, you can quickly view the policies which have the maximum data backed up.

See "About Top 7 Policies by Failed Jobs" on page 357.

See "About Top 7 Policies by No. of Jobs" on page 358.

About Top 7 Policies by Failed Jobs

The **Top 7 Policies by Failed Jobs** section lists seven policies which have the maximum failed jobs for the current **View** pane and time frame selection. Data for the last 24 hours is shown by default. You can also view data for the last 48 hours or 72 hours.

See "Controlling the scope of Monitor views" on page 320.

The table that is shown in the section lists the top seven policies which have maximum failed jobs associated with them. The table also shows the total number of failed jobs for each policy. Note that the failed jobs (shown in Total Number of Jobs column) are arranged in descending order in the table. From this section, you can quickly view the policies which have the maximum failed jobs associated with them.

Note: This section can also be viewed from **Monitor > Overview**.

See "About Top 5 Policies by Data Backed up" on page 357.

See "About Top 7 Policies by No. of Jobs" on page 358.

About Top 7 Policies by No. of Jobs

The **Top 7 Policies by No. of Jobs** section lists seven policies which have the maximum number of jobs. This data is based on the current **View** pane and time frame selection. Data for the last 24 hours is shown by default. You can also view data for the last 48 hours or 72 hours.

See "Controlling the scope of Monitor views" on page 320.

The table that is shown in the section lists the policies which have maximum number of jobs. The table also shows the total number of jobs for each policy. Note that the total number of jobs for each policy (shown in **Total Number of Jobs** column) are arranged in descending order in the table. From this section, you can quickly view the policies which have the maximum number of jobs associated with them.

See "About Top 5 Policies by Data Backed up" on page 357.

See "About Top 7 Policies by Failed Jobs" on page 357.

About monitoring NetBackup media

The **Monitor > Media** view provides details of NetBackup media. You can use the following views to see details about NetBackup media:

List View	The **List View** is shown by default when you select **Monitor > Media**. This view shows detailed information about NetBackup media for the current **View** pane selection. See "Monitor > Media List View options" on page 359.
Summary View	The **Summary View** displays the volume pool available for each master server for the current **View** pane selection. It also shows other media details that are associated with the master server like Frozen Media Count, Suspended Media Count etc. See "Monitor > Media Summary View options" on page 364.
Hierarchical View by Volume Pool	The **Hierarchical View by Volume Pool** shows details of all media and also groups media by volume pool for the current **View** pane selection. See "Hierarchical View by Volume Pool for monitoring media" on page 365.
Hierarchical View by Volume Group	The **Hierarchical View by Volume Group** shows details of all media and also groups media by volume group for the current **View** pane selection. See "Hierarchical View by Volume Group for monitoring media" on page 367.

Note: You can select these views from the drop-down list. The drop-down list is located at the top-right corner of the page.

Monitor > Media List View options

This view is displayed when you select **Monitor > Media**. This view contains detailed information for media.

This data is based on the current **View** pane selection.

See "Controlling the scope of Monitor views" on page 320.

The table that appears in this view has the following columns:

Table 8-8 Media List View options

Column Head/Option	Description
Media ID	Unique ID associated with a media. Click the link to view details about the media.
Master Server	Name of the master server that is associated with the media. Click the link to view details of master server.
Barcode	Barcode on the media
Media Type	Type of media like HCART, 8mm, or 4mm.
Robot Type	Specifies the robot type of the robot to inventory. Example: tl4, tl8.
Robot Number	Unique, logical identification number for the robot to inventory.
Slot	Slot in the robot that contains the volume.
Mounts	The number of times that the volume has been mounted.
Time Assigned	The date when the volume was assigned for use.
Max. Mounts	The maximum number of mounts (or cleanings) that are allowed for the volume. Zero (0) indicates unlimited mounts.
Data Expiration	Date when the images on the volume expire.
Last Written	The most recent time NetBackup used the volume for backups.
Media Status	Current media status like Frozen or Active
Used Capacity	Capacity that has been used.
On Hold	This relates to hold functionality of NetBackup. If an image on a media is placed on hold, the status of the media is **On Hold**. If the media is on hold, the value would be **Yes**. In other cases the value would be **-**.

Not all of the available columns appear initially in this view. The following columns do not appear, but can be added to your view by clicking the **Table Settings** icon:

- **Last Write Host**
- **Side**
- **Partner**
- **First Mount**
- **Last Mount**

- **Cleanings Remaining**
- **Created**
- **Description**
- **Vault Name**
- **Date Vaulted**
- **Return Date**
- **Vault Slot**
- **Session ID**
- **Vault Container ID**
- **Last Read**
- **Images**
- **Valid Images**
- **Number of Restores**
- **Conflicts**
- **Origin Host**
- **Media Owner**
- **Cleaning Media**
- **Imported**
- **Multiplexed**
- **Multiretention**
- **Last Restore**
- **Volume Expiration**
- **Retention Level**

See the *NetBackup Administration Console Help* for a detailed description of these fields.

More information about how to customize tables and view specific columns is available.

See "About using tables" on page 61.

About using the List View to monitor NetBackup media

You can perform the following tasks from this view:

View the details for a particular NetBackup media	See "Viewing the details for NetBackup media" on page 362.
View the details for a master server that is associated with the media	See "Viewing the details for a master server associated with the media" on page 362.
Use filters to view specific media	See "Filtering on NetBackup media type" on page 363.
Control media	See "Controlling media" on page 364.

Viewing the details for NetBackup media

All the details that are associated with a media can be viewed from the Details pane. The Details pane is located at the bottom of the view.

To view the details for a particular media

1. In the OpsCenter console, select **Monitor > Media**.
2. Click a link from the **Media ID** column. View the media properties from the Details pane. From the Details pane, you can also click the master server link to see details about the master server that is associated with the media.

Viewing the details for a master server associated with the media

Use the following procedure to view the details for a master server that is associated with a media.

To view the details for a master server associated with a media

1. In the OpsCenter console, select **Monitor > Media**.
2. Click the server name (link) associated with the media in the **Master Server** column of the table. The details of the master server are shown on a separate page.

Filtering on NetBackup media type

You can sort and filter this view to focus on the specific type of media that you want to see. For example, you can create and apply a filter that displays full media only. You can filter by using any of the built-in filters. These filters are available from the drop-down list which is present on top of the table.

The built-in filters are the following:

All Media (default filter)	Select this filter to view details of all media.
Assigned Media	Select this filter to view details of the media that have been assigned to an individual for further action.
Unassigned Media	Select this filter to view details of the media that are unassigned.
Frozen Media	Select this filter to view details of the media that are frozen.
Full Media	Select this filter to view details of the media that are full.
Suspended Media	Select this filter to view details of the media that are suspended.
Other Media	Select this filter to view details of all other media like Multi Retention Level media, BE media etc.
Active Media	Select this filter to view details of media with Active status.
Cleaning Media	Select this filter to view details of cleaning media.

In addition to the built-in filters, you can create your own custom filters.

See “Creating, applying, editing, and removing custom view filters” on page 64.

Use the following procedure to view details by type of media.

To filter details by type of media

1. In the OpsCenter console, select **Monitor > Media**.
2. Select a filter from the drop-down list. Note that the drop-down list is located on top of the table.

Controlling media

Use the following procedure to freeze, unfreeze, suspend, or unsuspend specific media. Note that to perform these tasks the media must be assigned to NetBackup. The media is assigned if there is a date in the **Time Assigned** column.

Note: These tasks are not visible if you log on with an Analyst or a Reporter role.

To perform media tasks

1. In the OpsCenter console, select **Monitor > Media**.
2. Select a media ID from the table (use the check box).
3. Click **Freeze**, **Unfreeze**, **Suspend**, or **Unsuspend**. Note that these options are present on top of the table.

   The OpsCenter console may take some time to show the updated status once you perform these tasks.

Monitor > Media Summary View options

This view is displayed when you select **Monitor > Media** and then select **Summary View** from the drop-down list. The drop-down list is located at the top-right corner of the page.

The data that is shown in this view is based on the current **View** pane selection.

See "Controlling the scope of Monitor views" on page 320.

The table that appears in this view displays the volume pool available for each master server. It also shows other media details that are associated with the master server like Frozen Media Count, Suspended Media Count etc.

The following columns are shown in the table:

Table 8-9 Media Summary View options

Option/Column Head	Description
Master Server	Name of the master server
Volume Pool name	Name of the volume pool that is associated with the master server
Frozen Media Count	Total number of the frozen media that is associated with the master server.

Table 8-9 Media Summary View options *(continued)*

Option/Column Head	Description
Suspended Media Count	Total number of the suspended media that is associated with the master server.
Full Media Count	Total number of the full media that are associated with the master server.
Active Media Count	Total number of active media that are associated with the master server.
Other Media Count	Total number of all other media like Multi Retention Level media, BE media etc. that are associated with the master server .
Available Media Count	Total number of the media that are available for the master server.
On Hold Media Count	Total number of the media that are on hold for the master server.

Hierarchical View by Volume Pool for monitoring media

This view is displayed when you select **Monitor > Media** and then select **Hierarchical View by Volume Pool** from the drop-down list. The drop-down list is located at the top-right corner of the page.

The data that is shown in this view is based on the current **View** pane selection.

See "Controlling the scope of Monitor views" on page 320.

The **Hierarchical View by Volume Pool** shows details of all media and also groups media by volume pool. Each volume pool that is shown in the **Media ID** column has a +sign before it. You can expand a volume pool to see all media that are a part of this volume pool. Note that the media are indented to the right-hand side in the Media ID column.

The sorting feature in this view applies only to media in the volume pool. When you expand a volume pool, the current selected sort order is applied to media in the pool.

The following tasks can be performed from this view:

View the details for volume pool	See "Viewing the details for volume pool" on page 366.
View details for the media that are a part of a specific volume pool	See "Viewing the details for media" on page 366.
Control media	See "Controlling media" on page 366.

Viewing the details for volume pool

Use the following procedure to view the details for a volume pool.

To view details for a volume pool

1. In the OpsCenter console, select **Monitor > Media**.
2. Select **Hierarchical View by Volume Pool** from the drop-down list. The drop-down list is located at the top-right corner of the page.
3. Click a volume pool (link) from the **Media ID** column. Note that a volume pool has a + sign on the left side. The details for the volume pool are shown in the **General** tab at the bottom of this view.

Viewing the details for media

Use the following procedure to view details for the media that are part of a specific volume pool.

To view the details for media

1. In the OpsCenter console, select **Monitor > Media**.
2. Select **Hierarchical View by Volume Pool** from the drop-down list. The drop-down list is located at the top-right corner of the page.
3. Expand a volume pool from the **Media ID** column. This column shows the media that are a part of the volume pool. Note that the media are indented to the right-hand side
4. Click the media ID (link). Details for the media are shown in the **General** tab at the bottom of the view.

Controlling media

Use the following procedure to freeze, unfreeze, suspend, or unsuspend specific media. Note that to perform these tasks the media must be assigned to NetBackup. The media is assigned if there is a date in the **Time Assigned** column.

Note: These tasks are not visible if you log on with an Analyst or a Reporter role.

To perform media tasks

1. In the OpsCenter console, select **Monitor > Media**.
2. Select **Hierarchical View by Volume Pool** from the drop-down list. The drop-down list is located at the top-right corner of the page.
3. Expand a volume pool from the **Media ID** column. This view shows the media that are a part of the volume pool. Note that the media are indented to the right-hand side
4. Select a media ID (use the check box).
5. Click **Freeze**, **Unfreeze**, **Suspend**, or **Unsuspend**. Note that these tasks are present on top of the table.

   The OpsCenter console may take some time to show the updated status once you perform these tasks.

Hierarchical View by Volume Group for monitoring media

This view is displayed when you select **Monitor > Media** and then select **Hierarchical View by Volume Group** from the drop-down list. The drop-down list is located at the top-right corner of the page.

The data that is shown in this view is based on the current **View** pane selection.

See "Controlling the scope of Monitor views" on page 320.

The **Hierarchical View by Volume Group** shows details of all media and also groups media by volume group. Each volume group shown in the **Media ID** column has a +sign before it. You can expand a volume group to see all media that are a part of this volume group. Note that the media are indented to the right-hand side in the Media ID column.

The sorting feature in this view applies to media in the volume group. When you expand a volume group, the current selected sort order is applied to media in that group.

You can perform the following tasks from this view:

View the details for a volume group	See "Viewing the details for a volume group" on page 368.

View details for the media that are part of a specific volume group	See "Viewing the details for media" on page 368.
Control media	See "Controlling media in OpsCenter" on page 368.

Viewing the details for a volume group

Use the following procedure to view the details for a specific volume group.

To view details for a volume group

1. In the OpsCenter console, select **Monitor > Media**.
2. Select **Hierarchical View by Volume Group** from the drop-down list. The drop-down list is located at the top-right corner of the page.
3. Click a volume group (link) from the **Media ID** column. Note that a volume group has a + sign on the left side. The details for the volume group are shown in the **General** tab at the bottom of this view.

Viewing the details for media

Use the following procedure to view details for media that are part of a specific volume group.

To view the details for media

1. In the OpsCenter console, select **Monitor > Media**.
2. Select **Hierarchical View by Volume Group** from the drop-down list. The drop-down list is located at the top-right corner of the page.
3. Expand a volume group from the **Media ID** column. This view shows the media that are a part of the volume group. Note that the media are indented to the right-hand side
4. Click the media ID (link). Details for the media are shown in the **General** tab at the bottom of the view.

Controlling media in OpsCenter

Use the following procedure to freeze, unfreeze, suspend, or unsuspend specific media. Note that to perform these tasks the media must be assigned to NetBackup. The media is assigned if there is a date in the **Time Assigned** column.

Note: These tasks are not visible if you log on with an Analyst or a Reporter role.

To perform media tasks

1. In the OpsCenter console, select **Monitor > Media**.
2. Select **Hierarchical View by Volume Group** from the drop-down list. The drop-down list is located at the top-right corner of the page.
3. Expand a volume group from the **Media ID** column. This view shows the media that are a part of the volume group. Note that the media are indented to the right-hand side
4. Select a media ID (use the check box).
5. Click **Freeze**, **Unfreeze**, **Suspend**, or **Unsuspend**. Note that these options are present on top of the table.

   The OpsCenter console may take some time to show the updated status once you perform these tasks.

Monitoring NetBackup devices

This view is displayed when you select **Monitor > Devices**.

This view contains the following two tabs:

Drives

This tab is shown by default when you select **Monitor > Devices**. The contents of the **Drives** tab are shown by default.

This view displays the current drive status information based on the current **View** pane selection.

See "Monitor > Devices > Drives List View options" on page 370.

See "Monitor > Devices > Drives Summary View" on page 374.

Disk Pools

This view displays detailed information about the disk pools that are configured for use by NetBackup based on the current View pane selection.

See "Monitor > Devices > Disk Pools options" on page 375.

Monitor > Devices > Drives List View options

This view is displayed when you select **Monitor > Devices > Drives**. This view shows the current drive status information. The data that is shown in this view is based on the current **View** pane selection.

See "Controlling the scope of Monitor views" on page 320.

The table that appears in this view shows the following information:

Table 8-10 Drives List View options

Option/Column Head	Description
Drive Name	The name that is assigned to the drive when it was added to NetBackup.
Device Host	The name of the device host where the drive is connected.
Master Server	Name of the master server that is associated with the drive.
Drive Type	Type of drive like 4mm, 8mm etc.
Robot Type	The type of robot that contains this drive.

Note: The List View does not show a drive that is unreachable or disabled. Similarly, if one of the paths for a drive is unreachable or disabled, it is not shown in the **Paths** tab that appears in the List View.

The Paths tab allows you to change the status of the selected drive: Up or Down.

Not all of the available columns appear initially in this view. The following columns do not appear, but can be added to your view by clicking the **Table Settings** icon:

- **Serial Number**
- **Cleaning Frequency**
- **Shared**
- **Inquiry Information**
- **Volume Header Path**
- **ACS**
- **LSM**
- **Panel**
- **Drive**

- **Vendor Drive Identifier**
- **Robot Number**
- **Robot Drive Number**
- **Recorded Media ID**
- **Assigned Host**
- **Control Host Name**
- **Control Mode**
- **Evsn**
- **Control Up**
- **Last Clean Time**
- **Local Control**
- **Mounted Time**
- **NDMP**
- **Occupy Index**
- **Opr Comment**
- **Ready**
- **Request ID**
- **Scan Host**
- **VM Host**
- **Write Enabled**

See the online *NetBackup Administration Console Help* for a detailed description of these fields.

More information about how to customize tables and view specific columns is available.

See "About using tables" on page 61.

About using the List View for monitoring drives

You can perform the following tasks from this view:

View the details for a single drive	See "Viewing the details for a single drive" on page 372.

View the details for a master server that is associated with a drive	See "Viewing the details for a master server associated with a drive" on page 372.
Use filters to view specific drives	See "Filtering on NetBackup drive category" on page 372.
Control drives	See "Controlling drives" on page 373.

Viewing the details for a single drive

All the details that are associated with a drive can be viewed from the Details pane. The Details pane is located at the bottom of the view.

To view the details for a single drive

1. Select **Monitor > Devices > Drives**. The List View is shown by default.
2. Click the drilldown link from the **Drive Name** column. The drive information can be viewed from the **General** and **Paths** tab of the Details pane. From the **General** tab, you can also click the master server link to see details about the master server that is associated with the drive.

Viewing the details for a master server associated with a drive

Use the following procedure to view details for a master server that is associated with a drive.

To view the details for a master server associated with a drive

1. Select **Monitor > Devices > Drives**. The List View is shown by default.
2. Click the drilldown link from the **Master Server** column. The master server information can be viewed from a separate page.

Filtering on NetBackup drive category

You can sort and filter this view to focus on the specific category of drives that you want to see. For example, you can apply a filter that displays only those drives that are up. You can filter by using any of the built-in filters. These filters are available from the drop-down list which is present on top of the table.

The following built-in filters are available:

All Drives	The All Drives filter is the default filter. Select this filter to view all drives.
Up Drives	Select this filter to view only those drives that are up. For up drives, all drive paths are up.
Down Drives	Select this filter to view only those drives that are down. For down drives, all drive paths are down.
Mixed Drives	Select this filter to view mixed drives. For mixed drives, some drive paths are up and some drive paths are down.

In addition to the built-in filters, you can create your own custom filters.

See "Creating, applying, editing, and removing custom view filters" on page 64.

Use the following procedure to view details of the drives by their status.

To filter details by type of drives

1. In the OpsCenter console, select **Monitor > Devices > Drives**. Ensure that **List View** is selected in the drop-down list.
2. Select a filter from the drop-down list. Note that the drop-down list is located on top of the table.

Controlling drives

See the *NetBackup Administrator's Guide, Volume I* for information on drive states and how to control drives.

Before you perform these tasks, manually refresh your Web browser to obtain an updated view of all drives. When you refresh, you also ensure that the drive is not involved in any tasks by other users.

Note: These tasks are not visible if you log on with an Analyst or a Reporter role.

To control drives

1. In the OpsCenter console, select **Monitor > Devices > Drives**. The List View is displayed by default.
2. Select a drive from the **Drive Name** column in the table.
3. Click **Up**, **Down**, or **Reset**. Note that these options are located on top of the drive details table.

   The OpsCenter console may take some time to show the updated status once you perform these tasks.

Monitor > Devices > Drives Summary View

This view is displayed when you select **Monitor > Devices > Drives** and then select **Summary View** from the drop-down list. The drop-down list is located at the top-right corner of the page.

The Summary view contains the following section:

See "Viewing the Drive Summary by Status" on page 374.

Viewing the Drive Summary by Status

The Drive Summary by Status section shows an overall distribution of drives by drive status for the current **View** pane selection. This information is shown in a pie chart as well as a table.

Note: The **Drive Summary by Status** section does not show the drives that are disabled or unreachable.

Each color of the pie chart represents how drives are distributed in your environment as per the drive status. You can also view the color code summary in this section to know the colors that represent different exit status. Moving your mouse over the pie chart shows the number and percentage of drives with up or down status in your NetBackup environment. For example, pointing to the green color in the pie chart shows that 5 drives or 100% drives in your environment are up.

Note: The **Drive Summary by Status** section can also be viewed from **Monitor > Overview**.

You can drill down from this section to see details of the drives that are up or down.

To view drives by drive status

1. In the OpsCenter console, select **Monitor > Devices > Drives**.
2. Select **Summary View** from the drop-down list. The drop-down list is located at the top-right corner of the page.
3. In the Drive Summary by Status section, do either of the following:
   - Click the number of drives (link) for a particular drive status from the table. For example, click the number for Up drives
     Or
   - Click a colored section of the pie chart that corresponds to a particular drive status. For example, click the green section of the pie chart to view details for the drives that are up.

Monitor > Devices > Disk Pools options

This view is displayed when you select **Monitor > Devices > Disk Pools**. This view displays detailed information about the disk pools that are configured for use by NetBackup. The data that is shown in this view is based on the current **View** pane selection.

See "Controlling the scope of Monitor views" on page 320.

Note: The following properties do not apply to cloud storage disk pools: Available Space, Raw Size, Usable Size, Low Water Mark (%), and High Water Mark (%).

All these values are derived from the storage capacity, which cannot be fetched from the cloud provider.

The table that appears in this view shows the following information:

Name	Name of the disk pool
Server Type	The storage server type. For OpenStorage, the server type depends on the vendor name.
Number of Volumes	Number of disk volumes in the disk pool.
Used Capacity	The amount of storage space in use.
Available Space	Space available on the disk pool
Raw Size	The total raw, unformatted size of the storage in the disk pool.

Usable Size	The estimated amount of disk space available for storage after file metadata overhead is taken into account.
Low Watermark (%)	The low water mark for the disk pool. (The default is 80%.) When the capacity of the disk pool returns to the low water mark, NetBackup again assigns jobs to the storage unit.
High Water Mark (%)	The high water mark for the disk pool (default is 98%.).
% Full	Percentage of the disk pool that is full.
Master Server	Name of the master server that is associated with the disk pool
State	State of the disk pool (like Up, Down etc.)

Not all of the available columns appear initially in this view. The following columns do not appear, but can be added to your view by clicking the **Table Settings** icon:

- **Imported**
- **Configured for Snapshots**
- **Primary**
- **Replication**

See the online *NetBackup Administration Console Help* for a detailed description of these fields.

More information about how to customize tables and view specific columns is available.

See "About using tables" on page 61.

You can perform the following task from this view:

View the details for a single disk pool	See "Viewing the details for a single disk pool" on page 376.

Viewing the details for a single disk pool

All the details that are associated with a disk pool can be viewed from the Details pane. The Details pane is located at the bottom of the view.

To view the details for a single disk pool

1. In the OpsCenter console, select **Monitor > Devices > Disk Pools**.
2. Click the drilldown link from the **Name** column. The disk pool information can be viewed from the **General** and **Disk Volume** tab of the Details pane. From the **General** tab, you can also click the master server link to see details about the master server that is associated with the disk pool.

About monitoring NetBackup hosts

This view is displayed when you select **Monitor > Hosts**.

This view contains the following subtabs:

Master Server	This tab is shown by default when you select **Monitor > Hosts**. This view displays detailed information about NetBackup master servers based on the current **View** pane selection. See "Monitor > Hosts > Master Servers view" on page 377.
Media Server	This view displays detailed information about NetBackup media servers based on the current **View** pane selection. See "Monitor > Hosts > Media Servers view" on page 379.
Client	This view displays detailed information about NetBackup clients based on the current **View** pane selection. See "Monitor > Hosts > Clients view" on page 380.

Monitor > Hosts > Master Servers view

This view shows details of master servers. The data that is shown in this view is based on the current **View** pane selection.

See "Controlling the scope of Monitor views" on page 320.

The table that appears in this view shows the following columns:

Table 8-11 Master Servers view options

Option/Column Head	Description
Master Server Name	Fully qualified domain name or IP address of the master server that is configured.
Display Name	The display name that you have chosen for the master server.
Operating System	Operating system of the master server.
Product	Back up product from where the data is being collected like PureDisk, Backup Exec etc.
Server Status	Shows the current state of the NetBackup Master Server: Connected, Not Connected, or Disabled. If the server status is 'Connected', the time since when the OpsCenter Server and the and master server are connected is also displayed. This does not necessarily represent the last time that OpsCenter collected information from the master server. See "NetBackup Master Server states in OpsCenter" on page 285.
Reason	Reason if any for the current server status.

You can perform the following task from this view:

Use filters to view specific master servers	See "Filtering by NetBackup master server type and status" on page 378.

Filtering by NetBackup master server type and status

You can sort and filter this view to focus on the specific type of master servers that you want to see. For example, you can apply a filter that displays Windows servers only. These filters are available from the drop-down list which is present on top of the table.

The built-in filters are the following:

All Servers (default filter)	Select this filter to view details of all master servers.
Connected Servers	Select this filter to view details of those master servers that are connected.
Not Connected Servers	Select this filter to view details of those master servers that appear as not connected.
Windows Servers	Select this filter to view details of Windows servers.
Solaris Servers	Select this filter to view details of Solaris servers.
Linux Servers	Select this filter to view details of Linux servers.
Other Servers	Select this filter to view details of all other master servers like AIX servers, HP-UX servers and so on.

In addition to the built-in filters, you can create your own custom filters.

See "Creating, applying, editing, and removing custom view filters" on page 64.

Use the following procedure to view details by type or status of master server.

To filter details by type or status of master server

1. In the OpsCenter console, select **Monitor > Hosts > Master Server**.
2. Select a filter from the drop-down list. Note that the drop-down list is located on top of the table.

Monitor > Hosts > Media Servers view

This view shows details of media servers. The data that is shown in this view is based on the current **View** pane selection.

See "Controlling the scope of Monitor views" on page 320.

The table that appears in this view shows the following columns:

Table 8-12 Media Servers view options

Option / Column Head	Description
Media Server Name	Name of the media server.

Table 8-12 Media Servers view options *(continued)*

Option / Column Head	Description
Master Server	Name of the master server that is associated with the media server.

You can perform the following tasks from this view:

View the details of a master server that is associated with a media server	See "Viewing the details of a master server that is associated with a media server" on page 380.

Viewing the details of a master server that is associated with a media server

Use the following procedure to view the details of a master server that is associated with a media server.

To view the details of a master server that is associated with a media server

1. In the OpsCenter console, select **Monitor > Hosts > Media Servers**.
2. Click the drilldown link from the **Master Server** column.

Monitor > Hosts > Clients view

This view shows details of NetBackup clients. The data that is shown in this view is based on the current **View** pane selection.

See "Controlling the scope of Monitor views" on page 320.

The table that appears in this view shows the following columns:

Table 8-13 Clients view options

Option / Column Head	Description
Client Name	Name of the client that is to be backed up.
Master Server	Name of the master server that is associated with the client.
OS Type	Operating system on the client like Linux, HP-UX etc.
Hardware	Hardware of the client computer like PC.
Is Offline	Shows Yes if the client is offline.

Table 8-13 Clients view options *(continued)*

Option / Column Head	Description
Offline Until	Date till the client is offline

You can click **Search Client** to search for specific clients on the page. You can search for clients using absolute host names or substrings.

You can perform the following task from this view:

View the details for a single master server	See "Viewing the details for a single master server" on page 381.

Viewing the details for a single master server

All the details for a master server that is associated with a client can be viewed from the **General** tab.

To view the details for a single master server

1. In the OpsCenter console, select **Monitor > Hosts > Client**.
2. Click the drilldown link in the **Master Server** column.

About monitoring NetBackup alerts

The **Monitor > Alerts** view provides details of NetBackup alerts. The data that is shown in this view is based on the current **View** pane and time frame selection. Data for the last 24 hours is shown by default. You can also view data for the last 48 hours or 72 hours.

See "Controlling the scope of Monitor views" on page 320.

Note: The OpsCenter console displays active alerts by default (these are the alerts that are not cleared).

You can view alerts that are specific to NetBackup Appliance 5330.

You can use the following views to see NetBackup alert information:

List View	The **List View** is shown by default when you select **Monitor > Alerts**. The **List View** shows active alerts by default. This view also lets you view detailed information about all NetBackup alerts and also filter, respond to alerts. See "Monitor > Alerts List View" on page 382.
Summary View	The **Summary View** only displays active alerts (these are the alerts that have not been cleared). The **Summary View** shows how active alerts are distributed in your environment as per the alert severity. This information is shown in a pie chart as well as a table. See "Summary View for monitoring NetBackup alerts" on page 390.

Monitor > Alerts List View

The List view is displayed when you select **Monitor > Alerts**. This view contains detailed information for alerts. This view provides tools to view and filter alerts, and to track user responses to alerts. The data that is shown in this view is based on the current **View** pane and time frame selection. Data for the last 24 hours is shown by default. You can also view data for the last 48 hours or 72 hours.

See "Controlling the scope of Monitor views" on page 320.

Note: The **List View** displays active alerts by default (these are the alerts that have not been cleared).

An option called **Ignore View filter** is added in the **View** drop-down list under **Monitor > Alerts**. **Ignore View filter** is selected by default when you click **Monitor > Alerts** List View. When you select **Ignore View filter** from the View Pane, all active alerts for the last 24 hours are displayed in the **Monitor > Alerts** view regardless of the views on which the alert policy is based. For example, selecting **Ignore View filter** displays an alert that is based on a view which has been deleted, or an alert that is based on a view for which you do not have access now. Also, the alert count shown in the **Alert Summary** pane at the bottom-left is based on the **Ignore View filter**. This means that the **Alert Summary** pane always displays all the alerts regardless of the views on which the alert policy is based.

The table that appears in this view shows the following information:

Table 8-14 Alerts List View options

Option	Description
Alert ID	Unique ID associated with each NetBackup alert.
Severity	The severity of the alert. The severity type helps you determine how quickly you want to respond.
Alert Policy	Name of the policy that is associated with the alert.
Alert Condition	The alert condition that is used for the alert.
Status	Current status of the alert like Active, Cleared etc.
Assigned To	Name of the individual to whom the alert has been assigned.
Time Raised	Time, date, and year when the alert was raised.
Last Update Time	Time, date, and year when the alert was modified.
Updated by	Name of the individual who last modified the alert.

Not all of the available columns appear initially in this view. The **Assignment State** column does not appear, but can be added to your view by clicking the **Table Settings** icon.

More information about how to customize tables and view specific columns is available.

See "About using tables" on page 61.

About using the List View to monitor NetBackup alerts

The following tasks can be performed from this view:

View the details for a single alert	See "Viewing the details for a single alert" on page 384.
View the details of an alert policy that is associated with the alert	See "Viewing the details of the alert policy associated with an alert" on page 385.
Use filters to view specific alerts	See "Filtering by alert type" on page 386.
Respond to alerts	See "Responding to alerts " on page 387.

Viewing the details for a single alert

All the details that are associated with an alert can be viewed from the Details pane. The Details pane is located at the bottom of the view.

To view the details of a single alert

1. In the OpsCenter console, select **Monitor > Alerts**.
2. Click a drill-down link from the **Alert ID** column. The alert details are shown under the **General** and **Comments** tabs. In addition to the information that is shown in the table, the **General** tab also shows master server, policy name, job ID, and exit status information. The Comments tab shows comments on the alert (if any), the time when these comments were provided, and the individual who last updated the alert.

Note: For certain alert types (for example High Job Failure Rate, High Drive Down, or High Suspended Media), the **Details** tab is also displayed. For example, for the High Job Failure Rate alert type, the **Details** tab shows the following details: % of failed jobs when the alert was raised and current failed Job count by master server, client, and policy.

See "Viewing the details of the alert policy associated with an alert" on page 385.

See "Filtering by alert type" on page 386.

See "Responding to alerts " on page 387.

Viewing the details of a single alert for Appliance hardware failure

In OpsCenter Monitor > Alerts UI, you can view the details that are associated with an Appliance hardware failure alert.

To view the details of a single hardware failure alert

1. On the OpsCenter GUI, click Monitor > Alerts.
2. Click the Alert ID link for which you want to view the details.
3. In the General tab at the bottom pane, the following details are displayed:

   Alert ID

   Alert Policy

   Alert Condition

   Assigned To

   Assignment State

   Status

   Last Update Time

   Updated By

   Severity

   Alert Raised on

   Tree Type

   Tree Name

   Nodes

   Host Name

   Hardware Failed

Viewing the details of the alert policy associated with an alert

Use the following procedure to view the details of the alert policy that is associated with an alert.

To view the details of alert policy associated with the alert

1. In the OpsCenter console, select **Monitor > Alerts**.
2. Click the drill-down link from the **Alert Policy** column.

See "Viewing the details for a single alert" on page 384.

See "Filtering by alert type" on page 386.

See "Responding to alerts " on page 387.

Filtering by alert type

Since the **Monitor > Alerts** view can include large numbers of alerts, a filter is available. You can use this filter to limit the types of alerts that appear.

You can filter on various severity levels or status settings, which lets you focus on only the specific alerts that interest you. For example, you can create and apply a filter that only displays the alerts that are acknowledged.

You can filter using any of the following built-in alert filters. These filters are available from the drop-down list which is present on top of the alert details table.

Active (default filter)	Select this filter to view Active alerts. This filter does not include the alerts that have been cleared.
Critical	Select this filter to only view the alerts whose severity is Critical.
Major	Select this filter to only view the alerts whose severity is Major.
Warning	Select this filter to only view the alerts whose severity is Warning.
Informational	Select this filter to only view the alerts whose severity is Informational.
Unassigned	Select this filter to only view the alerts that have not been assigned to anybody.
Assigned	Select this filter to only view the alerts that have been assigned to other OpsCenter users.
Acknowledged	Select this filter to only view the alerts that have been acknowledged by an OpsCenter user.

Cleared	Select this filter to only view the alerts that have been cleared. More information on cleared alerts is available. See "Responding to alerts " on page 387.
All Alerts	Select this filter to view the details of all alerts. This filter includes both active alerts and cleared alerts.

In addition to the built-in filters, you can create your own custom filters.

See "Creating, applying, editing, and removing custom view filters" on page 64.

Use the following procedure to view details by type of alerts.

To filter details by type of alert

1. In the OpsCenter console, select **Monitor > Alerts**.
2. Select a filter using the Filter drop-down list. For example, select **All Alerts** to view details of both active alerts and cleared alerts.

See "Viewing the details for a single alert" on page 384.

See "Viewing the details of the alert policy associated with an alert" on page 385.

See "Responding to alerts " on page 387.

Responding to alerts

You can manage OpsCenter alerts from the **Monitor > Alerts** view by adding comments or by assigning the alert to an individual for further review. You can also clear or acknowledge an alert. OpsCenter allows multiple users to process or take action on an alert.

When you acknowledge an alert, you inform other users who see the alert that action on the alert occurred. If you clear an alert, you cannot perform any further activity on the alert (for example, assign or acknowledge). Cleared alerts do not appear in the alert view by default.

Note: Under certain circumstances there may be issues among multiple OpsCenter users. For instance, an OpsCenter user comments on an alert while another OpsCenter user tries to clear the same alert.

The OpsCenter console displays active alerts by default (these are the alerts that have not been cleared). Some alerts (for example, Drive is Down) are cleared automatically when the condition is resolved.

You can view cleared alerts from **Monitor > Alerts** view (**List View**) by using the **Cleared** or **All Alerts** filter.

See "Filtering by alert type" on page 386.

The following alerts are cleared automatically when the condition is resolved:

- Drive is Down
- Lost Contact with Media Server
- Service Stopped
- Agent Server Communication Break
- Master Server Unreachable
- Frozen Media
- Suspended Media
- Disk Pool Full
- Disk Volume Down
- High Down Drives
- High Frozen Media
- High Suspended Media
- Low Available Media
- No Cleaning Tape
- Low Disk Volume Capacity
- Catalog Space Low
- Catalog not backed up
- Catalog backup disabled
- Incomplete Job
- Media Required for Restore
- Zero Cleaning Left
- Appliance Hardware Failure

Note: You can also purge NetBackup alert data from **Settings > Configuration > Data Purge** in the OpsCenter console based on a retention period that you specify. Any purged data is deleted permanently. This option is useful if you see OpsCenter performance degrade when there is a high number of alerts in the OpsCenter database.

See "Configuring the data purge period on the OpsCenter Server" on page 214.

To acknowledge an alert

1. In the OpsCenter console, select **Monitor > Alerts**.
2. Select an alert from the table.
3. Click **Acknowledge**.

To add a comment for an alert

1. In the OpsCenter console, select **Monitor > Alerts**.
2. Select an alert from the table.
3. Click **Add Comment**. You can add a comment as a reminder to yourself or for other users.

To clear an alert

1. In the OpsCenter console, select **Monitor > Alerts**.
2. Select an alert from the table.
3. Click **More** and then select **Clear** from the drop-down list.

To assign an alert to an individual

1. In the OpsCenter console, select **Monitor > Alerts**.
2. Select an alert from the table.
3. Click **Assign**.

   You can assign an alert to a user for their action or information.
4. Select a user to whom you want to assign the alert.
5. Click **OK**.

To change the policy that is associated with an alert

1. In the OpsCenter console, select **Monitor > Alerts**.
2. Select an alert from the table.

   The Alert Policy Wizard is also used to create a policy.
3. Click **More** and then select **Edit Policy** from the drop-down list.

See "About understanding alert counts in the Monitor view" on page 435.

See "Viewing the details for a single alert" on page 384.

See "Viewing the details of the alert policy associated with an alert" on page 385.

See "Filtering by alert type" on page 386.

Summary View for monitoring NetBackup alerts

The **Summary View** gives an overall summary of alerts by severity. It contains the **Alert Summary by Severity** section which shows an overall distribution of alerts by severity for the current **View** pane and time frame selection. This information is shown in a pie chart as well as a table. Data for the last 24 hours is shown by default. You can also view data for the last 48 hours or 72 hours.

See "Controlling the scope of Monitor views" on page 320.

A pie chart with different colors represents the alert distribution by severity in this section. Each color of the pie chart represents how alerts are distributed in your environment as per the alert severity. You can also view the color code summary in this section to know the colors that represent different severity.

Note: The **Summary View** only displays active alerts (these are the alerts that have not been cleared).

Moving your mouse over the pie chart displays the number and percentage of alerts with a particular severity in your NetBackup environment. For example, pointing to the green color in the pie chart shows that in the last 24 hours, 200 alerts, or 17% alerts in your environment are critical.

An option called **Ignore View filter** has been added in the **View** drop-down list under **Monitor > Alerts**. When you select **Ignore View filter** from the View Pane, all active alerts in the last 24 hours are displayed in the **Monitor > Alerts** view regardless of the views on which the alert policy is based. For example, selecting **Ignore View filter** displays an alert that is based on a view which has been deleted, or an alert that is based on a view for which you do not have access now. When you select a view from the **View** drop-down list (including **Ignore View filter**), the last 24 hours data is displayed by default.

Note that the **Alert Summary** pane at the bottom-left displays all the alerts that exist in the OpsCenter database. This means that the **Alert Summary** pane displays all the alerts regardless of the views on which the alert policy is based.

Note: The **Alert Summary by Severity** section can also be viewed from **Monitor > Overview**.

You can drill down from this section to see details for alert categories.

See "Viewing alerts by severity" on page 391.

See "Viewing alerts by NetBackup Master Server" on page 391.

See "About understanding alert counts in the Monitor view" on page 435.

Viewing alerts by severity

You can drill down to see details for alert categories.

To view alerts by severity

1. In the OpsCenter console, select **Monitor > Alerts**.
2. Select **Summary View** from the drop-down list. The drop-down list is located at the top-right corner of the page.
3. In the **Alert Summary by Severity** section, do either of the following:
   - Click the number of alerts (link) for a particular alert severity from the table. For example, click the number that is shown for Critical alerts.

     Or
   - Click a colored section of the pie chart that corresponds to a particular alert severity. For example, click the red section of the pie chart to view details for critical alerts.

See "Summary View for monitoring NetBackup alerts" on page 390.

Viewing alerts by NetBackup Master Server

You can view all the alerts that are grouped by NetBackup master server. The new Group Component Summary table shows the OpsCenter alerts grouped by master server.

To view the Group Component Summary table, do the following:

1. Logon to the OpsCenter GUI.
2. Carry out the following step as a prerequisite to display the Group Component Summary table:

   Go to **Settings > User Preferences > General tab** and clear the Allow Multiple Selection In View Pane check box.

3 Click **Monitor** > **Alerts**.

4 Select the Summary View from the drop-down list.

5 Select ALL_MASTER_SERVERS or the master server for which you want to view the alert summary. The Group Component Summary table is displayed.

Note: If you select 'Ignore View filter', the Group Component Summary table is not displayed.

From the Group Component Summary table you can click the server name link to view its details, namely, the Alert ID, Alert Policy, Nodes and so on.

About monitoring Audit Trails

You can manage and monitor audit trails using the OpsCenter features.

Additional information about the Audit Trails report

See "Audit Trails report" on page 393.

See "What Audit Trails track" on page 392.

See "About OpsCenter features for Audit Trails" on page 394.

See "Creating a custom filter to view audit trail data" on page 394.

See "About managing Audit Trails settings" on page 395.

What Audit Trails track

An audit trail is a record of all the user initiated activities. An audit trail consists of the changes that are made in the NetBackup environment. For example, changes such as creating a policy, deactivating a policy, or modifying a policy. The audit trails feature in OpsCenter lets you enable audit trail logging for NetBackup.

Note: OpsCenter monitors, reports, and manages audit trails for the NetBackup master servers for the version 7.1 or later.

You can control the audit settings and generate an Audit Trails Report. Through OpsCenter, you can set the audit logs retention period and also enable or disable audit trail logging.

Audit trails display the following information in the form of columns:

Column heading	Description
Category	Displays the changes that are made to policies, storage units, jobs, audit configuration, audit service, pool, and storage server. For example, when a storage unit is added, modified, or deleted.
Action	Displays the action performed, such as whether a policy is modified, a storage unit is created, or a storage server is deleted.
Description	Gives a brief information about the category and the action performed. It also gives the identity of the category.
User	Gives the information about the user who initiated the action.
Timestamp	Displays the time when the action was performed.
Master Server	Displays the name of the master server on which the action is performed.
Reason	Displays the reason for the change that is made, if given by the user who makes the change. By default, the column is hidden.
Details	Displays the old and new values of the attributes that are modified. Some of the attributes that are modified are Clients, Hardware, Operating System (OS), and Policy Generation.

Audit Trails report

The Audit Trails report is a high-level summary report that is added to the reports tree. This report displays the number of changes that are made in the NetBackup environment. The report is displayed in the form of a chart. You can view the report in a Distribution chart or Historical chart format

The chart displays the count of audit records for each category. Some of the categories are Policy, Audit Configuration, Job, Audit service, Storage unit, Pool, and Storage Server. You can hover the mouse on each colored section of the chart to know the count and the percent changes for each category. You can drill down the report by clicking any colored section of the chart. You can view the count of changes for each action for the selected category. For example, if you click the Policy section, the chart displays the total audit count for policies created, policies modified, and policies deleted.

To view the Audit Trails report, go to **Reports > Report templates > Audit Reports > Audit Trails Report**.

To view the details of the audit trails report in a tabular form, click the link **Show Chart as Table**. The table displays information about the Audit Category, Total

Audit Count, and Percentage. The table also displays the information about Audit Action when you drill down the chart.

About OpsCenter features for Audit Trails

OpsCenter helps you to configure audit logging and generate the Audit report. Through OpsCenter, you can:

- Manage the audit settings of the NetBackup master server.
- Monitor audit trails.
- Generate alerts if audit service goes down.
- Configure audit trail retention period in OpsCenter.

Use the various features of OpsCenter and generate the Audit report. You can enable or disable the audit settings, and set the retention period of the logs. You can set OpsCenter to generate alerts when the NetBackup Audit manager services are turned on or off. You can also set the retention period for the audit logs.

Creating a custom filter to view audit trail data

OpsCenter helps you to monitor the audit trails. To monitor them, select **Monitor** > **Audit Trails**. You can use predefined filters based on category and action to display the contents of the Audit trails and also create custom filters.

You can view information about predefined and custom filters.

See "Creating, applying, editing, and removing custom view filters" on page 64.

To create a custom filter to view audit trail data

1. Select the **Create Filter** icon. The **Edit Audit filter** dialog box is displayed.
2. Enter a name for the filter in the **Name** field.
3. Select the column name that you want to filter from the drop-down list. The options available are **Category, Action, User Name, Domain Name, Domain Type, Time Stamp, Object Name,** and **Master Server**. **Object Name** is filtered based on the entity names present in the description.

   From the **Operator** drop-down list, select the operator =. Use != if you do not want to match a specific value.

   In the **Value** text box, enter or select a value. If you select **Time Stamp** as the column, a calendar icon appears for value. Click the calendar icon to choose the required date and click **OK**.
4. Select **And** or **Or** from the drop-down list to build the filter query.

5. To add more columns to the query, click **Add** and select the required column name. To remove the column that is created, select **Remove**.
6. Once you are done adding the required columns to the filter, click **OK**. The new view filter is displayed in the filter drop-down list.

   You can view more information about applying the filter, editing the filter, and deleting the filter.

   See "View filters in OpsCenter" on page 314.

About managing Audit Trails settings

You can manage the settings to enable the auditing for the selected master server through OpsCenter. You must have Admin privileges to configure the audit settings.

See "Managing audit trails settings" on page 497.

Monitor > Appliance Hardware > Master Server

This view lets you monitor the hardware summary of appliance master servers that are added to the OpsCenter Analytics console. The view provides a quick visual cue to hardware status. You can monitor any hardware failures in the appliance master servers that are added to the OpsCenter console.

OpsCenter can monitor the appliance 2.0 master servers.

Adding an appliance master server is similar to adding a regular master server to OpsCenter. More information on how to add an appliance master server to the OpsCenter console is available.

See "Adding a master server or appliance in OpsCenter" on page 285.

This view provides the information that is monitored for each piece of hardware in your NetBackup appliance master server. The table displays the following details:

Name	This column lists the names of the appliance master servers (link) that are added to the OpsCenter console. Click the link to view the appliance summary. More information about the hardware details that are monitored is available. See "Appliance hardware details" on page 408.
Data Collection	This column lists the date and time when the last data collection occurred. Data collection takes place after every 15 minutes by NBSL.

CPU

The icon provides a quick visual cue to the CPU status. The following values are possible:

- Green/OK
- Yellow/Presence Unknown
- Red/failure.

The icon that is depicted is based on monitoring the CPU presence and voltage to the appliance CPU chip. A CPU failure is reported if any of the following conditions occur:

- No voltage
- Voltage less than 0.99 volts
- Voltage more than 1.25 volts

Disk

The icon provides a quick visual cue to the disk status. The following values are possible:

- Green/OK
- Yellow/Presence Unknown
- Red/failure

The icon that is depicted is based on monitoring the boot drive and the storage drives. A disk failure is reported if an internal erroneous state occurs.

RAID

The icon provides a quick visual cue to the RAID status. The following values are possible:

- Green/OK
- Yellow/Presence Unknown
- Red/failure.

The icon that is depicted is based on monitoring the RAID status. An error is reported if the status changes from optimal.

Fan	The icon provides a quick visual cue to the fan status. The following values are possible: ■ Green/OK ■ Yellow/Presence Unknown ■ Red/failure. The icon that is depicted is based on monitoring the fan speed and reports a fan failure when the following conditions occur: ■ Fan speed less than 1974 rpm ■ Fan speed more than 8977 rpm ■ If there is a failure with the Fan, a **Critical** warning is displayed. ■ If the Fan is not installed, a **Not Installed** warning is issued.
Power Supply	The icon provides a quick visual cue to the power supply. The following values are possible: ■ Green/OK ■ Yellow/Presence Unknown ■ Red/failure. The icon that is depicted is based on monitoring the power supply wattage and reports a failure when the following conditions occur: ■ Wattage is **0** watts ■ Wattage more than **700** watts The following status warning are also provided: ■ **Not Available** - Occurs if the power module is installed and no power is supplied. That can occur because it is not connected to the power outlet or some other reason. ■ **Not Installed** - Occurs if the Power Module is pulled out. ■ **Critical** - Occurs if the Power Module is operated with a warning.

Temperature	The icon provides a quick visual cue to the temperature. The following values are possible: ■ Green/OK ■ Yellow/Presence Unknown ■ Red/failure. The icon that is depicted is based on monitoring the temperature of the appliance at different points and reports a failure if the following limits are exceeded: ■ **Intake Vent Temp** Lower than 0° C or higher than 60° C ■ **Outtake Vent Temp** Lower than 0° C or higher than 60° C ■ **Backplane Temp** Lower than 0° C or higher than 60° C
FC HBA	The icon provides a quick visual cue to the Fibre Channel HBA's. The following values are possible: ■ Green/OK ■ Yellow/Presence Unknown ■ Red/failure. The icon that is depicted is based on monitoring the status and reports a failure if the status changes from online.
Manage	The icon is a link to the Appliance console. Click the icon to access the Appliance console.

See “Monitor > Appliance Hardware > Media Server” on page 398.

Monitor > Appliance Hardware > Media Server

This view lets you monitor the hardware summary of appliance media servers that are monitored from the OpsCenter Analytics console. The view provides a quick visual cue to the hardware status.

Only appliance 1.2 and 2.0 media servers that are attached to appliance 2.0 master server or to a regular NetBackup 7.5 master server can be monitored from OpsCenter. Data collection from the appliance media servers takes place after every 15 minutes via NBSL. You can monitor any hardware failures in the appliance media servers that are monitored from the OpsCenter console.

Note that you cannot add an appliance media server directly to the OpsCenter console. You can add an appliance master server or a regular master server to which it is connected.

See "Adding a master server or appliance in OpsCenter" on page 285.

This view provides the information that is monitored for each piece of hardware in your NetBackup media appliance. The table displays the following details:

Name	This column lists the names of the appliance media servers (link) that are monitored from the OpsCenter console. Click the link to view the appliance summary. More information about the hardware details that are monitored is available. See "Appliance hardware details" on page 408.
Master Server	This column lists the appliance master server or the regular NetBackup master server that the appliance media server is connected to.
Data Collection	This column lists the date and time when the last data collection occurred. Data collection takes place after every 15 minutes via NBSL.
CPU	The icon provides a quick visual cue to the CPU status. This may have the following values: ■ Green=OK ■ Yellow=warning ■ Red=failure The icon that is depicted is based on monitoring the CPU presence and voltage to the appliance CPU chip. A CPU failure is reported if any of the following conditions occur: ■ No voltage ■ Voltage less than 0.99 volts ■ Voltage more than 1.25 volts
Disk	The icon provides a quick visual cue to the disk status. This may have the following values: ■ Green=OK ■ Yellow=warning ■ Red=failure The icon that is depicted is based on monitoring the boot drive and the storage drives. A disk failure is reported if an internal erroneous state occurs.

RAID

The icon provides a quick visual cue to the RAID status. This may have the following values:

- Green=OK
- Yellow=warning
- Red=failure

The icon that is depicted is based on monitoring the RAID status. An error is reported if the status changes from optimal.

Fan

The icon provides a quick visual cue to the fan status. This may have the following values:

- Green=OK
- Yellow=warning
- Red=failure

The icon that is depicted is based on monitoring the fan speed and reports a fan failure when the following conditions occur:

- Fan speed less than 1974 rpm
- Fan speed more than 8977 rpm
- If there is a failure with the Fan, a **Critical** warning is displayed.
- If the Fan is not installed, a **Not Installed** warning is issued.

Power Supply

The icon provides a quick visual cue to the power supply. This may have the following values:

- Green=OK
- Yellow=warning
- Red=failure

The icon that is depicted is based on monitoring the power supply wattage and reports a failure when the following conditions occur:

- Wattage is **0** watts
- Wattage more than **700** watts

The following status warning are also provided:

- **Not Available** - Occurs if the power module is installed and no power is supplied. That can occur because it is not connected to the power outlet or some other reason.
- **Not Installed** - Occurs if the Power Module is pulled out.
- **Critical** - Occurs if the Power Module is operated with a warning.

Temperature	The icon provides a quick visual cue to the temperature. This may have the following values: ■ Green=OK ■ Yellow=warning ■ Red=failure The icon that is depicted is based on monitoring the temperature of the appliance at different points and reports a failure if the following limits are exceeded: ■ **Intake Vent Temp** Lower than 0° C or higher than 60° C ■ **Outtake Vent Temp** Lower than 0° C or higher than 60° C ■ **Backplane Temp** Lower than 0° C or higher than 60° C
FC HBA	The icon provides a quick visual cue to the Fibre Channel HBA's. This may have the following values: ■ Green=OK ■ Yellow=warning ■ Red=failure The icon that is depicted is based on monitoring the status and reports a failure if the status changes from online.
Manage	The icon is a link to the Appliance console. Click the icon to access the Appliance console.

See “Monitor > Appliance Hardware > Master Server” on page 395.

Monitor > Appliance Hardware > NetBackup

This view provides the summary of NetBackup appliances - master and media servers - that are added to the OpsCenter Analytics console. The view provides a visual cue to hardware status. You can monitor any hardware failures in the NetBackup appliances (master and media servers) that are added to the OpsCenter console.

See “Appliance hardware details” on page 408.

OpsCenter can monitor the NetBackup appliance 2.0 master servers.

Only appliance 1.2 and 2.0 media servers that are attached to NetBackup appliance 2.0 master server or to a regular NetBackup master server can be monitored by

OpsCenter. Data collection from the appliance media servers takes place after every 15 minutes via NBSL. You can monitor any hardware failures in the appliance media servers that are monitored from the OpsCenter console.

Adding a NetBackup appliance master server is similar to adding a regular master server to OpsCenter. More information on how to add an appliance master server to the OpsCenter console is available.

See "Adding a master server or appliance in OpsCenter" on page 285.

Note: Note that you cannot add a NetBackup appliance media server directly to the OpsCenter console. You can add an appliance master server or a regular master server to which the media server is connected.

This view provides the information that is monitored for each piece of hardware in your NetBackup appliance. The table displays the following details:

Host Name	Name of the NetBackup appliance host (master or media server) that is monitored by OpsCenter.
Master Server	Name of the NetBackup master server that is associated with this appliance.
Host Type	Type of the NetBackup appliance host: master server appliance or media server appliance.
Data Collection	This column lists the date and time when the last data collection occurred. Data collection takes place after every 15 minutes by NBSL.
CPU	The icon provides a quick visual cue to the CPU status. The following values are possible: ■ Green/OK ■ Yellow/Presence Unknown ■ Red/failure. The icon that is depicted is based on monitoring the CPU presence and voltage to the appliance CPU chip. A CPU failure is reported if any of the following conditions occur: ■ No voltage ■ Voltage less than 0.99 volts ■ Voltage more than 1.25 volts

Disk

The icon provides a quick visual cue to the disk status. The following values are possible:

- Green/OK
- Yellow/Presence Unknown
- Red/failure

The icon that is depicted is based on monitoring the boot drive and the storage drives. A disk failure is reported if an internal erroneous state occurs.

RAID

The icon provides a quick visual cue to the RAID status. The following values are possible:

- Green/OK
- Yellow/Presence Unknown
- Red/failure.

The icon that is depicted is based on monitoring the RAID status. An error is reported if the status changes from optimal.

Fan

The icon provides a quick visual cue to the fan status. The following values are possible:

- Green/OK
- Yellow/Presence Unknown
- Red/failure.

The icon that is depicted is based on monitoring the fan speed and reports a fan failure when the following conditions occur:

- Fan speed less than 1974 rpm
- Fan speed more than 8977 rpm
- If there is a failure with the Fan, a **Critical** warning is displayed.
- If the Fan is not installed, a **Not Installed** warning is issued.

Power Supply

The icon provides a quick visual cue to the power supply. The following values are possible:

- Green/OK
- Yellow/Presence Unknown
- Red/failure.

The icon that is depicted is based on monitoring the power supply wattage and reports a failure when the following conditions occur:

- Wattage is **0** watts
- Wattage more than **700** watts

The following status warning are also provided:

- **Not Available** - Occurs if the power module is installed and no power is supplied. That can occur because it is not connected to the power outlet or some other reason.
- **Not Installed** - Occurs if the Power Module is pulled out.
- **Critical** - Occurs if the Power Module is operated with a warning.

Temperature

The icon provides a quick visual cue to the temperature. The following values are possible:

- Green/OK
- Yellow/Presence Unknown
- Red/failure.

The icon that is depicted is based on monitoring the temperature of the appliance at different points and reports a failure if the following limits are exceeded:

- **Intake Vent Temp**
  Lower than 0° C or higher than 60° C
- **Outtake Vent Temp**
  Lower than 0° C or higher than 60° C
- **Backplane Temp**
  Lower than 0° C or higher than 60° C

FC HBA

The icon provides a quick visual cue to the Fibre Channel HBA's. The following values are possible:

- Green/OK
- Yellow/Presence Unknown
- Red/failure.

The icon that is depicted is based on monitoring the status and reports a failure if the status changes from online.

Manage	The icon is a link to the Appliance console. Click the icon to access the Appliance console.

Monitor > Appliance Hardware > Deduplication

OpsCenter can centrally monitor the hardware information of multiple deduplication appliances. You can monitor a deduplication appliance that is deployed as a standalone Storage Pool Authority (SPA), as a Content Router (CR), or as a PureDisk deduplication option (PDDO) storage server to a NetBackup domain. You can add a deduplication appliance master server in OpsCenter to monitor it. You can also configure hardware alerts for both NetBackup and deduplication appliances and view deduplication reports using OpsCenter.

This tab provides the summary of Deduplication appliances that are added to the OpsCenter Analytics console. The view provides a visual cue to hardware status. You can monitor any hardware failures in the Deduplication appliance master servers that are added to the OpsCenter console.

See "Appliance hardware details" on page 408.

Note: Where Amazon is the cloud service provider, OpsCenter cannot report on the data that MSDP cloud storage servers upload to the cloud.

This view provides the information that is monitored for each piece of hardware in your Deduplication appliance. The table displays the following details:

Host Name	Name of the Deduplication appliance host that is monitored by OpsCenter.
Host Type	Type of the Deduplication appliance host: SPA or CR.
Data Collection	This column lists the date and time when the last data collection occurred. Data collection takes place after every 15 minutes .

CPU

The icon provides a quick visual cue to the CPU status. The following values are possible:

- Green/OK
- Yellow/Presence Unknown
- Red/failure.

The icon that is depicted is based on monitoring the CPU presence and voltage to the appliance CPU chip. A CPU failure is reported if any of the following conditions occur:

- No voltage
- Voltage less than 0.99 volts
- Voltage more than 1.25 volts

Disk

The icon provides a quick visual cue to the disk status. The following values are possible:

- Green/OK
- Yellow/Presence Unknown
- Red/failure

The icon that is depicted is based on monitoring the boot drive and the storage drives. A disk failure is reported if an internal erroneous state occurs.

RAID

The icon provides a quick visual cue to the RAID status. The following values are possible:

- Green/OK
- Yellow/Presence Unknown
- Red/failure.

The icon that is depicted is based on monitoring the RAID status. An error is reported if the status changes from optimal.

Fan	The icon provides a quick visual cue to the fan status. The following values are possible: ■ Green/OK ■ Yellow/Presence Unknown ■ Red/failure. The icon that is depicted is based on monitoring the fan speed and reports a fan failure when the following conditions occur: ■ Fan speed less than 1974 rpm ■ Fan speed more than 8977 rpm ■ If there is a failure with the Fan, a **Critical** warning is displayed. ■ If the Fan is not installed, a **Not Installed** warning is issued.
Power Supply	The icon provides a quick visual cue to the power supply. The following values are possible: ■ Green/OK ■ Yellow/Presence Unknown ■ Red/failure. The icon that is depicted is based on monitoring the power supply wattage and reports a failure when the following conditions occur: ■ Wattage is **0** watts ■ Wattage more than **700** watts The following status warning are also provided: ■ **Not Available** - Occurs if the power module is installed and no power is supplied. That can occur because it is not connected to the power outlet or some other reason. ■ **Not Installed** - Occurs if the Power Module is pulled out. ■ **Critical** - Occurs if the Power Module is operated with a warning.

Temperature

The icon provides a quick visual cue to the temperature. The following values are possible:

- Green/OK
- Yellow/Presence Unknown
- Red/failure.

The icon that is depicted is based on monitoring the temperature of the appliance at different points and reports a failure if the following limits are exceeded:

- **Intake Vent Temp**
  Lower than 0° C or higher than 60° C
- **Outtake Vent Temp**
  Lower than 0° C or higher than 60° C
- **Backplane Temp**
  Lower than 0° C or higher than 60° C

FC HBA

The icon provides a quick visual cue to the Fibre Channel HBA's. The following values are possible:

- Green/OK
- Yellow/Presence Unknown
- Red/failure.

The icon that is depicted is based on monitoring the status and reports a failure if the status changes from online.

Manage

The icon is a link to the Appliance console. Click the icon to access the Appliance console.

Appliance hardware details

The following table describes the hardware that is monitored.

Table 8-15 Appliance hardware that is monitored

Monitored Hardware	Sample of collected data
CPU	Monitors the following: - **Status** - Monitors the status of the CPU, such as, **Presence detected** and **No CPU(s) detected**. - **Voltage** - Monitors the voltage to the appliance CPU chip

Table 8-15 Appliance hardware that is monitored *(continued)*

Monitored Hardware	Sample of collected data
Disk	This view provides the following information: ■ **Slot No** - Slot in the robot that contains the volume. ■ **Status** - Current status of the media. The status can be Frozen, Active, etc. ■ **Capacity** - Capacity that is in use. ■ **Type** - The type of disk that is configured. ■ **Enclosure ID** - ID of the enclosure that the disk resides in.
RAID	Monitors the RAID status and reports an error if the status changes from optimal. The following data is collected: ■ Name - The name of the RAID device. ■ Status - Shows the current status of the device, such as **Optimal**. ■ Capacity - The capacity of each device. ■ Type - The type of RAID device, such as RAID1 and RAID 6. ■ Disks - The disks being used .
Fan	Monitors the following: ■ **Status** - Monitors the status of the fan, such as, **Presence detected** and **No Fan(s) detected**. ■ **Speed** - Monitors the fan speed
Power Supply	Monitors the power supply wattage.
Temperature Information	Monitors the temperature of the appliance at different points.
Fibre Channel HBA	Monitors the status and reports a failure, if the status changes from online. The following data is collected: ■ Status - Current status of the HBA. ■ World Wide Port Name - The port currently in use for a specific device. ■ Speed - Speed at which the HBA operates like 8gbit/s ■ Mode - Mode that is configured for the HBA like Initiator
The following details are specific to NetBackup 5330 Appliance:	

Table 8-15 Appliance hardware that is monitored *(continued)*

Monitored Hardware	Sample of collected data
Expansion Storage Shelf: Disk	The following data of the Expansion Storage Shelf disk is collected: ■ ID ■ Slot No - Slot in the robot that contains the volume. For example: Slot 1 ■ Drawer no For example: Drawer 1 ■ Tray No For example: Tray 0 ■ Status - Current status of the media. For example: Optimal ■ Capacity - Capacity that is in use. For example: 2.794TB
Expansion Storage Shelf: Fan	The following data of the Expansion Storage Shelf fan is collected: ■ ID ■ Location For example: Tray 0 Right ■ Status - Current status of the device. For example: Optimal
Expansion Storage Shelf: Power Supply	The following data for the Expansion Storage Shelf power supply is collected: ■ ID ■ Location For example: Top ■ Status For example: Optimal
Expansion Storage Shelf: Temperature	The following data for the Expansion Storage Shelf temperature is collected: ■ ID ■ Location For example: Tray 0 Drawer 1 Left ■ Status For example: Optimal

Table 8-15 Appliance hardware that is monitored *(continued)*

Monitored Hardware	Sample of collected data
Primary Storage Shelf: Controller	The following data for the Primary Storage Shelf controller is collected: ■ ID ■ Location For example: Tray 99 Slot A ■ Data Cache ■ Status For example: Optimal
Primary Storage Shelf: Primary Storage Shelf to Expansion Storage Shelf Connection	The following data for the primary - expansion storage connection is collected: ■ ID ■ Primary Storage Shelf Port ■ Expansion Storage Shelf Port
Primary Storage Shelf: Volume	The following Primary Storage Shelf volume data is collected: ■ ID ■ LUN For example: 0 ■ Volume Group For example: 0_1 ■ Capacity For example: 19.099 TB ■ WWID For example: 60080e500032171c00000c7d531764f4
Primary Storage Shelf: Volume Group	The following data for the Primary Storage Shelf volume group is collected: ■ ID ■ Name For example: 0_1 ■ RAID Level For example: 6 ■ Disks For example: [Tray:0 Drawer:1 Slot:1 4] [Tray:0 Drawer:2 Slot:1 4] [Tray:0 Drawer:3 Slot:1 4] [Tray:0 Drawer:4 Slot:1] [Tray:0 Drawer:5 Slot:2 5] ■ Capacity For example: 19.099 TB

Table 8-15 Appliance hardware that is monitored *(continued)*

Monitored Hardware	Sample of collected data
Primary Storage Shelf: Disk	The following data for the Primary Storage Shelf disk is collected: ■ ID ■ Slot No - Slot in the robot that contains the volume. For example: Slot 1 ■ Drawer No For example: Drawer 1 ■ Tray No For example: Tray 0 ■ Status For example: Optimal ■ Capacity For example: 2.794TB
Primary Storage Shelf: Fan	The following data for the Primary Storage Shelf fan is collected: ■ ID ■ Location For example: Tray 99 Right ■ Status For example: Optimal
Primary Storage Shelf: Power Supply	The following data for the Primary Storage Shelf power supply is collected: ■ ID ■ Location For example: Top ■ Status For example: Optimal
Primary Storage Shelf: Temperature	The following data for the Primary Storage Shelf temperature is collected: ■ ID ■ Location For example: Tray 99 Drawer 1 Left ■ Status For example: Optimal

Monitor > Cloud options

The data on this page is applicable only if you select a view of type Master Server. Select the master server from the View Pane for which you want to view cloud data. Expanding the master server lists the media servers below it that are configured for Cloud.

The cloud data is collected from the master server through NBSL after every 15 minutes.

Select any or all of the media servers to view related data in the Content pane.

The **Cloud Storage Providers Overview** section lists the providers that are configured on the selected media servers.

The following cloud providers are supported by OpsCenter:

- Amazon S3
- AT&T
- Rackspace

Note: Among all Amazon S3-compatible cloud providers that NetBackup supports, OpsCenter can monitor and generate reports for Amazon S3 only.

The **Cloud Storage Providers Overview** section shows the data that is backed up and restored for the current month in GB. In case you have just installed OpsCenter, this section shows the current metering data which is collected after you add the master server to OpsCenter. Data is collected from the day the master server is added to OpsCenter.

The link at the bottom of each Cloud provider lists the number of media servers for which the specific Cloud provider is configured. Click the link to know the names of the media servers for which the specific cloud provider is configured.

The **Cloud Connect Overview** section shows what all data is being written to the Cloud and also data that is being read from the Cloud. The default timeframe for the Cloud Connect Overview section is Last 24 hours. You can also view data for the last 48 hours or the last 72 hours by clicking **Last 48 Hours** or **Last 72 Hours** respectively.

The **Live Metering: Data written to cloud** chart shows how much data is being written in accordance with the metering time. Similarly, **Live Metering: Data read from cloud** chart shows how much data is being read from the cloud in accordance with the metering time.

The **Summary of data transferred** table gives the summary of data downloaded and uploaded for each media server in the selected timeframe. The **Data transferred**

per provider table gives the data uploaded for each cloud provider in the selected timeframe.

The **Backup Job Summary** shows the backup job summary for the selected timeframe in the form of a pie chart. Only backup jobs for the Cloud are considered in this chart. It shows the number of Cloud backup jobs that are successful, partially successful, or failed. Click the link (number) to monitor the progress from **Monitor > Jobs**.

Chapter 9

Managing NetBackup using OpsCenter

This chapter includes the following topics:

- About the Manage views
- Controlling the scope of Manage views
- About managing alert policies
- About managing NetBackup storage
- About managing NetBackup devices
- About Operational Restore and Guided Recovery operations
- About managing NetBackup Hosts
- About managing NetBackup Deployment Analysis

About the Manage views

The NetBackup Appliance enables you to use the NetBackup Administration Console to manage your clients, create policies, run backups, and perform other administration functions. For information on how to perform these functions from the NetBackup Administration Console, you must refer to your NetBackup core documentation set. If you want to download the latest versions of this documentation set, you can do so from the Veritas Support Web site. For help using the NetBackup Administration Console, refer to the *NetBackup Administrator's Guide, Volume I* on the Support Web site.

From the **Manage** tab and associated subtabs, you can view and manage your NetBackup environment, which also includes OpsCenter alert policies, storage, and devices.

Note that OpsCenter or OpsCenter Analytics can only monitor and manage NetBackup or NetBackup Appliances. They cannot monitor or manage other products like NetBackup PureDisk or Backup Exec.

The OpsCenter server collects data from NetBackup master servers, stores it in a database, and displays it on demand. NetBackup sends most of the data and it appears almost instantaneously after it changes. (Network, system delays, or browser refresh settings can affect how quickly it appears). This data is collected mainly using notifications. For most operations and changes in NetBackup, NBSL sends a notification to OpsCenter.

See "How OpsCenter collects data from NetBackup" on page 275.

Controlling the scope of Manage views

The content that is shown in the **Manage** views is based on your current **View** pane selection.

You can select the following default option from the **View** pane:

ALL MASTER SERVERS	Select **ALL MASTER SERVERS** to view information for all the NetBackup servers in your environment.

In addition to using the default view i.e. **ALL MASTER SERVERS**, you can also create your own views from **Settings > Views** or by using OpsCenter View Builder. For example, you can create a view like Geography to view details about master servers in a particular region like Europe.

More information about how to create views from **Settings > Views** is available.

See "About OpsCenter views" on page 299.

See the online *NetBackup OpsCenter Analytics View Builder Help* to learn how you can create views using the OpsCenter View Builder.

Use the following procedure to view details of all master servers or specific master servers.

To view details of all master servers

- In the OpsCenter console, select **ALL MASTER SERVERS** from the drop-down list in the **View** pane.

To view details of specific master servers

1. In the OpsCenter console, select **ALL MASTER SERVERS** from the drop-down list in the **View** pane.
2. Deselect the checkbox next to **ALL MASTER SERVERS** and select specific master servers from the list of master servers. Ensure that other master servers are unchecked.
3. Click **Apply Selection**.

About managing alert policies

Table 9-1 lists the topics that describe how to manage alert policies.

Table 9-1 Topic contents and description

Topic	Description
See "About OpsCenter alert policies" on page 417.	Explains the concept of alert policies.
See "Viewing the details for a single alert policy" on page 419.	Explains how to view the details for an alert policy.
See "Filtering on type of alert policy" on page 419.	Explains how to filter and view the alert policies that are of interest to you.
See "About creating (or changing) an alert policy" on page 420.	Explains how to create an alert policy using the Alert Policy Wizard.
See "OpsCenter Alert conditions" on page 420.	Describes all available alert conditions in OpsCenter, for which you can generate alerts.
See "Managing an alert policy " on page 436.	Explains the tasks that are available for managing a single alert policy. Management includes tasks like editing, copying, deleting, activating, or deactivating an alert policy.
See "Viewing the alerts associated with an alert policy" on page 437.	Explains how you can view the alerts that are associated with an alert policy.

About OpsCenter alert policies

OpsCenter provides tools to create and manage alert policies and handle any resulting alerts that the policies generate. Alert policies help you manage your NetBackup environment by providing constant monitoring of your NetBackup systems. When certain events or conditions occur in your environment, OpsCenter

helps you manage your NetBackup server network by generating alerts or sending email and trap notifications (or both).

When a NetBackup system event triggers an alert (based on your alert policies), the following occurs:

- OpsCenter sends email or SNMP notices to any recipients that are configured in the policy.
- The OpsCenter console displays views to help you track and manage these alerts.

You can specify email or SNMP notification in response to an alert, which lets administrators focus on other job responsibilities. Administrators do not need to monitor a terminal continuously.

Alert policies are defined as informational, warning, major, or critical.

Under certain circumstances there may be issues among multiple OpsCenter users. For instance, an OpsCenter user changes a policy while another user tries to remove the same policy.

Manage > Alert Policies view

This view is displayed when you select **Manage > Alert Policies**.

This view displays detailed information for OpsCenter alert policies for the current **View** pane selection.

See "Controlling the scope of Manage views" on page 416.

An option called **Ignore View filter** has been added in the **View** drop-down list under **Manage > Alert Policies**. **Ignore View filter** is selected by default when you click **Manage > Alert Policies**. When you select **Ignore View filter** from the View Pane, all alert policies are displayed in the **Manage > Alert Policies** pane regardless of the views on which the alert policy is based. For example, selecting **Ignore View filter** displays an alert policy that is based on a view which has been deleted, or an alert policy that is based on a view for which you do not have access now.

The table that appears in this view shows the following columns by default:

Table 9-2 Manage > Alert Policies column headings

Column	Description
Name	This column lists the name of the alert policy. Click the link to view details about the policy.
Description	This column lists the description for the alert policy.

Table 9-2 Manage > Alert Policies column headings *(continued)*

Column	Description
Alert Condition	This column lists the alert condition that is used for the alert policy. Example: Hung Job, Job Finalized, High Frozen Media etc. See "OpsCenter Alert conditions" on page 420.
Enabled	This column determines whether the alert policy is enabled or not.
Severity	This column lists the severity that is associated with the alert policy.
Clear Severity	This column lists the severity of the email or trap that is sent when the alert is cleared.
Creation Time	This column lists the date and time when the alert policy was created.
Modification Time	This column lists the date and time when the alert policy was last modified.
Modified By	This column lists the OpsCenter user who last modified the alert policy.

Viewing the details for a single alert policy

All the details that are associated with an alert policy can be viewed from the bottom of the **Manage > Alert Policies** view under the **General** tab. The **General** tab displays all the details that are shown in the table.

To view the details for a single alert policy

1. In the OpsCenter console, select **Manage > Alert Policies**.
2. Click a drill-down link from the **Name** column. The alert policy details are shown at the bottom of this view under the **General** tab.

Filtering on type of alert policy

A filter is available in the **Manage > Alert Policies** view to limit the types of alert policies that appear.

You can filter using any of the following three built-in filters. These filters are available from the drop-down list which is present on top of the table.

All Alert Policies	Select this filter to view all alert policies.
Enabled Alert Policies	Select this filter to view the alert policies that are enabled.
Disabled Alert Policies	Select this filter to view the alert policies that are disabled.

You can also create your own filters which let you focus on only the specific alert policies that interest you.

See "Creating, applying, editing, and removing custom view filters" on page 64.

To filter on type of alert policy

1. In the OpsCenter console, select **Manage > Alert Policies**.
2. Select a filter from the drop-down list. Note that the drop-down list is located on top of the table.

About creating (or changing) an alert policy

You can create alert policies to detect when something goes wrong with NetBackup and troubleshoot it. You can create policies to automate responses to key events in your enterprise. For example, you can create a policy to alert you when a job fails on a specific master server. You can monitor for frozen media and email the operator when the number of frozen media exceeds a threshold value. You can then take corrective action.

OpsCenter periodically retrieves data from NetBackup based on notifications and a wait time (of up to 15 minutes). This time delay between the NetBackup Activity Monitor and the OpsCenter console can mean that many intermediate job states may be lost.

The following topics provide more information about alerts.

See "OpsCenter Alert conditions" on page 420.

See "Additional information on job policy change condition" on page 425.

See "Adding an alert policy" on page 428.

See "About understanding alert counts in the Monitor view" on page 435.

OpsCenter Alert conditions

OpsCenter comes with a set of predefined alert conditions. You can create alert policies based on these alert conditions to detect when something goes wrong in your NetBackup environment and troubleshoot NetBackup. The alerts help you to

anticipate and handle problems before they occur. You can receive these alerts by logging on to OpsCenter, and also by email or SNMP traps. You can specify email and SNMP recipients while creating an alert policy.

Alert conditions can be divided into the following categories:

Event-based alert conditions	For these alert conditions, OpsCenter retrieves data from NetBackup based on notifications from NBSL.
Periodic alert conditions	For these alert conditions, OpsCenter retrieves data from NetBackup based on a wait time (of up to 15 minutes).

Table 9-3 lists the alert conditions, alert category, and descriptions.

Table 9-3 Alert conditions in OpsCenter

Alert type	Alert condition	Alert category	Description
Job	High job failure rate	Event-based	An alert is generated when the job failure rate becomes more than the specified rate.
	Hung job	Periodic	An alert is generated when a job hangs (runs for more than the specified time) for a selected policy or a client for a specified period. The Hung Job condition is checked every 15 minutes. Depending upon when a job starts within a check cycle, an alert may not occur. For Hung Job alert, you can configure OpsCenter to ignore the time for which a job is in a queued state. While checking the Hung Job condition, OpsCenter considers the start time of a job by default. This also includes the time for which a job is in a queued state. A job may not always be in an active state after it starts. Due to unavailability of resources, a job may first be in a queued state before it becomes active. If you configure OpsCenter to ignore the queued time for a job, OpsCenter considers the time when a job becomes active while checking the Hung Job condition. Note that the active start time of the first attempt is considered. For example, suppose a policy is created with a job threshold of 25 minutes. A job starts 10 minutes after a first check cycle and ends 13 minutes after the third check cycle is done. This time is a total execution of 33 (5 + 15 + 13) minutes, but an alert is not raised. In this case, the policy is checked four times. The job was not yet started during the first check, was running less than the threshold during the second (job duration = 5 minutes) and third checks (job duration = 20 minutes), and the job completes (job duration = 33) before the fourth check. If a job starts at 4 minutes after a first check, an alert is raised at the third check, since the job has executed for 26 minutes (11 + 15 minutes).
	Job finalized	Events-based	An alert is generated when a job of specified type, of the specified policy or client ended in the specified status.
	Incomplete Job	Events-based	An alert is generated when a job of a specified type of the specified policy or client moves to an Incomplete state.

Table 9-3 Alert conditions in OpsCenter *(continued)*

Alert type	Alert condition	Alert category	Description
Media	Frozen media	Events-based	An alert is generated when any of the selected media is frozen.
	Suspended media	Events-based	An alert is generated when any of the selected media is suspended.
	Exceeded max media mounts	Events-based	An alert is generated when a media exceeds the threshold number of mounts.
	Media required for restore	Events-based	An alert is generated when a restore operation requires media. The restore operation may require a specific media which contains the specific image to be restored.
	Low available media	Periodic	An alert is generated when the number of available media becomes less than the predefined threshold value. **Note:** When you select **All Master Server** from the **View** drop-down list, low available media alert raises separate alerts for all the master servers listed under **All Master Server**. For example: If there are 5 master servers present under the **All Master Servers** view, opscenter will raise 5 alerts for each master server.
	High suspended media	Periodic	An alert is generated when the percentage of suspended media exceeds the predefined threshold value.
	High frozen media	Periodic	An alert is generated when the percentage of frozen media exceeds the predefined threshold value.
	Zero Cleaning Left	Events-based	An alert is generated when a cleaning tape has zero cleaning left.

Table 9-3 Alert conditions in OpsCenter *(continued)*

Alert type	Alert condition	Alert category	Description
Catalog	Catalog Space low	Periodic	An alert is generated when space available for catalogs becomes less than the threshold value or size. For Catalog Space low condition, you can specify the threshold value for a particular policy in percentage, bytes, kilobytes (KB), megabytes (MB), gigabytes (GB), terabytes (TB) or petabytes (PB) and generate alerts. The generated alert can also show available catalog space using these units.
	Catalog not Backed up	Periodic	An alert is generated when catalog backup does not take place for a predefined time period. This does not necessarily mean that if you do not receive this alert, the catalog backup was successful.
	Catalog Backup Disabled	Periodic	An alert is generated when all the catalog backup policies are disabled. If the policy has been defined for a server group, an alert is generated for every master server within the group that satisfies this criteria. The alert is not generated if no catalog backup policy exists for a master server.
Device	Mount Request	Events-based	An alert is generated on a media mount request.
	No Cleaning Tape	Periodic	An alert is generated when no cleaning tapes are left.
	Drive is Down	Events-based	An alert is generated when a drive in a specified robot or media server in the selected server context goes down.
	High Down Drives	Periodic	An alert is generated when the percentage of down drives exceeds the predefined threshold value.
	OpenStorage	Events-based	An alert is generated when specific events occur in the NetApp devices. See “About the Open Storage alert condition” on page 512. See “Adding an alert policy ” on page 514.
Disk	Disk Pool Full	Events-based	An alert is generated when a disk pool(s) reaches the high water mark. An alert policy based on Disk Pool Full condition generates an alert only when the used capacity of the disk pool reaches the high water mark.
	Disk Volume Down	Events-based	An alert is generated when the selected disk volume(s) is down.
	Low Disk Volume Capacity	Periodic	An alert is generated when a disk volume capacity is running below the threshold limit.

Table 9-3 Alert conditions in OpsCenter *(continued)*

Alert type	Alert condition	Alert category	Description
Host	Agent Server Communication break	Periodic	An alert is generated when the communication between Agent and OpsCenter Server breaks. By default, this alert is automatically cleared when the communication is re-established. An alert policy based on the Agent Server Communication Break condition is always based on the ALL MASTER SERVERS view. If you created an alert policy based on the Agent Server Communication Break condition, and you do not have access to the ALL MASTER SERVERS view, alerts are not generated for the alert policy.
	Master Server Unreachable	Events-based	An alert is generated when OpsCenter loses contact with the master server. This alert condition means that the connection between OpsCenter and the managed NetBackup master server is lost. It does not necessarily mean that NetBackup backups are not working.
	Lost Contact with Media Server	Events-based	An alert is generated when OpsCenter loses contact with the media server.
	Appliance Hardware Failure	Events-based	An alert is generated in case of OpsCenter Appliance hardware failure.
Others	Service Stopped	Events-based	An alert is generated when the selected appliance hardware fails. You can set this alert condition to monitor your NetBackup or deduplication appliance hardware.
	Job Policy Change	Events-based	An alert is generated when a policy attribute for a job policy is changed. Multiple alerts are generated if multiple attributes are changed for a job policy See "Additional information on job policy change condition" on page 425. If you select a particular job policy, only the selected job policy is monitored for change. If you do not select any job policy, all the job policies are monitored for changes.

Additional information on job policy change condition

Review the following text for job policy alert condition.

Only the following policy attributes are monitored for job policies:

Policy name	Policy client type
Checkpoint interval	Check point

Effective date	Backup network drives
Compression	Encryption
Block level incrementals	Offhost
Snapshot method	Snapshot arguments
Master server	Client name
Collect bmr info	Collect true image restore info
Fail on error	Ext sec info
Frozen image	Keyword phrase
Number of copies	Off host backup
Residence	Catalog
Schedules	Clients
Storage unit	Volume pool
Jobs/Policy	Priority
Cross mount points	True image recovery
Allow multiple data streams	Keyword phrase
Alternate client	Data mover
Individual file restore from raw	Status
Block increment	Backup copy
Data mover type	Disaster recovery
File list	Follows nfs mounts
Max fragmentation size	Max jobs per policy
Pfi enabled	Proxy client
Data classification name	Share group
Policy active	

About Appliance hardware components that can fail

This section lists the Appliance hardware components for which you can generate alerts when they fail. You can select one, more than one, or all Appliance hardware

components on this UI. When a selected component fails, an alert is generated that you can view on the **Monitor > Alerts** screen.

- Adapter
- CPU
- Disk
- Enclosure Disk
- Enclosure Fan
- Enclosure Power Supply
- Enclosure Temperature
- Expansion Storage Shelf Disk
- Expansion Storage Shelf Fan
- Expansion Storage Shelf Power Supply
- Expansion Storage Shelf Temperature
- Fan
- PCI
- Power Supply
- Primary Storage Shelf BBU
- Primary Storage Shelf Connection
- Primary Storage Shelf Controller
- Primary Storage Shelf Disk
- Primary Storage Shelf Fan
- Primary Storage Shelf Power Supply
- Primary Storage Shelf Temperature
- Primary Storage Shelf Volume
- Primary Storage Shelf Volume Group
- RAID
- Temperature

Adding an alert policy

Follow the screens of the Alert Policy Wizard to define an alert policy. The required information and the required number of screens vary depending on the alert condition you choose. For some alert conditions, you can skip the optional screens.

Note: The Alert Policy Wizard is also used when you edit an alert policy.

To add an alert policy

1. In the OpsCenter console, select **Manage > Alert Policies**.
2. Click **Add**. The Alert Policy Wizard appears.

   See "Alert Policy Wizard" on page 430.
3. Enter a **Name**, **Description**, and **Alert Condition** on the **General** panel.

   See "OpsCenter Alert conditions" on page 420.

   Click **Next** to continue. You may click **Cancel** to exit the wizard at any stage.
4. On the **Alert Condition Properties** panel, specify attributes for the alert condition that you selected. The attributes differ for each alert condition. For many alert conditions (for example, for the Job Finalized condition), you may need to enter threshold attributes and other required or optional attributes. These attributes define and limit the alert.

   Click **Next**.
5. On the **Scope** panel, select the view that should be verified for the alert condition from the drop-down menu.

   You can select a view and a node that contains a group of master servers and also specific objects. You may also select only specific objects of a particular view or node to be checked for the alert condition. To select a specific object like a master server, first deselect the view or node that contains the master server and then select the master server. You may also deselect a specific master server from a view by selecting the view and then deselecting the specific master server.

   See "Alert Policy Wizard" on page 430.

   You must select at least one object or node for a view from this page. Click **Next** to continue.

6 Optionally, on the **Actions** panel, in the **Email Recipients** and **Trap Recipients** sections, you can select email or SNMP recipients (or both) to receive the alert notification.

See "Adding email recipients" on page 429.

See "Adding SNMP trap recipients" on page 429.

Note that if you create an alert policy and do not define any recipients, the alert is still displayed in the **Monitor > Alerts** view.

7 Optionally on the **Actions** panel, do the following in the **Severity** section:

- Select a severity level from the **Alert Severity** drop-down list. (If this alert occurs, the alert is displayed in the **Monitor > Alerts** view.)
- Select an appropriate severity level from the **Severity of email/trap sent for cleared alert** drop-down list. With **Severity of email/trap sent for cleared alert** option, you can configure the severity for an email or trap that is sent when an alert is cleared. The default severity level is Informational.
- The **Activate Condition** option is checked by default. By default, the policy is active once you create it. Deselect the **Activate Condition** option if you want to deactivate the policy.
  You can always activate or deactivate the policy later from the OpsCenter console.
  See "Managing an alert policy " on page 436.

8 Click **Save** to save the alert policy.

9 Click **Finish** once the policy is successfully created.

Adding email recipients

Follow this procedure to add email recipients to an Alert Policy.

To add email recipients

1 While creating an alert policy using the Alert Policy Wizard, go to the **Actions** screen.

2 On the **Actions** screen, click **To**, **Cc**, or **Bcc** from the **Email Recipients** section.

3 In the **Add Email Recipients** dialog box, select the specific recipients from the **Recipient Name** column and click **To**, **Cc**, or **Bcc** based on your requirements.

4 Click **OK**.

Adding SNMP trap recipients

Follow this procedure to add SNMP trap recipients to an Alert Policy.

To add SNMP trap recipients

1. While creating an alert policy using the Alert Policy Wizard, go to the **Actions** screen.
2. On the **Actions** screen, click **To** from the **Trap Recipients** section.
3. In the **Add Trap Recipients** dialog box, select the specific recipients from the **Recipient Name** column and click **To**.
4. Click **OK**.

Add Trap Recipients dialog box

In the **Add Trap Recipients** dialog box, select the specific recipients from the **Recipient Name** column and click **To**.

Alert Policy Wizard

The Alert Policy Wizard consists of four panels.

Table 9-4 Alert Policy Wizard General Panel

Setting	Description
Name	Enter a name for the alert policy. The name must be unique. Name is a required field.
Description	Enter a description for the alert policy.
Alert Condition	Select an alert condition from the list of alert conditions that are available. See "OpsCenter Alert conditions" on page 420.

Table 9-5 Alert Policy Wizard Alert Condition Properties Panel

Setting	Description
Specify properties for the selected alert condition	Specify attributes for the alert condition that you selected. The attributes differ for each alert condition. For many alert conditions (for example, for the Job Finalized condition), you may need to enter threshold attributes and other required or optional attributes. These attributes define and limit the alert. For alert conditions like High Job Failure Rate and Job Finalized, you may need to enter values for **Exit Status to Include** or **Exit Status to Exclude** field. You can provide multiple values in this field that are separated by comma in the following format: 20-35, 36, <40, >50 A value can be a range of exit status like 20-35 or all exit status below 40 like <40. Any combinations of this format can be used like 20-40, >55 or >70, 76

Table 9-6 Alert Policy Wizard Scope Panel

Setting	Description
View	

Table 9-6 Alert Policy Wizard Scope Panel *(continued)*

Setting	Description
	Select the view that should be verified for the alert condition. You can select a view and a node that contains a group of master servers and also specific objects. For example, you can select the default view **ALL MASTER SERVERS** to be checked for the alert condition. When you select a view like **ALL MASTER SERVERS** or a node that contains a group of master servers, all the master servers that are currently in the view or node are automatically selected. In addition, master servers that you may add later to this view or node are automatically selected and hence verified for the alert condition. You may also select only specific objects of a particular view or node to be checked for the alert condition. For example, you may select only a specific master server(s) under the default view **ALL MASTER SERVERS** to be checked for the alert condition. To select a specific master server, first deselect the view or node that contains the master server and then select the master server. You may also deselect a specific master server from a view by selecting the view and then deselecting the specific master server. Consider a scenario where there are two objects `server A` and `server B` in a particular view like **ALL MASTER SERVERS**. In case, you have selected the **ALL MASTER SERVERS** view and then specifically deselected `server B` , and in addition if you have selected a view or node that also contains `server B`, `server B` is not verified for the alert condition even though it is a part of the selected view or node. This is because you have specifically deselected `server B` from the **ALL MASTER SERVER** view. When you specifically deselect a master server from a view, which is also part of another selected view, the deselection or exclusion is given a higher priority because of which the master server is not verified for the alert condition. For this reason, it is recommended that you do not repeat a master server across groups. Note that you can also view and select additional attributes like policies, clients, media servers etc. on expanding the views and nodes from this page (wherever applicable). These attributes are located under the applicable views or nodes for specific alert conditions. For example, for the Job Finalized alert condition, you can select the view as well as the specific

Table 9-6 Alert Policy Wizard Scope Panel *(continued)*

Setting	Description
	policies and clients that should be checked for the alert. You can view the applicable attributes like policy name, client name, media server name, robot number, drive IDs etc. for the following alert conditions: ■ Job Finalized ■ Drive is Down ■ Media Required for Restore ■ Service Stopped ■ Frozen Media ■ Suspended Media ■ Exceeded Max Media Mounts ■ Disk Group Full ■ Disk Volume Down ■ Job Policy Changed ■ Hung Job You must select at least one object, node, or view from this page.

Table 9-7 Alert Policy Wizard Actions Panel

Setting	Description
Email Recipients	Select email recipients to receive the alert notification.
Trap Recipients	Select SNMP recipients to receive the alert notification.
Alert Severity	Select a severity level from the **Alert Severity** drop-down list. (If this alert occurs, the alert is displayed in the **Monitor > Alerts** view.)

Table 9-7 Alert Policy Wizard Actions Panel *(continued)*

Setting	Description
Severity of email/trap sent for cleared alert	Select an appropriate severity level from the **Severity of email/trap sent for cleared alert** drop-down list. With **Severity of email/trap sent for cleared alert** option, you can configure the severity for an email or trap that is sent when an alert is cleared. The default severity level is Informational. In OpsCenter, an alert is raised with the severity specified in the alert policy. Whenever this alert is cleared, an email or trap informing the user that the alert is cleared is sent with the same severity that is defined in the alert policy. This is the default behavior. For example, you may have created an alert policy for a Hung Job alert condition with a Critical severity. As a result, you receive Hung Job alert with Critical severity. When this Hung Job alert gets cleared, you receive an email or trap that informs you that the alert has been cleared. This email or trap also has a Critical severity. You can now configure the severity for this email or trap from Critical to some other severity like “Informational” while creating the alert policy. Note that you can configure the severity only for email or trap.
Activate the Policy	The **Activate Condition** option is checked by default. By default, the policy will be active once you create it. Deselect the **Activate Condition** option if you want to deactivate the policy. You can always activate or deactivate the policy later from the OpsCenter console. See “Managing an alert policy ” on page 436.

See “Adding an alert policy” on page 428.

About understanding alert counts in the Monitor view

Alerts apply only to the object (master server) where the corresponding alert policy is created. When alerts are raised for that policy they are raised on the selected object. For example, a Frozen Media alert occurs when any of the selected media on the selected master server (object) are frozen. Consider a case where you create an alert policy for a selected view that contains two master servers. For creating the policy, you select an alert condition of Frozen Media type. Since this master server is present in the view, the alert is listed when you select the specific server and the specific view from the View Pane.

Alerts that apply across server groups

Some types of alerts, for example Low Disk Volume Capacity apply across managed server groups. In this case, the disk volume capacity is calculated based on the disks from all master servers in the selected group. The alert does not apply to a single master server in the group but applies to the server group on which the alert policy was created. This means that only one alert is raised for the group, if the disk volume capacity for the servers in the selected group is lower than the user-defined threshold. An alert is not generated for every master server that is a part of the group. Therefore, the alert is listed only when you select the server group on which alert policy is created (or a parent group of that group).

If you create this type of alert policy for a single managed server, the alert is raised on the server since the server is the selected object. The alert can also be viewed if all the nodes or views that contain the master server are selected.

The following OpsCenter alert policy conditions apply across groups:

- High Frozen Media
- Low Disk Volume Capacity
- Low Available Media

Alerts that apply to a single server

The following OpsCenter alert policy conditions apply for single managed server:

- High Down Drives
- High Job Failure Rate
- High Suspended Media

Some types of alerts for example, High Job Failure Rate apply to a single master server. In this case, the job failure rate is calculated based on the jobs per master server in the selected group. Alert is raised, if the job failure rate for any master server is greater than the user-defined threshold. Only one alert is raised for all those master servers, for which the job failure rate is greater than the user-defined threshold.

Managing an alert policy

Use the following procedure to edit, delete, copy, activate, or deactivate an alert policy. You can copy and use an alert policy on another managed master server. The copy of the alert policy is available in the alert policy details table where you can make changes to it.

To edit an alert policy

1. In the OpsCenter console, select **Manage > Alert Policies**.
2. Select an alert policy from the **Name** column in the table.
3. Click **Edit**.

   The Alert Policy Wizard is used to create or edit a policy. When you edit an alert policy, the alert condition specific to the policy is selected by default in the Alert Policy Wizard. You cannot select a different alert condition while editing an alert policy.

   See "Adding an alert policy" on page 428.

To delete an alert policy

1. In the OpsCenter console, select **Manage > Alert Policies**.
2. Select an alert policy from the **Name** column in the table.
3. Click **Delete**.

To copy an alert policy

1. In the OpsCenter console, select **Manage > Alert Policies**.
2. Select an alert policy from the **Name** column in the table.
3. Click **More** and then click **Copy** from the drop-down list.
4. In the **Copy Alert Policy** dialog box, enter the new name for the alert policy.
5. Click **OK**.

   The copy of the alert policy is available in the alert policy details table where you can make changes to it.

To enable or disable an alert policy

1. In the OpsCenter console, select **Manage > Alert Policies**.
2. Select an alert policy from the **Name** column in the table.
3. Click **More** and then click **Enable** or **Disable** from the drop-down list.

Viewing the alerts associated with an alert policy

Use the following procedure to view the alerts that are associated with an alert policy.

To view the alerts associated with an alert policy

1. In the OpsCenter console, select **Manage > Alert Policies**.
2. Select an alert policy from the **Name** column in the table.
3. Click **More** and then select **View Alerts** from the drop-down list.

About managing NetBackup storage

This view is displayed when you select **Manage > Storage**. Included in this view are subtabs for **Storage Unit**, **Storage Unit Group**, and **Storage Lifecycle Policy**. Using these subtabs you can view detailed information about NetBackup storage for the current View pane selection.

See "Controlling the scope of Manage views" on page 416.

Table 9-8 lists the topics on how to manage NetBackup storage.

Table 9-8 Topic contents and descriptions

Topic	Description
See "Manage > Storage > Storage Unit view" on page 438.	Explains the capabilities that are available using the **Manage > Storage > Storage Unit** view.
See "Manage > Storage > Storage Unit Group view" on page 440.	Explains the capabilities that are available using the **Manage > Storage > Storage Unit Group** view.
See "Manage > Storage > Storage Lifecycle Policy view" on page 442.	Explains the capabilities that are available using the **Manage > Storage > Storage Lifecycle Policy** view.

Manage > Storage > Storage Unit view

This view is displayed when you select **Manage > Storage > Storage Unit**. This view shows the details for a storage unit for the current **View** pane selection. There is one row in the table for each storage unit for the current selection in the **View** pane.

See "Controlling the scope of Manage views" on page 416.

The table that appears in this view shows the following columns by default:

Table 9-9 Manage > Storage > Storage Unit view

Column Heading	Description
Name	This column lists the name of the storage unit. Click the link to view details about the storage unit.
Robot Type	This column specifies the type of robot (if any) that the storage unit contains.
Robot Number	This column specifies a unique, logical identification number for the robotic library.
Density	This column lists the density of the storage unit like, hcart, hcart2, or hcart3
On Demand	This column specifies whether the storage unit is available exclusively on demand. This happens only when a policy or schedule is explicitly configured to use this storage unit. .
Path	This column specifies the absolute path to a file system or a volume available for disk backups.

Not all of the available columns appear initially in this view. The following columns do not appear, but can be added to your view by clicking the Table Settings icon:

- **Storage Unit Type**
- **Capacity**
- **Free Space**
- **High Water Mark**
- **Max. Concurrent Jobs**
- **Staging**
- **Low Water Mark**
- **Can Exist On Root**
- **NDMP Host**
- **Enable Block Sharing**
- **Transfer Throttle**
- **Master Server**
- **Last Seen Time**
- **Host**

- **Fragment Size**
- **Multiplexing**
- **Disk Type**
- **Time Last Selected**
- **Disk Pool**
- **Host List**
- **Configured for Snapshots**
- **Primary**
- **Replication**

See the online *NetBackup Administration Console Help* for a detailed description of these fields.

More information about how to customize tables and view specific columns is available.

See "About using tables" on page 61.

The following task can be performed from this view:

View the details for a single storage unit	See "Viewing the details for a single storage unit" on page 440.

Viewing the details for a single storage unit

Use the following procedure to view the details for a single storage unit.

To view details for a single storage unit

1. In the OpsCenter console, select **Manage > Storage > Storage Unit**.
2. Click a storage unit name (drilldown link) from the **Name** column in the table.

   The storage unit details are shown at the bottom of this view under the **General** tab. This tab displays many of the available columns of the table.

Manage > Storage > Storage Unit Group view

This view is displayed when you select **Manage > Storage > Storage Unit Group**. This view shows the details for a storage unit group for the current **View** pane selection. The table contains one row for each storage unit group for the current selection in the **View** pane.

See "Controlling the scope of Manage views" on page 416.

The table that appears in this view shows the following columns by default:

Table 9-10 Manage > Storage > Storage Unit Group view

Column heading	Description
Name	This column lists the name of the storage unit group. Click the link to view details about the storage unit group.
Storage Unit Selection	This column specifies the order that storage units are selected when they are included in a group. .
Last Seen Time	This column specifies the date and time when the storage unit group was last seen.

Not all of the available columns appear initially in this view. The following columns do not appear, but can be added to your view by clicking the Table Settings icon:

- **Configured for Snapshots**
- **Primary**
- **Replication**

The following task can be performed from this view:

View the details for a single storage unit group	See "Viewing the details for a single storage unit group" on page 441.

Viewing the details for a single storage unit group

Use the following procedure to view the details for a storage unit group.

The storage unit group details are shown at the bottom of this view under the following tabs:

General	This tab shows the details of the storage unit group that are also shown in the table.
Storage Unit	This tab shows the details of the storage units that are a part of the storage unit group.

To view details for a single storage unit group

1. In the OpsCenter console, select **Manage > Storage > Storage Unit Group**.
2. Click the name of a storage unit group (drilldown link) from the **Name** column in the table.

Manage > Storage > Storage Lifecycle Policy view

This view is displayed when you select **Manage > Storage > Storage Lifecycle Policy**. This view shows the storage lifecycle policy details for the current **View** pane selection. A storage lifecycle consists of one or more storage units. The table contains one row for each Storage lifecycle policy for the current selection in the **View** pane.

See "Controlling the scope of Manage views" on page 416.

The table that appears in this view shows the following columns by default:

Table 9-11 Manage > Storage > Storage Lifecycle Policy view

Column heading	Description
Name	This column lists the name of the storage lifecycle policy. Click the link to view details about the storage lifecycle Policy.
Version	This column lists the version of the storage lifecycle policy.
Data Classification	This column lists the data classification that has been selected for the storage lifecycle, which applies to all of the storage units in the lifecycle. For example, the data might be classified as gold or silver.
Job Priority	This column specifies the priority that a policy has for backup resources. The default for all policies is 0, the lowest priority possible. Any policy with a priority greater than zero has priority over the default setting. .
Master Server	This column lists the master server that is associated with the storage lifecycle Policy. Click the link to view more details about the master server.

The following tasks can be performed from this view:

View the details of a single storage lifecycle policy	See "Viewing the details for a single storage lifecycle policy " on page 442.
View the details of a master server that is associated with a storage lifecycle policy	See "Viewing the details for a master server associated with a storage lifecycle policy " on page 443.

Viewing the details for a single storage lifecycle policy

Use the following procedure to view the details for a single storage lifecycle Policy. The details are shown at the bottom of this view under the following tabs:

General	This tab shows the details of the storage unit group that are also shown in the table.
Operations	This tab shows the details of the storage destinations that are a part of the storage lifecycle policy.

To view the details for a storage lifecycle policy

1. In the OpsCenter console, select **Manage > Storage > Storage Lifecycle Policy**.
2. Click the name of a storage lifecycle policy (drilldown link) from the **Name** column in the table.

Viewing the details for a master server associated with a storage lifecycle policy

Use the following procedure to view the details for a master server that is associated with a storage lifecycle policy. The details are shown on a separate page.

To view the details for a master server associated with a storage lifecycle Policy

1. In the OpsCenter console, select **Manage > Storage > Storage Lifecycle Policy**.
2. Click the name of the master server (drilldown link) from the **Master Server** column in the table.

About managing NetBackup devices

Under certain circumstances there may be issues among multiple OpsCenter users managing devices. For instance, a user brings a drive down while another user tries to bring up the same drive.

Table 9-12 lists the topics on how to manage NetBackup devices.

Table 9-12 Topic contents and descriptions

Topic	Description
See "Manage > Devices > Drive view" on page 444.	Explains the capabilities that are available using the **Manage > Devices > Drive** view.
See "Manage > Devices > Robot view" on page 448.	Explains the capabilities that are available using the **Manage > Devices > Robot** view.

Table 9-12 Topic contents and descriptions *(continued)*

Topic	Description
See "Manage > Devices > Disk Pool view" on page 450.	Explains the capabilities that are available using the **Manage > Devices > Disk Pool** view.
See "Manage > Devices > SAN Client view" on page 452.	Explains the capabilities that are available using the **Manage > Devices > SAN Client** view.
See "Manage > Devices > FT Server view" on page 454.	Explains the capabilities that are available using the **Manage > Devices > FT Server** view.

Manage > Devices > Drive view

This view is displayed when you select **Manage > Devices > Drive**. This view shows details for the drives that are configured for use by NetBackup for the current **View** pane selection. This view shows information about all the drives and also includes disabled or unreachable drives.

See "Controlling the scope of Manage views" on page 416.

The table that appears in this view shows the following columns by default:

Table 9-13 Manage > Devices > Drive view

Column Heading	Description
Drive Name	This column lists the configured name of the drive. Click the link to view details about the drive.
Device Host	This column lists the name of the device host (media server) where this drive is attached. If multiple drive paths are configured, this column contains Multiple. If the drive is configured as a shared drive (SSO), this column contains Multiple.
Master Server	This column lists the name of the master server that is associated with the drive.
Drive Type	This column specifies the type of drive. Example: hcart2, hcart3, 4MM.

Table 9-13 Manage > Devices > Drive view *(continued)*

Column Heading	Description
Robot Type	This column specifies the type of robot that contains this drive. Example: TL4, TLD.
Enabled	This column contains **Yes** if the path is enabled. The column contains **No** if the path is not enabled. If multiple drive paths are configured, this column contains **Multiple**.

Not all of the available columns appear initially in this view. The following columns do not appear, but can be added to your view by clicking the **Table Settings** icon:

- **Serial Number**
- **Cleaning Frequency**
- **Shared**
- **Inquiry Information**
- **Volume Header Path**
- **ACS**
- **LSM**
- **Panel**
- **Drive**
- **Vendor Drive Identifier**
- **Robot Number**
- **Robot Drive Number**
- **Recorded Media ID**
- **Assigned Host**
- **Control Host Name**
- **Evsn**
- **Last Clean Time**
- **Local Control**
- **Mounted Time**
- **NDMP**

- **Occupy Index**
- **Opr Comment**
- **Ready**
- **Request ID**
- **Scan Host**
- **VM Host**
- **Write Enabled**

See the online *NetBackup Administration Console Help* for a detailed description of these fields.

More information about how to customize tables and view specific columns is available.

See "About using tables" on page 61.

The following tasks can be performed from this view:

View the details for a single drive	See "Viewing the details for a single drive" on page 446.
View the details of a master server that is associated with a drive	See "Viewing the details for a master server associated with a drive" on page 447.
Use filters to view specific drives	See "Filtering on NetBackup drive category" on page 447.

Viewing the details for a single drive

Use the following procedure to view the details of a single drive.

To view the details for a single drive

1. In the OpsCenter console, select **Manage > Devices > Drive**.
2. Click the name of the drive (drilldown link) from the **Drive Name** column in the table.

   Detailed properties and status for the drive are shown at the bottom of the view under the **General** tab. The **Paths** tab shows the paths that were configured for the drive.

Viewing the details for a master server associated with a drive

Use the following procedure to view the details of a master server that is associated with a drive.

To view the details for a master server

1. In the OpsCenter console, select **Manage > Devices > Drive**.
2. Click the name of the drive (drilldown link) from the **Master Server** column in the table.

   Details for the specific master server are shown on a separate page.

Filtering on NetBackup drive category

You can sort and filter this view to focus on the specific type of drives that you want to see. For example, you can apply a filter that displays only those drives that are up. You can filter by using any of the built-in filters. These filters are available from the drop-down list which is present on top of the table.

The following built-in filters are available:

All Drives	All Drives is the default filter. Select this filter to view all drives.
Up Drives	Select this filter to view only those drives that are up. For up drives, all drive paths are up.
Down Drives	Select this filter to view only those drives that are down. For down drives, all drive paths are down.
Mixed Drives	Select this filter to view mixed drives. For mixed drives, some drive paths are up and some drive paths are down.

In addition to using the built-in filters, you can also create your own custom filters.

See “Creating, applying, editing, and removing custom view filters” on page 64.

To filter details by type of drive

1. In the OpsCenter console, select **Manage > Devices > Drive**.
2. Select a filter from the drop-down list. Note that the drop-down list is located on top of the table.

Manage > Devices > Robot view

This view is displayed when you select **Manage > Devices > Robot**. This view shows details for the robots that are configured for use by NetBackup for the current **View** pane selection.

See "Controlling the scope of Manage views" on page 416.

The table that appears in this view shows the following columns by default:

Table 9-14 Manage > Devices > Robot view

Column heading	Description
Robot Name	This column contains the name of the robot. The robot name contains the type and number of the robot, for example TLD(3). Click the link to view details about the robot.
Device Host	This column lists the name of the device host where this robot is attached. Click the link to view details about the device host.
Serial Number	This column contains the robot serial number.
Robot Control Host	If the robot is controlled by a remote host, this column contains the name of the host that controls the robot.
Master Server	This column lists the master server that is associated with the robot. Click the link to view details about the master server.

Not all of the available columns appear initially in this view. The following columns do not appear, but can be added to your view by clicking the **Table Settings** icon:

- **Robot Type**
- **Robot Number**
- **Inquiry Information**
- **Last Seen Time**
- **Max Drive**
- **Max Slot**
- **Remote ID**
- **VM Host**

See the online *NetBackup Administration Console Help* for a detailed description of these fields.

More information about how to customize tables and view specific columns is available.

See "About using tables" on page 61.

The following tasks can be performed from this view:

View the details of a robot	See "Viewing the details for a single robot" on page 449.
View the details for a master server that is associated with a robot	See "Viewing the details for a master server associated with a robot" on page 449.
View the details for the device host that is associated with a robot	See "Viewing the details of a device host associated with a robot" on page 450.

Viewing the details for a single robot

Use the following procedure to view the details of a single robot.

To view the details for a single robot

1. In the OpsCenter console, select **Manage > Devices > Robot**.
2. Click the name of the robot (drilldown link) from the **Robot Name** column in the table.

   Detailed properties for the robot are shown at the bottom of the view under the **General** tab. The **Paths** tab shows the paths that were configured for the robot.

Viewing the details for a master server associated with a robot

Use the following procedure to view the details of a master server that is associated with a robot.

To view the details for a master server associated with a robot

1. In the OpsCenter console, select **Manage > Devices > Robot**.
2. Click the name of the master server (drilldown link) from the **Master Server** column in the table.

   Detailed properties for the master server are shown on a separate page.

Viewing the details of a device host associated with a robot

Use the following procedure to view the details of a device host that is associated with a robot.

To view the details for a device host associated with a robot

1. In the OpsCenter console, select **Manage > Devices > Robot**.
2. Click the name of the master server (drilldown link) from the **Device Host** column in the table.

   Detailed properties for the device host are shown on a separate page.

Manage > Devices > Disk Pool view

This view is displayed when you select **Manage > Devices > Disk Pool**. This view shows details for the disk pools that are configured for use by NetBackup in the current **View** pane selection.

See "Controlling the scope of Manage views" on page 416.

Note: The following properties do not apply to cloud storage disk pools: Available Space, Raw Size, Usable Size, Low Water Mark (%), and High Water Mark (%).

All these values are derived from the storage capacity, which cannot be fetched from the cloud provider.

The table that appears in this view shows the following columns by default:

Table 9-15 Manage > Devices > Disk Pool view

Column heading	Description
Name	This column lists the name of the disk pool
Server Type	This column lists the storage server type. For OpenStorage, the server type depends on the vendor name.
Number of Volumes	This column lists the number of disk volumes in the disk pool.
Used Capacity	This column lists the amount of storage space in use.
Available Space	This column lists the available space in the disk pool in GB.
Raw Size	This column lists the total raw, unformatted size of the storage in the disk pool.

Table 9-15 Manage > Devices > Disk Pool view *(continued)*

Column heading	Description
Usable Size	This column lists the estimated amount of disk space available for storage after file metadata overhead is taken into account.
Low Watermark (%)	This column lists the low water mark for the disk pool. (The default is 80%.) When the capacity of the disk pool returns to the low water mark, NetBackup again assigns jobs to the storage unit.
High Watermark (%)	This column lists the high water mark for the disk pool (The default is 98%.).
% Full	This column lists how full the disk pool is in percentage.
Master Server	This column lists the name of the master server (link) that is associated with the disk pool.
State	This column lists the state of the disk pool like Up.

Not all of the available columns appear initially in this view. The following columns do not appear, but can be added to your view by clicking the Table Settings icon:

- **Imported**
- **Configured for Snapshots**
- **Primary**
- **Replication**

See the online *NetBackup Administration Console Help* for a detailed description of these fields.

More information about how to customize tables and view specific columns is available.

See "About using tables" on page 61.

The following tasks can be performed from this view:

View the details for a disk pool	See "Viewing the details for a disk pool" on page 452.
View the details for a master server	See "Viewing the details for a master server associated with a disk pool" on page 452.

Viewing the details for a disk pool

Use the following procedure to view the details for a disk pool. The details for the disk pool are shown at the bottom of the **Manage > Devices > Disk Pool** view under the following tabs:

General	This tab shows the detailed properties for a disk pool. Click the master server link to view details about the master server that is associated with the disk pool.
Disk Volume	This tab shows details about the disk volumes that are associated with the disk pool.
Storage Server	This tab shows details about the storage servers that are associated with the disk pool.

To view the details for a disk pool

1. In the OpsCenter console, select **Manage > Devices > Disk Pool**.
2. Click the name of the disk pool (drilldown link) from the **Name** column in the table.

   The details are shown at the bottom of this view.

Viewing the details for a master server associated with a disk pool

Use the following procedure to view the details of a master server that is associated with a SAN client.

To view the details for a master server associated with a disk pool

1. In the OpsCenter console, select **Manage > Devices > Disk Pool**.
2. Click the name of the master server (drilldown link) from the **Master Server** column in the table.

   Detailed properties for the master server are shown on a separate page.

Manage > Devices > SAN Client view

This view is displayed when you select **Manage > Devices > SAN Client**. This view shows details for the SAN clients that are configured for use by NetBackup in the current **View** pane selection.

See "Controlling the scope of Manage views" on page 416.

The table that appears in this view shows the following columns by default:

Table 9-16 Manage > Devices > SAN Client view

Column heading	Description
Name	This column lists the name of the SAN client.
State	This column lists the state of the FT device on the SAN client. The different states can be active, disabled etc.
Usage Preference	This column determines when to use the FT media server.
No. of FT Media Servers	This column lists the number of NetBackup media servers that support FT transport and that the client can send data to or receive data from.
Backup Wait Period	The number of minutes to wait for an FT media server for a backup operation.
Restore Wait Period	The number of minutes to wait for an FT media server for a restore operation.
Master Server	This column lists the master server that is associated with the SAN client.

The **Version** column does not appear, but can be added to your view by clicking the **Table Settings** icon.

The following task can be performed from this view:

View the details of a SAN client	See "Viewing the details for a SAN client" on page 453.
View the details of a master server that is associated with a SAN client	See "Viewing the details for a master server associated with a SAN client" on page 454.

Viewing the details for a SAN client

Use the following procedure to view the details of a SAN client. The details for the SAN Client are shown at the bottom of **Manage > Devices > SAN Client** view under the following tabs:

General	This tab shows detailed properties and status for the SAN client. Click the master server link to view details about the master server that is associated with the SAN client.

FT device	This tab shows the FT target devices information for the selected SAN client.

To view the details for a SAN client

1. In the OpsCenter console, select **Manage > Devices > SAN Client**.
2. Click the name of the SAN client (drilldown link) from the **Name** column in the table.

   The details are shown at the bottom of this view.

Viewing the details for a master server associated with a SAN client

Use the following procedure to view the details of a master server that is associated with a SAN client.

To view the details for a master server associated with a SAN client

1. In the OpsCenter console, select **Manage > Devices > SAN Client**.
2. Click the name of the master server (drilldown link) from the **Master Server** column in the table.

   Detailed properties for the master server are shown on a separate page.

Manage > Devices > FT Server view

This view is displayed when you select **Manage > Devices > FT Server**. This view shows details for the FT (Fibre Transport) media servers that are configured for use by NetBackup for the current **View** pane selection.

See "Controlling the scope of Manage views" on page 416.

The table that appears in this view shows the following columns by default:

Table 9-17 Manage > Devices > FT Server view

Column heading	Description
Name	This column contains the name of the FT media server. Click the link to view details about the robot.
State	This column lists the state of the FT media server.
Master Server	This column lists the master server that is associated with the FT server.

Table 9-17 Manage > Devices > FT Server view *(continued)*

Column heading	Description
Max Allowed Connections	This column specifies the number of FT connections to allow to a media server.

The following tasks can be performed from this view:

View the details of an FT server	See "Viewing the details for an FT server " on page 455.
View the details for a master server that is associated with an FT server	See "Viewing the details for a master server associated with an FT server" on page 455.

Viewing the details for an FT server

Use the following procedure to view the details for an FT server. The details for the FT server are shown at the bottom of **Manage > Devices > FT Server** view under the following tabs:

General	This tab shows detailed properties and status for the FT server.
FT device	This tab shows the FT target devices information for the selected FT server.

To view the details for an FT server

1. In the OpsCenter console, select **Manage > Devices > FT Server**.
2. Click the name of the Fibre Transport server (drilldown link) from the **Name** column in the table.

   The details are shown at the bottom of this view.

Viewing the details for a master server associated with an FT server

Use the following procedure to view the details of a master server that is associated with an FT server.

To view the details for a master server associated with an FT server

1. In the OpsCenter console, select **Manage > Devices > FT Server**.
2. Click the name of the master server (drilldown link) from the **Master Server** column in the table.

   Detailed properties for the master server are shown on a separate page.

About Operational Restore and Guided Recovery operations

Use the **Manage > Restore** tab to perform operational restore or Guided recovery operations. The **Restore** subtab is not visible when you log on as Reporter.

The **Restore Files and Directories** link is enabled only if you have permission to access either a client view or a master server view and if any client or master server is connected to the OpsCenter console.

The **Clone Oracle Database** link is enabled only if you are permitted to access a master server view or if a master server is connected to the OpsCenter console.

About Operational Restores from OpsCenter

You can now search for and restore the backed up files or directories from multiple source clients easily from the OpsCenter console. The OpsCenter console lets you search for and view the backed up files or directories for multiple source clients in a consolidated manner.

Before restoring files and directories from the OpsCenter console, review the following considerations:

- You must have backups of files and directories that you want to restore.
- You must add the NetBackup master server to the OpsCenter console for restoring files and directories from a client that is associated with the master server.
- View-based access is used to control the clients that you can search and restore to. Only those views are displayed that you can access.
- Only one user session is allowed per user at a given time.
- OpsCenter supports normal restores only. Other restore types like Archived, Raw Partition, True Image, Virtual Machine and so on are not supported.
- For VMWare or HyperV clients, the search and restore operations work only if the client name is the same as hostname.

If the client name is the same as display name, UUID, or DNS name then only the search functionality is available. You cannot perform restore operations in this case. The following table provides the details on whether the search and restore functionality is available when the client name is the Host name, display name, UUID, DNS name etc.:

Client Name Type	Search	Restore
Host Name	Yes	Yes
Display Name	Yes	No
UUID	Yes	No
DNS Name	Yes	No

About timeframe selection

You can search for files and directories that were backed up in a specific timeframe.

The following options are available:

Today

If you have backed up a file today and want to restore it, select **Today**. The timeframe is displayed on the left side of the page at the top.

For example, if today is May 31st, OpsCenter searches all files and directories that were backed up from May 31, 2011 12 A.M. to June 1, 2011 12 A.M.

Day

Select **Day** if you want to view the files and directories that were backed up in the last 24 hours. The time interval associated with the selected timeframe (Day) is displayed on the left side of the page. You can also adjust the time interval by clicking the arrows on the left and right respectively.

For example, if you select **Day** and click **Search** on January 10th, 11:00 A.M. then OpsCenter searches files and directories that were backed up from Jan 9, 2012 11:00 A.M. to Jan 10, 2012 11:00 A.M.

Week

Select **Week** if you want to view files and directories that were backed up in the last seven days. The time interval associated with the selected timeframe (Week) is displayed on the left side of the page. You can also adjust the time interval by clicking the arrows on the left and right respectively.

Month	This is selected by default. Select **Month** if you want to view files and directories that were backed up in the last month. The time interval associated with the selected timeframe (Month) is displayed on the left side of the page. You can also adjust the time interval by clicking the arrows on the left and right respectively.
90 Days	Select **90 Days** if you want to view files and directories that were backed up in the last 90 days. The time interval associated with the selected timeframe (90 Days) is displayed on the left side of the page. You can also adjust the time interval by clicking the arrows on the left and right respectively.
Year	Select **Year** if you want to view files and directories that were backed up one year prior to the current date. The time interval associated with the selected timeframe (Year) is displayed on the left side of the page. You can also adjust the time interval by clicking the arrows on the left and right respectively.
Customize	You can customize the timeframe selection by clicking **Customize** and specifying an absolute timeframe or relative timeframe. Using the **Customize** option, you can view data for any timeframe that you want like you can view backed up data for the previous three weeks. The time interval associated with the selected timeframe is displayed on the left side of the page.

About the Restore Operator

A new user role named Restore Operator has been added to control access to the Manage > Restore view. You can view Manage > Restore only when you log on to OpsCenter with the following roles:

- Security Administrator
- Administrator
- Restore Operator
- Operator

The Restore subtab is not visible when you log on as Reporter. The Restore Operator can only select and perform operations on restore jobs in the Monitor > Jobs view. The Restore Operator can neither select any other jobs (like backup jobs) nor perform any operations on them like cancel, restart, resume etc.

See “User access rights and functions in OpsCenter user interface” on page 231.

Note: In addition, view-based access is used to control the clients that you can search and restore to. Only those views are displayed that you can access.

Files and Directories Restore Wizard

The Files and Directories Restore Wizard consists of three panels.

Table 9-18 Files and Directories Restore Wizard

Panel	Description
Select Files or Directories	The Select Files or Directories panel allows you to perform simple or advanced search operations for locating specific files or directories that you want to restore. You can restore these files and directories later by adding them to the Restore Cart. The Restore Cart also allows you to add files from multiple search and browse operations to a Cart. On this panel, you can see Select Files or Directories > Search view by default. You can also browse other tabs and subtabs like Restore Cart and Browse. See "Select Files or Directories > Search options" on page 460. See "Select Files or Directories > Browse options" on page 474. See "Restore Cart" on page 478.
Restore Options	The Restore Options panel lets you select a number of restore options like destination client and paths, overwrite options etc. for the selected client. See "Restore Options panel" on page 480.
Summary	The Summary panel displays the list of files or directories that you selected for restore. See "Summary panel" on page 486.

Select Files or Directories panel

Use the Select Files or Directroies panel to search files and directories, browse clients, or use the Restore Cart.

Select Files or Directories > Search options

This view is shown by default when you select **Manage > Restore** and then click the **Restore Files and Directories** link. The **Select Files or Directories > Search** view lets you perform simple or advanced search operations based on the timeframe and search options that you select. When you select a specific timeframe, only the backups that occurred in the selected timeframe are searched. By default, the files or directories that are backed up over the last one month are searched.

The following search options are displayed when you select **Select Files or Directories > Search**:

File or Directory name

Enter the name of the file or directory that you want to search for. This is a mandatory field.

For UNIX clients, the search pattern may optionally begin with a / to indicate that the matching should start at the root directory.

A pattern may optionally end with a / for UNIX clients or \ for Windows clients to indicate that only directory matches are returned.

You can search by the following methods:

- Enter a full path name.

  OpsCenter searches for the specific path and file in the selected clients, timeframe, and as per any advanced search criteria that you entered. Use forward slash (/) as the path delimiter for UNIX and back slash (\) as the path delimiter for Windows.
- Enter a specific file or directory name.

  OpsCenter searches for the specific file or directory (folder) in the selected clients, timeframe, and as per any advanced search criteria that you entered..
- Add a * or a ? wildcard to the entry.

  If you do not know the exact directory (folder) or file name, add one of these wildcards to the string. This is valid for both Windows and UNIX clients.

  Examples:
  - Enter *.doc to view the files that end with that suffix.
  - Enter ca?.doc to view all the files that have one character after ca and a .doc extension.
  - Enter etc/hos* to view files named `hos*` immediately inside directory etc.

    Enter C:\backup* to view files named backup* immediately inside C:.
  - Enter /etc/hos* to view files named `hos*` immediately inside directory `etc`. The `etc` directory must be a first level directory.

    Enter trace\backup* to view files immediately inside directory named `trace`.
  - Enter etc//hos* to view files named `hos*` immediately inside `etc` or any subdirectory of etc.

    Enter C:\\backup* to view files named backup* immediately inside C: or any subdirectory of C:.

Note: You cannot search by only typing `*` in the text box. This is not supported.

In addition, you cannot search by using a pattern like `/path/*` on UNIX or path* on Windows. To find related results, you can search using `path*` or `path`.

Search within Clients

In this field, you can specify the set of clients whose backup information you want to search. You can search multiple clients that are associated with one or more views or master servers at a given time.

Select one or more clients that are associated with one master server. A table appears that provides details like client name, the master server that it is associated with and a link to remove the client. To add the clients that are associated with a different view or master server, select the view, master server, and then type in or browse for the clients.

View

Select a view from the **View** drop-down list.

Only the following views are displayed in the **View** drop-down list:

- Views that you have access to
- Client type or Master Server type views

If you select a view of type Master Server, all NetBackup master servers that are added to the view are displayed in the **Master Server** drop-down list. If you select a client-type view, the **Master Server** drop-down list is disabled.

Master Server

Select a master server from the **Master Server** drop-down list. All NetBackup master servers that are a part of the selected view are displayed.

Note: NetBackup master servers are displayed in the **Master Server** drop-down list. Even if you have older master servers in the selected view, those master servers do not appear in the **Master Server** drop-down list.

The **Master Server** drop-down list is disabled in the following scenario:

- If you select a client-type view from the **View** drop-down list
- If you have access to client-type views only

To restore backed up files and directories (folders) on a client, first ensure that the master server that is associated with the client is added to the OpsCenter console.

Client

Specify the clients whose backup information you want to search. If you remember the client name, type the client name in the **Client** text box. Once you start typing the client name like *a1*, the protected clients that begin with these characters automatically appear beneath the drop-down list (auto-complete field). Select the client name when it appears.

As you select the clients that you want to search, a table appears beneath that provides details like client name that you selected for search, the master server that it is associated with and a link to remove the client. Click **Remove** if you want to remove the specific client.

Note: Only those clients on which files and directories are backed up (or protected clients) are displayed when you type in a client name or browse for a client. Clients that do not have any backups are not displayed.

Note: In addition, only those clients are displayed for which the user has been granted access through a view.

If you do not remember any client names or simply want to browse through the clients, click the **Browse and select client** link and select a list of protected clients that are associated with a master server or a client-type view.

See "Browse Client dialog box" on page 467.

Note: The time to display search results may increase with the number of selected clients.

Advanced Search

You can also search on the basis of more advanced parameters in addition to the simple search parameters. Click **Advanced Search** if you want to search using additional parameters like policy type, backup type, file size, policy name etc. These are optional parameters.

You are presented with the following options for an advanced search operation:

- Policy Name

  Enter a policy name to view the backups that are associated with the specific policy.
- Policy type

  By selecting the policy type, you can view the backups that are associated with the selected policy type. For restoring files and directories, policy types like FlashBackup, FlashBackup - Windows, MS-Windows, NDMP, Standard, Hyper-V, and VMware are supported.

  You can select only one policy type from the drop-down list.
- Policy associated keywords

  By specifying the policy associated keyword, you can view the backups that are associated with the specific keyword.
- Backup type

  By selecting the Backup type, you can view the backups that are associated with the selected backup type. You can select multiple backup types.
- Select File Extensions

  You can select one or more file extensions that you want to view from the **Select file extensions** drop-down list. The following file extensions are listed:
  - txt
  - doc
  - docx
  - pdf
  - xls
  - xlsx
  - ppt
  - pptx

  If a file extension is not listed, then you can type it under the **Specify extension** option

  Once you select or specify the file extensions, click **Add**. The selected file extensions are displayed in the list box on the right-hand side.

- Case-insensitive search

  This option is checked by default. You can uncheck the case-insensitive search option to make your search case-sensitive.

  The case-sensitive search applies to file or directory name and file extensions only.
- File/Directory modification time

  With this option you can search based on when the file or directory was last modified. The default selection is **Any**.

  In addition to other options, you can also specify an absolute timeframe by selecting **Specify date and time range**.and select **From** and **To** timeframes.

Note: A command named `nbfindfile` has been added that lets you search files or directories based on simple search criteria. This command can be executed from the NetBackup master server (and not the OpsCenter Server).

See nbfindfile on page 634.

Browse Client dialog box

You can also browse to view and select clients that are associated with a master server or a view. This option may be helpful if you do not remember any client names or if you want to browse through the clients that are associated with master servers or a view.

When you click **Browse and select clients** link from **Select files or directories > Search** view, the **Browse Clients** dialog box is displayed.

The following options are displayed in the dialog box:

Selected View	The view that you select from the **View** drop-down list is displayed. If you select a view of type Master Server, all NetBackup master servers that are added to the view are displayed under the Name column. If you select a client-type view, the clients are displayed under the selected view in the Name column.

Filter Clients	You may want to view specific clients when the client list is large. To filter specific clients, enter client name, part of a client name, or add the * wildcard. For example, when you enter *ary* in the **Filter Clients** field, then OpsCenter displays all results that start with or contain *ary* string. Click **Apply Filter** to apply this filter and view the filtered clients. Click **Clear Filter** to clear the filtered view and see all the clients.
Name	If you select a Master Server type view, then each master server (with a yellow folder icon) is displayed under the **Name** column with a + sign next to it. When you expand a master server, you can see the protected clients that are associated with it. If you select a Client-type view, you can view clients under the **Name** column. Select the checkbox next to one or more clients and click **OK**. A table appears that provides details like client name that are selected for search, the master server that the client is associated with and a link to remove the client. Click **Remove** if you want to remove the specific client. **Note:** The time to display search results may increase with the number of selected clients.

Performing a simple or advanced search

To restore a specific file or directory, you may first need to know the location of the file or directory. You can either perform a simple or advanced search. For performing a simple search, you must select the timeframe, enter a file or directory name (full, partial, or wildcard) or path along with the client name. By default, timeframe of the last one month is selected. This means that files or directories that were backed up over the last one month are searched by default.

While performing an advanced search, you can specify additional optional parameters like policy name, policy or backup type etc. in addition to the simple search parameters.

Use the following procedure to search files and directories for restore.

To search and select files and directories for restore

1. In the OpsCenter console, click **Manage > Restore**.
2. Click **Restore Files and Directories** under **Files and Directories**.
3. The contents of the **Select files or directories > Search** tab are displayed by default. From this view, you can search and select the files and directories that you want to restore. You can either perform a simple search or an advanced search.

   Instead of searching and selecting files, you can also browse and select the backed up files and directories on a client for restore.

   See "Browsing for files and directories on a client" on page 477.
4. Select a timeframe that you want to search. The default timeframe that is selected is **Month**.

   See "About timeframe selection" on page 457.
5. In the **Search files and directories based on name, path, wildcards etc.** section, enter the following parameters. To perform a simple search operation, enter all the details in **Search files and directories based on name, path, wildcards etc.** section.

   See "Select Files or Directories > Search options" on page 460.

   You can select multiple clients from one or more views or master servers to be searched at a given time. To search for clients from multiple views or master servers, you must enter details in the **Search within Clients** section for each view or master server. For example, to search for clients from two master servers, select the first master server and then select clients for the first master server. Similarly, complete the **Search within Clients** section for the second master server. You can use the same procedure to add clients from different views.

   The clients that you selected for search are displayed in a table in this section. The table displays the following details:

Client Name	This column displays the client name that is searched.
Master Server	This column displays the master server that is associated with the specific client.
Remove	Click **Remove** if you do not want the backup information of the specific client to be searched.

6 To perform an advanced search, you can also specify advanced search criteria in addition to the simple search criteria. The Advanced Search criteria are optional.

See "Select Files or Directories > Search options" on page 460.

7 Click **Search**.

It may take some time for OpsCenter to display the search results. The time to display the search results may increase with the number of selected clients.

OpsCenter highlights the search results at the bottom of the pane in a table. The most recent 500 results can be shown in the table.

The table lists the following default columns that are displayed:

File/Directory Name	Names of the files and directories that are backed up as per the search criteria are displayed. The directory (folder) name may have a + sign next to it. This indicates that the directory has files or sub-directories. You can choose if you want to restore the whole directory or specific files from the directory. If you want to restore the selected files and directories now, click **Restore now**. To restore the selected files and directories later, click **Add to Restore Cart**.
File/Directory Path	Current location of files and directories is displayed.
Backup History	This link shows the backup timeline window for a specific file or directory. A file or directory may have been backed up multiple times in the past. You may want to restore a previous copy. In addition, you may have multiple copies for a specific backup. The primary copy is selected by default. You may want to restore a copy other than the primary copy. Click the link if you want to to restore a previous backup and also specify a copy other than the primary copy. See "Backup Timeline Window" on page 472.
Backup Time	This is the most recent date and time when the file was last backed up.
Modified Time	Date and time when the backup was last modified.
Client	Name of the client on which the backup exists.

Size	Size of the backed up file or directory (folder) in bytes (B).

The columns that can be added to the table are the following:

- Master Server
- Last Accessed Time
- Backup ID

The filter button on top of search results table allows you to filter out the search results and display only the search results matching a criteria. The result is a filtered subset of the last search result from the OpsCenter database.

See "Creating, applying, editing, and removing custom view filters" on page 64.

Whenever you apply a filter on the search results, you see the following message on top of the search results table.

Search has been completed successfully. Filter is currently applied. Click here to remove filter.

You can click the link to clear the filter and view all search results.

You can also customize the search results table to allow standard table customizations like sort order, page size, columns displayed and the order in which columns are displayed. Click **Change Table Settings** icon on top of search result to access table customizations page.

See "About using tables" on page 61.

8 Select one or more files or directories. Click **Restore now** to restore the files or directories now.

Click **Add to Restore Cart** if you want to add the selected files and directories to the Restore Cart and restore at a later time.

See "Restore Cart" on page 478.

Click **Preview Media** to view the media required for the restore operation and to determine the availability of the required media. This helps you to know if the tape required for restore is in the library or not. This option applies only for tape backups. If the selected backups are on a disk, this option is not applicable.

The Preview Media dialog box contains details like Media ID, Volume Group, and whether the media is in the library.

9 In the Restore Options panel, select the restore options for each individual client.

See "Restore Options panel" on page 480.

Click **Next**.

10 In the Summary panel, click **Restore** to restore all the files or directories.

See "Summary panel" on page 486.

Backup Timeline Window

This is a timeline view of backups for a specific file or directory. By default, the search and browse results that are displayed in the OpsCenter console display the most recent backup that occured for the specific file or directory and is the primary backup copy. The Backup Timeline window allows you to select a previous backup for the specific file or directory in the selected timeframe and also select a copy other than the primary copy.

At the top of the Backup Timeline window, the name and location of the file or directory whose backup details are displayed is mentioned. Name of the client that contains the file or directory is also mentioned.

The X-axis represents the time while the Y-axis represents the device or source like disk pool, volume group etc. on which the specific file or directory resides. Each row in the table represent the backups on a single disk pool, basic disk, or a single volume group.

The timeline on top displays icons for each backup of the file or directory. Each icon represents a different backup or snapshot.

There are different icons for snapshot, disk, or tape backups. Also if single or multiple backups occur during a single timeline unit, then it is represented through different icons. For example, if a file was backed up twice in an hour, a different icon appears representing more than one backup.

When you open the Backup Timeline window, the latest backup (icon) in the selected timeline is already selected. Select another icon if you want to select a previous backup.

Multiple backups may be displayed on the timeline. To view all the instances of backups, you may need to increase the scope of the timeline. You can display the timeline in days, weeks, or months.

The following tabs are displayed:

Day	This selection shows the backups that occured at different times in the day. By default, the Day tab shows the day of the backup that was shown in the search or browse result. For example, if search result shows backup date for a file as June 15, 2011 and that link is clicked to view the timeline, then June 15 is shown by default. The timeline for a day is split up in 24 slots of an hour each. Each slot of one hour is in turn split up by 30 minute slots - that is 2 cells per hour. You can also adjust the time interval by clicking the arrows on the left and right respectively.
Week	Select Week to view a weekly summary of the backups. By default, the Week tab shows the week of the backup that was shown in search or browse result. For example, if search result shows backup date for a file as June 15, 2011 and that link is clicked to view the timeline, then the week of June 15 is shown by default. The timeline for week is split up in seven slots of one day each. Each slot of one day in turn is split up by 4 hour slots- that is six cells per day. You can also adjust the time interval by clicking the arrows on the left and right respectively.
Month	Select Month to view a monthly summary of the backups. By default, the Month tab shows the month of the backup that was shown in search or browse result. For example, if search result shows backup date for a file as June 15, 2011 and that link is clicked to view the timeline, then the month of June 15 is shown by default. The timeline for month is split up in five slots of one week each. Each slot of one week in turn is split up in seven cells - that is seven cells per week (and 35 cells per month). You can also adjust the time interval by clicking the arrows on the left and right respectively.

The Backup table in the middle of the window shows information about the icon (backup) that is selected from the timeline view. Click an icon to view the details of the specific backup in the Backup table. The Backup table lists the details of each backup image that is associated with the backup. It shows several details like backup time, policy name, policy type, backup type etc. Once you select the specific backup image that you want to restore from the Backup table, the copies that are associated with the backup image are displayed in another table at the bottom. The Copies of Selected Backup table at the bottom shows information about the copies that are associated with the selected backup image. By default, the primary copy is selected. You can select a different copy for restore and click Add to Restore Cart to add this to the restore cart.

Note: A multiple disk, tape, or snapshot backup may include many backup images.

Select Files or Directories > Browse options

This view is displayed when you select **Select Files or Directories > Browse**. The **Select Files or Directories > Browse** view allows you to select a client and then browse and select the backed up files and directories on the client for restore. You can browse the contents of only one client at a given time.

You first need to select the client from the Select Client section. The following options are displayed in the Select Client section:

View	All the views that are shown in the OpsCenter console are displayed in the drop-down list. Select a view from the drop-down list. You may select a view that is of Client-type or master server type. Only the following views are displayed in the **View** drop-down list: ■ Views that you have access to ■ Client type or Master Server type views If you select a view of type Master Server, all NetBackup master servers that are added to the view are displayed in the **Master Server** drop-down list. If you select a client-type view, the **Master Server** drop-down list is disabled.

Master Server	Select the master server that is associated with the client. NetBackup master servers that are added to the OpsCenter console are displayed. The **Master Server** drop-down list is disabled in the following scenario: ■ If you select a client-type view from the **View** drop-down list ■ If you have access to client-type views only
Client	Only protected clients or clients that have backups are displayed. Select the client that contains the protected files and directories. Specify the client whose backup information you want to browse. If you remember the client name, type the client name in the **Client** text box. Once you start typing the client name like *a1*, protected clients that begin with these characters automatically appear beneath the drop-down list (auto-complete field). Select the client name when it appears. **Note:** Only those clients on which files and directories are backed up (or protected clients) are displayed when you type in a client name or browse for a client. Clients that do not have any backups are not displayed. **Note:** In addition, only those clients are displayed for which the user has been granted access through a view. If you do not remember any client names or simply want to browse through the clients, click the **Browse and select client** link and select a list of protected clients that are associated with a master server or a client-type view. See "Browse Client dialog box" on page 467.

Once you select a client, you can see a two-pane view. The two-pane view shows the backed up client directories in the left pane and content of the selected directory in the right pane (like Windows Explorer). The backed up files and directories that are displayed is based on the timeframe that you select. The most recent backup

in the specified timeframe is shown on the top by default. This is also similar to the Java GUI or the BAR GUI browse capability. From this view, you can select one or more files or directories for restore.

The following properties are displayed when you select **Select Files or Directories > Browse**:

Change Client link	The Change Client link lets you select a different client and allows you to browse the protected files and directories on a different client. Note that you can browse the contents of one client at a time.
Directory Structure	The Directory structure shows the backed up directories on the selected client in the selected timeframe. The directory (folder) name may have a + sign next to it. This indicates that the directory has sub-directories. Expand the directories to view the subdirectories.
Contents of selected directory	Click a directory from the left pane. The contents of the selected directory are displayed in this pane.

The following details are displayed in the right pane that shows the contents of the selected directory:

File/Directory Name	Names of the files and directories that are a part of the selected directory in the left-pane are displayed. Select the files or sub-directories that you want to restore. If you want to restore the selected files and directories now, click **Restore now**. To restore the selected files and directories later, click **Add to Restore Cart**.
Backup Time	This is the most recent date and time when the file was last backed up.
Modified Time	Date and time when the backup was last modified.
Size	Size of the backed up file or directory in bytes (B).

Backup History	This link shows the backup timeline window for a specific file or directory. A file or directory may have been backed up multiple times in the past. You may want to restore a previous copy. In addition, you may have multiple copies for a specific backup. The primary copy is selected by default. You may want to restore a copy other than the primary copy. Click the link if you want to to restore a previous backup and also specify a copy other than the primary copy. See "Backup Timeline Window" on page 472.

Click **Preview Media** to view the media required for the restore operation and to determine the availability of the required media. This helps you to know if the tape required for restore is in the library or not. If the selected backups are all on disk, this option is not applicable. The **Preview Media** dialog box displays details like Media ID, volume group, and if the media is in library.

Browsing for files and directories on a client

You can also browse the protected files and directories on a client. The view allows you to select the client to be browsed and allows you to specify a timeframe for backup selection. You can select only one client at a time. The two pane browse view shows the backed up client directories in the left pane and content of the selected directory in the right pane. The most recent backup in the specified date range is shown by default.

Use the following procedure to browse for files and directories for restore.

To browse for files and directories for restore

1. In the OpsCenter console, click **Manage > Restore**.
2. Click **Restore Files and Directories** under **Files and Directories**.
3. Select **Select files or directories** > **Browse**.
4. Select a timeframe that you want to search. The default timeframe that is selected is **Month**.

   See "About timeframe selection" on page 457.
5. Select a view from the **Views** drop-down list.
6. Select a master server from the **Select Master Server** drop-down list.

7 Type a client name in the **Client** box. When you start typing a client name, a list of client names that start with the characters that you entered is displayed. Select a client from this list and then click **Select Client**.

You can also click **Browse and select clients** and then browse to select a client. You can browse and select only one client at a time.

The directory structure of the selected client and the contents of the directory are displayed in two panes. From this view, you can browse and select the specific files and directories that you want to restore.

8 Click **Restore now** to start the restore process.

Click **Add to Restore Cart** if you want to add the selected files and directories to the Restore Cart and restore at a later time.

See "Restore Cart" on page 478.

Click **Preview Media** to view the media required for the restore operation and to determine the availability of the required media. If the selected backups are all on disk, this option is not applicable. The Preview Media dialog box displays details like Media ID, volume group, and if the media is in library.

9 In the Restore Options panel, select the restore options for each individual client.

See "Restore Options panel" on page 480.

Click **Next**.

10 In the Summary panel, click **Restore** to restore all the files or directories.

See "Summary panel" on page 486.

Restore Cart

The files shown in the Search and Browse subtabs, can be added to a Restore Cart. The Restore Cart allows you to view file selections from multiple search and browse operations and restore them at a later point in time. You may choose to restore all the file or directory selections in one go. The Restore Cart selection persists for each user across different OpsCenter sessions. Once a file belonging to the Restore Cart is sent for restore, it is automatically removed from the Cart for the specific user.

Click **Preview Media** to view the media required for the restore operation and to determine the availability of the required media. This helps you to know if the tape required for restore is in the library or not. This option only applies to tape backups. If the selected backups are on disk, this option is not applicable. The Preview Media dialog box displays details like Media ID, volume group, and if the media is in library.

You can also email, export, or restore from the Restore Cart.

See "Performing operations on the Restore Cart" on page 479.

Performing operations on the Restore Cart

You can perform several operations on the files and directories in the Restore Cart. You can email or export the contents of the Restore Cart. You can also restore or remove files from the Restore Cart.

Use the following procedures for performing specific Restore Cart operations.

To export the Restore Cart

1. In the OpsCenter console, click **Manage > Restore**.
2. Click **Restore Files and Directories** under **Files and Directories**.
3. Click **Restore Cart**.
4. On the top-right corner of the Restore Cart table, click the **Export Report** icon (in green).
5. Select the file format in which you want to export the contents of the Restore Cart such as PDF, CSV, TSV, or HTML and click **OK**.
6. Click **Open** or **Save** to open or save the file on your system.

To email the Restore Cart

1. In the OpsCenter console, click **Manage > Restore**.
2. Click **Restore Files and Directories** under **Files and Directories**.
3. Click **Restore Cart**.
4. In the Content pane at the right-hand side, click the **Email Report** icon. The Email Report pop-up screen opens.
5. On the Email Report pop-up screen, select the file format, such as PDF, CSV, TSV, or HTML.
6. Enter email IDs in To, Cc, and Bcc text boxes, to which you want to send emails. Alternatively, you can add existing email recipients.
7. Enter the subject of the email.
8. Enter the message that may be a short description regarding the report data that you want to email.
9. Click **OK**.

To restore the files or directories from the Restore Cart

1. In the OpsCenter console, click **Manage > Restore**.
2. Click **Restore Files and Directories** under **Files and Directories**.
3. Click **Restore Cart**.

4 Select one or more files or directories that you want to restore.

5 Click **Restore Now**. When you click Restore now, the selected file or directories are automatically removed from the Restore Cart.

6 In the Restore Options panel, select the restore options for each individual client.

See "Restore Options panel" on page 480.

Click **Next**.

7 In the Summary panel, click **Restore** to restore all the files or directories.

See "Summary panel" on page 486.

To remove files or directories from the Restore Cart

1 In the OpsCenter console, click **Manage > Restore**.

2 Click **Restore Files and Directories** under **Files and Directories**.

3 Click **Restore Cart**.

4 Select one or more files or directories that you want to remove from the Restore Cart.

5 Click **Remove from cart**.

Restore Options panel

You can specify restore options for the files and directories that you selected like destination client and paths, overwrite options etc. This panel allows you to specify the restore options for each source client from which a file or directory has been selected to be restored.

Select individual clients on the left side and specify the restore options for each client.

You can specify the following restore options for a client:

Specify destination (where to restore selected files/directories)

Restore all files/directories to their original file path location on the source client	This option is the default. Select this option to restore the selected files and directories to the same location from where they were backed up. This option works best when you restore from archived backups, since the backed up files are deleted from their original location after successful backup. If the original location contains items with the same names, the restore operation (by default) does not replace or overwrite those items.
Restore all files or directories to alternate file path location (maintaining existing structure) on source client or alternate client	Select this option to restore all selected files and directories to a different location from where they were backed up. You may choose to restore at a different location on the same client or may choose to restore on a different client. Note that a different destination client can only be a client that is associated with the same master server. You cannot restore to a client that is associated with a different master server. In the Destination field, enter the path for the new destination. You can also click **Browse** to locate the destination client.

Restore all files or directories to individually specified path and destination client	Restore individual directories and files to different locations and file paths and with different names. When you select this option, a table appears that lists the source files, and default values for destination client and path, and the destination file name. You can edit most columns of this table (except the Source File Name) and specify the destination client, file path, and the destination file name. Click on each cell under these columns and select **Edit**. Enter the appropriate values and click **OK**. Click the **Saved Table Edited Info** icon to save your edits in the table. This icon is located on the top-right corner of the table. **Note:** A destination client can only be a client that is associated with the same master server. You cannot restore to a client that is associated with a different master server.
Overwrite and access control options	
Overwrite the file that exists at the destination	By default, this option is not selected to avoid overwriting a current file. Select this option to replace a file with the same name in the destination directory with the file you want to restore.
Restore the file using a temporary file name (Windows clients only)	Restore the file using a different name than before.

Do not restore the file at all	By default, this option is selected to prevent the restore operation from overwriting a file with the same name in the destination folder. For example, if your destination choice is set to Restore all files/directories to their original location, marked files with the same names are not restored. If you deselect this option and your destination choice is set to Restore everything to its original location, files in the destination folder with the same names are overwritten. To avoid overwriting current files, you must do one of the following: ■ Select **Restore the file with different file name** ■ Select a different restore destination

Restore without access control (Windows clients only)	By default, files are restored with the same access control attributes that existed at the time of their backup. On Windows systems, be aware of the following if the access control attributes of a file have changed since the backup: ■ A user that was granted access to the file after the backup does not have access to the file after the restore. ■ A user with previous access to the backed up file retains access to the file after the restore. Select this option to restore files without the original access control attributes. This option is available only when the following conditions exist: ■ You are logged on as the system administrator. ■ The Operating System of the client computer is Windows Server 2003/XP, Windows Server 2008/Vista, or Windows Server 2008 R2/Windows 7. ■ NetBackup server software is installed on the computer where the client software is running. ■ The NetBackup master server, media server, and client are all at the same release level (software version).
Other options	

Rename hard links	This option applies to UNIX and Linux systems only. By default, hard link path names are restored exactly as they exist in the backup. Select this option to rename the hard link path names, if any exist. Veritas recommends that you select this option in the following situation: ■ You restore system files to an alternate disk and not to the current system disk. ■ You use the alternate disk as the system disk with the original file paths. In this situation, Veritas recommends that you select **Rename hard links**. Then, make sure that **Rename soft links** is not selected so that you can use the alternate disk and still have the correct file paths.
Rename soft links	This option applies to UNIX and Linux systems only. By default, soft (symbolic) link path names are restored exactly as they exist in the backup. Select this option to rename the soft link path names, if any exist. Veritas recommends that you do not select this option if you rename hard links.
Restore without crossing mount point	This option applies to UNIX and Linux systems only. By default, all file systems that are mounted in the selected directories are restored. Select this option to restore the selected directories without restoring all file systems that are mounted in those directories. **Note:** Mount points inside a backup image are always restored whether or not this option is selected.

Override default priority	You can change the priority of this restore by selecting Override default priority, and then set a priority number. The default is 90000. The available range is 0 to 99999. Higher numbers are higher priority.

Summary panel

The Summary panel shows the list of selected files and directories that have been selected for restore. It also shows details like the current location of these files and directories and where they will be restored.

The Summary page shows a table with the following columns:

Source File Name	This column lists the files or directories that have been selected for restore.
Source File Path	This column lists the current location of the file or directory.
Source Client	This column lists the client that contains the source file.
Destination File Path	This column lists the location that you specified for restoring the file or directory.
Destination Client	This column lists the name of the destination client where you want to restore the file or directory. Based on your selections, the destination client may be the same or different from the source client.

Click **Preview Media** to view the media required for the restore operation and to determine the availability of the required media. This helps you to know if the tape required for restore is in the library or not. This option only applies to tape backups. If the selected backups are on disk, this option is not applicable. The Preview Media dialog box displays details like Media ID, volume group, and if the media is in library.

Removing files or directories from the Summary panel

You can remove files or directories from the Summary panel. Use the following procedure to remove files or directories that you do not want to restore.

To remove files or directories from the Summary panel

1. On the Summary panel, select one or more files or directories that you want to remove.
2. Click **Remove files or directories**.

File or Directory Restore Launch Status dialog box options

The following options are displayed on the File or Directory Restore Launch Status dialog box:

Job ID	Job ID of the restore job
Master Server Name	Name of the master server that is associated with the client on which the file resides.
Client Name	Name of the source client

Restoring files or directories from the Summary panel

Use the following procedure to restore files or directories.

To restore files or directories from the Summary panel

1. The Summary panel shows the selected files or directories that you want to restore.

   Click **Restore** to restore all the files and directories that are displayed.

   Note: If you want to restore only specific files and directories and not all the files and directories that are displayed, click **Remove files or directories** to remove files or directories that you do not want to restore.

2. The corresponding restore job(s) are triggered. The **File/Directory Restore Launch Status** dialog is displayed. This dialog box shows basic job details for the jobs triggered. It also shows a link to access these jobs. Click the link to go to the **Monitor > Jobs** view and look for the specific Job ID.

   See "File or Directory Restore Launch Status dialog box options" on page 487.

About OpsCenter Guided Recovery

The use of the OpsCenter web-based user interface to guide a user through the Oracle cloning operation offers several benefits:

- The process is more automated, making the operation easier to perform.
- OpsCenter retrieves information for you such as databases and control files, shortening the Oracle clone setup time.
- A validation process increases the rate of successfully completing the cloning operation.
- You do not need access to the original database to perform the cloning operation.

Setting up for Guided Recovery cloning

Guided Recovery cloning requires metadata cataloging, which enables database information to display in OpsCenter. Metadata cataloging must occur during the backup from the Oracle database to be cloned. The collected metadata displays within the OpsCenter interface to guide the Clone operation. Cloning also requires that the Oracle destination file paths exist before the operation begins.

Do the following before you perform a Guided Recovery cloning operation:

- Configure metadata cataloging before taking the backup, that is used for the cloning operation, using one of these methods.
  - Place the following text into a text file (for example:*new_config.txt*) on the master or the media server that has access to the client:

    ```
    ORACLE_METADATA=YES
    ```

    Then send this configuration to the client host by using the following `bpsetconfig` command:

    ```
    bpsetconfig -h myoracleclient new_config.txt
    ```

    The `bpsetconfig` command is located in the `admincmd` directory.

    Windows: *install_path*\NetBackup\bin\admincmd

    UNIX: /usr/openv/netbackup/bin/admincmd
  - Alternatively on UNIX and Linux, ensure that the Oracle metadata parameter in the client's `bp.conf` is set at backup time as follows:

    ```
    ORACLE_METADATA=YES
    ```
  - Alternatively, the RMAN commands can include a SEND statement at the time of the backup.

    ```
    ... allocate channels ...
    SEND 'NB_ORA_METADATA=YES';
    ... backup command ...
    ```
- Set up all destination file paths before you run the cloning operation because the operation does not create new file paths during the process. Ensure that the Oracle user has write access to these paths.

Guided Recovery cloning pre-operation checks

Check the following items before you begin the cloning process:

- Ensure that the source and the destination systems and the source and the destination databases are compatible. Examples are Solaris 9 to Solaris 10 and Oracle 11 to Oracle 11.
- The cloning operation does not support offline tablespaces or raw tablespaces.
- The cloning operation does not support Oracle Automatic Storage Management (ASM).
- To use a different user or a different group for the clone, change the permissions of the backup image at backup time. Add the 'BKUP_IMAGE_PERM=ANY' to the send commands during the backup of the source database.
- If the destination client is different than the source client, perform an alternate restore procedure.
- On Windows systems, if the NetBackup Legacy Network Service runs as the Oracle user, that user needs the right to "Replace a process level token".
- On Oracle 9 for Windows, run the Oracle service under the Oracle user account. By default, it runs under the local system. On Oracle 10G systems and later, you can run under the local system.
- On Windows systems, if you clone to the same system, shut down the source database to successfully complete the operation. Otherwise, an error indicating the database cannot be mounted in exclusive mode appears.
- On UNIX and Linux systems, if the cloning user shares an existing Oracle home, the user must have write access to some directories such as `DBS`.
- On UNIX and Linux systems, shut down the source database before you clone in the following situation: You clone to the same system and you either use the same user or use the same home as the source database.

Performing a Guided Recovery cloning operation

You need to log onto OpsCenter, to perform a cloning operation. OpsCenter is the web GUI that you use to perform all guided recovery operations.

To perform a cloning operation on an Oracle database in OpsCenter

1. When you log onto OpsCenter, the first screen that appears is the **Monitor Overview** screen. Along the top of the screen, click **Manage > Restore**.
2. On the **What do you want to restore?** screen, click **Clone Oracle Database**.
3. On the small **Select a Master Server** dialog box, use the drop-down menu to select the master server that you want to work with, then click **OK**.

   See “Select a Master Server dialog” on page 491.

4 The **Select Source Database** screen lets you filter the list of databases by database name, host name, database version, platform, and date. The default condition is to display all databases that are backed up in the default date range. Click **Show Databases**.

More information is available on this screen.

See "Select Source Database panel" on page 491.

5 The databases appear under the filtering part of the same screen. Click **option** at the left side of the desired database entry to select the database on which you want to perform a cloning operation. Then click **Next>**.

6 The **Select Control File Backup** screen shows a timeline view of the control file backups. Select the icon for the desired control file backup from the timeline view. You can hover over the icon to display the control file details. If the icon represents multiple backups, you can hover over the icon to display all versions of the backup for that time periods.

Additional information is available to verify that you have selected the correct control file. The lower left corner of the screen lists three links. More information is available about these links.

See "Select Control File Backup panel" on page 492.

Click on the icon of the control file backup you want to restore for the clone of the selected database. The default is the latest backup selected. Then click **Next>**.

7 The **Destination Host and Login** screen contains parameters for the destination of the clone to be created. Enter the destination host name in the text box that is provided or click **Browse** and select from a list of available hosts. Note the following prerequisites concerning the destination host:

- The platform type of the source and destination must be the same.
- A NetBackup client must be installed.
- A compatible version of Oracle must be installed.

See "Destination host and login panel" on page 492.

For operating system authentication, enter a user name, password (Windows), and domain (Windows). Then click **Next>**.

8 The **Define Destination Parameters** screen appears. The five tabs on this screen are used to change database attributes, the destination paths of control files, data files, redo logs, and restore options. After you have changed the destination parameters, click **Next>**.

See "Destination Parameters panel" on page 493.

9 The **Selection Summary** screen lets you scan the information you have entered on the previous screens. Links to the recovery sets and destination database attributes let you view and verify any changes you have made. When you are satisfied with the summary information, click **Next>**.

See "Selection summary panel" on page 494.

10 The **Pre-clone Check** screen lets you validate the database attributes and the file paths. To validate, click the underlined word **here**. If a directory path does not already exist, the validation check flags the error. If a file already exists, the validation check also flags the error, so that the cloning operation does not overwrite the file.

See "Pre-clone check panel" on page 494.

When you are ready to launch the cloning operation, click **Launch Cloning Process**. A display appears that is similar to the NetBackup Activity Monitor.

Note: In NetBackup (7.1 or greater), validation of the data files that reside in raw devices may fail even though the Clone operation was successful. You may receive an error that states the validation for specific paths failed.

Select a Master Server dialog

From the pulldown menu, select the NetBackup master server that collected the backup information to be used for the cloning operation.

Select Source Database panel

When the **Select Source Database** screen first appears, the lowest portion of the screen shows a list of the latest backups for all the databases that the master server knows about for the default date range.

The upper portion of the screen shows parameters for filtering the list of databases. If the list is long, you can filter what databases appear by database name, host name, database version, and date range. Multiple filter parameters can be used at the same time.

For example, to show only the Solaris databases that are backed up between 11/05/2011 and 11/12/2011, select Solaris from the Platform: pulldown menu. Then select the dates from the calendar icons. Then click **Show Databases** to display the new filtered list of databases.

Select Control File Backup panel

The Guided Recovery **Select Control File Backup** screen is a timeline view of all the control files that are backed up for the selected database. The timeline displays an icon for each control file that is associated with the backed up database. When you first enter this screen, the latest backup control file is already selected.

Hover over the icon on the timeline to display a popup that shows information about that file: backup name, type of media, the size of the backup, etc.

Multiple control files may be displayed on the timeline. To view all the instances of control files, you may need to increase the scope of the timeline. You can display the timeline in days, weeks, months, or years. If multiple control files were backed up during a single timeline unit, a different icon appears representing more than one control file (for example, if the database was backed up twice in an hour). To select from among these files, hover over the icon. A popup lists each control file in table format. It shows several items including the backup name and the type of media. Click **option** next to the desired control file.

You can also click one of the links in the lower left of the screen to verify that you have selected the proper control file.

- **View Database Schema** shows the schema of the selected control file. It shows how the database is laid out by listing each data file name, tablespace name, and its size.
- **View Datafiles Recovery Set** shows the data file backups to be used for the restore process. It also shows the backup and image information that is displayed for each data file. The data file recovery set is generated only for the files that are backed up as part of an incremental strategy. Even though files that are backed up as part of a full backup do not appear in this list, the clone still completes successfully.
  If the image spans media, only the first media is shown in the list.
- **View Archived Log Recovery Set** shows the archive log backups that may be used to recover the database to the latest point in time of that control file. This set is generated only for the files that are backed up as part of an incremental strategy. Even though files that are backed up as part of a full backup do not appear in this list, the clone still completes successfully.

Destination host and login panel

The Select Destination Parameters screen lets you enter the destination host and the Oracle logon information. For Windows, you are asked for the domain name, user name, and password. For UNIX and Linux, you are asked only for the user name.

The following rules apply to the selection of the destination host:

- The destination must be of the same platform type as the source of the clone.
- A NetBackup client must be installed.
- A compatible version of Oracle must be installed.

Destination Parameters panel

Guided Recovery uses many values from the source database as default values for the destination database. You can modify these values if not appropriate for the destination database.

Note: The Windows information you enter on this screen is case-sensitive. Be sure to enter the Windows information appropriately.

The **Destination Parameters** screen contains the following tabs:

- **Database Attributes**. This pane appears when you first enter the Database Attributes screen. Each attribute name has identical source and destination attributes. You can change the destination attribute of the instance name, database name, and database home. Note that the instance name is case-sensitive while the database name is not case-sensitive.

  If you use a temporary tablespace or data files, and you plan to write the data files back to the same location, do not modify the path. If you must modify the path, make sure that it is identical to the source path including case (upper, lower, mixed). Otherwise, the clone fails with an error that indicates the temporary file already exists. This limitation does not affect UNIX and Linux systems.
- **Control File Paths**. This pane displays the source path and the destination path for each control file. You can change a control file destination path by clicking in the associated text window and entering the new path. You can also click Browse to navigate to the desired path. When you change a path, a highlight bar appears around the text window as a visual indicator that this path has changed.
- **Data File Paths**. This pane lets you change the destination path for one or more data files. Enter the path in the text window provided, then select the data files on which to apply it, and press the Apply option.
- **Redo Log Paths**. This pane displays the source path and the destination path for all redo logs. You can type in a new destination path or click Browse to navigate to the desired path. When you change a path, a highlight bar appears around the text window as a visual indicator that this path has changed.
- **Restore Options**. This pane displays restore options. The option that is displayed on this pane is **Number of parallel streams for restore and recover**.

When you are done making changes on this screen, click **Next>**. All the information from the previous screen is saved in preparation for the cloning operation. All the changes that are made in this screen are temporary and are active only for the cloning session.

Selection summary panel

The following information appears on this screen:

- The selected master server and the source database attributes.
- The date and time of the selected control file backup, and the backup media type.
- The database recovery set and the archived log recovery set.
- The destination database attributes selected in the previous screen and the database initialization parameters to be used for the cloning operation.

Pre-clone check panel

The Guided Recovery **Pre-clone Check** screen lets you validate the database attributes and the file paths. To validate, click the underlined word **here**. If a file path does not already exist, the validation check flags the error. If a file already exists, the validation check also flags the error, so that the cloning operation does not overwrite the file.

You can also specify an email address, so when the cloning process completes, an email is sent to you that gives you the status of the cloning operation along with other pertinent information.

Job Details panel

The Job Details screen is intended to reflect the NetBackup Activity Monitor. More information is available on the Activity Monitor.

For more information, see the NetBackup Administrator's Guide, Volume I.

Guided Recovery post-clone operations

Perform the following after the cloning operation has completed:

- On Windows systems, if the cloning operation fails, use the `dbca` utility to delete the database. `dbca` sometimes removes directories, so verify before retrying the operation.
- On UNIX systems, update the `oratab` file with the appropriate instance information.

- On UNIX systems, if the cloning operation fails, do the following cleanup:
  - If the database is active, shut down the database.
  - Remove init<SID>.ora, spfile<SID>.ora, and any other files that are associated with the SID being used, from the <$ORACLE_HOME>/DBS directory.
  - Remove all data files.
- If a cloned Oracle database contains read-only tablespaces or data files, you must make them read-write before RMAN backs them up, or RMAN cannot restore them. After the backup (cloning operation), you can return the items to read-only.

  The following shows an example of the sequence of steps in the process:
  - Back up Oracle database A which contains read-only tablespace TABLE1.
  - Clone database A to database B.
  - Use the Oracle `alter tablespace` command to make tablespace TABLE1 read-write. You may revert to read-only if you want.
  - Back up database B.
  - Use RMAN to restore database B.

Troubleshooting Guided Recovery

Guided Recovery operations are in addition to the normal NetBackup for Oracle operations.

On UNIX and Linux systems, gather all legacy logs at VERBOSE=5. On Windows systems, gather them at General=2, Verbose=5, and Database=5. All unified logs should be gathered at DebugLevel=6 and DiagnosticlLevel=6.

In addition to the troubleshooting methods and evidence that you use for resolving NetBackup for Oracle operations, there is also information that is required specifically for troubleshooting Guided Recovery when it fails.

For more information about NetBackup debug logs and reports, refer to the NetBackup Administrator's Guide, Volume I.

Troubleshooting files for metadata collection operations at the time of the backup

The information in the following log files can be helpful when you troubleshoot Guided Recovery metadata collection operations.

From the Oracle client host:

- netbackup/logs/bphdb legacy logs

- netbackup/logs/dbclient legacy logs (The directory must be writable by the Oracle users.)
- ncf unified logs, OID 309, New Client Framework
- ncforautil unified logs, OID 360, New Client Framework Oracle Utility
- ncforaclepi, OID 348, New Client Framework Oracle Plugin

From the NetBackup media server: netbackup/logs/bpbrm legacy logs

From the NetBackup master server:

- netbackup/logs/bprd legacy logs
- nbars unified logs, OID 362, NetBackup Agent Request Service
- dars unified logs, OID 363, Database Agent Request Service

For more information about NetBackup debug logs and reports, refer to the NetBackup Administrator's Guide, Volume I.

Troubleshooting files for Guided Recovery validation operations

The information in the following log files can be helpful when you troubleshoot Guided Recovery validation operations.

From the Oracle client host:

- netbackup/logs/vnetd legacy logs
- ncf unified logs, OID 309, New Client Framework
- ncfnbcs unified logs, OID 366, New Client Framework NetBackup Client Services

From the NetBackup master server:

- netbackup/logs/vnetd legacy logs
- nbars unified logs, OID 362, NetBackup Agent Request Service
- dars unified logs, OID 363, Database Agent Request Service

From the Veritas OpsCenter server:

- <SYMCOpsCenterServer>/config/log.conf file
- opscenterserver unified logs, OID 148 (The default location is <SYMCOpsCenterServer >/logs)
- opscentergui unified log, OID 147 (The default location is <SYMCOpsCenterGUI>/logs)

For more information about NetBackup debug logs and reports, refer to the NetBackup Administrator's Guide, Volume I.

Troubleshooting files for Guided Recovery cloning operations

The information in the following log files can helpful when you troubleshoot Guided Recovery cloning operations.

From the Oracle client host:

- netbackup/logs/bphdb legacy logs (Includes the obk_stdout and obk_stderr logs.)
- netbackup/logs/bpdbsbora legacy logs
- netbackup/logs/dbclient legacy logs (The directory must be writable by the Oracle users.)
- A tar of netbackup/logs/user_ops (UNIX/Linux)
- A compress of NetBackup\Logs\user_ops (Windows)

From the NetBackup master server:

- netbackup/logs/vnetd legacy logs
- netbackup/logs/bprd legacy logs
- nbars unified logs, OID 362, NetBackup Agent Request Service
- dars unified logs, OID 363, Database Agent Request Service

From the Veritas OpsCenter server:

- <SYMCOpsCenterServer>/config/log.conf file
- opscenterserver unified logs, OID 148 (The default location is <SYMCOpsCenterServer >/logs)
- opscentergui unified log, OID 147 (The default location is <SYMCOpsCenterGUI>/logs)

About managing NetBackup Hosts

This view is displayed when you select Manage>Hosts. This view displays detailed information for OpsCenter audit reports. for the current Master server selection.

Managing audit trails settings

You can manage the settings to enable the auditing for the selected master server through OpsCenter. You must have Admin privileges to configure the audit settings.

To enable the Audit trail logging

1. Log on to OpsCenter server host with administrator privileges.
2. Click **Manage** and click **Hosts**.

3 From the **Master Server** tab, select the required master server and click **Edit Audit Settings**.

Select the **Enable audit trail logging with NetBackup Environment** check box to enable the audit logging process.

Note: If audit logging is initiated in NetBackup, the **Enable audit trail logging with NetBackup Environment** check box appears as selected. You can disable audit logging by clearing this check box.

---

4 Under **Retention period**, select the **Always retain all audit trail logs** option to retain the logs forever. To retain logs for a specific period of time, enter the value in the **Retain audit logs for days** text box. By default, the retention period is set to 90 days.

5 Click **Save** to save the settings.

About managing NetBackup Deployment Analysis

This view is displayed when you select Manage > NetBackup Licensing. This view lets you run OpsCenter traditional licensing and capacity licensing reports for all or selected master servers.

Only Administrators or Security Administrators can access Manage > NetBackup Licensing. The NetBackup Licensing subtab is not visible to any other user role.

About the traditional license report

The traditional licensing report is helpful if you use the traditional NetBackup licensing model. The traditional NetBackup licensing model is based on the number of NetBackup clients, servers, and options in use. As per this model, you purchase licenses based on the number of NetBackup clients, servers, and options on which you want to run NetBackup. As you deploy additional NetBackup clients or servers or attach additional tape drives or storage to NetBackup, you must license additional copies of the appropriate NetBackup product.

NetBackup Server, Client, and Agent offerings are charged on the basis of their hardware tier. Tape options are charged on a per drive basis. AdvancedDisk potions are charged on a per terabyte basis.

The traditional licensing report is generated in the form of an Excel sheet. Basically OpsCenter invokes the `nbdeployutil` executable on the master server to collect the required data. OpsCenter invokes the `nbdeployutil` executable (bundled with OpsCenter) to analyze the collected data.

More information about `nbdeployutil` is available in the *NetBackup Administrator's Guide, Volume II*.

The traditional license report provides details about your utilization of the NetBackup components. The report lists all the NetBackup components and the associated tier for each component. The traditional licensing report also provides detailed information about each master server, clients, tapes, capacity etc.

The traditional license report is a Microsoft Excel spreadsheet with seven tabs:

- **Summary**
  This tab shows the final details about master servers, media servers, and clients. This tab lists the source data for generating the report. The number of media servers and the number of clients is provided, as well as capacity information.
- **Hosts**
  This tab provides a listing of host names, along with associated computer information. The associated information includes information such as: platform, computer type, database software installed, SAN media server, and NDMP.
- **NDMP**
  This tab shows the computers that the utility determined are NDMP servers and the corresponding tier number of the client. When you reconcile the report, you need to address the clients that are found on this tab.
- **Virtual Servers**
  This tab shows the number of virtual servers or virtual hosts detected in the environment.
- **Drives**
  This tab details the type of drives as well as the host or the library where the drive resides. The tab provides the host names that are associated with each drive as well as information about virtual tape libraries, shared drives, and vaulted drives.
- **Interpreting the results**
  This tab provides a general overview of how to reconcile the information in the report which your actual environment.
- **Disclaimer**
  This tab shows text explaining the limits of the report's calculations and proper use of the data. For example, the figures should not be used to audit compliance.

Much of the report information does not affect the final values on the **Summary** tab. This information is useful for having a better understanding of your environment.

More information about the traditional licensing report is available in the *NetBackup Administrator's Guide, Volume II*.

Prerequisites and data collection for a traditional licensing report

Consider the following prerequisites before running the traditional licensing report:

- For the Traditional License report, you must install the `nbdeployutil` on master servers lower than 7.5.
  This utility automatically gets installed when you install a NetBackup 7.5 master server. Hence you do not need to install this utility on 7.5 master servers.
  The `nbdeployutil`utility is issued as an Emergency Engineering Binary (EEB) and must be installed on all master servers lower than 7.5.
  http://www.veritas.com/docs/000081541
  More information about installing EEBs is available on the Veritas Support site.

  Note: The `nbdeployutil` utility was earlier shipped with 7.1.x master servers. However the utility that is shipped with NetBackup 7.1.x does not support traditional license reporting.

  More information about the utility is available in *NetBackup Administrator's Guide, Volume II*.
- You must enable traditional license deployment data collection for the master server. The NetBackup user name and password is a must for the user to access a remote NetBackup master server (a master server is remote if it is not installed on the OpsCenter Server).
- Only Administrators or Security Administrators can access **Manage > NetBackup Licensing** subtab and hence run this report.
- At any point of time, only a single user is allowed to generate the traditional licensing report.
  Once a traditional licensing report is generated successfully, the last report is overwritten.

Traditional Licensing page

The traditional licensing page displays the last successfully created traditional license report (if applicable) and also lets you create a new traditional licensing report.

Create Traditional Licensing Report Wizard

The Create Traditional Licensing Report Wizard consists of the following panels:

- Data Collection
- Export or Email Report Options

The Data Collection panel shows the following options:

Collect data and run report for all configured master servers	Select this option if you want to run the traditional license report for all the master servers that are configured on the OpsCenter console. When you select this option, the panel shows the number of configured master servers. This is the number of master servers that are currently added to the OpsCenter console. The panel also displays the number and details of master servers for which the prerequisite status is Incomplete (or not successful) in a table. The table only shows those master servers that did not pass the prerequisite check. Click the link under the **Prerequisite Status** column to know and troubleshoot the issue. Note that the master servers for which the **Prerequisite Status** is **Incomplete** are not included in the traditional licensing report.
Collect data and run report for specific master servers	Select this option if you want to run the traditional license report for only specific master servers. When you select this option, you can view a table underneath that shows the available master servers by default. From the list of available master servers, you can select the master servers for which you want to run the traditional licensing report. You must select at least one master server. Once you select the master servers from the list of available master servers, click **Selected Master Servers** tab to view details for the selected master servers.

A table in the middle of the Data Collection panel displays the following columns:

Master Server:	This column displays the name of master servers for which the report is generated. If you select **Collect data and run report for all configured master servers**, this column displays only those master servers for which the prerequisite status is incomplete.
Licensing Data Collection Status	This column displays the status of traditional licensing data collection for the specific master server.
Last Licensing Data Collection Date	This column displays the date and time when the last licensing data was collected. The column shows a blank when the data collection fails.
Exceptions	This column displays the reason for data collection failure.
Prerequisites Status	This column displays a link named `Incomplete` when one or more of the prerequisites are not met. Click the link to know the details about the prerequisites that need to be completed for each master server. When the prerequisite check is successful, a green checkmark appears in this column. The following prerequisites are checked for each master server: ■ Is an Agent configured for data collection? ■ Is the **Enable Traditional License Deployment Data Collection** option checked? ■ Did you enter a user name or password to access the master server? Besides the prerequisites that are listed above, there are other prerequisites that must be satisfied. More information about all the prerequisites is available. See "Prerequisites and data collection for a traditional licensing report" on page 500.

In the **Export or Email Report Options** panel, you must specify email recipients and optionally can choose to export the report. It is mandatory that you email the report so that you have the report for future reference.

The Export or Email Report Options panel displays the following options:

To, **CC**, or **BCC** fields	Enter the recipients email address in these fields. The recipients receive emails when the report generation is complete.

Subject This field displays the default text Traditional Licensing Report. You can change the subject line if required.

Message Enter a message in this field.

Export report Select this option to export report to *INSTALL_PATH*\server\export\NDAReportExport directory on Windows and *INSTALL_PATH*/SYMCOpsCenterServer/export/NDAReportExport directory on UNIX.

You can change the export location from **Settings** > **Configuration** > **Report Export Location**.

Generating a Traditional Licensing report

The Traditional Licensing report is generated in the form of an Excel sheet. This report can be emailed or exported in the XLS format to the required email address or location.

To generate a Traditional Licensing report

1. Before running a traditional licensing report, review the prerequisites in the following topic.

   See "Prerequisites and data collection for a traditional licensing report" on page 500.

2. In the OpsCenter console, click **Manage** > **NetBackup Licensing**.
3. The **Traditional Licensing** page contains details about the previously created report, log file, and data collection. You can view the previously generated report by clicking **Download**. A calculation log file is also created when the traditional license report is generated. You can view the calculation log file by clicking the **View Log** link.
4. Click **New Report** to generate a new report. The **Create Traditional Licensing Report** wizard is displayed.
5. Select the **Collect data and run report for all configured master servers** to generate a report for all the master servers.

   Select the **Collect data and run report for specific master servers** to generate a report for specific master servers. Select the required master servers from the **Available Master Servers** tab. The master servers that you select are displayed in the **Selected Master Servers** tab.

6. Click **Next**.

7 In the **Report Options** panel, enter the recipients email address in the **To** and **CC** fields. The **Subject** field displays the default text Traditional Licensing Report, you can change the subject line if required.

8 Enter a message in the **Message** field.

9 To export the report to the required location, select the **Export report (XLS format)** check box. You can change the export location path from **Settings** > **Configuration** > **Report Export Location**.

See "Setting report export location in OpsCenter" on page 222.

10 Click **Finish** to initiate the report creation. A message to show that report creation is in progress is flashed.

When report generation is complete, you can open the .xls file or save the file for later viewing.

Note: Re-running the report when report generation is in progress is not possible as it displays errors in the report. It is advisable to wait till the report is generated.

Traditional Licensing report and log file locations

The traditional licensing reports are located at the following locations:

- The final report is located at INSTALL_PATH\server\fsdb\nda\report on Windows or INSTALL_PATH/SYMCOpsCenterServer/fsdb/nda/report on UNIX.
- The last successful backed up report is located at INSTALL_PATH\server\fsdb\nda\backup on Windows or INSTALL_PATH/SYMCOpsCenterServer/fsdb/nda/backup on UNIX.

The following log files are generated when you run the traditional licensing report:

NdaReportManager*.log	This log file contains the output of `nbdeployutil` executable. This file is located in INSTALL_PATH\server\logs on Windows and INSTALL_PATH/SYMCOpsCenterServer/logs on UNIX.

148.log	This log file contains the OpsCenter logs for traditional licensing report. This file is located in INSTALL_PATH\server\logs on Windows and INSTALL_PATH/SYMCOpsCenterServer/logs on UNIX.
Calculation log file (`log_timestamp.log`)	You can validate the data in the traditional licensing report using the calculation log file. The calculation log files contain the logs for report generation which can be used to check the authenticity of the final report. This file is located in INSTALL_PATH\server\fsdb/nda/logs on Windows and INSTALL_PATH/SYMCOpsCenterServer/fsdb/nda/logs on UNIX.

Possible Traditional License report issues

The Traditional Licensing report requires a user to enable master servers and configure Agents to generate the correct report. When the master server is not enabled or when the Agents are not configured, the report is not generated and shows errors. Another cause of errors when a report is not generated is the network connectivity issue. Make sure that you have network connectivity.

Always review the list of prerequisites before running a traditional license report.

See "Prerequisites and data collection for a traditional licensing report" on page 500.

Table 9-19 describes the possible Traditional License report issues and their solution.

Table 9-19 Traditional License report issues, causes, and solution

Error and cause	Solution
Master server not connected or it might be disabled Master server is not connected or disabled	Confirm that the master server is connected.

Table 9-19 Traditional License report issues, causes, and solution *(continued)*

Error and cause	Solution
Data collection failed as the NetBackup Deployment Analysis utility has not been installed on the master server. You must install the utility to run the Traditional License report. Refer the Admin Guide for more details.	You must install `nbdeployutil` on master servers lower than 7.5. This utility is issued as emergency engineering binary (EEB). More information about installing EEBs is available on the Veritas Support site. More information about the utility is available in *NetBackup Administrator's Guide, Volume II*.
Unable to log in into NetBackup Master server. Login credentials might be incorrect.	You must always enter the user name and password to access a remote NetBackup master server. If the credentials are not present, you must re-enter them. You can re-enter credentials while adding or editing a master server by clicking **Settings > Configuration > NetBackup**.

Capacity License report

A Capacity Licensing report gives a summary of the amount of data that is protected. The report is classified by the options Enterprise Disk, PureDisk, and RealTime.

The report gives capacity totals for each client, thus making it easier to verify capacity totals for each client. The report displays totals on the basis of the number of policies and subtotals for each capacity tier. A log file is also created, which gives information about how the totals are calculated.

The report is generated in the form of an Excel sheet. The report contains information about capacity totals backed up for each client. The report displays details such as number of policies per client and their name and the total kilobytes backed up. The report also gives information about the terabytes stored on:

- BasicDisk
- Physical Tape
- OpenStorage
- Visual Tape Library
- Flexible Disk

- Enterprise Disk Subtotal
- NDMP
- NASSnapVault
- PureDisk
- RealTime

Using the details of the Capacity Licensing report you can compare the actual amount of data that is backed up with the licensed amount. You can thus ensure that the data that is backed up is within the permitted license amount. The report displays the amount of data with the licensed amount for the Capacity Totals for Enterprise Disk, PureDisk, and RealTime.

See "Data compilation for the Capacity License report" on page 507.

See "Possible Capacity License report issues" on page 510.

Data compilation for the Capacity License report

Capacity Licensing is a way of determining the total terabytes of data NetBackup protects. The data can either be on the clients or the devices where the software is installed. The data can also be on the software that is used to provide the backup functionality.

About determining the capacity licensing

The `bpimagelist` command is used to obtain image and fragment information for all backups for the past 90 days. The NetBackup Deployment Analyzer examines the image headers in the NetBackup catalog to determine the amount of data that NetBackup protects.

The data is measured in terabytes. The final total is the sum of terabytes for each client and policy combination that the analyzer examines. The Deployment Analyzer calculates the total data that needs to be protected. The analyzer uses the size of the last full backup for the last 90 days.

A day is defined as the 24 hour period from midnight to midnight. The analyzer sums all backups that started within that period. For some policy types, the analyzer considers the day with the largest total volume of protected data as an estimate of the approximate size of active data under protection for the client and policy.

Generating a Capacity Licensing report

The Capacity Licensing report is generated in the form of an Excel sheet. This report can be emailed or exported in the XLS format to the required email address or location.

To generate a Capacity Licensing report

1. In the OpsCenter console, click **Manage** > **NetBackup Licensing**. The **Capacity Licensing** page is displayed.
2. The **Capacity Licensing** page contains details about the previously created report, log file, and data collection. You can view the previously generated report with the available link under the **Last Successful Report Date** header. A log file is generated when the Capacity License report is generated. You can view the log file with the **View Log** link.

   See "About the Capacity Licensing page" on page 509.
3. Click **New Report** to generate a new report. The **Create Capacity Licensing Report** page is displayed.
4. Select the **Collect data and run report on all Master Servers** option to generate a report for all the master servers.

   Select the **Collect data and run report on specific Master Servers** option to generate a report for only the required master servers. Select the required master servers from the list.
5. Click **Next**. The Report Options page is displayed.
6. Enter the recipients email address in the **To** and **CC** fields. The **Subject** field displays the default text Capacity Licensing Report, you can change the subject line if required.
7. Enter a message in the **Message** field.

8 To export the report to the required location, select the **Export report (XLS format)** check box. You can change the export location path from the **Settings** > **Configuration** > **Report Export Location** tab.

See "Setting report export location in OpsCenter" on page 222.

9 Select **Run Report** to initiate the data collection. A message is displayed to show that report generation has started is flashed.

When report generation is complete, you can open the .xls file or save the file for later viewing.

Note: Re-running the report when report generation is in progress is not possible as it displays errors in the report. Veritas recommends that you wait till the report is generated.

See "Data compilation for the Capacity License report" on page 507.

See "About the Capacity Licensing page" on page 509.

About the Capacity Licensing page

The Capacity Licensing page contains information about the Capacity License report and the data collection status. The report section contains details about the report in the form of a table. The headers are:

- **Last Successful Report Date**: Displays a link to the previously generated report. The link itself contains information about the date and time of the last successful report.
- **Status**: Displays the report status as the name suggests. The status shows as **Failed** when the report is not generated.
- **Exceptions**: Displays the reasons for the report generation failure. An example exception detail message can be: Data collection failed for selected master servers. If the report generation is successful, this column shows a blank.
- **Last Successful Report Log**: Displays a link to the log file that is generated when the report is generated. The log file is very useful in analyzing the Capacity Licensing report. If the report generation fails, this column shows a blank.

The **Capacity Licensing** page also contains details about data collection in the form of a table. The headers are:

- **Master Server**: Displays the list of master servers for which the report is generated. If you select the **Collect data and run report on specific Master Servers** option, then the column displays only those master servers that you select.

- **Data Collection Status**: Displays the status of data collection.
- **Last Licensing Data Collection Date**: Displays the date and time when the last licensing data is collected. The column shows a blank when data collection fails.
- **Exceptions**: Displays the reason for data collection failure.
- **Prerequisites Status**: Displays a link when the prerequisites have not been completed. Click the link to know the details about the prerequisites that need to be completed. Prerequisites can be, an agent not configured, or data status collection is not enabled for a master server.

Final location of the Capacity Licensing reports and logs

The reports and log files are located at the following locations:

- The final report is located at SERVER_INSTALL_DIR/fsdb/fetb/report.
- The log file is located at SERVER_INSTALL_DIR/fsdb/fetb/log.
- The last successful backup report is located at SERVER_INSTALL_DIR/fsdb/fetb/backup.
- The output of `bpimagelist` for each server is located at SERVER_INSTALL_DIR/fsdb/fetb/data.

Possible Capacity License report issues

The Capacity Licensing report requires a user to enable master servers and configure agents to generate the correct report. When the master server is not enabled or when the agents are not configured, the report is not generated and shows errors. Another cause of errors when a report is not generated is the network connectivity issue. Make sure that you have network connectivity.

Table 9-20 describes the possible Capacity License report issues and their solution.

Table 9-20 Capacity License report issues, causes, and solution

Error and cause	Solution
Master server is not connected or it might be disabled Master server is not connected or disabled	Confirm that the master server is connected.

Table 9-20 Capacity License report issues, causes, and solution *(continued)*

Error and cause	Solution
Unable to log in into NetBackup Master server. Login credentials might be incorrect.	You must always enter the user name and password to access a remote NetBackup master server. If the credentials are not present, you must re-enter them. You can re-enter credentials while adding or editing a master server by clicking **Settings > Configuration > NetBackup**.

See "Generating a Capacity Licensing report" on page 508.

Chapter 10

Supporting Replication Director in OpsCenter

This chapter includes the following topics:

- About monitoring Replication Director from OpsCenter
- About the Open Storage alert condition
- How the events are generated
- Adding an alert policy
- About monitoring replication jobs
- Disk pool monitoring
- Storage lifecycle policy reporting
- Reporting on storage units, storage unit groups, and storage lifecycle policies

About monitoring Replication Director from OpsCenter

OpsCenter lets you monitor, alert, and report on the Replication Director functionality in NetBackup. The following sections provide an overview of the changes that have been made in OpsCenter with regards to the Replication Director functionality.

About the Open Storage alert condition

A new event-based alert condition named **Open Storage** has been added under the Device alert category in OpsCenter. For event-based alert conditions like **Open**

Storage, OpsCenter retrieves data from NetBackup based on notifications from NBSL.

An OpenStorage alert is generated when specific events occur in the storage server (in this case NetApp DataFabric Manager server). When you configure an alert policy based on the **Open Storage** alert condition, you can receive alerts for the NetApp (NTAP) events in OpsCenter.

Table 10-1 lists the NTAP events that OpsCenter supports.

Table 10-1 NTAP events supported by OpsCenter

General Category	Event Type
Space Management and Alerting	Threshold alarms or Volume Almost Full (DataFabric Manager (DFM) generated). If the particular volume crosses the high water mark, then DFM generates this event.
Unprotected Data	Unprotected Data is a custom event generated by NetApp NetBackup plug-in when resource pool has some volumes that are configured but are not protected. The event generation occurs where there is an auto-discovery of unprotected NAS file services data.

NBSL passes these NTAP events from NetApp devices to OpsCenter. Depending on the alert policy configuration, OpsCenter filters these events based on storage server, severity, and message filter values and raises the alert. The raised alert can be configured to be sent as an email or SNMP trap.

You can clear the **Open Storage** alert manually. To clear the alert, go to the **Monitor > Alerts (List View)**, select the alert and then click **More > Clear**.

How the events are generated

When you configure disk pools in NetBackup, NetBackup connects to the DFM server through the NetApp NetBackup plug-in. The plug-in scans the volumes that are not protected and takes some time to find out the details of unprotected volumes. If the master server asks for the event list while the event list is being prepared, then the same master server who triggered this does not receive the events at that time. However, the master servers which connect to the DFM server after the event list is prepared receive those events. After every 24 hours from the time the first call is made, the current list of events are sent again to all master servers that are connected to this DFM server. Currently this is a fixed cycle unless NetBackup is restarted. Maximum eight event channels are supported by default which means that maximum eight master servers are capable of receiving events from DFM. If more than eight master servers are connected to the DFM server and all are

monitored by OpsCenter then it is not predictable which eight master servers receive those events.

The value for maximum number of event channels is configurable in a file on the NetBackup plug-in host (usually the same as DFM host):

Windows	C:\Program Files\netapp\NBUPlugin\config\NBUPlugin.cfg
UNIX	/usr/NetApp/NBUPlugin/config/NBUPlugin.cfg ([NBUPlugin:NumEvCh] Value=8)

It is recommended that the value for maximum event channels is configured as 8. Increasing the value may affect the DFM performance.

Consider a scenario where one master server is connected to one DFM server and is monitored by OpsCenter. When NetBackup initially connects to the NetApp NetBackup plug-in, then it does not receive any event until the complete cycle of 24 hours assuming that the event cycle is of 24 hours. After 24 hours, the events are sent to OpsCenter by NBSL. So even if the condition like Volume almost Full has occurred, you see events only after the cycle is complete.

Consider a scenario where multiple master servers monitored by OpsCenter are connected to one DFM server. In this scenario, the first master server that connects to the DFM server by NetApp NetBackup plug-in never receives the event for the first cycle. The master servers which connect later receive events only if they are connected after DFM prepares the event list. No events are sent in the time between when the first master server connected to DFM server and the time DFM is ready with events. If some master server connects during that time then it does not receive any events. Which master servers receive the events depends a lot on when they connect to the NetApp NetBackup plug-in. But after 24 hours, all master servers should receive the events from NetApp NetBackup plug-in provided that maximum eight master servers are connected.

Adding an alert policy

Use the following procedure to create an alert policy based on the **Open Storage** alert condition.

To add an alert policy

1. In the OpsCenter console, select **Manage > Alert Policies**.
2. Click **Add**. The Alert Policy Wizard appears.
3. Enter a Name, Description, and Alert Condition on the **General** panel. For Alert Condition, select **Open Storage** under **Device**.
4. Click **Next**.

5 On the **Alert Condition Properties** panel, specify attributes for the **Open Storage** alert condition. These attributes or filters define and limit the alert. You can select or define the following attributes:

Event Severity	Select the event severity that should be evaluated for the alert condition. By default, All event severities are selected.
Event message contains words	Specify words from the event message to get alerts on specific events.
Event vendor type contains words	Specify words for vendor type to get alerts on specific events.

6 Click **Next**.

7 On the **Scope** panel, select the storage server that should be verified for the **Open Storage** alert condition. You must select at least one object, node, or view from this page. Click **Next** to continue.

8 From the **Actions** panel, you can send the alert as an email or SNMP trap. You can also assign severity for the alert. In the Email Recipients and Trap Recipients sections, select email or SNMP recipients (or both) to receive the alert notification.

Note that if you create an alert policy and do not define any recipients, the alert is still displayed in the **Monitor > Alerts** view. In the Severity section, do the following:

- Select a severity level from the **Alert Severity** drop-down list. (If this alert occurs, the alert is displayed in the **Monitor > Alerts** view.)
- Select an appropriate severity level from the **Severity of email/trap sent for cleared alert** drop-down list. With **Severity of email/trap sent for cleared alert** option, you can configure the severity for an email or trap that is sent when an alert is cleared. The default severity level is Informational.
- The **Activate Condition** option is checked by default. By default, the policy is active once you create it. Deselect the **Activate Condition** option if you want to deactivate the policy. You can always activate or deactivate the policy later from the OpsCenter console.

About monitoring replication jobs

A new filter named **Snapshot Replication** has been added in the **Monitor > Jobs (List View)**. To view the replication jobs in the OpsCenter console, go to **Monitor**

> Jobs (List View or Hierarchical View) and select the **Snapshot Replication** filter from the **Filter** drop-down list.

The duplication method is shown in the **Method** column. The **Method** field is also available in the **Details** pane under the **General** tab.

You can also view the data that is transferred for each of the replication jobs. This is reflected in the **Job Size** column when you select **Monitor > Jobs** (**List View** or **Hierarchical View**).

Disk pool monitoring

To view disk pool details, select the **Monitor** tab, and then the **Devices** sub-tab.

Select the **Disk Pools** tab above the table. Disk pool monitoring is divided into three tabs:

General tab

The **General** tab (Figure 10-1) contains information about the selected disk pool, including the used and available space in the selected disk pool and whether the images in the disk pool have been imported.

The table also contains the following columns that pertain to snapshot replication:

- **Configured for Snapshots**
  Identifies whether the disk pool is configured to contain snapshots, making it eligible for snapshot replication.
- **Mirror**
- **Primary**
- **Replication**

Disk Volume tab

The **Disk Volume** tab contains information about the selected disk pool, including the location or path to the volume, and whether the volume is configured for snapshots.

Storage Server tab

The **Storage Server** tab (Figure 10-2) contains information about the selected disk pool, including the server type and the number of active jobs for the storage server.

The table also contains a **Configured for Snapshots** column, which identifies whether the storage server is configured to contain snapshots.

Figure 10-1 Disk Pool General tab

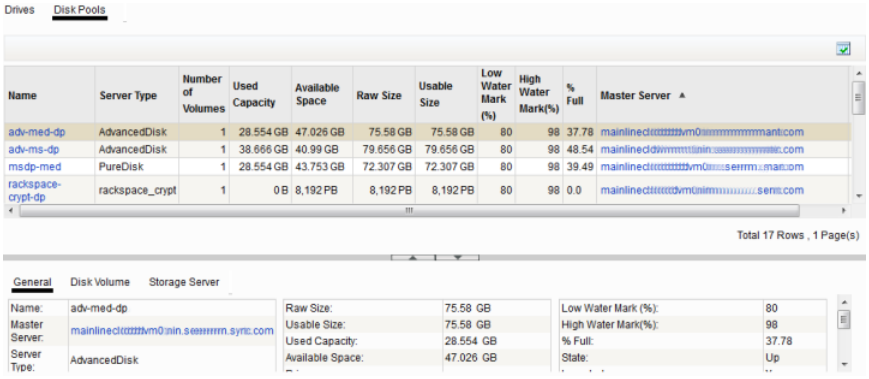
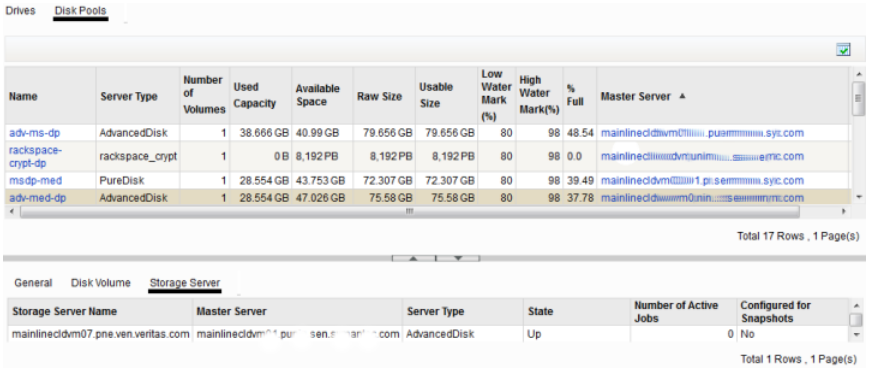


Figure 10-2 Disk Pool Storage Server tab



Storage lifecycle policy reporting

The **Storage Lifecycle Policy** status report provides a summary of the SLPs of a selected master server.

Many columns in the report contain data that links to additional reports:

- **SLP Status by SLP**
- **SLP Status by Client**
- **SLP Status by Image**
- **SLP Status by Image Copy**

The **SLP Status by Image Copy** report displays the details of any snapshot copy that is a part of a SLP.

Reporting on storage units, storage unit groups, and storage lifecycle policies

To view the details of storage units, storage unit groups, and storage lifecycle policies, select the **Manage** tab, and then the **Storage** sub-tab.

Select the **Storage Unit** tab above the table to display storage unit details, including whether the storage unit is enabled for snapshots and the name of the disk pool to which the storage unit belongs.

Storage Unit tab

The **General** tab (Figure 10-3) contains information about the selected storage unit.

The table also contains the following columns that pertain to snapshot replication:

- **Configured for Snapshots**
  Identifies whether the storage unit is configured to contain snapshots, making it eligible for snapshot replication.
- **Mirror**
- **Primary**
- **Replication**

Storage Unit Group tab

The **Storage Unit Group** tab contains information about the selected storage unit group.

The table contains a **Configured for Snapshots** column which identifies whether the storage unit group can contain snapshots.

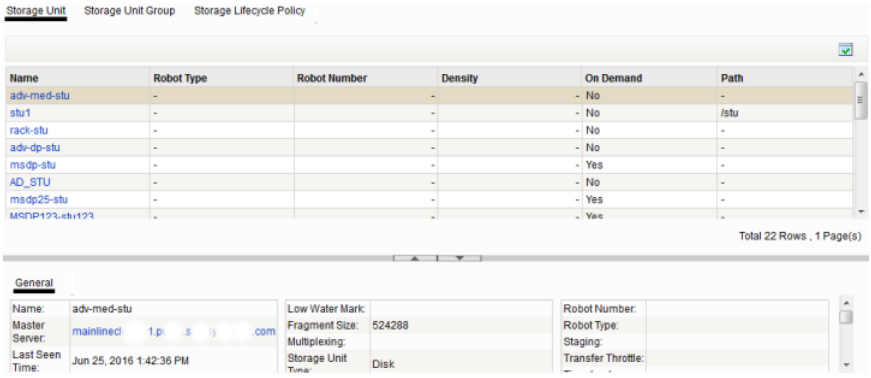
Storage Lifecycle Policy tab

The **Storage Lifecycle Policy** tab contains two subtabs:

- **General**
  Displays SLP details, including whether the SLP is configured to preserve multiplexing, and the data classification on the SLP.
- **Operations**

Displays the operation type and storage unit that is assigned to each operation in the SLP.

Figure 10-3 Storage Unit General tab



Chapter 11

Understanding and configuring OpsCenter alerts

This chapter includes the following topics:

- About using SNMP
- About managing OpsCenter alerts using Microsoft System Center Operations Manager 2007
- About managing OpsCenter alerts using HP OpenView Network Node Manager 7.50/7.51 on Windows

About using SNMP

This section provides information about SNMP and how OpsCenter uses SNMP.

See “About SNMP” on page 521.

See “About SNMP versions” on page 521.

See “ SNMP versions supported in OpsCenter” on page 522.

See “About the Management Information Base (MIB) and OpsCenter support” on page 522.

See “Configuring the SNMP trap community name for OpsCenter” on page 537.

See “Configuring the SNMP version for sending SNMP traps” on page 538.

See “Frequently asked SNMP and OpsCenter questions” on page 540.

About SNMP

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

SNMP is based on the manager model and agent model. This model consists of a manager, an agent, a database of management information, managed objects, and the network protocol.

The manager provides the interface between the human network manager and the management system. The agent provides the interface between the manager and the physical devices being managed.

The manager and agent use a Management Information Base (MIB) and a relatively small set of commands to exchange information. The MIB is organized in a tree structure with individual variables, such as point status or description, being represented as leaves on the branches. A numeric tag or object identifier (OID) is used to distinguish each variable uniquely in the MIB and in SNMP messages.

About SNMP versions

Many versions of SNMP are available.

The versions of SNMP protocol are as follows:

- SNMPv1
  The SNMPv1 version is the first version of the protocol and is defined by RFC 1157. This document replaces the earlier versions that were published as RFC 1067 and RFC 1098. Security is based on community strings.
- SNMPv2
  It was created as an update of SNMPv1 adding several features. The key enhancements to SNMPv2 are focused on the SMI, manager-to-manager capability, and protocol operations.
  SNMPv2c combines the Community-based approach of SNMPv1 with the protocol operation of SNMPv2 and omits all SNMPv2 security features.
  - The original SNMPv2 (SNMPv2p)
  - Community-based SNMPv2 (SNMPv2c)
  - User-based SNMPv2 (SNMPv2u)
  - SNMPv2 star (SNMPv2*).
- SNMPv3

This version of the protocol is a combination of user-based security and the protocol operations and data types from SNMPv2p, and support for proxies. The security is based on that found in SNMPv2u and SNMPv2*. RFC 1905, RFC 1906, RFC 2261, RFC 2262, RFC 2263, RFC 2264, and RFC 2265 define this protocol.

SNMP versions supported in OpsCenter

OpsCenter supports the following SNMP versions:

- SNMPv1
- SNMPv2c
- SNMPv3

About the Management Information Base (MIB) and OpsCenter support

Each SNMP element manages specific objects with each object having specific characteristics. Each object and characteristic has a unique object identifier (OID) that is associated with it. Each OID consists of the numbers that are separated by decimal points (for example, 1.3.6.1.4.1.2682.1).

These OIDs form a tree. The MIB associates each OID with a readable label and various other parameters that are related to the object. The MIB then serves as a data dictionary that is used to assemble and interpret SNMP messages.

See "SNMP traps" on page 522.

See "Alert descriptions in OpsCenter" on page 525.

SNMP traps

This section explains the content of an SNMP trap that is sent from Veritas NetBackup OpsCenter.

Each OpsCenter trap contains 2 standard object identifiers and 12 OpsCenter-specific object identifiers. An object identifier (or OID) is a numeric string that is used to uniquely identify an object.

The following table shows the contents of a trap that is sent from OpsCenter. A total of 14 bindings (or 14 name-value pairs) are present in each trap that is sent from OpsCenter. Each binding associates a particular Management Information Base (MIB) object instance with its current value.

Table 11-1 shows the name-value pairs that the traps pass to the SNMP manager.

Table 11-1 OpsCenter trap binding

Name	Value
1.3.6.1.2.1.1.3.0	This field is the time (in hundredths of a second) between when OpsCenter server service starts and the OpsCenter trap is sent. See Request for Comment (RFC) 1905 and 2576 for a detailed definition. http://www.ietf.org/rfc/rfc1905.txt http://www.ietf.org/rfc/rfc2576.txt Example: 1173792454
1.3.6.1.6.3.1.1.4.1.0	This field is the unique identifier for this trap. See RFC 1905 and RFC 2576 for a detailed definition. http://www.ietf.org/rfc/rfc1905.txt http://www.ietf.org/rfc/rfc2576.txt Example: 1.3.6.1.4.1.1302.3.12.10.2.0.4
1.3.6.1.4.1.1302.3.12.10.1.1 (`iso.org.dod.internet.private.enterprises.products.veritascc.ccTrapDefinitionsBranch.ccTrapVarsBranch.alertRecipients`)	This field is the alert recipient name. Example: Nancy Nieters
1.3.6.1.4.1.1302.3.12.10.1.2 (`iso.org.dod.internet.private.enterprises.products.veritascc.ccTrapDefinitionsBranch.ccTrapVarsBranch.alertSummary`)	This value specifies the alert ID, alert status, and alert summary in the following format: Alert ID (Alert Status) Alert Summary Example: 100 (Active) Job Completed with Exit Status 0
1.3.6.1.4.1.1302.3.12.10.1.3 (`iso.org.dod.internet.private.enterprises.products.veritascc.ccTrapDefinitionsBranch.ccTrapVarsBranch.alertDescription`)	This field is the alert description. Examples for each alert condition are available. See "Alert descriptions in OpsCenter" on page 525.

Table 11-1 OpsCenter trap binding *(continued)*

Name	Value
1.3.6.1.4.1.1302.3.12.10.1.4 (`iso.org.dod.internet.private.enterprises.products.veritascc.ccTrapDefinitionsBranch.ccTrapVarsBranch.policyName`)	This field is the alert policy name.
1.3.6.1.4.1.1302.3.12.10.1.5 (`iso.org.dod.internet.private.enterprises.veritas.products.veritascc.ccTrapDefinitionsBranch.ccTrapVarsBranch.objectType`)	This field is blank and not used.
1.3.6.1.4.1.1302.3.12.10.1.6 (`iso.org.dod.internet.private.enterprises.veritas.products.veritascc.ccTrapDefinitionsBranch.ccTrapVarsBranch.collectorName`)	This field is blank and not used.
1.3.6.1.4.1.1302.3.12.10.1.7 (`iso.org.dod.internet.private.enterprises.veritas.products.veritascc.ccTrapDefinitionsBranch.ccTrapVarsBranch.ccHost`)	This field is the IP address of the OpsCenter server. Example: 10.212.12.148
1.3.6.1.4.1.1302.3.12.10.1.8 (`iso.org.dod.internet.private.enterprises.veritas.products.veritascc.ccTrapDefinitionsBranch.ccTrapVarsBranch.sourceId`)	This field is blank and not used.
1.3.6.1.4.1.1302.3.12.10.1.9 (`iso.org.dod.internet.private.enterprises.veritas.products.veritascc.ccTrapDefinitionsBranch.ccTrapVarsBranch.ccObject`)	This field is blank and not used.
1.3.6.1.4.1.1302.3.12.10.1.10 (`iso.org.dod.internet.private.enterprises.veritas.products.veritascc.ccTrapDefinitionsBranch.ccTrapVarsBranch.sampleData`)	This field is blank and not used.

Table 11-1 OpsCenter trap binding *(continued)*

Name	Value
1.3.6.1.4.1.1302.3.12.10.1.11 (`iso.org.dod.internet.private.enterprises.veritas.products.veritascc.ccTrapDefinitionsBranch.ccTrapVarsBranch.ccAlertSeverity`)	This field shows the alert severity level. Example: Informational
1.3.6.1.4.1.1302.3.12.10.1.12 (`iso.org.dod.internet.private.enterprises.veritas.products.veritascc.ccTrapDefinitionsBranch.ccTrapVarsBranch.ccAlertTime`)	This field shows the time when the alert gets cleared. Example: 13-10-2008 `06:57:34` 00

The first two OIDs listed in the table are standard SNMP OIDs. The other OIDs starting from 1.3.6.1.4.1.1302.3.12.10.1.1 to 1.3.6.1.4.1.1302.3.12.10.1.12 are OpsCenter OIDs. As per SNMPv2c trap definition, the two standard SNMP OIDs must be present as part of every trap.

All the 12 OpsCenter OIDs are defined in the OpsCenter MIB files. However, the two standard OIDs are not defined in the OpsCenter MIB files.

Alert descriptions in OpsCenter

This section shows the content that is sent for each OpsCenter alert as OID 1.3.6.1.4.1.1302.3.12.10.1.3.

In

Note: 1.3.6.1.4.1.1302.3.12.10.1.3 represents iso.org.dod.internet.private.enterprises.products.veritascc.`ccTrapDefinitionsBranch.ccTrapVarsBranch.alertDescription`.

Most of the alert information in OpsCenter is sent as OID 1.3.6.1.4.1.1302.3.12.10.1.3.

Table 11-2 shows the content that each OpsCenter alert sends as OID 1.3.6.1.4.1.1302.3.12.10.1.3.

Table 11-2 Alert conditions in OpsCenter

Alert type	Alert condition	Description (Example)
Job	High job failure rate	Alert Raised on: September 5, 2009 `5:00 PM` Tree Type : Policy Nodes : Root Node % Failed Jobs: 100.0 Alert Policy: high job failure rate policy view OpsCenter Server: ccs-sol-qe-17 Severity: Warning
	Hung job	Alert Raised on: September 7, 2009 `2:21 PM` Job: 25888 Tree Type : Policy Nodes : ccs-win-qe-5 Job Policy: ccsqasol1 Client: ccs-win-qe-5 Alert Policy: Hung Job OpsCenter Server: ccs-sol-qe-17 Severity: Warning
	Job finalized	Alert Raised on: September 9, 2009 `4:54 PM` Job: 26356 Tree Type : Policy Nodes : node1 Job Policy: sample_policy Exit Status: 150 (`termination requested` by administrator) Client: ccs-win-qe-5 New State: Done Alert Policy: Job Finalized OpsCenter Server: ccs-sol-qe-11 Severity: Warning
	Incomplete Job	

Table 11-2 Alert conditions in OpsCenter *(continued)*

Alert type	Alert condition	Description (Example)
		Alert Raised on: September 9, 2009 4:54 PM Job: 26356 Tree Type : Policy Nodes : node1 Job Policy: sample_policy Client: ccs-win-qe-5 Alert Policy: Incomplete Job OpsCenter Server: ccs-sol-qe-11 Severity: Warning

Table 11-2 Alert conditions in OpsCenter *(continued)*

Alert type	Alert condition	Description (Example)
Media	Frozen media	Alert Raised on: August 17, 2009 `12:24 PM` Tree Type : Server Nodes: node1 Frozen Media Name: A00004 Media server : `ranjan` Alert Policy: frozen media policy OpsCenter Server: localhost Severity: Warning
	Suspended media	Alert Raised on: August 12, 2009 `3:36 PM` Suspended Media Name: 0122L2 Tree Type : Server Nodes: node1 Media server : ccs-win-qe-13 Alert Policy: Suspended media policy OpsCenter Server: localhost Severity: Informational
	Exceeded max media mounts	Alert Raised on: August 12, 2009 `3:27 PM` Media Name: A00009 Tree Type : Server Nodes: node1 Media server : ccs-win-qe-13 Number of mounts: 3402 Alert Policy: Exceeded Max Media Mounts policy OpsCenter Server: localhost Severity: Critical
	Media required for restore	

Table 11-2 Alert conditions in OpsCenter *(continued)*

Alert type	Alert condition	Description (Example)
		Alert Raised on: December 4, 2008 `4:39 PM` Tree Type : Server Nodes: node1 Media: 000_00000_TL4 Required for restore Master server: omwin12(omwin12) Client: omwin12 Media server: `macy` Restore Job ID: 615 Alert Policy: Media Required for Restore_root OpsCenter Server: ccs-sol-qe-10 Severity: Warning
	Low available media	Alert Raised on: September 13, 2012 `4:53 PM` Tree Type: Server Tree Name : ALL MASTER SERVERS Nodes: omhp5 Available Media: 0 Alert Policy: Low Available Media OpsCenter Server: ccs-sol-qe-12 Severity: Informational
	High suspended media	Alert Raised on: August 12, 2009 `11:40 AM` Tree Type : Server Nodes: node1 Suspended Media: 1 % Suspended Media: 25.0 Alert Policy: high percentage suspended media OpsCenter Server: localhost Severity: Warning
	High frozen media	

Table 11-2 Alert conditions in OpsCenter *(continued)*

Alert type	Alert condition	Description (Example)
		Alert Raised on: December 8, 2008 `10:24 AM` Tree Type : Server Nodes: node1 Frozen media: 6 % Frozen Media: 66 Alert Policy: `highfrozenmedia` OpsCenter Server: winfor11 Severity: Warning

Table 11-2 Alert conditions in OpsCenter *(continued)*

Alert type	Alert condition	Description (Example)
Catalog	Catalog Space low	Alert Raised on: December 8, 2008 `10:08 AM` Master server : sargam(sargam) Tree Type : Server Nodes: node1 Available Catalog Space: 6480880 KB Threshold Catalog Space: 102400 TB Alert Policy: test_catalogspacelow OpsCenter Server: winfor11 Severity: Warning
	Catalog not Backed up	Alert Raised on: September 7, 2009 `9:54 AM` Tree Type : Server Nodes : ccs-sol-qe-13 Threshold: 10 Minute(s) Last Catalog `BackUp` Time: September 6, 2009 `5:21 PM` Alert Policy: Catalog not Backed up OpsCenter Server: ccs-sol-qe-17 Severity: Warning
	Catalog Backup Disabled	Alert Raised on: September 5, 2009 `3:44 PM` Tree Type : Server Nodes : ccs-win-qe-1 Alert Policy: Catalog Backup Disabled OpsCenter Server: ccs-sol-qe-17 Severity: Warning

Table 11-2 Alert conditions in OpsCenter *(continued)*

Alert type	Alert condition	Description (Example)
Tape	Mount Request	Alert Raised on: September 7, 2009 `6:52 PM` Tree Type : Server Nodes : ccs-win-qe-1 Barcode: 000014 Density: `dlt` `evsn`: 000014 Mode: 82 Request ID: 120 `rvsn`: 000014 User: - Volume Group: 000_00000_TLD Request Time: February 4, 1991 `12:56 AM` Alert Policy: Mount Request OpsCenter Server: ccs-sol-qe-12 Severity: Warning
	No Cleaning Tape	Alert Raised on: August 17, 2009 `12:30 PM` Tree Type : Server Nodes : ccs-win-qe-1 Media server : `ranjan` Robot Number: 0 Alert Policy: no cleaning tape left OpsCenter Server: localhost Severity: Warning
	Zero Cleaning Left	

Table 11-2 Alert conditions in OpsCenter *(continued)*

Alert type	Alert condition	Description (Example)
		Alert Raised on: December 13, 2008 `12:02 PM` Tree Type : Server Nodes : ccs-win-qe-1 Master server : ORLP-SPEECH01 Media server : ORLP-SPEECH01 Robot Number: 0 Cleaning Tape: CLN084 Alert Policy: test_zerocleaningleft_public OpsCenter Server: winfor11 Severity: Warning

Table 11-2 Alert conditions in OpsCenter *(continued)*

Alert type	Alert condition	Description (Example)
Disk	Disk Pool Full	Alert Raised on: August 20, 2009 `5:25 PM` Tree Type : Server Nodes : ccs-win-qe-1 Disk Pool ID: SSOD_Pool Disk Pool Name: SSOD_Pool Total Capacity: 1007664128 KB Used Capacity: 1005702144 KB Alert Policy: Disk Pool Full OpsCenter Server: localhost Severity: Informational
	Disk Volume Down	Alert Raised on: August 17, 2009 `5:08 PM` Tree Type : Server Nodes : ccs-win-qe-1 Disk Volume ID: /vol/luns/nbusd_sun10 Disk Pool ID: SSOD_Pool Alert Policy: disk volume down `pol` OpsCenter Server: localhost Severity: Informational
	Low Disk Volume Capacity	Alert Raised on: August 26, 2009 `10:35 AM` Tree Type : Server Nodes : ccs-win-qe-1 Disk Volume Free Capacity: 106 MB Threshold: 20 % OpsCenter Server: localhost Severity: Major
	Drive is Down	

Table 11-2 Alert conditions in OpsCenter *(continued)*

Alert type	Alert condition	Description (Example)
		Alert Raised on: August 12, 2009 `10:39 AM` Tree Type : Server Nodes : ccs-win-qe-1 Media server : omlinux2 Drive Name: BNCHMARK.VS640.000 Drive Number: 1 Robot Number: 0 Alert Policy: drive down-individual alert Device Path: /dev/nst0 OpsCenter Server: localhost Severity: Critical
	High Down Drives	Alert Raised on: August 12, 2009 `3:13 PM` Tree Type : Server Nodes : ccs-win-qe-1 Drive Number: 1 % Down Drive Paths: 100.0 Alert Policy: high down drives OpsCenter Server: localhost Severity: Major

Table 11-2 Alert conditions in OpsCenter *(continued)*

Alert type	Alert condition	Description (Example)
Host	Agent Server Communication Break	Agent `Host Name` : `pinacolada` Server `Host Name` : PINACOLADA Severity: Warning
	Master Server Unreachable	Alert Raised on: October 23, 2009 `12:20 AM` Alert Policy: `MasterServer` Unreachable OpsCenter Server: CCSQAWINSP1 Severity: Major
	Lost Contact with Media Server	Alert Raised on: February 18, 2008 `1:33 PM` Master server : pmsun22 Media server : pmsun22 Alert Policy: `lcm` OpsCenter Server: pmwin9 Severity: Warning
	Appliance Hardware Failure	

Table 11-2 Alert conditions in OpsCenter *(continued)*

Alert type	Alert condition	Description (Example)
Others	Service Stopped	Alert Raised on: August 31, 2009 `5:59 PM` Tree Type : Server Nodes : ccs-win-qe-1 Media server : omlinux2 Process Name: `nbkms` Alert Policy: Service stopped OpsCenter Server: ccs-sol-qe-14 Severity: Major
	Job Policy Change	Alert Raised on: September 7, 2009 `12:29 PM` Tree Type : Server Nodes : ccs-win-qe-5 Changed Policy Name: BMRPolicy Alert Policy: `job policy_change` OpsCenter Server: ccs-sol-qe-17 Modified Policy Attributes : Severity: Warning

Configuring the SNMP trap community name for OpsCenter

For OpsCenter traps, the SNMP trap community name is `OpsCenter` (by default). Veritas NetBackup OpsCenter uses a public community named OpsCenter. Public community implies a read-only access to SNMP traps.

Use the following procedures to configure the SNMP trap community name on Windows and UNIX.

To configure the SNMP trap community name for OpsCenter traps on Windows

1. On the OpsCenter server host, stop all the OpsCenter server services.

   ```
   INSTALL_PATH\OpsCenter\server\bin\opsadmin.bat stop
   ```

2. Navigate to `INSTALL_PATH\OpsCenter\server\config` directory and open the `nm.conf` file.

   The file shows the following entry:

   ```
   nm.trapCommunity=OpsCenter
   ```

   Modify the value of `nm.trapCommunity` from OpsCenter to some other name.

3. Save the `nm.conf` file after making the changes.

4. Restart all OpsCenter services.

   ```
   INSTALL_PATH\OpsCenter\server\bin\opsadmin.bat start
   ```

To configure the SNMP trap community name for OpsCenter traps on UNIX

1. On the OpsCenter server host, stop all the OpsCenter services.

   ```
   <INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh stop
   ```

2. Navigate to `<INSTALL_PATH>/SYMCOpsCenterServer/config` directory and open the `nm.conf` file.

   The file shows the following entry:

   ```
   nm.trapCommunity=OpsCenter
   ```

   Modify the value of `nm.trapCommunity` from OpsCenter to some other name.

3. Save the `nm.conf` file after making the changes.

4. Restart all OpsCenter services.

   ```
   <INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh start
   ```

Configuring the SNMP version for sending SNMP traps

The default SNMP version through which SNMP traps are sent in OpsCenter is SNMPv2c. However, this SNMP version can be changed by modifying a configuration file.

The following procedure explains how to configure the default SNMP version on Windows and UNIX.

To configure the SNMP version for sending SNMP traps on Windows

1. On the OpsCenter server host, stop all the OpsCenter services.

   ```
   INSTALL_PATH\server\bin\opsadmin.bat stop
   ```

2. Navigate to `INSTALL_PATH\OpsCenter\server\config directory` and open the `nm.conf` file.

   The file shows the following entry:

   ```
   nm.trapVersion=v2c
   ```

   Modify the value of `nm.trapVersion` from v2c to v1 (for SNMPv1) or v3 (for SNMPv3).

3. Save the `nm.conf` file after making the changes.

4. Restart all OpsCenter services:

   ```
   INSTALL_PATH\OpsCenter\server\bin\opsadmin.bat start
   ```

To configure the SNMP version for sending SNMP traps on UNIX

1. On the OpsCenter server host, stop all the OpsCenter services:

   ```
   <INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh stop
   ```

2. Navigate to the OpsCenter configuration directory:

   ```
   cd <INSTALL_PATH>/SYMCOpsCenterServer/config
   ```

3. Open the `nm.conf` file. The file shows the following entry:

   nm.trapVersion="v2c"

   Modify the value of `nm.trapVersion` from v2c to v1 (for SNMPv1) or v3 (for SNMPv3).

4. Save the `nm.conf` file after making the changes.

5. Restart all OpsCenter services:

   ```
   <INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh start
   ```

About customizing Alert Manager settings

You can customize a few Alert Manager settings using the `am.conf` configuration file.

The `am.conf` configuration file is located at the following default location:

Windows	`<INSTALL_DIR>\config\am.conf`

The Alert Manager configuration settings are described as follows:

Note: By default all Alert Manager configuration parameters are set to “true”.

`am.autoClear`	Set this parameter to “true”, if you want the Alert Manager to automatically clear the alerts that are generated in OpsCenter.
`am.notifyOnAutoClear`	Make sure that the `am.autoClear` parameter is set to “true”, to apply the change in the `am.notifyOnAutoClear` parameter setting on the Alert Manager functionality. Set this parameter to “true”, if you want to send notification after an alert was automatically cleared.
`am.notifyOnManualClear`	Set this parameter to “true”, if you want to send notifications after manually clearing alerts.

Note: If you set an Alert Manager configuration parameter to a value other than “true” or “false”, OpsCenter assumes it as “false”.

Frequently asked SNMP and OpsCenter questions

Question	Answer
What are the default versions of SNMP that are supported in OpsCenter?	SNMPv1, SNMPv2c, and SNMPv3.
What is SNMPv2c? How it is different from SNMPv2?	See “About SNMP versions” on page 521.
Is the OpsCenter SNMP community name configurable?	Yes. See “Configuring the SNMP trap community name for OpsCenter” on page 537.

Question	Answer
How is the OpsCenter community related to the public community?	The "OpsCenter" community used by OpsCenter is public, but the community name is maintained as "OpsCenter".
Is the default community name of "OpsCenter" just a name for the community, but still considered public because of certain attributes?	Generally, the "default read community string" for the public community is "public". Public community means read-only access to SNMP traps.

About managing OpsCenter alerts using Microsoft System Center Operations Manager 2007

Microsoft System Center Operations Manager 2007 (SCOM), formerly Microsoft Operations Manager (MOM), is a next-generation performance and event-monitoring product from Microsoft. Microsoft System Center Operations Manager Management Pack for NetBackup lets you monitor and manage NetBackup alerts using Microsoft System Center Operations Manager 2007 (SCOM 2007). By detecting and alerting you on critical conditions, this Management Pack helps prevent possible service outages.

The SCOM Management Pack for NetBackup and the documentation is available for download on the Veritas Support Web site.

http://www.veritas.com/docs/000008818

About managing OpsCenter alerts using HP OpenView Network Node Manager 7.50/7.51 on Windows

You can monitor and manage NetBackup alerts using HP OpenView Network Node Manager 7.50 or 7.51 on Windows. By detecting and alerting you on critical conditions, HP OpenView Network Node Manager (NNM) can help you to prevent possible service outages.

You can download and use the `nom_trapd.conf` file to monitor and manage NetBackup alerts using HP OpenView Network Node Manager 7.50 or 7.51. By using `nom_trapd.conf` file and configuring NNM and OpsCenter, NNM can receive the SNMP traps that have been configured in OpsCenter. As a result, NNM can be used for the centralized management of NetBackup alerts.

Note: The term HP OpenView Network Node Manager (NNM) in this section refers specifically to HP OpenView Network Node Manager 7.50 or 7.51.

`nom_trapd.conf` file and the documentation is available for download on the support site.

https://www.veritas.com/support/en_US/article.100041202

More information about OpsCenter alerts is available.

See "OpsCenter Alert conditions" on page 420.

Chapter 12

Reporting in OpsCenter

This chapter includes the following topics:

- About OpsCenter reports
- Report Templates in OpsCenter
- About managing reports in OpsCenter
- Creating a custom report in OpsCenter
- Creating an OpsCenter report using SQL query
- About managing My Reports
- About managing My Dashboard
- About managing reports folders in OpsCenter
- Using report schedules in OpsCenter
- Reports > Schedules options
- About managing report schedules in OpsCenter
- About managing time schedules in OpsCenter

About OpsCenter reports

OpsCenter is a web-based software application that helps organizations by providing visibility into their data protection environment. By using OpsCenter, you can track the effectiveness of data backup and archive operations by generating comprehensive business-level reports.

OpsCenter displays customizable, multi-level views of backup and archive resources and customizable reports for tracking service usage and expenditures. It also

contains tools for defining cost metrics and chargeback formulas or handling alerts. A wide range of audiences benefit from the reporting and the management capabilities of OpsCenter. The audiences include IT (Information Technology) managers, application owners, IT finance teams, external compliance auditors, legal teams, line-of-business managers, external customers, IT architects, and capacity planning teams.

OpsCenter reporting user interface

The OpsCenter reporting user interface consists of the following components:

Report Templates tab

This tab lists all **Report Templates** (or standard or canned reports) that are available in OpsCenter. You can modify the default parameter values of a **Report Template** as required and generate a new report of that kind.

For example, use the existing **Backup > Job Activity > Client Count Report Template**, change the relative timeframe to four weeks (default timeframe is two weeks) and generate a new Client Count report. You can see all clients that are backed up over the last four weeks.

My Reports tab

You can save generated reports for your future use. These saved reports are stored in the **My Reports** tab. Use this section to view the saved reports or modify the parameters of the saved reports and generate new reports out of them. You can also delete the saved reports using the **My Reports** tab.

See "About managing My Reports" on page 575.

See "Saving an OpsCenter report" on page 554.

My Dashboard tab

Your saved reports are preserved in **My Reports** tab, which you can select and publish on **My Dashboard** tab. You can select multiple reports and add them in the same dashboard section. Thus, you can create multiple dashboard section containing a number of reports.

See "About managing My Dashboard" on page 578.

Schedules tab

This tab contains all report schedules.

You can create, edit, or delete schedules using this tab.

See "Using report schedules in OpsCenter" on page 582.

Manage Folders tab

Use this tab to manage folders where you have saved your reports.

See "About managing reports folders in OpsCenter" on page 580.

Report creation wizards in OpsCenter

OpsCenter provides wizards, which guide you through the entire report creation procedure.

To create a report, in the OpsCenter console on the **Reports** tab, click **Create New Report**. The following report creation options are available on the **Select Report Creation Option** panel:

- Create a report using an existing Report Template .
  See "Creating an OpsCenter report using a Report Template" on page 550.
- Create a custom report.
  See "Creating a custom report in OpsCenter" on page 559.
- Create a report using SQL Query.
  See "Creating an OpsCenter report using SQL query" on page 573.

Reports > Report Templates

This section provides details of the Report Templates that are available in OpsCenter.

OpsCenter provides a number of Report Templates (or standard or canned reports) that you can modify and generate a new report of that kind.

In the OpsCenter console, when you click the **Reports** tab, the **Report Templates** home page is displayed.

From the Reports > Report Templates page, you can click any of the **Report Templates** to view the respective report with default parameter values.

You can also click the following options on the **Reports > Report Templates** page:

Create New Report

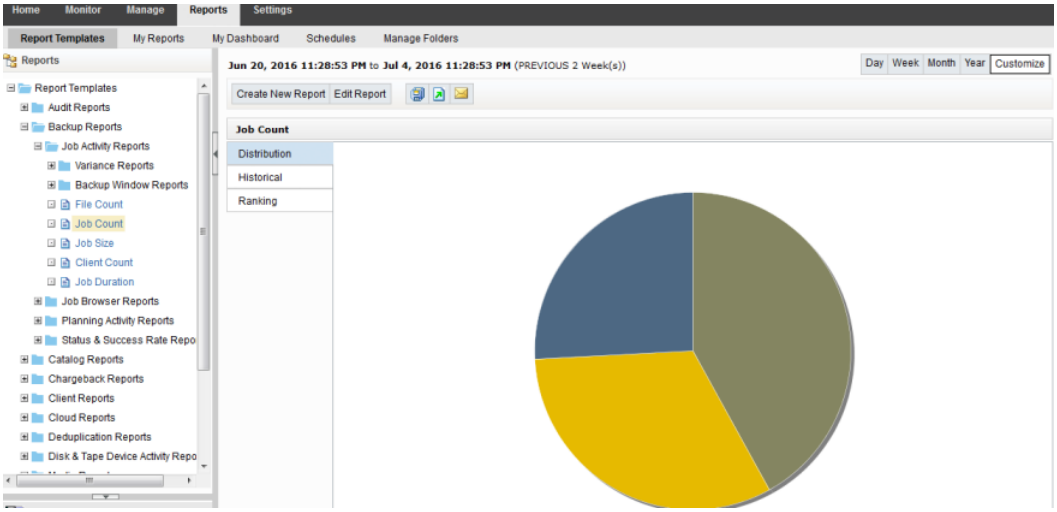
Click **Create New Report** to create a standard report, custom report, or run an SQL query.

Edit Report

If you do not want to run a report template with default parameter values, you can directly edit it from **Reports > Report Templates** page. To edit a report template, first select the report template by selecting the checkbox on the extreme left of the report template. Click **Edit Report** to edit and save the report without executing it.

Figure 12-1 shows various components of a report that is generated using a template.

Figure 12-1 Report Template



Report Templates tree	This tree lists all Report Templates that are available in OpsCenter.
Manage report toolbar	Use this toolbar to save, export, or email the generated report.
Time filters	Use these time filters to view the data for a specific period of time:
Report area	OpsCenter reports are displayed here.
Report views	Reports can be viewed in different forms or views, **Distribution**, **Historical**, or **Ranking**. Use these options to change the current report view. These options are available only for chart-based reports.

About custom reports in OpsCenter Analytics

Apart from generating reports using the existing templates, you can also create custom reports in OpsCenter by changing the report parameters as required.

See "Creating a custom report in OpsCenter" on page 559.

About custom SQL query in OpsCenter Analytics

In OpsCenter, you can create reports by directly running SQL queries. Using this report creation option, you do not need to go through multiple parameter selections.

OpsCenter provides detailed information about the OpsCenter database schema that you may want to know before running any SQL query to generate reports. On the Report Wizard > SQL Query page, click the OpsCenter Schema Document link to open the PDF that contains all relevant information.

Note: You can create only tabular reports by running SQL queries. You can also run stored procedures using this feature.

See "About supporting OpsCenter custom reports and custom SQL queries" on page 547.

See "Creating an OpsCenter report using SQL query" on page 573.

About supporting OpsCenter custom reports and custom SQL queries

Veritas is committed to product quality and will support the accuracy and validity of the data collected and stored in the OpsCenter database and the documentation of the OpsCenter database schema. However, no Technical Support will be provided on the actual creation of custom reports, custom SQL queries for specific reports, or for 3rd party reporting applications (for example, Microsoft Excel, Access, or Crystal Reports).

See "About custom reports in OpsCenter Analytics" on page 546.

See "About custom SQL query in OpsCenter Analytics" on page 547.

Report Templates in OpsCenter

OpsCenter provides a set of Report Templates or standard or canned reports that have parameters set to default values. You can modify the default parameters and generate reports to view the required data. OpsCenter reports help you to have a good visibility into your data protection environment.

See "Reports > Report Templates" on page 545.

Report Templates are categorized as follows:

Backup Reports	The backup reports show the information that is related to backups, such as success rate, job status, and protected bytes. This category also includes recovery reports. **Note:** If you select **Reports > Activity Planning > Job Size** in the OpsCenter user interface, the report that appears displays the wrong client name. Instead of showing the client names, a list of backed up VM images is displayed in this report. In addition, the list of VM images may not be accurate.
Catalog Reports	These reports provide details about the catalogs.
Chargeback Reports	The chargeback reports provide details of the backup services expenditures. Using these reports you can track the backup and the recovery usage and the associated cost. You can calculate the cost of data protection management and chargeback to customers and business units.
Client Reports	These reports provide details about clients such as backup status, restore job details, or summary dashboard.
Cloud Reports	These reports provide details about NetBackup cloud storage servers. The following cloud providers are supported by OpsCenter: ■ Amazon S3 ■ AT&T ■ Rackspace **Note:** Among all Amazon S3-compatible cloud providers that NetBackup supports, OpsCenter can monitor and generate reports for Amazon S3 only.
Disk & Tape Device Activity Reports	Disk-based data protection (DBDP) reports show disk pool capacity and its usage, performance of clients on LAN or SAN, NetBackup storage lifecycle Map

Media Reports	These reports provide media data, such as tape count or usage.
Performance Reports	These reports provide details of throughput.
Policy Reports	These reports show all details about the backup job policies in NetBackup.
Restore Reports	These reports provide details about restore operation.
Storage Lifecycle Policy	The SLP reports in OpsCenter show an end-to-end view of the SLP process that includes backup to import of duplicated image into different NetBackup domains. The SLP reports help you to verify if each step in the SLP is executed and identify the possible bottlenecks.
Workload Analyzer	The Workload Analyzer report gives information about the activities that are done across a period of seven days. The activities are number of jobs running at a given period of time and the amount of data that is transferred during this period. The report contains 168 data points of analysis in terms of the activities that are done for each hour for a period of seven days.

About report filters in OpsCenter

There can be hundreds of records or thousands of MB of the data that you may not be concerned about. For example, you want to view only those jobs that were successful. To view this specific data, you need to use the ‘status’ filter. By setting this filter to **Successful** while generating the Job Count report, you can view all jobs that were successful.

OpsCenter provides a number of filters that you can use to view the required data. For each report category there is a different set of filters.

Note the following considerations with respect to using the report filters:

- If you edit certain standard reports and select **Backup from Snapshot** Job type from the **Filters** section, incorrect data is shown if data for Backup from Snapshot jobs exists. This also happens when you create image-related reports via custom reporting and apply **Backup from Snapshot** job type filter.

  The following standard reports display incorrect data when you select **Backup from Snapshot** job type from the **Filters** section:

- Backup > Planning Activity > Stored Backup Images > Duplicate copies
- Backup > Planning Activity > Stored Backup Images > Stored Backup Images on Media
- Backup > Planning Activity > Stored Backup Images > Valid Backup Images
- Backup > Planning Activity > Capacity Planning > Forecasted Size
- Backup > Planning Activity > Capacity Planning > Historical Size

- The Backup Media Role filter when applied to the Tapes Expiring In Future and Tapes Expiring Now reports does not return any data as data is miscalculated in OpsCenter.

Creating an OpsCenter report using a Report Template

This section provides the procedure to create a report using an existing Report Template .

To create a report using an existing Report Template

1. In the OpsCenter console, click **Reports**.
2. On the **Report Template** tab, click **Create New Report**.

   To view a report output of a template, select a template in the reports tree. The report output is as per the default parameter values. You cannot modify any of the report parameters.

   By clicking the **Create New Report** option, you can launch the report creation wizard that guides you through the entire report creation procedure. Here you can modify the report parameters and view the required data.
3. In the Report Wizard, retain the default selection **Create a report using an existing Report Template** and click **Next**.
4. On the **Report Templates** list, expand a report category to see the Report Templates within it. Select the Report Template that you want to create a report from.

   Click **Next**.
5. Select time frame and other filters as required and click **Next**.
6. Modify display options and click **Next**.

Using report formats

The following formats are available for standard reports in OpsCenter.

About report formats

Report formats are described as follows:

Rankings reports	Display a horizontal bar graph showing all the data for each view level object, from greatest to least, within the selected time frame.
Distribution reports	Display a pie chart showing all the data for each view level object within the selected time frame.
Historical reports	Display a stacked (segmented) bar graph with a trend line superimposed over it, showing the average upward and downward trends of the data over time. For example the total size of each day's backup jobs broken out by geography. Some backup reports use a different bar chart format, displaying clustered columns for easy comparison between two classes of objects or events
Tabular reports	Display backup data in a table

About viewing data in a graphical report

Graphical reports present data in a convenient, 'at a glance' fashion. However, some precision may be lost when you use this format. When you are viewing a graphical report, tool tips are available to provide the precise numerical data. To view the numerical data on which a graphical report is based, move your mouse pointer over an area of the graph.

You can also click **Show Chart as Table** at the bottom of the report to view the data in a tabular format.

When you are viewing a backup report, you can easily view lower-level reports. On a graphical report, when you click an area within a graph, the report refreshes to display data for the next lowest object level.

For example, in a Geography view, you can click a bar labeled Canada to display a bar chart showing data for Toronto and Vancouver. You can select the bar for a host to display data for the host's file systems.

About managing reports in OpsCenter

This section provides information on the operations that you can carry out on the standard reports that you generate in OpsCenter.

You can carry out the following operations:

- Saving a report
  See "Saving an OpsCenter report" on page 554.

- Exporting a report
  See "Exporting an OpsCenter report" on page 554.
- Emailing a report
  See "Emailing a report in OpsCenter" on page 556.

Save report and email report dialog boxes

A description of the **Save report** and **Email report** dialog box options follows in the table.

Table 12-1 Save report dialog box options

Option	Description
Report name	Enter the report name. For example, if you generated the Job Count standard report with the group by option that is selected as **Policy Type** and report view as **Historical**, you can name this report NumberofJobsbyPolicies. When you select this report on the **Saved Reports** tab, the report is displayed with the saved filters and in the report view that were selected when the reports were saved, with respect to the current time. Review the following points about report names: ■ The report name must be unique in the folder where you create it. For example, if you create a report in the **Private Reports** folder under **My Reports**, the report name that you specify must be unique in the Private Reports folder. The same user can have two reports with the same name - like one in **Public Reports** and one in **Private Reports** folder. ■ The report name must not contain any special characters like (/ \ * ? | ") ■ The report name must not be more than 220 characters.
Description	Enter the short description for the report.
Folder	Select **Public** or **Private** folder. If you save the report in a public folder, all other OpsCenter users can view it. If you save the report in a private folder, only you can view it. Expand the **Public** or **Private** folder and select a folder where you want to save the report. Depending on the folder type that you have selected - public or private - the folders displayed for selection vary.

Table 12-1 Save report dialog box options *(continued)*

Option	Description
Create New	Click this option to create a new public or private folder. Clicking this option changes the view of Folder. Enter the folder name and click **OK**. This folder is made available in the Folder tree for selection. Select this newly created folder where you want to save the report.
Overwrite if report already exists in the selected folder	Select this check box if you want to overwrite the existing report with the same name in the same folder. If you do not select this check box and save a report with a name identical to any of the existing reports in the selected folder, a confirmation message is displayed before you overwrite the existing report.

Table 12-2 Email report dialog box options

Option	Description
Select Format	Select one of the following formats: ■ PDF ■ HTML ■ CSV ■ TSV ■ XML **Note:** Some of these formats may not be available for specific reports. For example, the Drive Throughput and Drive Utilization reports can be exported and emailed only in the HTML format.
Select Content	Select one of the following report formats: ■ Distribution ■ Historical ■ Ranking ■ Tabular Distribution, Historical, and Ranking formats are available only for chart-based reports.
Email	Enter appropriate email details like address, subject, and message.

Saving an OpsCenter report

You can save a standard report. This action saves the filters that you have selected while generating a report. You can use this set of filters to regenerate the reports with the current time selections.

These reports are saved in the OpsCenter database, which you can view using the **My Reports** tab.

You cannot save a report whose name contains any special characters like (/ \ * ? | ").

See "About managing My Reports" on page 575.

To save a report

1. In the OpsCenter console, click **Reports > Report Templates**.
2. From the **Reports** tree, select the report template that you want to save.
3. In the right-hand report view area, click the **Save As Report** icon. The **Save Report** pop-up screen opens.
4. On the **Save Report** screen, enter the required details.

   See "Save report and email report dialog boxes" on page 552.
5. Click **OK**.

   After a successful save, **My Reports** tab is displayed with this report selected.

Note: You cannot save a report name that contains special characters like (/ \ * ? | ")

Exporting an OpsCenter report

Using OpsCenter, you can preserve report data in files or print the data.

See " File formats available in OpsCenter" on page 555.

You can open the exported file using other applications, such as a spreadsheet program or a text editor.

To export a report

1. In the OpsCenter console, click **Reports > Report Templates**.

   You can also export reports that you may have created from **Reports > My Reports**.
2. From the **Reports** tree, select the report template or report that you want to export.

3. In the report view area at the right-hand side, click the **Export Report** icon. The **Export Report** pop-up screen opens.
4. On the **Export Report** pop-up screen, select the export options that you want to export the report with: File format, such as PDF, HTML, CSV, TSV, or XML and content or report view, such as **Tabular**, **Distribution**, **Historical**, or **Ranking**.

   Note that only the applicable formats and report views appear for specific reports.

   See "Save report and email report dialog boxes" on page 552.
5. Click **OK**. The system displays the export options pertaining to the file format you have selected. Select those options and export the report.

File formats available in OpsCenter

You can export or email OpsCenter reports in the following file formats:

PDF (Portable Document Format)	Can be viewed using a PDF reader, such as Adobe Reader
CSV (comma-separated values)	Use with spreadsheet programs, such as Microsoft Excel.
TSV (tab-separated values)	Compatible with word-processing applications and text editors
HTML (hypertext markup language)	Can be opened using with Web browsers
XML (Extensible Markup Language)	Can be imported (using user-written scripts) by other programs like databases or billing applications.

The following is the XML format:

```
<Report>
  <ReportView>
    <Name> {nameValue} </Name>
    <Description> {descriptionForReportView} </Description>
    <TimeDuration> {timeValue} </TimeDuration>

    <ViewName> {viewNameValue} </ViewName>
    <ViewSelections>
      <SelectedItem value="{selectedNodeNameValue1}">
        <ExcludedItem> {excludedNodeName1} </ExcludedItem>
```

```
        <ExcludedItem> {excludedNodeName2} </ExcludedItem>
        ...
      </SelectedItem>

      <SelectedItem value="{selectedNodeNameValue2}">
        <ExcludedItem> {excludedNodeName3} </ExcludedItem>
        <ExcludedItem> {excludedNodeName4} </ExcludedItem>
        ...
      </SelectedItem>
    </ViewSelections>
    <Table>
      <Header>
                    <Row>…</Row>
                </Header>
                <Rows>
                    <Row>…</Row> …
                </Rows>
    </Table>
  </ReportView>

  <ReportView>

</Report>
```

In the new format <Table> has been moved under a new tag called <ReportView>. If multiple views (distribution, historical, ranking) are selected for export or email, each of the views will have one <ReportView> tag corresponding to it. Name, Description and TimeDuration tags inside ReportView tag will always be present for each view. However, ViewName, GroupBy, and ViewSelections tags will be present only if applicable. If report is edited and view selections are changed, these tags will be added in export.

Emailing a report in OpsCenter

Using OpsCenter, you can email report data to the selected recipients. You can email a report in a number of different file formats.

See " File formats available in OpsCenter" on page 555.

To email a report

1. In the OpsCenter console, click **Reports > Report Templates**.

   You can also export reports that you may have created from **Reports > My Reports**.

2. From the **Reports** tree, select the report template or the report that you want to email.

3. In the report view area at the right-hand side, click the **Email Report** icon. The **Email Report** pop-up screen opens.

   See "Save report and email report dialog boxes" on page 552.

4. On the **Email Report** pop-up screen, select the email options: File format, such as PDF, HTML, CSV, TSV, or XML and content or report view, such as **Tabular**, **Distribution**, **Historical**, or **Ranking**

   Note that only the applicable formats and report views appear for specific reports.

5. Enter email IDs in **To**, **Cc**, and **Bcc** text boxes, to which you want to send emails.

   If these email IDs do not already exist, they are automatically added to the database.

   Alternatively, you can add existing email recipients.

   See "Adding email recipients to an OpsCenter report mailing" on page 559.

6. Enter the subject of the email.

7. Enter the message that may be a short description regarding the report data that you want to email.

8. Click **OK**.

Configuring number of rows in a tabular report for email or export

When you export, email, or schedule a tabular report, 4000 rows are exported by default.

You can configure the maximum number of rows in a tabular report that you can export or email.

To configure the maximum number of rows for export

1. Log on to the OpsCenter Server.
2. Stop all the OpsCenter Server services or processes by using the following commands on Windows and UNIX:

Windows	INSTALL_PATH\OpsCenter\server\bin\opsadmin.bat stop
UNIX	<INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh stop

3. Navigate to the following location:

Windows	C:\Program Files\Symantec\OpsCenter\server\config
UNIX	<INSTALL_PATH>/SYMCOpsCenterServer/config

4. Open the `report.conf` file.
5. You may want to export all the rows or you may want to increase or decrease the maximum value. Note that if you export all rows or increase the number of rows, exporting a report may take time when there are a large number of rows.
   - To export all the rows, you can either comment out `report.schedule.max.tabular.rows` parameter or specify any value less than or equal to -1 for `report.schedule.max.tabular.rows` parameter.

     To comment out `report.schedule.max.tabular.rows` parameter, add two forward slashes before the parameter in this manner:

     `//report.schedule.max.tabular.rows=4000`

     or

     Edit the value 4000 in `report.schedule.max.tabular.rows=4000` to -1.

     `report.schedule.max.tabular.rows=-1`
   - To change the maximum number of rows to say 5000, you can set the value of `report.schedule.max.tabular.rows` as 5000.

     Configure report.schedule.max.tabular.rows=5000
6. Start all OpsCenter Server services or processes by using the following command for Windows and UNIX:

Windows	INSTALL_PATH\OpsCenter\server\bin\opsadmin.bat start
UNIX	<INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh start

Adding email recipients to an OpsCenter report mailing

This section provides information on how to add email recipients to whom you want to send emails. This procedure assumes you've already started the email report procedure. More information is available about this procedure.

See "Emailing a report in OpsCenter" on page 556.

To add email recipients

1. On the **Add Email Recipients** screen, select the check boxes in front of the email recipients to whom you want to send emails.

   See "Add email recipients dialog box options" on page 559.

   Click **To..**, **Cc..**, or **Bcc..** depending on where you want to add the selected recipients.

2. Click **OK**.

Add email recipients dialog box options

Table 12-3 Add email recipients dialog box options

Option	Description
Recipient Name/Email Address	Select the check boxes in front of the email recipients to whom you want to send emails.
To.../Cc.../Bcc...	Click **To..**, **Cc..**, or **Bcc..** depending on where you want to add the selected recipients.

Creating a custom report in OpsCenter

In addition to using the reports that come by default with OpsCenter, you can use the Custom Report Wizard to create custom reports that are unique to your installation.

After creating a custom report, you can modify the report, print, save, and email it.

As you work with different report categories, the Report Wizard displays different parameters. Many of the parameters are used for multiple report categories, and they appear in different combinations for each type.

You can create a custom report by using the parameters that are available in the Custom Report Wizard.

See "About Custom Report Wizard parameters" on page 566.

To create a custom report

1. In the OpsCenter console, click **Reports > Report Templates**.
2. Click **Create New Report**.
3. On the **Select Report Creation Option** page, click **Create a Custom Report** to start the Custom Report Wizard.
4. Select a report category from the **Category** drop-down list:

Agent	Select this category if you want to know about the configured Agents on the OpsCenter Server.
Backup/Recovery	Select this category to create reports on jobs, disk pool, logs, image, media, tape drive etc.

5 The Subcategories appear as per what you select from the Category drop-down list. From the Subcategory drop-down list, select one of the following report subcategories:

The following subcategory appears when you select **Agent** as the main category:

Agent Status	Select to view information specific to the Agent. For example, you can create a report that shows the configured Agents on the OpsCenter Server and the Agent status.

The following subcategories appear when you select Backup/Recovery as the main category:

Disk Pool	Select to view a consolidated report related to disk pool.
Job/Image/Media/Disk	Select to view job, image, media, or disk data. The reports based on this subcategory provide a consolidated view of job, image, media, and disk. For example, you can create a custom report that tells the number of images per job type or a tabular report that tells which image is backed up on which media. You can also view the backups that are taken on the disk.
Log	Select to view logs that are generated as a result of backup and recovery activity in NetBackup and Backup Exec.
Media	Select to view reports on media like tape media etc.
Tape Drive	Select to view reports on tape drives. This subcategory does not show reports related to media servers.The associated filter parameters, such as Tape Drive Device Host or Tape Drive Type appear.
Scheduled Jobs	Generate reports on Scheduled Jobs using this category. For example you can create a report that compares the scheduled time and the actual time for scheduled jobs.

6 Select a report format from the following formats in the **View Type** drop-down list:

Distribution	Display groupings or objects or resources in a pie chart.
Ranking	Display a horizontal bar graph showing all the data for each view level object, from greatest to the least, within the selected time frame.
Historical	Display a stacked (segmented) bar graph with a trendline superimposed over it showing the average upward and downward trends of the data over time.
Tabular	Display data in the form of a table.

7 Click **Next**.

8 In the **Select Parameters** panel of the Custom Report Wizard, select values for one or more report parameters. The report parameters that appear depend on the report category and the view type that you selected.

See "Configuring timeframe parameters" on page 566.

See "About Custom Report Wizard parameters" on page 566.

As you select parameters, the Content pane may refresh to display additional selections. For example, when you select a view filter, you are then given a choice of items on which to filter the report display.

9 Click **Next**.

10 In the **Modify Display Options** panel, define the measurements to be collected for historical, ranking, tabular, and distribution reports. Different display options are displayed for different view types.

See "About display options" on page 569.

Click **Next**.

11 In the **View Report Data** panel, you can view the report that is created as per your selection.

Click **Next**.

To return to the Custom Report Wizard and make changes to the report, click **Back**.

12 Save the report. Enter a report name, a description (optional), and location where you want to save the report.

Click **Save**.

Example 1: You may want to create a custom report based on your specific requirements. For example, you may want to create a daily status report of the clients that are backed up everyday.

This report gives the detailed tabular information of the jobs directory being backed up, its status (if it's successful, partially successful or failed), Level Type (Incremental, Full, Differential Incremental), the job file count and job size in the datacenter . You can enhance this report by adding more available columns based on the report requirement.

See the procedure to know how you can create a daily status report of the clients that are backed up everyday.

To create a daily status report of the clients that are backed up everyday

1. In the OpsCenter console, click **Reports**.
2. On the **Report Templates** tab, click **Create New Report**.
3. On the Report Wizard, select the **Create a custom report** option and click **Next**.
4. Select the **Report Category** as **Backup/Recovery** and the **Subcategory** as **Job/Images/Media/Disk**.
5. Select the **Report View type** as **Tabular**.

   Click **Next**.
6. Select the appropriate timeframe for which you want to view the data.
7. Select the **Job** filter. Select the **Column** as **Backup Job data type**, **Operator** as **=**, and **Value** as **Yes**. Click **Add**.
8. Click **Next**.
9. Under **Tabular Report Properties**, select the **Time Basis** as **Job End Time**. Change the **Display Unit** as per your requirement.
10. Select **Available columns** from the list that appears:
    - Backup Job File Count
    - Backup Job Size
    - Job Directory
    - Job End Time
    - Job Start Time
    - Job Status
    - Job Status Code

- Job Type
- Master Server
- Schedule Name
- Schedule/Level Type

Click **Add**.

11 Click **Next** to run the report.

Example 2: You may want to create a report that examines the number of tapes in each status category and its percentage.

To report on the distribution of tape status in your environment

1 In the OpsCenter console, click **Reports**.

2 On the **Report Templates** tab, click **Create New Report**.

3 On the Report Wizard, select the **Create a custom report** option and click **Next**.

4 Select the **Report Category** as **Backup/Recovery** and the **Subcategory** as **Media**.

5 Select the **Report View type** as **Distribution**.

Click **Next**.

6 Select the appropriate timeframe for which you want to view the data. You can also select **No Time Basis**.

7 Optionally, select any filters based on your requirement.

Click **Next**.

8 In the Distribution Chart Properties section, make the following selections:

Chart Type	Pie Chart
Report On	Media History Status
Report Data	Media ID
	Count

9 Click **Next**.

Example 3: You may want to create a custom tabular report that shows the following information:

- Know what jobs were successful in the past week for a specific master server

- Show the amount of time the backup took
- Show how large the backup was

To create a report showing successful backup job details for a master server

1. In the OpsCenter console, click **Reports**.
2. On the **Report Templates** tab, click **Create New Report**.
3. On the Report Wizard, select the **Create a custom report** option and click **Next**.
4. Select the **Report Category** as **Backup/Recovery** and the **Subcategory** as **Job/Image/Media/Disk**.
5. Select the **Report View type** as **Tabular**.
6. Change Relative Time Frame to Previous 1 Week
7. Under **Filters**, select **Job**. In the Column area, select **Job Type**, select the **=** Operator and choose a value of **Backup**.

   Click **Add**.
8. Back under the Column heading, select **Job Status** leave the Operator at "=" and choose **Successful** as the value

   Click **Add**.
9. Click **Next**.
10. Select the Time Basis as **Job Start Time**
11. You may change the Display Unit or Time Duration. For example if the master server takes smaller backups, then you may change the Display Unit to MB.
12. From the Available Columns list, select the following:
    - Backup Job Size
    - Client Name
    - Job Duration

    Click **Add** to move them under the Selected Columns area.
13. In the Selected Column area, perform the following operations for each of the rows:
    - Click the check box next to **Client Name** on the right and click **Move Up** to make it the first row.
    - On the Job Duration row, change Operation to **Total**.

- On the Job Size row, change Sort Order to **Descending** and Operation to **Total**.

14 Click **Next**.

About Custom Report Wizard parameters

The Custom Report Wizard displays a set of parameters that varies depending on the report type. The following topics describe all the available parameters:

- Define Time frame parameters
  See "Configuring timeframe parameters" on page 566.
- About display options
  See "About display options" on page 569.
- Report conditions
  See "Defining report conditions" on page 573.
- Filter parameters
  See "Selecting and using filter parameters" on page 568.

Configuring timeframe parameters

You use the Time Frame parameters to define the report's overall time frame and the intervals for which data is reported.

You can specify absolute or relative time frame for a report.

You can select the following timeframe parameters:

Relative Timeframe	Select **Previous** or **Next** from the drop-down list (wherever applicable), and then specify the number of hours, days, weeks, months, quarters, or years to define the period. The report displays data collected within the specified time period, for example, data of the previous 3 months. The Relative Timeframe is especially useful for reports that you plan to generate on a regular basis. Such reports always show data collected over the most recent time interval.

Start from the beginning of <*selected unit*>	This applies only to Relative time frames. In Start from the beginning of <*selected unit*>, the <*selected unit*> may stand for Hours, Days, Weeks, Months, Quarters, or Years depending on what unit you select as a Relative Timeframe. If you specify a relative timeframe and check **Start from the beginning of <selected unit>**, the Relative timeframe is calculated starting from the first day for week, month, quarter, or year selection, from 12 A.M. for day selection, and from the earliest whole number (no minutes or seconds) for hour selection. Do not select the **Start from the beginning of <unit>** check box if you want to view data for the entire period specified in Relative Timeframe. Examples: ■ The current date is June 13, 2010. If you select the Relative Timeframe as Previous 1 Month and do not select the **Start from the beginning of Month** check box, the report shows data from May 14, 2010 to June 13, 2010. However if you select the **Start from the beginning of Month** check box, the report shows data from June 1, 2010 to June 13, 2010. ■ The current date and time is September 13, 10:30 PM. If you select the Relative Timeframe as Previous 2 Days and do not select the **Start from the beginning of Days** check box, the report shows data from September 11, 10:30 P.M. to September 13, 10:30 P.M. However if you select the **Start from the beginning of Days** check box, the report shows data from September 12, 12 A.M. to September 13, 10:30 P.M. ■ The current time is 4:25 P.M. If you select the Relative Timeframe as Previous 2 Hours and do not select the **Start from the beginning of Hour** check box, the report shows data from 2:25 P.M. to 4:25 P.M. However if you select the **Start from the beginning of Hours** check box, the report shows data from 3 P.M. to 4:25 P.M. **Note:** If you specify relative time frame and check **Start from the beginning of <*selected unit*>**, the report is configured to display data collected over the interval ending at the current date. This is effectively equivalent to specifying an absolute time frame; the report's contents remain static whenever you display it.
Absolute Timeframe	Define the beginning and end of the time interval to be covered by the report. When you enter absolute dates, the report's contents remain static whenever you display it.

Ignore From Date	This applies only to Absolute timeframes. Check this option to view all the data on and before the **To** date that you enter in the Absolute timeframe. **Example**: Suppose you specify an absolute timframe: From March 1, 2004, 12:00 A.M. to April 30, 2004, 12:00 A.M. The report displays data from the time period between the start and end dates. Now if you check **Ignore From Date**, the report ignores the From Date and displays all data before April 30, 2004, 12:00 A.M.
Ignore To Date	This applies only to Absolute timeframes. Check this option to view all data on and after the **From** date that you enter in the Absolute timeframe. **Example:** Suppose you specify an absolute timframe: From March 1, 2004, 12:00 A.M. to April 30, 2004, 12:00 A.M. The report displays data from the time period between the start and end dates. Now if you check **IgnoreTo Date**, the report ignores the To Date and displays all data on and after March 1, 2004, 12:00 A.M.
No Time Basis	This signifies that the data shown should not be grouped with time. The report includes all the data in the OpsCenter database irrespective of time. The timeframe grouping is not applicable.
Day Window	Day Window is applicable when you specify an Absolute or Relative timeframe. From the Day Window, you can specify the time interval that constitutes one day. Select values from the **From** and **To** drop-down lists. Example: 6:00 PM to 6:00 AM Example: 12:00 AM (midnight) to 12:00 PM (noon)
Report Time Frame Grouping	This option appears only when you select a Historical view type. Select the time interval by which you want to group the records. For example, if you selected 1 month as the Report Time Frame and 10 days as the Group By interval, the report shows records in three chunks of data grouped by 10 days.

Selecting and using filter parameters

You can use filter parameters to obtain additional filtering capability for the report that you want to display. For example depending on the category or subcategory that you select, you may filter on the following:

- Client Operating System
- Client is Active

- Policy Active: Select **Yes** to view policies that are active. Select **No** to view policies that are not active.
- **Media is On Hold** column has been added under the **Media** filter.
- **Image is on hold** and **Image Copy is on hold** columns have been added under the **Image** filter.

To specify additional filtering criteria

1. On the Custom Reports Wizard, select a report category, subcategory and view type. Click **Next**.
2. On the **Select Parameters** panel, the respective filters appear in the **Filters** section.

   The list of filters that appear depend on the report category and view type that you select.
3. Click the filter that you want to use, and then specify one or more values using the fields provided.

About display options

Use the **Modify Display Options** panel to define the measurements to be collected for historical, ranking, tabular, and distribution reports. Different display options are displayed for different view types.

About Historical view display options

The following display options are available for historical reports. The following parameters are displayed:

Report On	Define the report's scope using the drop-down list. This field denotes the entity on which grouping is required. For example, when you select the Report On parameter as Client, the Y-axis report data is grouped per client. Example: Job Status, Image type etc.
Description	Description to display along with the report. If you leave this field blank, no description is provided by default.
X-Axis	
Display Name	For Historical reports, a label for the horizontal (X) axis. If you leave this field blank, a default label is provided.

Report Data	The metric used to define the graph's horizontal (X) axis. Examples: `Attempt End Time`, `Client Name` If you choose a Report Data parameter like Client Name which is not time-based, another parameter called Time Basis appears.
Time Basis	This parameter appears if you select a Report Data parameter like Client Name that is not related to time. Time Basis resembles the time attribute on which time filter is applied as criteria. This attribute is not shown if you select No Time Basis while configuring the timeframe in the Wizard. Time Basis is the metric used for assigning a time to each item in the report, if not specified by the Report Data parameter. Example: The start time or the end time for each backup job.
Y1 or Y2 -Axis	
Display Name	For Historical reports, a label for the horizontal (Y1 or Y2) axis. If you leave this field blank, a default label is provided.
Report Data	For Historical reports, the metric used to define the graph's vertical (Y1 or Y2) axis. Examples: Job Size, Status Code etc.
Display Unit	For numeric data types, such as Job Size, the units in which to display the data. This is applicable only for size-related attributes like Job size, image size, fragment size etc. Examples: MB, GB.
Chart Type	The report format. Additional formats may be available depending on the values specified in Report Data.
Show Forecast with forecast periods	Use the Trendline and Forecast parameters to project future trends by averaging actual data from the recent past. Check **Show forecast with forecast periods**, and use the drop-down list to specify a number of forecast periods (intervals). This displays a forecast line extending to future dates, using linear regression to predict values based on the trend of data within the report's time frame. Example: 12 shows forecast data for the next 12 months (if the Time Frame Group By is 1 month). The following Web site helps in calculating the forecast: http://easycalculation.com/statistics/regression.php

Show trendline with moving average period of	Use the Trendline parameter to indicate a general pattern or direction by averaging actual data from the recent past. Check **Show trendline with moving average**, and use the drop-down list to specify the number of data points to factor into the average. At each interval on the graph, the trendline shows a moving average of the most recent data points. Example: 3 displays a trendline that, at each interval, shows the average of the current data point and the two previous data points.
Target Performance	For Historical reports, select the **Target Performance** checkbox and then either Y1 or Y2-Axis radio button. Type a value in the text box to include a target level or threshold in the report display. The target value appears as a horizontal line, useful for making quick visual comparisons between the target value and the actual values being reported.

About Ranking chart display options

The following display options are available for Ranking reports. The following parameters are displayed:

Chart Type	Select **Bar Chart** from the drop-down list.
Report On	Select the entity that you want to see in the report like Image Type.
Display	Select how many rankings you want to see and how you want them arranged (in Ascending or descending order).
Y-Axis Display Name	Enter a label for the Y-Axis.
Report Data	This is the data that should be plotted on the Y-axis.
Time Basis	Metric used for assigning a time to each item in the report, if not specified by the Report Data parameter. Example: The start time or the end time for each backup job.
Description	Description to display along with the report. If you leave this field blank, no description is provided by default.

About Distribution chart display options

The following display options are available for Distribution reports:

Chart Type	Select **Pie Chart** from the drop-down list.

Report On	Select the entity that you want to see in the report like Attempt Status.
Report Data	This is the data that should be plotted on the pie chart.
Time Basis	Metric used for assigning a time to each item in the report, if not specified by the Report Data parameter. Example: The start time or the end time for each backup job.
Description	Description to display along with the report. If you leave this field blank, no description is provided by default.

About Tabular display options

Use the **Modify Display Options** panel to establish the column titles for a tabular report.

The following display options appear for a tabular report:

Time Basis	From the **Time Basis** drop-down list, select a time basis like Job End Time or Job Start Time. Time Basis is used to assign a time to each item in the report.
Description	Enter a description for the report. This is optional.
Display Unit	From the **Display Unit** drop-down list, select one of the following units: ■ B ■ KB ■ MB ■ GB ■ TB
Time Duration	From the **Time Duration** drop-down list, select one of the following time intervals: ■ Seconds ■ Minutes ■ Hours ■ Days ■ Weeks ■ Months ■ Years

Available Columns	From the **Available Columns** list, select one or more values for table columns, for example, Client Name, Status, Job Group ID. Click **Add**. The columns selected from the **Available Columns** list are added to the **Selected Columns**, which you can rearrange as you want them to be displayed on reports.
Selected Columns	The columns selected from the **Available Columns** list are added to the **Selected Columns**, which you can rearrange as you want them to be displayed on reports using the following controls: ■ Sort order ■ Operation ■ Move Up ■ Move Down ■ Remove All the columns from the **Selected Columns** list are displayed in the report.
Rows per page	From the **Rows Per Page** drop-down list, select number of rows of records that you want to display on one report page.
Display unique rows in the report	When you select this option, all duplicate rows are replaced by a single row in the report and only distinct records are shown. Duplicate rows generally appear if the rows do not have a unique ID.

Defining report conditions

In the **Conditions** section of the **Modify Display Options** panel, specify exception conditions for notification. Exception conditions represent potential problems, for example an unusually high percentage of backup job failures or an unusually low quantity of data being backed up. Each condition is defined by assigning threshold values for a particular metric, such as Success Rate or Total Backup Job Size. You can set a low threshold, a high threshold, or both. The conditions are applicable only for numeric values like Job Size (and not for values like Job Type, Master Server). You can apply condition for attributes like Job type or Master server provided you have applied a function like Count, Distinct Count etc. on it.

After you specify your conditions, you can create a report schedule so that when a condition is true, an email notification is sent or the report is exported, or both. The conditions are applied only when a report is scheduled.

Creating an OpsCenter report using SQL query

This section provides the procedure to create a report using SQL query.

Only OpsCenter Analytics users can access the custom SQL query function.

See "About custom SQL query in OpsCenter Analytics" on page 547.

Note: OpsCenter provides detailed information about the OpsCenter database schema that you may want to know before running any SQL query to generate reports. On the Report Wizard > SQL Query page, click the following link to open the PDF that contains all relevant information: Refer to the OpsCenter Database Schema Document

---

Note: OpsCenter Reporter and Restore Operator do not have access to the custom SQL query option.

To create a report using SQL query

1. In the OpsCenter console, click **Reports**.
2. On the **Report Templates** tab, click **Create New Report**.
3. On the Report Wizard, select the **Create a report using SQL Query** option and click **Next**.
4. On the SQL Query page, enter an SQL query to view the required data.

   For example, to view all NetBackup master servers that monitored and managed by OpsCenter, enter the following SQL query: select * from domain_masterserver
5. Click **Next**.

   You can view all master server details that are stored in the domain_masterserver database table.

   Note: When you run a stored procedure that has multiple result sets, then output of only the first result set is displayed on the GUI. The output of other result sets is not shown on the GUI.

Note that Opscenter stores most of the time fields in Gregorian. If you want to see the value for a given Gregorian date field in a timezone that is configured on the OpsCenter host, you should use `utcbiginttonomtime`(*gregorianDatefield*) function, where *gregorianDatefield* is any time value in gregorian. The function `utcbiginttonomtime` function cannot consider DST time offset. Hence it ignores any DST offset while showing the date and time value.

You must not use `utcbiginttoutctime()` function as it does not show time in a time zone that is configured on your OpsCenter host.

About managing My Reports

You can save generated reports for your future use. These saved reports are stored in the **My Reports** tab. Use this section to view the saved reports or modify the parameters of the saved reports and generate new reports out of them. You can also delete the saved reports using the **My Reports** tab.

The following topics provide more information about managing reports.

See " Creating a report using the My Reports tab" on page 575.

See "Deleting a saved report using the My Reports tab" on page 575.

See "Viewing a saved report using the My Reports tab" on page 576.

See "Editing a saved report using the My Reports tab" on page 576.

See "Exporting a saved report" on page 576.

See "Emailing a saved report" on page 577.

Creating a report using the My Reports tab

This section provides the procedure to create a report using **My Reports** tab.

To create a report using the My Reports tab

1. In the OpsCenter console, click **Reports > My Reports**.
2. On the **My Reports** tab, click **Create New Report**.

   You can create a report in any of the following ways:

   See "Creating an OpsCenter report using a Report Template" on page 550.

   See "Creating a custom report in OpsCenter" on page 559.

   See "Creating an OpsCenter report using SQL query" on page 573.

Deleting a saved report using the My Reports tab

This section provides the procedure to delete a saved report.

To delete a saved report

1. In the OpsCenter console, click **Reports > My Reports**.
2. On the **My Reports** tab, in the **Reports** list, expand a report folder to view the reports that are saved within it.
3. Select the check box in front of the report name.
4. Click **Delete**.

Viewing a saved report using the My Reports tab

You can view the saved reports using the **My Reports** tab.

To view a saved report

1. In the OpsCenter console, click **Reports > My Reports**.
2. On the **My Reports** tab, in the **Reports** list, expand a report folder to view the reports that are saved within it. Select the saved report that you want to view.

Editing a saved report using the My Reports tab

You can edit a saved report. You can edit the report details, such as the report name or the folder where you want to save the edited report.

To edit a saved report

1. In the OpsCenter console, click **Reports > My Reports**.
2. On the **My Reports** tab, in the **Reports** list, expand a report folder to view the reports that are saved within it. Select the saved report that you want to edit.
3. In the report view area at the right-hand side, click the **Save As Report** icon. The **Save Report** pop-up screen opens.
4. On the **Save Report** screen, enter the required information.

   See "Save report and email report dialog boxes" on page 552.
5. Click **OK**.

Exporting a saved report

Using OpsCenter, you can preserve saved report data in files or print the data. You can email a report in a number of different file formats.

See " File formats available in OpsCenter" on page 555.

You can open the exported file using other applications, such as a spreadsheet program or a text editor.

To export a saved report

1. In the OpsCenter console, click **Reports > My Reports**.
2. On the **My Reports** tab, in the **Reports** list, expand a report folder to view the reports that are saved within it. Select the saved report that you want to export.
3. In the report view area at the right-hand side, click the **Export Report** icon. The **Export Report** pop-up screen opens.

4 On the **Export Report** pop-up screen, select the export options that you want to export the report with. Select file format, such as PDF, CSV, or XML and content or report view, such as Distribution, Historical, or Ranking.

5 Click **OK**. The system displays the export options pertaining to the file format you have selected. Select those options and export the saved report.

Emailing a saved report

Using OpsCenter, you can email the saved report data to the selected recipients. You can email the report in the following file formats:

PDF (Portable Document Format)	Can be viewed using a PDF reader, such as Adobe Reader
CSV (comma-separated values)	Use with spreadsheet programs, such as Microsoft Excel.
TSV (tab-separated values)	Compatible with word-processing applications and text editors
HTML (hypertext markup language)	Can be opened using with Web browsers
XML (Extensible Markup Language)	Can be imported (using user-written scripts) by other programs like databases or billing applications

To email a report

1 In the OpsCenter console, click **Reports > Saved Reports**.

2 On the **My Reports** tab, in the **Reports** list, expand a report folder to view the reports that are saved within it. Select the saved report that you want to email.

3 In the report view area at the right-hand side, click the **Email Report** icon. The **Email Report** pop-up screen opens.

4 On the **Email Report** pop-up screen, select the email options: File format, such as PDF, CSV, or XML and content or report view, such as Distribution, Historical, or Ranking.

5 Enter email IDs in To, Cc, and Bcc text boxes, to which you want to send emails.

6 Enter the subject of the email.

7 Enter the message that may be a short description regarding the report data that you want to email.

8 Click **OK**.

About managing My Dashboard

Your saved reports are preserved in **My Reports** tab, which you can select and publish on **My Dashboard** tab. You can select multiple reports and add them in the same dashboard section. Thus, you can create multiple dashboard sections containing a number of reports.

You can add only 10 reports in a dashboard.

See "Adding reports to a dashboard" on page 579.

See "Modifying a dashboard section" on page 579.

See "Deleting a dashboard section" on page 579.

See "Emailing dashboard sections" on page 580.

See "Refreshing My Dashboard" on page 580.

Reports > My Dashboard options

Select and publish reports on **My Dashboard** tab. You can select multiple reports and add them in the same dashboard section. Thus, you can create multiple dashboard sections containing a number of reports.

You can add only 10 reports in a dashboard.

Table 12-4 Reports > My Dashboard options

Option	Description
Add/Edit/Delete	You can add multiple Dashboards on this page and one or more reports from My Reports to each of the dashboards. Use Add, Edit, Delete tasks to add, edit, or remove dashboard
Email Dashboard	Select this option if you want to email all the dashboard reports. In the **Email Dashboard** dialog box that opens, you can specify the format in which you want to email the dashboard reports.along with the other email details. Click **OK**.
Refresh Dashboard	Select this option to update the reports in the dashboard.

Adding reports to a dashboard

This section provides the procedure to add reports to a dashboard.

To add reports to a dashboard

1. In the OpsCenter console, click **Reports > My Dashboard**.
2. Click **Add**.
3. On the **Add Dashboard Section** pop-up screen, enter the section name.
4. Expand the Private or Public Reports folder to view existing reports.
5. Select the check boxes in front of the report names, which you want to publish on the dashboard.
6. Click **OK**.

Modifying a dashboard section

This section provides the procedure to modify dashboard section.

To modify a dashboard

1. In the OpsCenter console, click **Reports > My Dashboard**.
2. Click **Edit**.
3. On the **Edit Dashboard Section** pop-up screen, select the dashboard section from the drop-down list, that you want to modify.
4. Modify the section name.
5. Expand the Private or Public Reports folder to view existing reports.
6. Select or clear the check boxes in front of the report names, which you want to publish on or remove from this dashboard section.
7. Click **OK**.

Deleting a dashboard section

This section provides the procedure to delete a dashboard section.

To delete a dashboard section

1. In the OpsCenter console, click **Reports > My Dashboard**.
2. Click **Delete**.
3. On the **Delete Dashboard Section** pop-up screen, select the dashboard section from the drop-down list, that you want to delete.
4. Click **OK**.

Emailing dashboard sections

You can email your dashboards.

To email a dashboard

1. In the OpsCenter console, click **Reports > My Dashboard**.
2. Click the **Email Dashboard** icon.
3. On the **Email Dashboard** pop-up screen, select the format in which you want to send the email.
4. Select email recipients from the To.., Cc.., and Bcc.. as appropriate.

   Alternatively, enter new email recipients, which are added into the database.
5. Enter the email subject and message.
6. Click **OK**.

Refreshing My Dashboard

This section provides the procedure to refresh **My Dashboard**.

To refresh My Dashboard

1. In the OpsCenter console, click **Reports > My Dashboard**.
2. Click the **Refresh** icon.

About managing reports folders in OpsCenter

OpsCenter provides a way to manage folders where you have saved your reports. They can be both private reports and public reports.

Using the **Manage Folders** tab in the **Reports** section, you can add new report folders, edit names of the existing folders, or delete them.

You can also select reports in a particular folder and delete them using this tab.

See “Adding a reports folder in OpsCenter” on page 581.

See “Editing a reports folder in OpsCenter” on page 581.

See “Deleting reports folders in OpsCenter” on page 581.

See “Deleting reports from a folder in OpsCenter” on page 582.

Reports > Manage Folders options

Using the **Manage Folders** tab in the **Reports** section, you can add new report folders, edit names of the existing folders, or delete them.

Adding a reports folder in OpsCenter

This section provides a procedure to add a report folder.

To add a folder

1. In the OpsCenter console, click **Reports > Manage Folders**.
2. On the **Reports** tree, select a check box in front of a private folder node or public folder node in which you want to create a new folder.
3. Click **Add**.
4. In the **Create new folder** pop-up window, make sure that you have selected only one folder. If multiple folders are selected, the **Add** option is disabled.
5. Enter the folder name.
6. Click **OK**.

   This folder is added in the selected node.

Editing a reports folder in OpsCenter

This section provides a procedure to edit a report folder.

To edit a folder

1. In the OpsCenter console, click **Reports > Manage Folders**.
2. On the **Reports** tree, select a check box in front of a private folder or public folder that you want to edit.
3. Click **Edit**.
4. In the **Edit folder name** pop-up window, make sure that you have selected only one folder. If multiple folders are selected, the **Edit** option is disabled.
5. Edit the folder name.
6. Click **OK**.

Deleting reports folders in OpsCenter

This section provides a procedure to delete a report folder. If you delete a report folder, all reports that are saved in that folder are deleted.

To delete folders

1. In the OpsCenter console, click **Reports > Manage Folders**.
2. On the **Reports** tree, select a check boxes in front of the private folders or public folders that you want to delete.
3. Click **Delete**.

Deleting reports from a folder in OpsCenter

This section provides a procedure for deleting the reports that are saved in a public folder or private folder.

To delete reports from a folder

1. In the OpsCenter console, click **Reports > Manage Folders**.
2. On the **Reports** tree, select a private folder or public folder from which you want to delete the reports. A list of reports that are saved in the selected folder displays at the right-hand side of the page.
3. From the list of reports, select the check boxes in front of the reports that you want to delete.
4. Click **Delete**.

Using report schedules in OpsCenter

Using report schedules, you can email or export reports at a scheduled time. Each report schedule is associated with a time schedule at which it emails or sends the specified reports.

OpsCenter provides a wizard to create a report schedule.

See "Creating a report schedule in OpsCenter" on page 588.

The following table describes the steps that you need to carry out to email or export a report on a specific schedule.

See "About managing time schedules in OpsCenter" on page 590.

Table 12-5 Creating a report schedule

Step Number	Step and reference topic
1	Create a time schedule. See "Creating a time schedule" on page 591.

Table 12-5 Creating a report schedule *(continued)*

Step Number	Step and reference topic
2	Create a report schedule. OpsCenter provides a wizard to create a report schedule. This wizard lets you specify the following details: ■ Report schedule name ■ File format in which you want to email or export reports ■ Select a time schedule. You can either select an existing time schedule that you have created in the first step or create a new schedule from here to associate it with this report schedule. ■ Specify details of export or email options. ■ Select the reports that you want to export or email on a specific schedule. **Note:** You can select only saved reports in a schedule. See "Creating a report schedule in OpsCenter" on page 588.

Table 12-6

Steps	Reference topic
◆ Create a time schedule. Create a time schedule.	See "Creating a time schedule" on page 591.

Table 12-6 *(continued)*

Steps	Reference topic
◆ Create a report schedule. Create a report schedule. OpsCenter provides a wizard to create a report schedule. This wizard lets you specify the following details: ■ Report schedule name ■ File format in which you want to email or export reports ■ Select a time schedule. You can either select an existing time schedule that you have created in the first step or create a new schedule from here to associate it with this report schedule. ■ Specify details of export or email options. ■ Select the reports that you want to export or email on a specific schedule. **Note:** You can select only saved reports in a schedule.	See "Creating a report schedule in OpsCenter" on page 588.

Reports > Schedules options

Using report schedules, you can email or export reports at a scheduled time. Each report schedule is associated with a time schedule at which it emails or sends the specified reports.

Table 12-7 Report Schedules tab options

Option	Description
Add/Edit	Select **Add** or **Edit** to start the Report Schedule Wizard.
Delete	Select **Delete** to remove the selected report schedules.
Enable/Disable	Select **Enable** or **Disable** to enable or disable the selected report schedules.
Name	Name of a report schedule.
Time Schedule Name	Name of a time schedule that is associated with this report schedule.

Table 12-7 Report Schedules tab options *(continued)*

Option	Description
Enabled	Specifies whether the report schedule is enabled or not.
Start Date	Date on which this schedule runs.
End Date	Date on which this schedule stops.
Export	Specifies whether you have exported the associated reports.
Email	Specifies whether you have emailed the associated reports.
Reports	Number of the reports that are exported or emailed when this schedule runs.

Table 12-8 Time Schedules tab options

Option	Description
Add/Edit	Select **Add** or **Edit** to go to the Time Schedule page.
Delete	Select **Delete** to delete the selected time schedules.
Name	Name of the time schedule.
Schedule Time	Time when the associated reports are exported or emailed.
Recurrence Pattern	A pattern with which this schedule runs.
Start Date	Date when the schedule starts.
End Date	Date when the schedule stops.

About managing report schedules in OpsCenter

NetBackup OpsCenter provides a way to export or email a report on a specific schedule. For this task you need to create a report schedule that is associated with a time schedule on which the specified reports are exported or emailed.

Each report schedule can be associated with a single time schedule. A single time schedule can be associated with multiple report schedules.

See “About managing time schedules in OpsCenter” on page 590.

The following topics describe how to create and manage report schedules.

See “Viewing report schedule details in OpsCenter” on page 586.

See “Creating a report schedule in OpsCenter” on page 588.

See "Editing a report schedule in OpsCenter" on page 589.

See " Deleting a report schedule in OpsCenter" on page 589.

See "Enabling or disabling a report schedule" on page 589.

Viewing report schedule details in OpsCenter

This section provides information on viewing the list of report schedules.

If you have applied conditions for the selected report, the list of applicable conditions is shown on the last page of the wizard. You can select the appropriate conditions. An email notification is sent to the relevant recipients if the selected condition is satisfied.

To view report schedule details

1. In the OpsCenter console, click **Reports > Schedules**.

   By default, the **Report Schedules** tab is selected.

2. On the **Report Schedules** tab, view the report schedule details.

   See "Reports > Schedules options" on page 584.

Report Schedule Wizard

The Report Schedule Wizards contains five panels to help you create a schedule.

Table 12-9 Enter Report Schedule Details panel options

Option	Description
Report Schedule Name	Enter a report schedule name. This field must be filled.
Select Format	Select a file format in which you want to export or email report the associated reports. See " File formats available in OpsCenter" on page 555.

Table 12-10 Select Time Schedule panel options

Option	Description
Create new Time Schedule	Select this option if you want a new time schedule to be associated with the report schedule.
Use existing Schedule	Select this option if you want the report schedule to be associated with an existing time schedule

Table 12-11 Select Export/Email Report Options panel options

Option	Description
Export	Select this check box if you want to export the reports that are associated with this schedule. See " File formats available in OpsCenter" on page 555.
Location	Enter a directory path where you want to save the exported report or click **Browse** to select the desired location.
Overwrite if file exists	Select this check box if you want to overwrite a file that already exists at the specified location.
Email	Select this check box if you want to email the reports that are associated with this schedule.
To	Select email IDs to which you want to email reports.
Cc	Select email IDs to add in the **Cc** list of email.
Bcc	Select email IDs to add in the **Bcc** list email.
Subject	Type the email subject. For example: Daily Job Count Report
Message	Type any other related information.

Table 12-12 Select Reports panel options

Option	Description
Private Reports	Select private reports from the list that you want to schedule. You can select both public reports and private reports.
Public Reports	Select public reports from the list that you want to schedule. You can select both public reports and private reports.

Table 12-13 Select a report condition to be applied panel options

Option	Description
Send email only if the report meets one or more selected conditions	Check this option if you want the report to be emailed only if it meets one or more of the selected conditions. You can create conditions for custom reports while editing the report.
Report Name	The custom reports that have conditions and are selected to be scheduled are displayed.
Condition	The condition that is associated with the custom report is displayed. You can create a condition only for custom reports.

Creating a report schedule in OpsCenter

To create a report schedule

1. In the OpsCenter console, click **Reports > Schedules**.
2. On the **Report Schedules** tab, click **Add**. OpsCenter provides a Report Schedule Wizard that guides you through the procedure of creating a report schedule.

   The **Enter Report Schedule Details** panel appears.

   Enter the report schedule details.

   See "Report Schedule Wizard" on page 586.
3. Click **Next**.

   The **Select Time Schedule** panel appears:

   Select the **Use existing schedule** option if you want to run this schedule on any existing time schedule. If you want to create a new time schedule for this report schedule, select **Create new time schedule**.

   See "Creating a time schedule" on page 591.

   If you have selected **Create new time schedule**, the system takes you to the Time Schedule Wizard. After creating a time schedule you can select the export and the email report options.
4. Click **Next**.
5. If you have selected the **Use existing schedule option** in the previous step, in the **Configure Export/Email Report Settings** panel, specify the following details:

   You can select either **Export**, **Email**, or both options.

   See "Report Schedule Wizard" on page 586.
6. Click **Next**.
7. In the **Select Reports** panel, select the public reports or private reports that you want to export or email on this schedule.

   These reports should be saved.

   Click **Back** if you want to change the previous selections.

8 In the **Select a report condition to be applied** panel, select a report and report condition to be applied. You can apply report conditions to custom reports.

   You can also select the option **Send email only if the report meets one or more of the selected conditions** if you want the report to be emailed only when the report meets one or more of the selected conditions.

9 Click **Save**.

Editing a report schedule in OpsCenter

This section describes how to edit report schedule details.

To edit a report schedule

1 In the OpsCenter console, click **Reports > Schedules**.

   By default, the **Report Schedules** tab is selected.

2 On the **Report Schedules** tab, select a report schedule from the list that you want to edit.

3 Click **Edit**.

4 Edit the report schedule details using the wizard.

5 Click **Save**.

Deleting a report schedule in OpsCenter

This section describes how to delete a report schedule.

To delete a report schedule

1 In the OpsCenter console, click **Reports > Schedules**.

   By default, the **Report Schedules** tab is selected.

2 On the **Report Schedules** tab, select one or more report schedules from the list that you want to delete.

3 Click **Delete**.

Enabling or disabling a report schedule

This section describes how to enable or disable a report schedule.

To enable or disable a report schedule

1. In the OpsCenter console, click **Reports > Schedules**.

   By default, the **Report Schedules** tab is selected.

2. On the **Report Schedules** tab, select one or more report schedules from the list that you want to enable or disable.

3. Click **Enable** or **Disable**.

About managing time schedules in OpsCenter

This section provides procedures to create and manage a report schedule.

Each report schedule can be associated with only a single time schedule. A single time schedule can be associated with multiple report schedules.

See "About managing report schedules in OpsCenter" on page 585.

The following topics provide more information about managing time schedules.

See "Viewing time schedule details" on page 591.

See "Creating a time schedule" on page 591.

See "Editing a time schedule" on page 591.

See "Deleting a time schedule" on page 592.

Reports > Schedules > Create or Edit Time Schedule options

Use the page to create or edit a time schedule.

Table 12-14 Create or Edit Time Schedule options

Option	Description
Schedule Name	Enter name of the time schedule.
Schedule Time	Enter the time when the schedule runs and the associated reports are exported or emailed.

Table 12-14 Create or Edit Time Schedule options *(continued)*

Option	Description
Schedule Pattern	Select a pattern with which you want this schedule to be run. The following schedule patterns are available: ■ One Time ■ Daily ■ Weekly ■ Monthly ■ Quarterly ■ Yearly Depending on the pattern-selected , options change.

Viewing time schedule details

This section provides a procedure to view the details of time schedules.

To view a time schedule

1. In the OpsCenter console, click **Reports > Schedules**.
2. Click **Time Schedules**.

   The time schedule details appear:

   See "Reports > Schedules options" on page 584.

Creating a time schedule

Use the following procedure to create a time schedule.

To create a time schedule

1. In the OpsCenter console, click **Reports > Schedules**.
2. Click **Time Schedules**.
3. On the **Time Schedules** tab, click **Create**.
4. On the **Create Time Schedule** page, specify the necessary details.

   See "Reports > Schedules > Create or Edit Time Schedule options" on page 590.

5. Click **OK**.

Editing a time schedule

Use the following procedure to edit a time schedule.

To edit a time schedule

1. In the OpsCenter console, click **Reports > Schedules**.
2. Click **Time Schedules**.
3. On the **Time Schedules** tab, in the table, select the time schedule that you want to edit.
4. Click **Edit**.
5. Edit the time schedule details.
6. Click **OK**.

Deleting a time schedule

Use the following procedure to delete a time schedule.

To delete a time schedule

1. In the OpsCenter console, click **Reports > Schedules**.
2. Click **Time Schedules**.
3. On the **Time Schedules** tab, in the table, select the time schedules that you want to delete.
4. Click **Delete**.

Appendix A

Additional information on PureDisk data collection

This appendix includes the following topics:

- About AT configuration in OpsCenter
- About Scenario 1: Root brokers on local hosts
- About Scenario 2: Local root broker for OpsCenter server and remote root broker for PureDisk SPA
- Setting up a trust between the PureDisk SPA AT host and the OpsCenter Server host

About AT configuration in OpsCenter

The user authentication service (Veritas Product Authentication Service or AT) is embedded with OpsCenter Server. Each OpsCenter setup has its own AT configuration, which is called OpsCenter AT.

See "About OpsCenter AT" on page 27.

OpsCenter Server has local AT configuration that no other product can share. In a similar way, PureDisk SPA will also have local or integrated AT configuraion.

To collect PureDisk data from OpsCenter Server, you need to set up a unidirectional trust between the OpsCenter Server host and PureDisk SPA host. You need to establish trust between the authentication brokers of OpsCenter and PureDisk SPA for secure communication. This set up is a pre-requisite for PureDisk data collection from OpsCenter.

Note: Setting up trust between the PureDisk SPA host and OpsCenter AB host is a manual process.

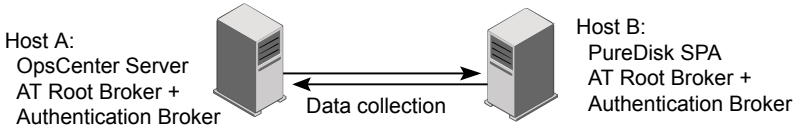
See "Setting up a trust between the PureDisk SPA AT host and the OpsCenter Server host" on page 595.

About Scenario 1: Root brokers on local hosts

This section talks about the scenario where the OpsCenter server and PureDisk SPA use their own embedded AT root broker configurations.

Figure A-1 describes a scenario where the OpsCenter server and PureDisk SPA use the AT root brokers that are configured on their respective hosts.

Figure A-1 Root brokers on local hosts



Note: You need to set up a trust between the two root broker hosts, that is between Host A and Host B.

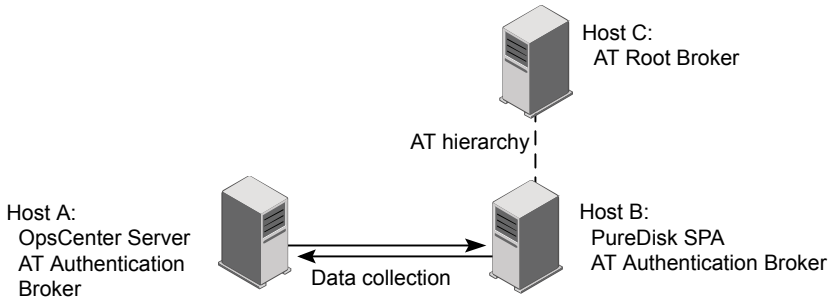
See "Setting up a trust between the PureDisk SPA AT host and the OpsCenter Server host" on page 595.

About Scenario 2: Local root broker for OpsCenter server and remote root broker for PureDisk SPA

This section talks about the scenario where the OpsCenter server host uses the local AT configuration (OpsCenter AT) and PureDisk SPA host uses a remote AT root broker.

Figure A-2 describes a scenario where the OpsCenter PureDisk SPA host uses a remote AT root broker and the OpsCenter server host uses OpsCenter AT.

Figure A-2 Local root broker for OpsCenter server and remote root broker for PureDisk SPA



Note: You need to set up a trust between the two root broker hosts, that is between Host A and Host C.

Setting up a trust between the PureDisk SPA AT host and the OpsCenter Server host

This section provides the steps that are required to set up trust between the OpsCenter Server host and PureDisk SPA AT host.

Note: The OpsCenter Server host has a local AT configuration (OpsCenter AT).

See "About OpsCenter AT" on page 27.

To set up a trust between the OpsCenter server host and PureDisk SPA AT host

- On the OpsCenter server host, run the following command depending on the OpsCenter server operating system :

  These are the default directory paths.

  Windows 64-bit
  ```
  C:\Program Files\Symantec\OpsCenter\server\authbroker\bin>vssat.bat setuptrust --broker <PureDiskSPAAThost:port> --securitylevel high
  ```

  UNIX
  ```
  /opt/VRTSat/bin/vssat setuptrust --broker <PureDiskSPAAThost:port> --securitylevel high
  ```

  The registered port for authentication is 2821. If the AT root broker is configured with another port number, contact your security administrator for more information.

  After successfully setting up a trust between the OpsCenter server host and PureDisk SPA AT host, the following message is displayed:

  ```
  setuptrust

   ----------------------

  ----------------------

  Setup Trust With Broker: PureDiskSPAAThost
  ```

After setting up the trust between OpsCenter Server host and PureDisk SPA host, logon to the OpsCenter GUI and configure PureDisk data collector to start collecting PureDisk data.

See “Configuring PureDisk data collector” on page 297.

Appendix B

Attributes of NetBackup data

This appendix includes the following topics:

- Backup data attributes

Backup data attributes

This section lists all attributes pertaining to data that OpsCenter collects from NetBackup. You can select these attributes while generating custom reports.

The following tables list all NetBackup attributes that OpsCenter collects.

- Table B-1
- Table B-2
- Table B-3
- Table B-4
- Table B-5
- Table B-6
- Table B-7
- Table B-8
- Table B-9
- Table B-10
- Table B-11
- Table B-12

Table B-1 Backup Job Attributes

Data Attributes	Sample Data	Explanation
Agent Server	host.veritas.com	The name of the server where a OpsCenter data collection agent is installed
Backup job Comment	Host cannot be reached	Filled in by the user in the Job Reconciliation page to indicate why a job failed so others can see.
Backup job File Count Deduplication Factor	321	The deduplication file factor for each PureDisk backup job. Meaning that for every 321 files that were backed up only one file was actually stored. (321 to 1 file deduplication rate)
Backup job File Count Deduplication Savings	456	The number of files not needing to be backed up for every backup job in PureDisk because they were already stored with deduplication. Meaning that if 500 files were targeted for backup, only 44 were stored since the saving was 456.
Backup job Is Ignored	Yes/No	Within OpsCenter there is the ability to mark a job as ignored (yes/no). If it is ignored it does not count towards things like success rate or time since last successful backup. This marking of a job as ignored is done in the "Reports > Explorers" section.

Table B-1 Backup Job Attributes *(continued)*

Data Attributes	Sample Data	Explanation
Backup job Protected File Count	400 files	The number of files that are processed in a PureDisk backup. Note that this number is not actually stored since it is before deduplication.
Backup job Protected Size	200GB	The size in byes of a PureDisk backup job before deduplication.
Backup job Size Deduplication Factor	567	The deduplication size factor for each PureDisk backup job. Meaning that for every 567KB that were backed up only 1KB was stored.
Backup job Size Deduplication Savings	345	The number of KB's not needing to be backed up for every backup job in PureDisk because they were already stored with deduplication. Meaning that if 346KB were backed up, the savings of 345KB means only 1 KB was needed to be stored.
Backup job Sub Type	Catalog, File System, MS Exchange, NDMP, Sybase	Each directory under a job and it's type of backup.
Backup job Transport Type	LAN, SAN	The transport that was used to move the backup from backup client to media server
Job Attempt Count	4	The number of times a backup job had to be attempted before being successful or reaching the maximum allowable number of retries

Table B-1 Backup Job Attributes *(continued)*

Data Attributes	Sample Data	Explanation
Job Client	backup-client.veritas.com	The name of a host being backed up as seen by a backup job
Job Directory	C:\, /var, ALL_LOCAL_DRIVES	The file system directory being backed up as seen by a backup job
Job Duration	300 seconds	The amount of time in seconds for a backup to start and finish as seen by a backup job
Job End Time	Tues 3/23/2008 03:34:43	The date and time that a backup ended
Job Error Code	0,1,2,3…	The exit code, status code, or error code for a particular job
Job Expiration Time	Aug 01, 2008 22:03:48	The time at which this job (the image that the job generates) will expire.
Job File Count	300	The number of files a backed up during a backup job
Job Group ID	6114	The group ID that the product group specifies. Note:The secondary ID and the Group ID are intended for the same purpose. These IDs group the jobs in some way that is useful in reporting.
Job Level	Full, Differential Incremental, User Backup	The Schedule Type for the backup job, Full, Incremental, Cumulative, User etc.

Table B-1 Backup Job Attributes *(continued)*

Data Attributes	Sample Data	Explanation
Job Primary ID	5,234,234	A unique number for each backup job in a backup domain that identifies a backup job
Job Secondary ID	5,234,235	When a unique job number is not enough to distinguish a job, a secondary ID may be used. For NBU, this field is the job Process ID
Job Size	2048	The amount in KB that a backup job transferred from client to media server for backing up
Job Start Time	Tues 3/23/2008 02:34:43	The date and time that a backup started
Job Success Rate (Complete and partial)	98	A percent number that is calculated based on the number of jobs that were successful (NetBackup status 0) and partially successful (NetBackup status 1) divided by the total number of jobs ran in that period of time. Example: 98 successful jobs / 100 total jobs (2 failures) = 98%
Job Success Rate (Complete only)	99	A percent number that is calculated based on the number of jobs that were successful (NetBackup status 0) divided by the total number of jobs ran in that period of time. Example: 98 successful jobs / 100 total

Table B-1 Backup Job Attributes *(continued)*

Data Attributes	Sample Data	Explanation
Job Throughput (Kbytes/sec)	3,234	The speed of a backup job in Kbytes/sec. This is the speed of the overall job which takes in to account transfer time from client to media server and media server to disk or tape storage. It is not just the speed of a tape drive.
Job Type	Backup, Restore, duplication, archive, label, erase	The type of operation done by the backup product
Level Type	Full, Differential Incremental, User Backup	The Schedule Type for the backup job grouped into just two options. Full vs. Other
Master Server	nbu-master.example.com	The name of the master server that executed the backup job
Media Server	nbu-media.example.com	The name of the media server that performed the backup job
Policy	Oracle Backup Policy, User Backup Policy, File System Backup Policy	The name of the backup policy as seen by a backup job
Policy Description	‘This policy is for doing Oracle backups’	The user-defined description of a policy as seen by a backup job
Policy Domain Name	NetBackup Policy Domain, PureDisk Policy Domain	The backup product that a backup policy executed a job from
Policy Type	Standard, NT, Oracle, Exchange	The type of policy as seen by a backup job

Table B-1 Backup Job Attributes *(continued)*

Data Attributes	Sample Data	Explanation
Product	NetBackup, PureDisk	The backup product that performs backup, from which OpsCenter collects data
Schedule	(user-defined), ex: Weekly-Fulls, Daily-Incrementals	The name of a schedule which resides within a policy as seen by a backup job
Status	Success, Partial, Failure	A word description for each job that coorelates status codes to their english meaning. All failures are mapped to the word 'Failure'
Storage Unit Name	(user-defined), ex: tld0-hcart-0	The name of a storage unit, which is chosen by a policy to receive and store backups. Storage Units are usually groupings of tape drives within a library or multiple disk locations that are grouped together in pools. This is the storage unit name that was used by a backup job.
Storage Unit Type	Disk, Media Manager (tape)	The type of storage unit used and seen by a backup job

Table B-2 Backup Image Attributes

Data Attributes	Sample Data	Explanation
Backup Image Compression State	Yes/No	A yes/no property of if a backup image stored in the catalog was compressed or not.

Table B-2 Backup Image Attributes *(continued)*

Data Attributes	Sample Data	Explanation
Backup Image Copy Expiration Time	Mon 4/23/2008 4:32:34	The date/time that a backup image copy is set to expire
Backup Image Copy Is Currently Expired	Yes/No	A yes/no property of if a backup image is expired or not. If it is expired it can no longer be restored and that space may be rewritten to by the backup application. If it is not expired it is available for restore.
Backup Image Copy Is Primary	Yes/No	A yes/no property of if a backup image is the primary copy. If the image is a 2nd or greater copy this value would be ‘no’.
Backup Image Copy Media Server	backup-server.veritas.com	The name of the backup server that performed the copy of a backup to a second location.
Backup Image Copy Multiplexed State	True/False	A true/false property as to if the backup image copy was written using multiplexing or not (multiple clients/jobs streamed to one image)
Backup Image Copy Storage Unit Type	Media Manager (tape), Disk	The type of storage unit that the backup image was copied to. This could be disk, tape etc.

Table B-2 Backup Image Attributes *(continued)*

Data Attributes	Sample Data	Explanation
Backup Image Copy Unexpired Fragment Count	30	The number of fragments that make up a complete unexpired backup. A single backup can have 1 or a multiple of fragments which are blocks of data seperated by tape marks on tape or seperated in to separate files on the file system if written to disk.
Backup Image Copy Unique ID	backupclient_23423	A unique ID or key for every backup stored in the catalog. This key or ID can be used to look up an image in the catalog for restore or other activity
Backup Image Encryption State	Yes/No	A yes/no property of if a backup image was encrypted between the backup client and backup media server. This value does NOT represent if tape drive or other encryption was used or not.
Backup Image Expiration Time	Mon 4/23/2008 4:32:34	The date and time that a backup image will expire. When a backup image expires it is no longer available for restore and the space that the backup occupied can be reused for additional backups (overwritten)
Backup Image File Count	432	The actual number of files that are stored within a backup image.

Table B-2 Backup Image Attributes *(continued)*

Data Attributes	Sample Data	Explanation
Backup Image Fragment Expiration Time	Mon 4/23/2008 4:32:34	The date/time that the backup image fragment is set to expire
Backup Image Fragment Is Currently Expired	Yes/No	A yes/no property of if the backup image fragment is expired or not. Even if a backup fragment is expired, that space can not be reused until the whole backup image is expired (disk) or the whole backup tape media is expired (tape)
Backup Image Fragment Is TIR	TIR Info on Disk, TIR Rsv Synthetic Info on Disk	The true image restore status for a backup image fragment. True image restores allow a restore to take place at the directory level without overwriting files that weren't backed up but are still in the directory. For this to be possible a ‘true image restore’ backup image must exist.
Backup Image Fragment Size	2048	The size of the backup image fragment. By default NetBackup uses 1TB fragments (ie no fragments) but this can be configured to different values
Backup Image Fragment Unique ID	backupimagefragment_124	A unique ID associated with every backup image fragment
Backup Image Is Currently Expired	Yes/No	A yes/no property as to if the backup image is expired or not

Table B-2 Backup Image Attributes *(continued)*

Data Attributes	Sample Data	Explanation
Backup Image TIR Status	TIR Info on Disk, TIR Rsv Synthetic Info on Disk	The true image restore status for a backup image. True image restores allow a restore to take place at the directory level without overwriting files that weren't backed up but are still in the directory. For this to be possible a "true image restore" backup image must exist.
Backup Image Type	Regular, Catalog	The type of backup image. Catalog being a NBU catalog image for disaster recovery
Backup Image Unexpired Copy Count	1, 2, 3 etc.	The number of copies that exist for a primary backup image. These are copies that are unexpired and can be used for a restore.
Backup Image Unique ID	backupclient_23423	A unique ID or key for every backup stored in the catalog. This key or ID can be used to look up an image in the catalog for restore or other activity
Backup Image Write End Time	Mon 4/23/2008 4:32:34	The date and time that the backup image was finished writing.
Backup Image Write Start Time	Mon 4/23/2008 4:32:34	The date and time that the backup image began to be written.

Table B-2 Backup Image Attributes *(continued)*

Data Attributes	Sample Data	Explanation
Data Classification Master Server	master-server.veritas.com	The name of the server that classified the backup image in some sort of ranking (gold, silver, bronze etc)
Data Classification Name	Gold, Silver, Bronze, Non-DataClassification-Name	The name of the classification of data
Data Classification Rank	1,2,3,etc	The number ranking that corresponds with the name of data classification. A 1 would mean the data is more important than a 2 for example.

Table B-3 Backup Attempt Attributes

Data Attributes	Sample Data	Explanation
Attempt Duration	3500	The number in seconds that a backup was attempted
Attempt End Time	Mon 4/23/2008 4:32:34	The date and time that a backup attempt ended (each attempt is unique)
Attempt Error Code	0, 1, 2, 3 etc.	The error code that the backup attempt finished with
Attempt File Count	0, 1, 2, 3 etc.	The number of files the backup attempted to process
Attempt Size	2048	The number in KB for the amount an attempted backup tried to process
Attempt Start Time	Mon 4/23/2008 4:32:34	The start time that a backup attempt began

Table B-3 Backup Attempt Attributes *(continued)*

Data Attributes	Sample Data	Explanation
Attempt Status	Success, Partial, Failure	A named status that maps to the error code numbers in the backup application (for example a status 0 in NetBackup is a success, a status 1 is partial and all other numbers are failures)
Attempt Success Rate	98%	The average success rate across all attempts in all backups. Example would be the average of 2 backups were each was attempted 3 times. The success rate would be the success rate average of the 3 attempts within each backup job. (Note that this is different than the success rate across all jobs which does not take in to account attempts)
Attempt Throughput	2048Kbytes/sec	The speed of a backup attempt in Kbytes/sec. This is different than the overall KB/sec for a job which would take in to account all attempts.

Table B-3 Backup Attempt Attributes *(continued)*

Data Attributes	Sample Data	Explanation
Backup Attempt Partial Success Rate	98%	The average success rate across all attempts in all backups but also including partial successes (status 1 in NetBackup). Example would be the average of 2 backups were each was attempted 3 times. The success rate would be the success rate average of the 3 attempts within each backup job. (Note that this is different than the success rate across all jobs which does not take in to account attempts)
Backup Attempt Sequence	1, 2, 3	The attempt number in a sequence. 1 would represent the first attempt, 2 would represent the second attempt etc.
Backup Skipped File Time	Mon 4/23/2008 4:32:34	The date and time that a particular file was skipped over during a backup
Skipped File Code	1	The status code for why that file was skipped (usually a status 1)
Skipped File Reason	File is open by another process	The reason a file was skipped. (Usually because file was in use)
Skipped File Name	C:\Windows\an_open_file.dll	The actual file name that was skipped over during a backup.

Table B-4 Backup Policy Attributes

Data Attributes	Sample Data	Explanation
Backup Policy Domain Master Server	nbu-master.example.com	The host name of the backup application host that contains the backup policy. In the case of NetBackup this is the master server.
Backup Policy Name	Oracle Backup Policy, User Backup Policy, File System Backup Policy	The name of a backup policy that exists in the backup application. Note that this is similar and can be the same as the 'backup job Attribute: Policy' which shows what policy the backup job was executed from. It is different though since this Policy Name simply means that this Policy exists not that anything was executed from it yet.
Backup Policy Type	Standard (UNIX), Windows-NT, Oracle, Exchange	The type of backup policy that exists in the backup application. Note that this is different than the 'backup job Attribute: Policy Type'

Table B-5 File System Attributes

Data Attributes	Sample Data	Explanation
Business Classification	'Business Critical'	User defined field. Can be one of 'Mission Critical', 'Business Critical' or 'Business Support'
File System: OID	asset123 etc.	A user defined field for an object ID of the file system. Typically used as a pairing with an asset management database

Table B-5 File System Attributes *(continued)*

Data Attributes	Sample Data	Explanation
Filesystem Name	C:\Documents and Settings\All Users\	The file system directory being backed up.
Filesystem Type	NTFS, UFS, ZFS, EXT3	A user-defined field (this is not collected automatically) of what type of file system was backed up.

Table B-6 Host Attributes

Data Attributes	Sample Data	Explanation
Host Architecture	SPARC, x86	User defined field (this is not automatically collected) for filling in architecture type such as x86, x86-64, SPARC, POWER, PA-RISC, IA64 etc
Host: Misc Info	Pete's server	A user defined field for inserting any extra information regarding a host
Host: OID	asset123, etc.	A user defined field for inserting an object ID from an asset management database
Hostname	hostname.example.com	The name of the host object that contains file systems.
O.S. Version	10	The version of the operating system. Usually grouped with Operating System name since this will have values like ‘10’ (that is Solaris 10)
Operating System	Windows, Solaris	The operating system name of the host

Table B-7 Backup Media Attributes

Data Attributes	Sample Data	Explanation
Agent Server	ops-agent.example.com	The name of the OpsCenter agent that collected the media information.
Backup Media Allocation Time	Mon 3/4/2008 3:34:34	The date/time that a piece of media was first allocated or had it's first backup written to it. Once the media expires it will have a new allocation date/time when it is reused
Backup Media Available Free Capacity	500,000 KB	How much is left on tape in KB. Value here per sample is either the free capacity if the media is active, or 0 otherwise.
Backup Media Available Total Capacity	19,000,000KB	Total capacity of the tape in KB. Value here per sample is either the total capacity if the media is active, or 0 otherwise.
Backup Media Barcode	JFP000L2	The full barcode as ready by the physical robot. This can be longer than the 6 characters used by a NetBackup Media.
Backup Media Expiration Time	Mon 3/4/2008 3:34:34	The date/time that a backup media is set to expire
Backup Media Free Capacity	500,000 KB	How much is left on tape in KB. This number may be estimated using an algorithm.

Table B-7 Backup Media Attributes *(continued)*

Data Attributes	Sample Data	Explanation
Backup Media Is Active	Yes/No	A yes/no property of a particular tape indicating whether the tape has been sampled in the last two collections.
Backup Media Is Available	Yes/No	A yes/no property of a particular tape indicating whether it can still be written to.
Backup Media Is Current	Yes/No	A yes/no property of if the backup media exists in the current configuration (and not historical)
Backup Media Is Data Expired	Yes/No	A yes/no property of if the backup media has expired data on it or not
Backup Media Is Full	Yes/No	A yes/no property of if the backup media is marked as full (no more backups can be written to it)
Backup Media Is Imported	Yes/No	A yes/no property of if the backup media was imported. Imported media simply means that this paticular backup domain did not originally write the data to the media. This could be due to disaster recovery where the catalog could not be moved from an existing domain so the tapes were read individually to determine what data was on them. It also is commonly used to import Backup Exec media to NetBackup.

Table B-7 Backup Media Attributes *(continued)*

Data Attributes	Sample Data	Explanation
Backup Media Is Physically Expired	Yes/No	A yes/no property of if the physical media is expired or not. Once all the backup images (data) has been expired on a tape that entire cartridge is marked as Physically Expired=Yes and it can be overwritten or used by future backups.
Backup Media Is Total Capacity Estimated	Yes/No	Since capacity of a tape is often estimated using an algorithm. This specifies whether it was actually calculated, or provided exactly by the DP product.
Backup Media Last Read Time	Mon 3/4/2008 3:34:34	A date/time that the backup media was last used to be read (restored)
Backup Media Last Write Time	Mon 3/4/2008 3:34:34	A date/time that the backup media was last used to be written to (duplicates, backups)
Backup Media Library Slot Number	1, 2, 3 etc.	The physical slot number that a given piece of media resides in
Backup Media Multiple Retention Levels Allowed	Yes/No	A yes/no property of if a given piece of tape media will allow for multiple expiration dates. Multiple expiration dates means that the whole tape can not be reused until the last backup has expired on the media.

Table B-7 Backup Media Attributes *(continued)*

Data Attributes	Sample Data	Explanation
Backup Media Multiplexing Allowed	Yes/No	A yes/no property of if multiplexing is allowed on a piece of tape media. Multiplexing means that multiple clients were multiple clients or jobs were backed up to one image so that particular image could have more than one client inside it.
Backup Media Percent Available Free Capacity	0-100%	Calculated value representing (available free capacity /available total capacity) in percentage
Backup Media Percent Free Capacity	0-100%	Calculated value representing (free capacity total capacity) in percentage
Backup Media Percent Used Capacity	0-100%	Calculated value representing (used capacity / total capacity) in percentage
Backup Media Physical Expiration Time	Mon 3/4/2008 3:34:34	The date/time that a piece of media will physically expire (all images on the media) and be able to be reused
Backup Media Retention Level	63072000.00, 31536000.00, 1209600.00	The retention level of the media in number of seconds. Divide by 86400 to get the retention level in days

Table B-7 Backup Media Attributes *(continued)*

Data Attributes	Sample Data	Explanation
Backup Media Snapshot Time	Mon 3/4/2008 3:34:34	The date/time that all the media information was collected from the backup application to OpsCenter. History is kept so a history of the state of all media can be determined.
Backup Media Storage Type	Disk, Tape	The type of storage for a given piece of media (disk or tape)
Backup Media Total Capacity	19,000,000 KB	Total capacity of the tape in KB. This number may be estimated using an algorithm.
Backup Media Type	HCART, DLT, 8MM etc.	The density or type of media. This is used to match what drives the media can go in for a mixed media environment.
Backup Media Unexpired Image Count	1, 2, 3 etc.	The number of images that are unexpired on a given piece of media
Backup Media Used Capacity	500,000 KB	Amount in KB used up in the tape. This value is provided by the DP product and is NOT estimated.
Backup Media Volume Group Name	User defined but defaults to things like ‘000_00002_TLD’	A user defined field for grouping volumes. By default NetBackup assigns the robot number and type so that TLD(2) would read ‘000_00002_TLD’

Table B-7 Backup Media Attributes *(continued)*

Data Attributes	Sample Data	Explanation
Backup Media Volume Path	/disk_staging_file_system/, C:\disk_staging\	The path on disk where backup images are stored.
Disk Pool High Water Mark	95%	This is the high water mark that is set for a Flexible Disk pool, OpenStorage disk pool or PureDisk backend storage pools. When this threshold is reached by the file system on the disk pools backups will not be attempted to that disk location since it will be considered ‘full’.
Disk Pool Low Water Mark	80%	This is the low water mark that is set for a Flexible Disk pool, OpenStorage disk pool or PureDisk backend storage pools. When this threshold is reached by the file system on the disk pools backups will not be sent to the location as often
Disk Pool Master Server	nbu-master.example.com	The name of the NetBackup master server that the disk pool belongs to
Disk Pool Name	netappfi::fas3050-1a, DDPool, etc.	The name of the disk pool which defaults to the disk array string or a user defined value

Table B-7 Backup Media Attributes *(continued)*

Data Attributes	Sample Data	Explanation
Disk Pool Raw Size	69,990.40	The raw size is the size of the disk volume(s) in a disk pool. Raw size does not mean you can actually write to that amount (that's what usable size is) but just tells you there is more possible disk space that could be allocated from raw to usable.
Disk Pool Server Type	AdvancedDisk, SharedDisk	The type of flexible disk that the pool is
Disk Pool Snapshot Time	Mon 3/4/2008 3:34:34	The date/time that a snapshot was taken to produce the backup image that exists in the disk pool
Disk Pool Status	UP, DOWN	Similar to tape drive status, this tells if the disk pool is UP meaning it is usable and can be used or DOWN meaning it is not usable. When in the DOWN state jobs will not attempt to use the disk pool.
Disk Pool Usable Size	1,208,893.44	The usable size is the size of the formatted file system and tells you how much data can be written to the disk pool
Disk Pool Volume Count	4	The number of disk volumes that make up the disk pool

Table B-7 Backup Media Attributes *(continued)*

Data Attributes	Sample Data	Explanation
Media Density	HCART, DLT, 8MM etc.	The type of tape media as defined by the backup application. For NetBackup this is also called the 'density' and specifies what types of drive the tape can go in.
Media Hsize	1024	Optical media header size of a backup image
Media ID	JFP000	The Media ID for a given piece of media, usually a subset of the barcode. For NetBackup this is a 6-digit ID.
Media Image Count	54	The number of backup images on a given piece of tape media or disk pool
Media L Offset	2048	Logical block address of the beginning of the block that a backup image exists
Media Restore Count	0, 1, 2, 3, etc.	The number of times a given piece of backup media has been used for restores.
Media Ssize	1024	Optical media sector size of a backup image.
Partner	A/B	The ID of the opposite side of a optical platter. If on side A of a platter this would show Side B
Product	NetBackup	The backup product that this piece of media belongs to

Table B-7 Backup Media Attributes *(continued)*

Data Attributes	Sample Data	Explanation
Status	Active, Non-active, Suspended, Frozen	The status of a given piece of media. Active meaning it is being used at a given point in time, Frozen meaning errors have occurred on the tape media and it is no longer being used for backups, etc.
Volume Pool ID	1, 2, 3, 4 etc.	The volume pool ID which automatically starts at 1 for the default pool "NetBackup". Things like Scratch Pools or onsite/offsite pools are typically also used and these all have unique volume pool ID's. Many encryption solutions such as Decru and IBM use the volume pool ID to determine what backups to encrypt or not
Volume Pool Name	NetBackup, Scratch, CatalogBackup, MSEO, WORM, etc.	This user defined field is the name of the volume pool that media is placed in to. The default is NetBackup but many others are typically created to segment tapes in to groups
Volume/EMM Database Server	nbu-master.example.com	The name of the EMM server. This is the NetBackup master server.

Table B-8 Tape Library Attributes

Data Attributes	Sample Data	Explanation
Tape Library Agent Product	NetBackup	The backup application that controls the tape drive
Tape Library Agent Server	ops-agent.example.com	The server host name that the OpsCenter agent is installed on that is used to collect tape drive information.
Tape Library Device Database Server	NBU-device-host.example.com	The device database server that is controlling the particular library. This is the Enterprise Media Manager server (EMM).
Tape Library Manufacturer	STK, Quantum, IBM etc.	The manufacturer as determined by the SCSI inquiry string in the backup application.
Tape Library Serial Number	ADIC203100468_LL0	The serial number, unique, to each tape library
Tape Library Slot Count	40, 120, 360	The total number of slots that exist in a tape library
Tape Library Type	Tape Library DLT, Tape Library 8MM, Tape Library ACS	The type of tape library (TLD, ACS, 8MM, 4MM, TLM, TLH etc)
Tape Library Unique ID	0, 1, 2 etc.	The unique number given to each tape library in the EMM database. This ID is put together with the library type in the NBU GUI to show TLD(0), TLD(1) etc.

Table B-9 Tape Drive Attributes

Data Attributes	Sample Data	Explanation
Name	IBM.ULTRIUM-TD2.000	The name of a tape drive as given by the backup application, usually default names are based on SCSI inquiry strings that contain the manufacturer name and model number
Number	0, 1, 2, 3 etc.	The number of a tape drive as given by the backup application which is unique for each physical drive (a number could be shared between media servers though)
Shared	true/false	A simple true/false on weather the tape drive is shared across backup servers or not
Tape Drive Device Host	NBU-device-host.example.com	The device host (Media Server) that the tape drive is connected to.
Tape Drive Is Current	true/ false	A simple true/false on weather the tape drive exists in the current configuration (true) or if it is historical and no longer exists (false)
Tape Drive Serial Number	768ZD03034	The unique serial number for a physical tape drive
Tape Drive Storage Unit Name	dcdell214-dlt-robot-tld-0	The storage unit that the tape drive is assigned to

Table B-9 Tape Drive Attributes *(continued)*

Data Attributes	Sample Data	Explanation
Tape Drive Type	hcart, hcart2, dlt, 8mm etc.	The type of tape drive as defined by the backup application. For NetBackup this is also called the 'density' and specifies what types of tape can go in the drive.
Tape Drive Unique ID for Library	1, 2, 3, 4, 5, 6 etc.	The tape drive number inside the library

Table B-10 Tape Usage Attributes

Data Attributes	Sample Data	Explanation
Storage Unit Group Name	Storage Unit Tape Group	The storage unit group that the storage unit that the tape drive belongs to
Tape Drive Assigned	nbu-host.example.com	The host (Media Server) that the tape drive is assigned to for use at time of tape drive information collection
Tape Drive Control	TLD, ACS, DOWN-TLD, DOWN-ACS etc.	The robot type that is controlling the tape drive and it's associated status of up or down at time of tape drive information collection
Tape Drive Enabled	true / false	A true / false for if the tape drive was enabled at the time of tape drive information collection
Tape Drive In Use	true / false	A true / false for if the tape drive was in use at the time of tape drive information collection

Table B-10 Tape Usage Attributes *(continued)*

Data Attributes	Sample Data	Explanation
Tape Drive Recorded Media ID	VT0036	The tape that was in the drive at the time of tape drive information collection
Tape Drive Snapshot Time	Apr 05, 2008 22:57:17	The date and time that the tape drive information was collected when snapshot was taken

Table B-11 Backup Log Attributes

Data Attributes	Sample Data	Explanation
Backup Log Agent Server	ops-server.example.com	The host name of the OpsCenter server where the database and web interface resides
Backup Log Message	backup of client dcdell211 exited with status 71 (none of the files in the file list exist)	The detailed status messages for each job
Backup Log Source Host	nbu-host.example.com	The host server with the backup application that logged the error message
Backup Log Client	nbu-client.example.com	The backup client that was associated with the logged error message
Backup Log Daemon Name	bptm, ndmpagent, nbpem, bpbrm	The process or daemon name that wrote the error message
Backup Log Job Group ID	5980	The group ID that can be specified by the backup product to group them in a certain way. Note:The secondary ID and the Group ID are basically intended for the same purpose, that is to group the jobs in some way that is useful in reporting.

Table B-11 Backup Log Attributes *(continued)*

Data Attributes	Sample Data	Explanation
Log Primary ID	6021	A unique number for each backup job in a backup domain that identifies what backup job caused the error message to be logged
Log Time	Mon 3/4/2008 3:34:34	The date/time that the error message or log was written to
Product	NetBackup	The backup application name that caused the error message to be created
Severity Code	1, 2, 3, 4 etc.	The severity code of the error message
Type Code	1, 2, 3, 4 etc.	The code representing the type of the log and error message
Version	1, 2, 3, 4 etc.	The version of the log/error message

Table B-12 Agent Monitoring Attributes

Data Attributes	Sample Data	Explanation
Agent Configuration ID	1, 2, 3, 4 etc.	A unique number for each data collection agent under the OpsCenter server
Agent Host	ops-agent.example.com	The host name of the OpsCenter data collection agent
Last Heartbeat	May 04, 2008 10:52:28	The date and time of the last heartbeat from the data collection agent to the OpsCenter server

Table B-12 Agent Monitoring Attributes *(continued)*

Data Attributes	Sample Data	Explanation
Server	ops-server.example.com	The host name of the OpsCenter server where the database and web interface resides
Time Since Agent Last Heartbeat	44	The number of seconds since the last heartbeat from the data collection agent to the OpsCenter server

Appendix C

Man pages for CLIs

This appendix includes the following topics:

- changedbpassword
- configurePorts
- dbbackup
- dbdefrag
- nbfindfile
- opsadmin
- opsCenterAgentSupport
- opsCenterSupport
- runstoredquery
- startagent
- startdb
- startgui
- startserver
- stopagent
- stopdb
- stopgui
- stopserver
- view_exportimport

changedbpassword

`changedbpassword` – This script changes the OpsCenter database password. This is supported only for DBA user and not for guest and server passwords.

SYNOPSIS

```
changedbpassword | [-h|-?|--help]
```

DESCRIPTION

Sybase SQL Anywhere database management system is used to store the OpsCenter data. You require a user name and a password to access the database. The following database user account is shipped with OpsCenter:

DBA	The database administrator account. The `DBA` account is required by the database queries that are used to update the database schema or upgrade to a new product version.

When the tool changes the `DBA` password, it updates a configuration file on the file system so that the server can still access the database. The password is encrypted before it is stored in the configuration file. However, since the server needs to retrieve the password it cannot be stored with a one-way hash. Thus, someone can obtain the password. When the tool is run, the system administrator is advised to check the permissions on the configuration file to ensure that only an administrator can read the file.

OPTIONS

`--h|-?|--help`

Shows the command-line usage statement and exits.

NOTES

Enter the following command to change the database password on Windows:

```
INSTALL_PATH\OpsCenter\server\bin\changedbpassword.bat
```

Enter the following command to change the database password on UNIX:

```
<INSTALL_PATH>/SYMCOpsCenterServer/bin/changedbpassword.sh
```

You are prompted to enter the OpsCenter Administrator's password and the new password that you want to set.

configurePorts

`configurePorts` – This script is used to configure Web server ports on UNIX or Linux systems.

SYNOPSIS

```
configurePorts.sh [-status]|[-httpsPort <httpsPort>][-shutdownPort
<shutdownPort>]
```

DESCRIPTION

The `configurePorts` script is used for the following purposes:

- For configuring https and Tomcat shutdown ports
- For querying the current values for the above ports

OPTIONS

`-status`

Queries the current values for https and Tomcat shutdown ports

This option is to be used exclusive of other attributes.

`-httpsPort <httpsPort>`

Modifies the httpsPort to the new value in web.xml of Tomcat

`- shutdownPort <shutdownPort>`

Modifies the shutdownPort to the new value in web.xml of Tomcat

NOTES

To know the HTTPS port that OpsCenter uses, run the `configurePorts` utility.

Run the following command on Windows:

```
INSTALL_PATH\OpsCenter\gui\bin\goodies\configurePorts.cmd -status
```

Run the following command on UNIX:

```
<INSTALL_PATH>/SYMCOpsCenterGUI/bin/goodies/configurePorts.sh -status
```

dbbackup

`dbbackup` – This script backs up the OpsCenter database and the associated files.

SYNOPSIS

```
dbbackup <DB_BACKUP_DIR> [-v | -restore]
```

DESCRIPTION

The `dbbackup` script backs up the OpsCenter database files, database password file, and encryption key file .

OPTIONS

DB_BACKUP_DIR

(Required) *DB_BACKUP_DIR* is the directory where the OpsCenter database files, database password file, and encryption key file are backed up to, or restored from. *DB_BACKUP_DIR* should be an absolute path.

`-v`

Option to validate the database after backup

`- restore`

Option to restore database, database password file, and the encryption key file from the *backupDir* to the respective database , database password file, and encryption key file directory.

Note: Veritas strongly recommends that you change the password for the admin user account after you restore the OpsCenter database.

NOTES

On Windows, you perform backups with the `dbbackup.bat` batch file.

The backup script creates the following files in the backup directory: `vxpmdb.db` and `vxpmdb.log`

Data spaces are started when the main database is started; therefore, starting and stopping the data space file is not required.

EXAMPLES

The following command backs up the OpsCenter database, database password file, and encryption key file to the `my_db_backups` directory on Windows:

```
INSTALL_PATH\OpsCenter\server\bin\dbbackup.bat C:\my_db_backups
```

The following command backs up the OpsCenter database, database password file, and encryption key file to the `my_db_backups` directory on UNIX:

```
<INSTALL_PATH>/SYMCOpsCenterServer/bin/dbbackup.sh /my_db_backups
```

dbdefrag

`dbdefrag` – This script defragments the OpsCenter database.

SYNOPSIS

```
dbdefrag
```

DESCRIPTION

The `dbdefrag` script is used to defragment the OpsCenter database.

OPTIONS

Not applicable

NOTES

To defragment the OpsCenter database run the following commands.

Run the following command on Windows:

```
INSTALL_PATH\OpsCenter\server\bin\dbdefrag.bat
```

Run the following command on UNIX:

```
<INSTALL_PATH>/SYMCOpsCenterServer/bin/dbdefrag.sh
```

Note: The `dbdefrag` command requires the OpsCenter services to be stopped. This can cause the command to fail in an OpsCenter cluster setup. To successfully defragment the database in a cluster, you need to freeze the nodes before you run the `dbdefrag` command.

See "About OpsCenter clusters" on page 139.

---

nbfindfile

`nbfindfile` – This utility searches for files or folders based on simple search criteria. This utility must be run on the master server and not the OpsCenter Server.

SYNOPSIS

nbfindfile -c *client_name*[,...] -p *search_pattern* [-s *mm/dd/yyyy* [*HH:MM:SS*] | -s_ut *unix_time*] [-e *mm/dd/yyyy* [*HH:MM:SS*] | -e_ut *unix_time*] [-backupid *backup_id*] [-policy *policy_name*] [-keyword "*keyword_phrase*"] [-extn *file_extn*[,...]] [-st *sched_type*] [-pt *policy_type*] [-kb_min *min_size_kb*] [-kb_max *max_size_kb*] [-mtime_min *mm/dd/yyyy* [*HH:MM:SS*]] [-mtime_max *mm/dd/yyyy* [*HH:MM:SS*]] [-atime_min *mm/dd/yyyy* [*HH:MM:SS*]] [-atime_max *mm/dd/yyyy* [*HH:MM:SS*]] [-ctime_min *mm/dd/yyyy* [*HH:MM:SS*]] [-ctime_max *mm/dd/yyyy* [*HH:MM:SS*]] [-only_dirs | -only_files] [-max_results *number*] [-I] [-l [-ctime | -atime] | -raw] [-help | -h]

On UNIX and Linux systems, the directory path to this command is /usr/openv/netbackup/bin/admincmd/

On Windows systems, the directory path to this command is *<install_path>*\NetBackup\bin\admincmd\

DESCRIPTION

The `nbfindfile` command lets you search files or folders based on simple search criteria like file name and path including wildcard and backup date range. Users can specify a set of clients, possibly belonging to different master servers, for which backups are to be searched. You can specify advanced search criteria including policy type, schedule type, policy name, policy associated keywords, file extensions, file modification date range, and file size.

OPTIONS

`-atime`

When used with the `-l` option, `-atime` displays the last access time in place of the last modification time.

`-atime_max` *mm/dd/yyyy* [*HH:MM:SS*]

Specifies the maximum last access time of objects to be returned. The default is infinite.

`-atime_min` *`mm/dd/yyyy`* `[`*`HH:MM:SS`*`]`

Specifies the minimum last access time of objects to be returned. The default is 01/01/1970 00:00:00.

`-backupid` *`backup_id`*

The backup ID of the backup image that should be searched.

`-c` *`client_name`*`[,...]`

Specifies the names of the NetBackup clients whose backups need to be searched. The client names must be specified as they appear in the NetBackup configuration. Multiple clients can be specified as a list that is separated by commas.

`-ctime`

When used with the *-l* option, `-ctime` displays the last change time in place of the last modification time.

`-ctime_max` *`mm/dd/yyyy`* `[`*`HH:MM:SS`*`]`

Specifies the maximum last change time of objects to be returned. The default is infinite.

`-ctime_min` *`mm/dd/yyyy`* `[`*`HH:MM:SS`*`]`

Specifies the minimum last change time of objects to be returned. The default is 01/01/1970 00:00:00.

`-e` *`mm/dd/yyyy`* `[`*`HH:MM:SS`*`] | -e_ut` *`unix_time`*

Specifies the end date for the search. Backups that occurred at or before the specified date and time are searched. The default is the current date and time.

`-extn` *`file_extn`*`[,...]`

Returns only the files with the specified extensions. For example, `-extn txt,do*,jp?`.

`-h | -help`

Displays usage information.

`-i`

Performs case insensitive matching.

`-kb_max` *`max_size_kb`*

Specifies the maximum size in kilobytes (1024 bytes) of files to be returned. The default is infinite.

`-kb_min` *`min_size_kb`*

Specifies the minimum last modification time of objects to be returned. The default is 01/01/1970 00:00:00.

`-keyword "keyword_phrase"`

Searches only the backup images that contain a matching keyword phrase are searched. The keyword phrase can contain wildcards (*, ?) and square bracket expressions. Examples are `[Kk]ey*`, `[a-z]e?`, and `[!K]ey`.

`-l`

Displays output in long list format. The default condition is the last modification time of objects.

`-max_results number`

Specifies the maximum number of results to be displayed. The default is infinite.

`-mtime_max mm/dd/yyyy [HH:MM:SS]`

Specifies the maximum last modification time of objects to be returned. The default is infinite.

`-mtime_min mm/dd/yyyy [HH:MM:SS]`

Specifies the minimum last modification time of objects to be returned. The default is 01/01/1970 00:00:00.

`-only_dirs | -only_files`

Specifies the type of objects to be returned.

`-p search_pattern`

Specifies the search pattern. File and directory entries matching this pattern are displayed.

`-policy policy_name`

Searches only backup images that are created using the specified policy.

`-pt policy_type`

Searches only the backups with the specified policy type. Valid values for *policy_type*: Any, Standard, FlashBackup, MS-Windows, NDMP, FlashBackup-Windows.

`-r`

Displays raw output.

`-s mm/dd/yyyy [HH:MM:SS] | -s_ut unix_time`

Specifies the start date for the search. Backups that occurred at or after the specified date and time are searched. The default is 30 days before the end date.

`-st sched_type`

Specifies a schedule type for the image selection. The default is any schedule type. Valid values, in either uppercase or lowercase, are as follows:

- ANY

- FULL (full backup)
- INCR (differential-incremental backup)
- CINC (cumulative-incremental backup)
- UBAK (user backup)
- UARC (user archive)
- SCHED
- USER (user backup and user archive)
- NOT_ARCHIVE (all backups except user archive)

opsadmin

`opsadmin` – This script is used to monitor/start/stop the OpsCenter services on UNIX or Linux systems

SYNOPSIS

```
opsadmin.sh {start|stop|monitor}
```

DESCRIPTION

The `opsadmin` script is used for monitoring/starting/stopping the OpsCenter services.

OPTIONS

`start`

Starts all OpsCenter services. These services include OpsCenter database, OpsCenter server, and Web server services.

`stop`

Stops all OpsCenter services. These services include OpsCenter database, OpsCenter server, and Web server services.

`monitor`

Monitors all OpsCenter services and also Authentication Service) and PBX Veritas Private Branch Exchange) services. This option is not available for Windows.

NOTES

`opsadmin`

`opsadmin.sh` resides by default in the `<INSTALL_PATH>/SYMCOpsCenterServer/bin` directory.

EXAMPLES

EXAMPLE 1

The following command starts all OpsCenter services:

```
<INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh start
```

EXAMPLE 2

The following command monitors OpsCenter services:

```
<INSTALL_PATH>/SYMCOpsCenterServer/bin/opsadmin.sh monitor
```

opsCenterAgentSupport

`opsCenterAgentSupport` – This script collects OpsCenter Agent configuration files and logs.

SYNOPSIS

```
opsCenterAgentSupport
```

DESCRIPTION

The `opsCenterAgentSupport` script collects OpsCenter Agent configuration files and logs for troubleshooting.

OPTIONS

Not applicable

NOTES

Run the following commands to execute the support scripts for OpsCenter Agent.

Run the following command on Windows:

```
INSTALL_PATH\OpsCenter\Agent\bin\opsCenterAgentSupport.bat
```

You can view the following status messages on the command prompt:

```
Stopping the OpsCenter Agent Service...

Support Directory Exists. This will be deleted...

Support Directory Deleted...

Created Support Directory... Zipping Support Folder...

Please collect Support.zip file from
C:\PROGRA~1\Symantec\OPSCEN~1\Agent\temp\support.zip

Starting the OpsCenter Agent...

C:\Program Files\Symantec\OpsCenter\Agent\bin>
```

opsCenterSupport

`opsCenterSupport` – This script collects OpsCenter server configuration files and logs for troubleshooting.

SYNOPSIS

```
opsCenterSupport
```

DESCRIPTION

`opsCenterSupport` is a script used for collecting OpsCenter server configuration files and logs for troubleshooting.

OPTIONS

Not applicable

NOTES

Run the following command to collect OpsCenter server configuration information:

Run the following command on UNIX:

```
<INSTALL_PATH>/SYMCOpsCenterServer/bin/opsCenterSupport.sh
```

Run the following command on Windows:

```
INSTALL_PATH\OpsCenter\server\bin\opsCenterSupport.bat
```

You can view the following statuses on the command prompt:

```
Support Directory Exists. This will be deleted...

Support Directory Deleted...

Created Support Directory...

SupportDir=E:\OPSCEN~1\OPSCEN~1\server\temp\support

Collecting Installed Paths Collecting System Properties

Collecting Memory & Processor Properties

Collecting Disk Allocation for OpsCenter Installed Drive

Collecting Directory Structure for OpsCenter Collecting version file
Collecting Version File...

Getting Customized Collections...
```

```
Do you want to Collect Configuration files [y/n]: (y)y

Do you want to Collect Application Log files [y/n]: (y)y

Do you want to Collect OpsCenter GUI(147) Log files [y/n]: (y)y

Collecting 147 files...

Do you want to Collect OpsCenter Server(148) Log files [y/n]: (y)y

Collecting 148 files...

Do you want to Collect db Log files [y/n]: (y)y

Collecting db logs...

Do you want to Collect WebServer Log files [y/n]: (y)y

Collecting WebServer logs...

Do you want to Collect setEnv file [y/n]: (y)y

Collecting setenv file...

Do you want to Collect Database files [y/n]: (y)y

Collecting vxpmdb file...

Collecting vxpmdb.log file...

If this is an Upgrade scenario Do you want to Collect Old Database
files and logs [y/n]: (y)y

Enter the location where the database files of the previous OpsCenter
version were stored. The opsCenterSupport utility backs up these
files at
OPSCENTER_INSTALL_DIR/server/temp/OpsCenterServerSupport/upgrade

You can revert to this database version in case of upgrade failure.

For example: C:\\Program
Files\Symantec\OpsCenter_SavedData\OpsCenter\server\db\data

or

:/var/symantec/OpsCenterServer_backup/SYMCOpsCenterServer/db/data

Collecting old db files
```

Note: If the location that you have provided is not valid, the utility dipslays the following message:

```
The opsCenterSupport utility cannot back up the database files of
the previous OpsCenter version because the file location that you
have provided is not valid
```

```
Collecting upgrade logs...

Do you want to collect OpsCenter usage data [y/n]: (y)y
```

Note: If you opt for this option, the utility collects the Telemetry data.

```
Starting usage collection...

Do you want to collect OpsCenter startup config files [y/n]: (y)y

Zipping Support Folder...

Please collect Support.zip file from
E:\OPSCEN~1\OPSCEN~1\server\temp\support.zip
```

runstoredquery

`runstoredquery` –

SYNOPSIS

```
runStoredQuery <Report Name> <User Name> <Domain Name> <Domain Type>
[<Output Type> pdf | csv]
```

DESCRIPTION

The `runstoredquery` script runs saved customSQL and the OpsCenter Administrator generates output in the desired format.

OPTIONS

`Report Name`

Name of the report (surrounded with double-quotes)

Example: runStoredQuery "My Report" admin OpsCenterUsers vx pdf

`User Name`

Name of the user who has saved the report

`Domain Name`

Domain name for the user

`Domain Type`

Domain type for the user

`Output Type`

Report output type (pdf/csv). The default is csv.

EXAMPLE

```
runStoredQuery "My Report" admin OpsCenterUsers vx pdf
```

startagent

`startagent` – This script starts the OpsCenter Agent service.

SYNOPSIS

```
startagent
```

DESCRIPTION

The `startagent` script is used to start the OpsCenter Agent service.

OPTIONS

Not applicable

NOTES

Enter the following command to start the OpsCenter Agent service on Windows:

```
INSTALL_PATH\OpsCenter\Agent\bin\startagent.bat
```

startdb

`startdb` – This script starts the OpsCenter database.

SYNOPSIS

```
startdb
```

DESCRIPTION

The `startdb` script is used to start the OpsCenter database.

OPTIONS

Not applicable

NOTES

To start the database server, enter the following command on Windows:

```
INSTALL_PATH\OpsCenter\server\bin\startdb.bat
```

To start the database server, enter the following command on UNIX:

```
<INSTALL_PATH>/SYMCOpsCenterServer/bin/startdb
```

startgui

`startgui` – This script is used to start the OpsCenter Web server service.

SYNOPSIS

```
startgui.sh
```

DESCRIPTION

The `startgui` script is used for starting the OpsCenter Web server service.

OPTIONS

Not applicable

NOTES

The following command starts the OpsCenter WebServer service on Windows:

```
INSTALL_PATH\OpsCenter\gui\bin\startgui.cmd
```

The following command starts the OpsCenter WebServer service on UNIX:

```
<INSTALL_PATH>/SYMCOpsCenterGUI/bin/startgui.sh
```

startserver

`startserver` – This script starts the OpsCenter Server.

SYNOPSIS

```
startserver
```

DESCRIPTION

The `startserver` script is used to start the OpsCenter Server.

OPTIONS

Not applicable

NOTES

Run the following command to start the OpsCenter Server on Windows:

```
INSTALL_PATH\OpsCenter\server\bin\startserver.bat
```

Run the following command to start the OpsCenter Server on UNIX:

```
<INSTALL_PATH>/SYMCOpsCenterServer/bin/startserver
```

stopagent

`stopagent` – This script is used to stop the OpsCenter Agent.

SYNOPSIS

```
stopagent
```

DESCRIPTION

The `stopagent` script is used to stop the OpsCenter Agent.

OPTIONS

Not applicable

NOTES

Run the following command to stop the OpsCenter Agent on Windows:

```
<INSTALL_PATH>\OpsCenter\Agent\bin\stopagent.bat
```

stopdb

`stopdb` – This script is used to stop the OpsCenter database.

SYNOPSIS

```
stopdb
```

DESCRIPTION

The `stopdb` script is used to stop the OpsCenter database.

OPTIONS

Not applicable

NOTES

Run the following command to stop the OpsCenter database on Windows:

```
INSTALL_PATH\OpsCenter\server\bin\stopdb.bat
```

Run the following command to stop the OpsCenter database on UNIX:

```
<INSTALL_PATH>/SYMCOpsCenterServer/bin/stopdb
```

stopgui

`stopgui` – used to stop the OpsCenter Web server service.

SYNOPSIS

```
stopgui.sh
```

DESCRIPTION

The `stopgui` script is used for stopping the OpsCenter Web server service.

OPTIONS

Not applicable

NOTES

The following command stops the OpsCenter Web server service on Windows:

```
INSTALL_PATH\OpsCenter\gui\bin\stopgui.cmd
```

The following command stops the OpsCenter Web server process on UNIX:

```
<INSTALL_PATH>/SYMCOpsCenterGUI/bin/stopgui.sh
```

stopserver

`stopserver` – This script stops the OpsCenter Server.

SYNOPSIS

```
stopserver
```

DESCRIPTION

The `stopserver` script is used to stop the OpsCenter Server.

OPTIONS

Not applicable

NOTES

Run the following command to stop the OpsCenter Server on Windows:

```
INSTALL_PATH\OpsCenter\server\bin\stopserver.bat
```

Run the following command to stop the OpsCenter Server on UNIX:

```
<INSTALL_PATH>/SYMCOpsCenterServer/bin/stopserver
```

view_exportimport

`view_exportimport` – The `view_exportimport` script is used to import, export, alias, or merge your CSV, TSV, or XML files. You can create CSV, TSV, or XML files that describe the views that you want to create. You can then import the CSV, TSV, or XML file into OpsCenter by using this utility.

SYNOPSIS

```
view_exportimport {-i|-e|-m|-a} {-f <file name>} {-type <xml|csv|tsv}
{-host <host name>} {-port <port number>} {-usr <user name>} {-pass
<password>} {-domain <domain>} {-domaintype <type>} [-l <logfile
name>] [-v <Level #>]
```

DESCRIPTION

You can use the OpsCenter console to create views, but you may find it faster and more convenient to create CSV, TSV, or XML files that describe the views that you want to create. You can then import the CSV, TSV, or XML file into the OpsCenter database. This script lets you import, export, alias, or merge a CSV, TSV, or XML file.

Note: You can also use the View Builder GUI to import, export, merge, or alias a CSV, TSV, or XML file. See the OpsCenter View Builder help for more information.

See the Appendix titled *Creating views using CSV, TSV, and XML files* for detailed information on how to create CSV, TSV, or XML files.

OPTIONS

`-i`

Imports the view structure as defined in the XML, CSV, or TSV file into the OpsCenter database. It can import multiple views at a time.

`-e`

Exports the entire view structure existing in the OpsCenter database into XML, CSV, or TSV files. You can update these XML, CSV, or TSV files according to the business needs and then import these files in the OpsCenter database.

This option exports all the views that are present in the OpsCenter database.

`-m`

Merge multiple objects simultaneously that are saved in XML, CSV, or TSV file. Note that the source hosts and destination hosts that you merge must be of the same type (masterservers/mediaservers/clients).

A merge objects file (XML, CSV, or TSV) contains the following object details:

First column	DB ID of the resultant object
Second column	Primary display name of the resultant object
Third column	DB ID of the object that is merged
Fourth column	Primary display name of the object that is merged

Here is a typical example of a file that contains details of objects to be merged:

First Column	Second Column	Third Column	Fourth Column
1500	host1	1000	host1.veritas.com
2100	host2.abc.com	2355	host2
4000	host3	3000	10.209.19.10

Note: After successfully merging the two objects, the object being merged (second object in a record) is deleted and the resultant object is retained. However all aliases that are designated for both objects - object being merged and resultant object - are retained and assigned to the resultant object.

`-a`

Using the -a option, you can give an alternate name to a host. You can alias multiple hosts simultaneously that are saved in XML, CSV, or TSV file.

Caution: The alias names should be compatible with your hosts' DNS names. Alternatively, they should be compatible with the names by which they are known to applications such as NetBackup and Backup Exec. For example: If you use an alias that is unknown to NetBackup, the explorer stops collecting information from the NetBackup host. It attempts to collect data from a host with the alias name.

A host alias file (XML, CSV, or TSV) typically contains the following details:

First column	DB ID of the object
Second column	Primary display name of the resultant object
Third column	Alias to be created for the host. You can create multiple aliases for a host, which you can add in the subsequent columns.

Here is a typical example of a file that contains aliases to be created for hosts:

First Column	Second Column	Third Column	Fourth Column	Fifth Column
1500	host1	host1.diablo.com	host1.veritas.com	
2100	host2	host2.river.com	10.100.22.55	host2.veritas.com
4000	host3	host3.tunnel.com		

`-f <file name and path>`

Path of the XML, CSV, or TSV file to be used for import, export, merge, alias. Note that the file name is case-sensitive.

In case of export, information from the OpsCenter database is exported. Hence, you need to specify the name or path of the file that gets exported in *<file name and path>*.

`--type <xml | csv | tsv>`

Type of file format (Default: xml)

`--host <host name>`

Host name of the OpsCenter server to connect to (default: localhost)

`--port <port number>`

OpsCenter Server port number (default: 1556)

`--usr <user name>`

The username for connecting to the OpsCenter server (default: `admin`)

`--pass <password>`

The password for connecting to the OpsCenter server (default: `password`)

`--domain <domain>`

The domain to which the user belongs (default: OpsCenterUsers)

`--domaintype <type>`

Domain type. For example: vx/nt/nis etc. (default: vx)

`-l <logfile name>`

Specify name of the log file that is generated.

`-v [Level #]`

Specify the logging level [0:Off, 1:Severe, 2:Warning, 3:Info, 4:Config, 5:Fine, 6:Finer, 7:Finest, 8:All]

`--h|-?|--help`

Shows the CLI usage statement and exits.

EXAMPLES

EXAMPLE1

Run the following command on Windows to import the `import-add-object.xml` file in the OpsCenter database:

```
INSTALL_PATH\OpsCenter\server\bin>view_exportimport.bat -i -f
"C:\Users\Administrator\Desktop\import-add-object.xml" --type xml
--host win2k8r2.abc.veritas.com --port 1556 --usr admin --pass
password --domain OpsCenterUsers --domaintype vx
```

Run the following command on UNIX to import the `import-add-object.xml` file in the OpsCenter database:

```
<INSTALL_PATH>/SYMCOpsCenterServer/bin/view_exportimport.sh -i -f
"C:\Users\Administrator\Desktop\import-add-object.xml" --type xml
--host win2k8r2.abc.veritas.com --port 1556 --usr admin --pass
password --domain OpsCenterUsers --domaintype vx
```

EXAMPLE2

Run the following command on Windows to export all the OpsCenter views as `importviews.xml` file in `C::`

```
INSTALL_PATH\OpsCenter\server\bin>view_exportimport.bat -e -f
"C:\importviews.xml" --type xml --host win2k8r2.abc.veritas.com --port
1556 --usr admin --pass password --domain OpsCenterUsers --domaintype
vx
```

Run the following command on UNIX to export all the OpsCenter views as `importviews.xml` file in `opt` directory:

```
/opt/SYMCOpsCenterServer/bin/view_exportimport.sh -e -f
"/opt/importviews.xml" --type xml --host win2k8r2.abc.veritas.com
```

```
--port 1556 --usr admin --pass password --domain OpsCenterUsers
--domaintype vx
```

Appendix D

Creating views using CSV, TSV, and XML files

This appendix includes the following topics:

- About using CSV, TSV, and XML files to create views
- About creating CSV files
- About creating TSV files
- About creating XML files
- XML DTD structure
- DTD elements
- DTD <application> element
- DTD <objects> and <object> elements
- DTD <attribute> elements
- DTD <view> element
- DTD <node> elements
- DTD <aliaslevel> elements
- Examples of XML files
- Example 1: Adding an object
- Example 2: Adding a view
- Example 3: Updating an object

- Example 4: Merging objects

About using CSV, TSV, and XML files to create views

You can use the OpsCenter Analytics console to create views. However, you may find it faster and more convenient to create the CSV, TSV, or XML files that describe the views that you want to create.

This Appendix describes how you can create views using CSV, TSV, or XML files.

You can then import, export, merge, or alias the CSV, TSV, or XML file into the OpsCenter database from the OpsCenter View Builder GUI or by using the `view_exportimport` script.

Refer to the Opscenter View Builder help for information on how to import, export, merge, or alias a CSV, TSV, or XML file using the OpsCenter View Builder GUI.

Information on how to import, export, merge, or alias a CSV, TSV, or XML file to OpsCenter Analytics by using the `view_exportimport` utility is available.

About creating CSV files

You can create views in OpsCenter Analytics by creating and importing the comma-separated values (CSV) file that describes the views. You can create the CSV files in a text editor or Microsoft Excel and save the file as *`filename`*`.csv`. Note that you can only create objects of type Generic when you create views using a CSV file.

Note: You can export and import view structures using the CSV file. However, you cannot export or import attributes that are collected by OpsCenter data collectors using a CSV file.

A CSV file typically contains the following details:

First column	View type View Type must be one of the following: ■ **Master Server** ■ **Client** ■ **Policy** ■ **File System** **Note:**
Second column	Name of the view
Third column	Level of the view (hierarchy). The third column and subsequent columns contain the name that you give to each level. You can have as many levels as you want, which must be specified in the third column or subsequent columns in the CSV file.
Last column	Host name **Note:** The last column must be the host name. If the last column of a row is not the host name, the specific row or entry is ignored and not considered.

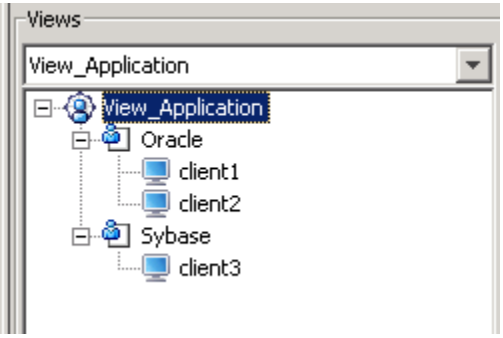
The CSV file contains comma-separated values. Each row defines the hierarchy of one host.

The following is the format of a sample CSV file. This CSV file contains only one level of view.

```
Client, View_Application, Oracle, client1
Client, View_Application, Oracle, client2
Client, View_Application, Sybase, client3
```

Figure D-1 shows the view that is created when you import the sample CSV file.

Figure D-1 Sample view

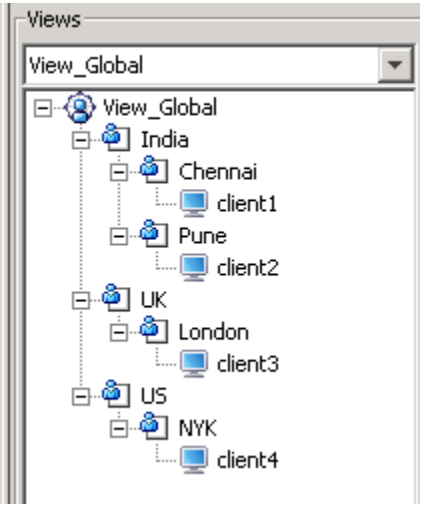


The following is the format of a sample CSV file containing two levels of view.

```
Client, View_Global, India, Chennai, client1
Client, View_Global, India, Pune, client2
Client, View_Global, UK, London, client3
Client, View_Global, US, NYK, client4
```

Figure D-2 shows the multi-level view that is created when you import the sample CSV file that contains two levels of view.

Figure D-2 Sample multi-level view



Note: If you create a view using a CSV file that already exists in OpsCenter Analytics, the view gets deleted. You cannot modify an existing view by using a CSV file.

About creating TSV files

You can create views in OpsCenter Analytics by creating and importing the Tab-separated values (TSV) file that describes the views. You can create the TSV files in any text editor, Excel etc. and save the file as `filename.tsv`. Note that you can only create objects of type Generic when you create views using a TSV file.

Note: You can export and import view structures using the TSV file. However, you cannot export or import attributes using a TSV file.

A TSV file typically contains the following details:

First column	View type View Type must be one of the following: ■ **Master Server** ■ **Client** ■ **Policy** ■ **File System**
Second column	Name of the view
Third column	Level of the view. The third column and subsequent columns contain the name that you give to each level. You can have as many levels as you want, which must be specified in the third column or subsequent columns in the TSV file.
Last column	Host name **Note:** The last column must be the host name. If the last column of a row is not the host name, the specific row or entry is ignored and not considered.

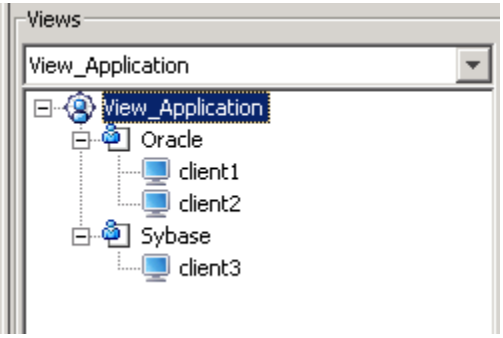
The TSV file contains tab-separated values. Each row defines the hierarchy of one host.

The following is the format of a sample TSV file containing one level of view.

```
Client View_Application Oracle client1
Client View_Application Oracle client2
Client View_Application Sybase client3
```

Figure D-3 shows the view that is created when you import the sample TSV file.

Figure D-3 Sample view

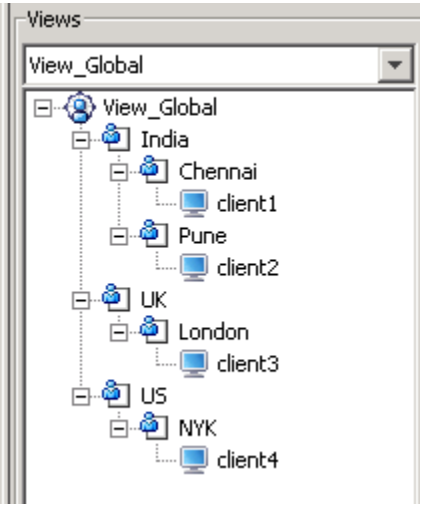


The following is the format of a sample TSV file containing two levels of view.

```
Client  View_Global India Chennai client1
Client View_Global India Pune client2
Client View_Global UK London client3
Client View_Global US NYK client4
```

Figure D-4 shows the multi-level view that is created when you import the sample TSV file that contains two levels of view.

Figure D-4 Sample multi-level view



Note: If you create a view using a TSV file that already exists in OpsCenter Analytics, the view gets deleted. You cannot modify an existing view by using a TSV file.

About creating XML files

You can create views in OpsCenter Analytics by creating and importing the XML files that describe the views.

By using the XML API, you can import IT asset data and their relationships that you maintain through in-house or third-party systems (for example, Peregrine `AssetCenter`). The XML import capability enables you to import arbitrary groupings of master servers, clients, policies, and file systems. For example, you can import the groupings that are defined around business units by using the XML import capability.

Note: You can export and import view structures using the XML file. However, the attributes that are collected by data collectors like Network Name, OS etc. are not exported or imported. Only user-defined attributes like location, `isTagged` etc. can be exported or imported using an XML file.

You can create user-defined attributes from the OpsCenter GUI (**Settings > Configuration > Object Type**).

See "About managing Object Types in OpsCenter" on page 223.

The following examples illustrate the practical use of OpsCenter Analytics XML import functionality.

Example 1: You can use a spreadsheet to define Host A as the marketing host and Host B as the sales host. By importing the XML using the View Builder GUI or the `view_exportimport` utility, you can import the data in the spreadsheet, create a view using the imported data, and chargeback the services based on business units.

Example 2: You can build a view of a chart of accounts that shows server ownership by company department for chargeback purposes. With large enterprises, the chart of accounts can easily exceed a thousand. Entering this data into OpsCenter Analytics is cumbersome and error prone. By importing the XML using the View Builder GUI or the `view_exportimport` utility, you can import this data from your local system. While importing the data into OpsCenter Analytics, you can continue with the maintenance of data in the local system.

Importing data using XML is the best example of OpsCenter Analytics's open architecture that enables integration with other systems. See the following sections to know how you can create views in an XML file.

XML DTD structure

The XML DTD is constructed as follows:

```
<?xml version="1.0"?>
<!-- Note : This DTD is provided for viewing the XML
with tools like Microsoft's Internet Explorer.
if it fails to work, the DTD should be replaced by the DTD
provided with documentation. -->
<!DOCTYPE application [

<!ELEMENT application (objects?,view*,user*,mergeitems*)>
 <!ATTLIST application version CDATA #REQUIRED>
<!ELEMENT objects (object+)>
<!ELEMENT view (node*,aliaslevels?)>
 <!ATTLIST view identifier CDATA #REQUIRED>
 <!ATTLIST view type CDATA #REQUIRED>
 <!ATTLIST view action (add|delete|update|declare) "declare">
 <!ATTLIST view id ID #IMPLIED>
<!ELEMENT object (attribute*)>
 <!ATTLIST object id ID #IMPLIED>
 <!ATTLIST object name  CDATA #IMPLIED>
 <!ATTLIST object action (add|delete|update|declare) "declare">
```

```
 <!ATTLIST object type CDATA #IMPLIED>
 <!ATTLIST object dbid CDATA #IMPLIED>
<!ELEMENT node (object?,node*)>
 <!ATTLIST node id ID #IMPLIED>
 <!ATTLIST node action (add|delete|declare) "declare">
 <!ATTLIST node object IDREF #IMPLIED>
 <!ATTLIST node parents IDREFS #IMPLIED>
<!ELEMENT aliaslevels (level*)>
 <!ATTLIST aliaslevels action (add|update|delete|declare) "declare">
<!ELEMENT level EMPTY>
 <!ATTLIST level number CDATA #REQUIRED>
 <!ATTLIST level label CDATA #REQUIRED>
<!ELEMENT mergeitems (mergeitem+)>
<!ELEMENT mergeitem EMPTY>
 <!ATTLIST mergeitem toobject IDREF #IMPLIED>
 <!ATTLIST mergeitem fromobject IDREF #IMPLIED>
<!ELEMENT attribute (name,value*)>
 <!ATTLIST attribute name CDATA #IMPLIED>
 <!ATTLIST attribute value CDATA #IMPLIED>
<!ELEMENT name (#PCDATA)>
<!ELEMENT value (#PCDATA)>
]>
```

DTD elements

The elements of the XML DTD are as follows:

- See “ DTD <application> element” on page 666.
- See “DTD <objects> and <object> elements” on page 667.
- See “ DTD <attribute> elements” on page 668.
- See “DTD <view> element” on page 668.
- See “DTD <node> elements” on page 669.
- See “DTD <aliaslevel> elements” on page 670.

DTD <application> element

The `<application>` element is the root level tag that encloses rest of the XML definitions. This tag contains `<objects>` tag and zero or more other tags, namely `<view>` and `<mergeitems>` in this order.

DTD <objects> and <object> elements

The `<objects>` tag holds the definition of the objects to be acted on, and so contains a number of `<object>` tags. Each object tag represents a single asset in the OpsCenter Analytics configuration.

Each object has the following properties that define it in the XML file:

`id`	The ID of the object. This value is not the actual object ID but a unique value that identifies the object in the working XML.
`name`	The actual name of the object.
`action`	The action to be taken for the object.
`add`	Add the object.
`delete`	Delete the object. Note that for an object, delete operation does not delete the object from the OpsCenter database. For a view or node, the delete operation deletes the view or node but does not delete the related object from the OpsCenter database.
`update`	Update the properties of the object.
`declare`	No action. You may need this object in XML at a later stage. In some cases, another object already present in the OpsCenter Analytics configuration may be required to take action using this object (for example, setting it as a master object for a newly defined object). To be able to do that, the object must first be “declared” in the XML.
`type`	The type of the object. Currently, an object can be one of the following types: ■ **MASTER_SERVER** ■ **CLIENT** ■ **POLICY** ■ **MASTER_MEDIA** ■ **MASTER_CLIENT** ■ **MASTER_MEDIA_CLIENT** ■ **MEDIA_CLIENT** ■ **FILE_SYSTEM** ■ **MEDIA_SERVER**

GENERIC	A generic object such as a hierarchical node in the View tree.
FILE_SYSTEM	A file system object.
MEDIA_CLIENT	Host that acts as both media server and client.
MEDIA_SERVER	Host that is only a media server.
POLICY	A policy object
dbid	The database ID of the object. This field is optional and is written when the data is exported. It is very useful in cases where you want to update or declare objects. Because the dbid is an ID in the database, lookups are much faster. So, it is recommended to use the dbid to speed up the overall XML processing whenever possible. This ID is entirely database dependant and is created when the object is created. One cannot specify an object to have a specific dbid.

DTD <attribute> elements

Each object has a set of attributes that defines it in the OpsCenter Analytics configuration. These attributes are defined in the <attribute> tag. Each attribute tag can contain a <name> tag and multiple <value> tags. The <name> tag defines the name of the attribute and a <value> tag defines a value for it. The attribute tags can be defined in several ways, such as in the following example:

```
<attribute>
  <name>attrname</name>
  <value>attrvalue 1</value>
</attribute>
```

Or:

```
<attribute name="attrname" value="attrvalue"/>
```

DTD <view> element

The <view > tag defines a view in the OpsCenter Analytics configuration. A view is a hierarchical association of objects. So, this tag contains multiple nested <node > tags that define the nodes of the tree. The tree tag contains the following properties:

`identifier`	The name of the view.
`action`	The action to be taken for the tree.
`add`	Create a new view.
`delete`	Delete an existing view.
`update`	Update the view.
`declare`	No action. This property defines an already existing tree in the XML.
`id`	Deprecated and no longer used.
`type`	Specifies the view type

DTD <node> elements

A node can be viewed as a container that holds a single object. The same object can be contained in more than one node in the tree, but a node can contain only one object. The properties of nodes are as follows:

`id`	The unique identifier of the node in XML.
`object`	The ID of the object that the node contains. This value is the ID given to that object in the working XML file and not the actual ID. There can be multiple parents for a node. In such a case, separte the parent node IDs by spaces in the XML.
`parent`	The node ID of this node's parent node. The current node is added as a child to the specified parent node. This value is the ID given to the parent node in the working XML file and not the actual ID.
`action`	The action to be taken for the node.
`add`	Add the node to the tree.
`delete`	Delete the node.
`declare`	No action. You may need this node in XML at a later stage. In some cases, another node already present in the OpsCenter Analytics configuration may be required to take action using this node (for example, adding a child node). To use the node in XML as a parent for some other node, the node must first be "declared" in the XML.

DTD <aliaslevel> elements

In OpsCenter Analytics, you can set aliases or labels for levels in views. Using the `<aliaslevel>` element, you can specify names for view levels. A view contains number levels. By default, the levels are labeled Level 1, Level 2, and Level 3, which is not intuitive. To name the levels as per your requirements, you can use the `<aliaslevel>` element.

`action`	The action to be taken for the `aliaslevel`.
`add`	Add the level number and level label.
`update`	Update the level number and level label.
`delete`	Delete the level number and level label.
`declare`	Default action.
`level number`	Enter the level number like 1 or 2.
`level label`	Enter the label for the level.

Examples of XML files

You can create several types of XML files, including the following:

- Add an object.
  See "Example 1: Adding an object" on page 670.
- Add a view.
  See "Example 2: Adding a view" on page 671.
- Update an object
  See "Example 3: Updating an object" on page 672.
- Merge two objects into a single object.
  See "Example 4: Merging objects" on page 674.

Example 1: Adding an object

Example 1, when imported into OpsCenter Analytics, adds the object `Detroit` under the `MyMasterServers` view.

(The DTD header has been snipped.)

```
<application version="2.0">
<objects>
<object id="o3" name="master.abc.domain.com" action="declare"
type="MASTER_SERVER" dbid="58">
<attribute>
<name>Location</name>
<value>Illinois</value>
</attribute>
</object>
<object id="o4" name="master1" action="declare"
type="MEDIA_CLIENT" dbid="61" />
<object id="o5" name="dailybackuppolicy" action="declare"
type="POLICY" dbid="62" />
<object id="o6" name="weeklybackuppolicy" action="declare"
type="POLICY" dbid="63" />
<object id="o7" name="monthlybackuppolicy" action="declare"
type="POLICY" dbid="64" />
</object>
<object id="o10" name="Detroit" action="add" type="GENERIC" />
</objects>
<view identifier="MyMasterServers" type="Master Server"
action="update">
<node id="n268" action="add" object="o9" />
<node id="n269" action="add" object="o3" parents="n268" />
</view>
</application>
```

Example 2: Adding a view

Example 2, when imported into OpsCenter Analytics, the `TestMasterServers` view is created with top-level branch as `Chicago` that contains a host object `master1.abc.domain.com`.

(The DTD header has been snipped.)

```
<application version="2.0">
<objects>
<object id="o3" name="master.abc.domain.com" action="declare"
type="MASTER_SERVER" dbid="58">
<attribute>
<name>Location</name>
<value>Illinois</value>
</attribute>
```

```
</object>
<object id="o4" name="master2" action="declare"
type="MEDIA_CLIENT" dbid="61" />
<object id="o5" name="dailybackuppolicy" action="declare"
type="POLICY" dbid="62" />
<object id="o6" name="weeklybackuppolicy" action="declare"
type="POLICY" dbid="63" />
<object id="o7" name="monthlybackuppolicy" action="declare"
type="POLICY" dbid="64" />
<object id="o9" name="Illinois" action="declare"
type="GENERIC" dbid="66">
<attribute>
<name>Name</name>
<value>Illinois</value>
</attribute>
</object>
<object id="o10" name="Chicago" action="declare"
type="GENERIC" dbid="67">
<attribute>
<name>Name</name>
<value>Chicago</value>
</attribute>
</object>
</objects>
<view identifier="MyMasterServers" type="Master Server"
action="update">
<node id="n268" action="add" object="o9" />
<node id="n269" action="add" object="o3" parents="n268" />
</view>
<view identifier="TestMasterServers" type="Master Server"
action="add">
<node id="n271" action="add" object="o10" />
<node id="n272" action="add" object="o3" parents="n271" />
</view>
</application>
```

Example 3: Updating an object

Example 3, when imported into OpsCenter Analytics, updates the Location attribute of master1.abc.domain.com (to Illinois). The Name attribute of Chicago object is also updated (to Chicago).

(The DTD header has been snipped.)

```
<application version="2.0">
<objects>
<object id="o3" name="master.abc.domain.com" action="update"
type="MASTER_SERVER" dbid="58">
<attribute>
<name>Location</name>
<value>Illinois</value>
</attribute>
</object>
<object id="o4" name="master3" action="declare"
type="MEDIA_CLIENT" dbid="61" />
<object id="o5" name="dailybackuppolicy" action="declare"
type="POLICY" dbid="62" />
<object id="o6" name="weeklybackuppolicy" action="declare"
type="POLICY" dbid="63" />
<object id="o7" name="monthlybackuppolicy" action="declare"
type="POLICY" dbid="64" />
<object id="o9" name="Illinois" action="declare"
type="GENERIC" dbid="66">
<attribute>
<name>Name</name>
<value>Illinois</value>
</attribute>
</object>
<object id="o10" name="Chicago" action="update"
type="GENERIC" dbid="67">
<attribute>
<name>Name</name>
<value>Chicago</value>
</attribute>
</object>
</objects>
<view identifier="MyMasterServers" type="Master Server"
action="update">
<node id="n268" action="add" object="o9" />
<node id="n269" action="add" object="o3" parents="n268" />
</view>
</application>
```

Example 4: Merging objects

Example 4, when imported into OpsCenter Analytics, merges object “o2” into the object “o1.” Objects “o1” and “o2” represent the same host. One has a host name of “hostA.veritas.com” and the other has the host name as “hostXYZ.somedomain.veritas.com.” While merging object “o2” into object “o1,” you can specify “hostXYZ.somedomain.veritas.com” as an alias for object “o1.” After merging object “o2,” it is deleted and only object “o1” remains.

In Example 4, a host object has the hostname “hostA.veritas.com” which also goes by the name “hostXYZ.somedomain.veritas.com.” The XML export of this object looks like the following:

(The DTD header has been snipped.)

```
<object id="o1" action="declare" type="Host" dbid="50">
</object>
```

This example has another host object whose host name is “`hostA`” and whose XML export is as follows:

```
<object id="o2" action="declare" type="Host" dbid="70">
</object>
```

Now, whenever a particular OpsCenter Analytics Agent refers to a host as “`hostA`,” the OpsCenter Analytics Server identifies the object since one of its host names matches this object. After this object update, you can merge the two hosts with the following syntax:

```
<mergeitems>
<mergeitem toobject = "o1" fromobject = "o2"/>
</mergeitems>
```

Merging of two hosts moves all data from the `hostA` object to the newly updated object and deletes the `hostA` object.

Appendix E

Error messages in OpsCenter

This appendix includes the following topics:

- OpsCenter Error Messages

OpsCenter Error Messages

Following table lists OpsCenter error messages with the possible root cause of the problem and details about the solutions that can be applied.

Table E-1 OpsCenter Error codes with Description

Error Code	Description	Root Cause	Solution
401	The user does not have permissions of the selected view.	This error occurs when user ‘A’ saves the report with a given view ‘V’ (master/media/client) in public folder. Later in time, if administrator changes permission on the view ‘V’ for user ‘A’, then next time on running the report by user ‘A’, will raise this exception.	Make sure that user running the report has permission on the view selected. If no permission for the view then user can edit the report and re-run by selecting available views.
402	Provided user details are invalid.	This error occurs when user ‘A’ saves the report ‘S’ in public folder and later in time if administrator delete user ‘A’ , and if User ‘B’ or Admin runs the saved report ‘S’ , will fail to run because the original user does not exists.	`There is no direct way to solve this problem. Best way is to re-create the report and re-run it.`

Table E-1 OpsCenter Error codes with Description *(continued)*

Error Code	Description	Root Cause	Solution
10500	OpsCenter Database Error	This error signifies OpsCenter database related generic issue. (Connectivity, Timeouts . . .etc.)	Check Database is up and running. Do basic sanity around database. Contact Support with screenshot and relevant log-files.
10501	OpsCenterDb PK Violation around:{<table/entity>} while executing {<add/delete-API>}	Primary Key violation / Duplicate entries were tried to insert in the same table.	Contact Support with screenshot and relevant log-files
10502	OpsCenterDb FK Violation around:{<table/entity>} while executing {<add/delete-API>}	This error signifies Foreign Key violation or Reference records do not exist.	Contact Support with screenshot and relevant log-files.
10503	OpsCenterDb Column value issue around:{<table/entity>} while executing {<add/delete-API>}	This error occurs when NULL value is added for Non-Nullable columns in database.	Contact Support with screenshot and relevant log-files.
10504	OpsCenterDb Column Truncation around:{<table/entity>} while executing {<add/delete-API>}	This error occurs when a value is too large, and does not fit into database column.	Contact Support with screenshot and relevant log-files.
10505	OpsCenterDb Constraints failed around:{<table/entity>} while executing {<add/delete-API>}	This error occurs when database constraints failed. This can occur under multiple reasons. Eg.Entity based constraint or trigger based constraints.	Contact Support with screenshot and relevant log-files.
10506	OpsCenterDb SQL Parsing Error around:{<table/entity>} while executing {<add/delete-API>} DBAL component consists of generated code from the database.	This error resembles that the generated code has a problem and is a serious issue.	Contact Support with screenshot and relevant log-files.
10507	OpsCenterDb Query Execution failed around:{<table/entity>} while executing {<add/delete-API>} DBAL component consists of generated code from the database.	This error resembles that the generated code has a problem and is a serious issue.	Contact Support with screenshot and relevant log-files.
Messages related to Reporting Services			

Table E-1 OpsCenter Error codes with Description *(continued)*

Error Code	Description	Root Cause	Solution
10802	The selected view for this report is not available. The view that was associated with this report might have been deleted.	A view which is used in the saved report has been deleted. View can be deleted without validating that it is associated with a report.	Edit the saved report and select the views which are currently available and try again.
10804	You have no permissions to see the report {0}.	The user accessing the report may not have permission to run/view the report. User is actually trying to access the private reports of other user by modifying the URL parameters.	User can see reports created by that user itself or the reports from a public folder.
10805	Filter {0} is not defined in XML definition file. Please define the filter in FilterAttributeList.xml.	Incorrectly or undefined filter may cause the problem.	Undefined filter should be defined properly in filter definition xml file.
10806	Failed to load the XML definition file {0}. Please contact customer support for assistance.	Each report is associated with xml definition file. This error occurs when there is no corresponding definition file for a report.	Make sure that OPS_INSTALL_DIR/definitions/reports.zip file is not corrupted or modified.
10807	Failed to read the XML file.	XML definition file may be in use and therefore cannot be read.	Make sure that no process is using the XML definition file.
10808	Failed to execute stored procedure {0}.	Stored procedure may fail due to formation of invalid query inside the procedure.	Based on stack trace message, it is possible to figure out where the problem exists in the stored procedure.
10809	Failed to get the database connection.	DBAL component exposes connection to reporting.	Stack trace helps in finding the root cause.
10810	Definition mapping for report ID {0} is failed to load from the database. Please check report_cannedReportMapping table for the mapping.	Each report has an entry in report_cannedReportMapping table. This table keeps the mapping between report ID and XML file. If there is no mapping for the running report, then this error occurs.	Make sure that the table has entry for the running report.
10811	Failed to fetch the schedule workflow details from the database.	Exception occurred while running the query at the database level.	Stack trace helps in finding the root cause.

Table E-1 OpsCenter Error codes with Description *(continued)*

Error Code	Description	Root Cause	Solution
10814	Failed to fetch the report condition list from the database for report ID {0}.	Exception occurred while running the query at the database level.	Stack trace helps in finding the root cause.
10815	Failed to fetch the saved report details from the database for report {0}.	Exception occurred while running the query at the database level.	Stack trace helps in finding the root cause.
10816	Failed to fetch the user details from the database for report {0}.	Exception occurred while running the query at the database level.	Stack trace helps in finding the root cause.
10817	Failed to fetch the custom saved report details from the database for report {0}.	Exception occurred while running the query at the database level.	Stack trace helps in finding the root cause.
10818	Failed to fetch the custom template category mapping list from the database.	Exception occurred while running the query at the database level.	Stack trace helps in finding the root cause.
10819	Failed to fetch the custom template from the database for {0} category.	Exception occurred while running the query at the database level.	Stack trace helps in finding the root cause.
10820	Failed to fetch saved report list from the database for user {0}.	Exception occurred while running the query at the database level.	Stack trace helps in finding the root cause.
10821	Failed to fetch the information for upgrade report from the database for user {0}.	Exception occurred while running the query at the database level.	Stack trace helps in finding the root cause.
10822	Failed to process the query result for report {0}.	Each result set is processed before sending to the GUI. This error message conveys that the logic that is written to process the result is broken.	This should be escalated to CFT/engineers to understand the problem.
10823	Failed to execute the query at the database for report {0}.	Exception occurred while running the query at the database level.	Stack trace helps in finding the root cause.
10824	Failed to execute the query for report {0}.	Exception occurred while running the query at the database level.	Stack trace helps in finding the root cause.
10825	Failed to update report {0}.	Exception occurred while updating the report at the database level.	Stack trace helps in finding the root cause.

Table E-1 OpsCenter Error codes with Description *(continued)*

Error Code	Description	Root Cause	Solution
10826	Failed to save report {0}.	Exception occurred while saving the report at the database level.	Stack trace helps in finding the root cause.
10828	Failed to delete report {0}.	Exception occurred while deleting the report at the database level.	Stack trace helps in finding the root cause.
10830	Failed to update the schedule workflow in the database.	Exception occurred while updating the workflow at the database level.	Stack trace helps in finding the root cause.
10831	Failed to update the Finish Time of schedule workflow in the database.	Exception occurred while updating the schedule finish time at the database level.	Stack trace helps in finding the root cause.
10832	Failed to create report schedule {0} in the database.	Exception occurred while running the query at the database level.	Stack trace helps in finding the root cause.
10833	Failed to delete schedule workflow in the database.	Exception occurred while running the query at the database level.	Stack trace helps in finding the root cause.
10834	Failed to delete reports from schedule workflow.	Exception occurred while running the query at the database level.	Stack trace helps in finding the root cause.
10835	No report schedule is found.	This error occurs while adding reports to a report schedule which does not exists in the database.	Re-create the report schedule and try to add reports to this newly created schedule.
10836	Tree ID and Tree Type information is missing from saved report {0}.	This can be an upgrade issue. Each report that is migrated should have a tree ID and tree type information (if it is view based report) in report_savedreport table.	Re-create the saved report and re-run it.
10837	Time column ID {0} used in definition is not present in the database.	Either the time filter is wrongly defined in the definition .xml file or reports.zip file under OPS_INSALL_DIR/definitions folder is corrupted.	Make sure reports.zip file is not corrupted. If the problem still persists, escalate to engineering/CFT.
10838	Time condition column ID {0} used in the definition file is not present in the database.	Either the time filter is wrongly defined in the definition .xml file or reports.zip file under OPS_INSALL_DIR/definitions folder is corrupted.	Make sure reports.zip file is not corrupted. If the problem still persists, escalate to engineering/CFT.

Table E-1 OpsCenter Error codes with Description *(continued)*

Error Code	Description	Root Cause	Solution
10839	You do not have permissions to run any report with the specified view. However, you can edit the view filter for which you have permissions and can re-run the report.	The report with selected view cannot be run because the user does not have permission to access the selected view.	Edit the report and select the view available from the drop down menu and re-run the report.
10840	View filter is not applicable for the report.	This error is due to inconsistency in the definition. Example: Suppose user has created and saved a report with some view. In the next release, if the support for the view is removed from the definition, then there is a mismatch in saved definition versus XML definition. If there is a mismatch in the saved definition and XML definition, then it means that database is not updated properly to reflect the new change.	In such cases, edit the report and re-run by applying any valid views that are applicable.
10841	Vault view is not applicable for the report.	The report does not support the vault view filtering.	Edit the report and select the view available from the drop down menu and re-run the report.
10842	Policy view is not supported for this report. However, you can edit the view filter and re-run the report.	The report does not support the policy view filtering.	Edit the report and select the view available from the drop down menu and re-run the report.
10843	Exchange view is not supported for this report. However, you can edit the view filter and re-run the report.	The report does not support the exchange view filtering.	Edit the report and select the view available from the drop down menu and re-run the report.
10844	Master Server view is not supported for this report. However, you can edit the view filter and re-run the report.	The report does not support the Master Server view filtering.	Edit the report and select the view available from the drop down menu and re-run the report.

Table E-1 OpsCenter Error codes with Description *(continued)*

Error Code	Description	Root Cause	Solution
10845	Client view is not supported for this report. However, you can edit the view filter and re-run the report.	The report does not support the Client view filtering.	Edit the report and select the view available from the drop down menu and re-run the report.
10846	File system view is not supported for this report. However, you can edit the view filter and re-run the report.	The report does not support the file system view filtering.	Edit the report and select the view available from the drop down menu and re-run the report.
10848	No definition of report {0} is found.	Missing XML definition for the report.	Make sure that OPS_INSTALL_DIR/definitions/reports.zip file is not corrupted or modified.
10849	Please upload the .csv file with client name, to run the report.	This error can occur while running client coverage report, if user runs the report without uploading the .csv file.	The .csv file with client names should be uploaded while running the client coverage report.
10850	Report {0} does not have support to run with {1} view. View in this context refers to Distribution/Ranking/Historical/Tabular.	This error can occur in case of upgraded reports Or when reports.zip file is corrupted.	Make sure that OPS_INSTALL_DIR/definitions/reports.zip file is not corrupted or modified. If problem persists, upgraded report needs to be re-created.
10851	Report {0} does not have correctly defined java type.	This error can occur while running any Java based reports. This can occur if reports.zip file is corrupted.	Make sure that OPS_INSTALL_DIR/definitions/reports.zip file is not corrupted or modified. If problem persists, escalate to CFT/Engineering.
10852	Java type executor {0} for report {1} should be appropriately created and used for each java-based report.	This error can occur while running any Java-based reports. This can occur if reports.zip file is corrupted.	Make sure that OPS_INSTALL_DIR/definitions/reports.zip file is not corrupted or modified. If problem persists, escalate to CFT/Engineering.
10853	Report {0} already exists in the selected folder. Either save the report with a different name or overwrite the existing report.	User cannot save the report which already exists; else he needs to overwrite the existing once.	Save report with a different name.

Table E-1 OpsCenter Error codes with Description *(continued)*

Error Code	Description	Root Cause	Solution
10854	The folder does not exist for saving report {0}. Each report should be saved under the specific folder.	This error occurs when user tries to save a report in a folder while at the same time someone has deleted that folder.	Re-save a report under the existing folder.
10855	No node is present in view node for report ID {0}.	This error occurs when there is major problem with the data in the database. However, it will occur only in case of saved report.	Re-create the report and save it.
10856	Failed to execute report {0} at view level. Reporting component uses view layer component for view related queries.	This error signifies that there is an issue with the view component.	Stack trace helps in finding the root cause.
10857	Failed to fetch child nodes at view level. Reporting component uses view layer component for view related queries.	This error signifies that there is an issue with the view component.	Stack trace helps in finding the root cause.
10858	Failed to fetch the report tree.	Failed to execute the query, by the view component while fetching the view tree.	Stack trace helps in finding the root cause.
10859	Failed to delete a report.	Failed to execute the query, by the view component while deleting the report node from database.	Stack trace helps in finding the root cause
10860	Failed to add report to the view tree. .	Failed to execute the query, by the view component while adding the report to the report tree.	Stack trace helps in finding the root cause
10861	Failed to update report to the view tree.	Failed to execute the query, by the view component while updating the report to the report tree.	Stack trace helps in finding the root cause.
10862	Failed to fetch report details at view level.	Failed to execute the query, by the view component while fetching the report details from the report tree.	Stack trace helps in finding the root cause.
10863	Column {0} does not exist in the database.	This error occurs when an incorrectly defined column exists in the XML definition.	Make sure reports.zip file under {OPS_INSTALL_DIR}/definitions folder is not corrupted. If problem persists, escalate to CFT/Engineers.

Table E-1 OpsCenter Error codes with Description *(continued)*

Error Code	Description	Root Cause	Solution
10864	Report schedule {0} already exists. Please specify a different name.	Duplicate report schedule names are not allowed.	Save the report schedule with a different name.
10865	Data collection failed for selected Master Servers.	This error occurs only when we run explicit data collection for License report (Capacity and Traditional). It implies that agent is not able to collect the data from the Master Server.	Make sure that agent is configured correctly. Stack trace helps in finding the root cause.
10866	An error has occurred while running the licensing report.	This error occurs only while running license report (Capacity /Traditional). It resembles that an error has occurred while performing File IO operation.	Stack trace helps in finding the exact issue.
10867	Generating license report is failed due to {0}.	This error is caused while running nbdeployutil. Capacity license report is generated via nbdeployutil executable and any error thrown will be the root cause.	From the log file, check if any exception is thrown by nbdeployutil. Since this is an executable, it creates its own log file which is shown as a link in the License report GUI.
10868	Generating license report is failed. From the log file, check if any exception is thrown by nbdeployutil.	Capacity license report generation depends on nbdeployutil executable.	From the log file, check if any exception is thrown by nbdeployutil. Since this is an executable, it creates its own log file which is shown as a link in the License report GUI.
10869	No Master Server is configured for collecting the licensing data.	License report (Capacity /Traditional) can be executed only when at least one Master Server is configured in OpsCenter.	Configure Master Server for which license report needs to be generated.
10870	License Data Collection or Report Generation is already in progress.	This error occurs when user tries to run license report multiple times at the same time. User cannot run license report multiple times at any given point in time.	Make sure you run the report only when previous request for run is completed.
10871	Failed to fetch licensing details from the database.	This error occurs when Licensing report (Capacity /Traditional) fails to perform some of the database activity like fetching status of the failed master server.	Log file will help in finding the exact root cause.

Table E-1 OpsCenter Error codes with Description *(continued)*

Error Code	Description	Root Cause	Solution
10872	License report is not generated as none of the Master Server license data collections is successful.	License Report (Capacity /Traditional) will be generated only when at least one Master Server data collection (Licensing specific) is successful. Report is not generated if none of the Master Server collection is successful.	Make sure the data collection (Licensing Specific) is successfully collected for at least one Master Server.
10873	Unable to send the email. Please verify the email address, SMTP server settings and then try again.	Email component failed to send email because SMTP configuration might be incorrect or email ID specified might be incorrect.	If not specified, set SMTP configuration from Settings > Configuration > SMTP configuration page.
10875	Failed to create report {0}.	This error occurs when charting component fails to create the chart while exporting and emailing a report.	Log file will help in finding the root cause of failure.
10876	PDF format is not supported for report {0}.	This error occurs when a report not supported for PDF format is added in the scheduled report and expected to be exported in PDF format.	Remove the non-PDF format supported report from scheduled report if the export format expected is PDF.
10877	Only HTML export format is supported for report {0}.	This error occurs when a HTML format supported report is added in the scheduled report and expected to be exported other than HTML format.	If the export format selected (while defining the report schedule) is HTML, then make sure you add only HTML supported reports in the schedule.
10878	Query builder failed to build a query for report {0}.	Query Builder forms the metadata required to build actual SQL query. This meta data is then passed to DBAL component to get the actual query.	This error denotes serious problem in the Query builder forming SQL meta data. This problem needs to be diagnosed from the log file to find the root cause.
10879	One or more reports failed to execute and therefore cannot be sent by email.	This error will occur when dashboard is emailed and one or more reports failed to be exported in specified format (PDF/HTML/CSV). For eg, week at a glance report do not support PDF format.	While emailing the dashboard report, make sure that all the reports under dashboard supports the given export format.

Table E-1 OpsCenter Error codes with Description *(continued)*

Error Code	Description	Root Cause	Solution
10880	The selected combination of report parameters for this report is not valid. However, you can edit the report, change the parameters and then run the report.	Custom reporting allows user with a lot of combinations to create customized report. However, not all combinations are valid.	Example: Y1-axis Report data and Y2-axis Report data cannot be same. Edit the created custom report and specify valid parameters.
10881	Failed to execute specified SQL-- {0}. Please make sure the SQL syntax is correct.	This error signifies that SQL specified by the user is invalid.	Log file will help in finding the exact problem of the SQL.
10882	Failed to read file {0} from report.zip. Each report is associated with XML definition file.	This error is due to non-availability of particular XML file for a given report.	Make sure reports.zip file under {OPS_INSTALL_DIR/definitions} folder is not corrupted. If problem persists, escalate to CFT/Engineers.
10883	Invalid table join set ID {0} specified in the report {1}.	This error indicates that definition is incorrect for specified report.	This issue needs to be escalated to CFT/Engineers to get XML definition corrected.
10884	Failed to load chargeback definition XML file.	This error is due to invalid XML definition for chargeback reports.	Make sure the definition file reports.zip is not corrupted. If problem persists, escalate to CFT/Engineers.
10885	Failed to execute chargeback report {0}.	This error is due to failure to fetch chargeback variable/formulae from the database.	Log file helps in finding the exact root cause.
10887	Report {0} already exists in some other folder. Please save the report with a different name.	You cannot overwrite the report that exists in another folder. Duplicate report names are not allowed even across different folders. It should be unique across the saved report tree.	Save the report with a different name.
10888	Please select report-on parameter by editing the report as it is a mandatory field.	This error signifies that report-on parameter is mandatory field while creating custom report.	Select appropriate report-on parameter by editing the report.

Table E-1 OpsCenter Error codes with Description *(continued)*

Error Code	Description	Root Cause	Solution
10889	You do not have permission to execute the SQL-- {0}. Custom SQL allows user to fire any SQL as per choice.	This can be harmful if user fires delete/update query on OpsCenter database and thus getting corrupted. This error denotes that user do not have permission to execute the specified SQL. However he can fire update/delete on tables which he has created on OpsCenter Database.	User needs to fire only those queries which will NOT corrupt OpsCenter database
10890	Please select Y-axis report-data parameter by editing the report as it is a mandatory field.	This error signifies that Y-axis report data parameter is mandatory field while creating a custom report.	Select appropriate Y-axis report data parameter by editing the report.
10891	Please select Time-basis parameter by editing the report as it is a mandatory field.	This error signifies that Time-basis parameter is mandatory field while creating custom report.	Select appropriate Time-basis parameter by editing the report.
10892	Please select Y-axis function parameter by editing the report as it is a mandatory field.	This error signifies that Y-axis function parameter is mandatory field while creating custom report.	Select appropriate Y-axis function parameter by editing the report.
10893	Please select X-axis Report-data parameter by editing the report as it is a mandatory field.	This error signifies that X-axis Report data parameter is mandatory field while creating custom report.	Select appropriate X-axis report data parameter by editing the report.
10894	One or more selected columns are invalid. Please edit the report and remove invalid columns.	This error signifies that one or more columns in custom tabular report created are invalid. The label of the invalid columns is usually “-“. Remove all such columns that are selected and re-run the report. This issue usually occurs in case of upgraded reports. If one or more columns are not mapped correctly while upgrading, then such issue occurs.	Remove all invalid columns and re-run the report.
Messages related to SCL			

Table E-1 OpsCenter Error codes with Description *(continued)*

Error Code	Description	Root Cause	Solution
10901	An error has occurred. Please contact your system administrator.	This is an unknown error. This is the rarest scenario for which the root cause cannot be predicted. It is an unknown error for Opscenter.	Log will help in finding the cause.
10902	The specified master server already exists.	This error occurs when we try to add master server that already exists in OpsCenter.	Do not try to add same master server twice.
10903	Master Server with the same display name already exists.	Each master server should have a unique display name associated with it.	Try giving another display name.
10904	The specified Master Server is not a valid NetBackup Master Server.	Trying to add NetBackup media server to OpsCenter.	Try adding NBU Master Server, instead.
10905	Action not permitted. Please verify that the OpsCenter host is listed in NetBackup configuration file (host properties or bp.conf) and/or trust is established in case of NBAC.	This error occurs when you try to add a master server for which there is no entry of OpsCenter host in bp.conf file. The other problem could be insufficient trust between OpsCenter and NetBackup in NBAC case.	Make sure bp.conf file has proper entry for OpsCenter host. In case of NBAC, proper trust setup should be established.
10906	Deletion is already in progress for the specified Master Server.	This error occurs if user tries to delete Master Server for which the delete request is already in progress.	Do not perform delete operation multiple times. Wait till the previous delete operation completes.
10908	The specified Master Server could not be located. Please check if the machine is reachable and the NetBackup services are running.	This error occurs while adding a Master Server which is not reachable from the OpsCenter.	Make sure NetBackup host is reachable from OpsCenter and vice-a-versa via ping command.
10909	The specified Master Server could not be located. Please check if the machine is reachable and the NetBackup services are running.	This error occurs while adding a Master Server which is not reachable from OpsCenter and vice-a-versa. Or when NBSL service on NBU master is not running. Or there might be firewall configuration blocking OpsCenter-NetBackup communication.	Make sure NetBackup host is reachable from OpsCenter and vice-a-versa via ping command. Also check if NBSL service on NetBackup Master is running. And if firewall is configured, check TCP port 1556 is opened on OpsCenter and NetBackup machine.

Table E-1 OpsCenter Error codes with Description *(continued)*

Error Code	Description	Root Cause	Solution
10910	Unable to connect with NetBackup event channel. Please check if the NetBackup services are running.	If nbevtmgr (NetBackup Event Manager) service is not running.	Make sure that nbevtmgr is up and running on NetBackup Master Server.
10911	Unable to create consumer for the event.	This can occur, when OpsCenter Server process is out of resources. This is a symptom of OpsCenter going out of resource.	Root cause might be Object leak/Thread leak.
10912	The specified Master Server is currently disabled.	This is only in case of reconnection master server task is present and at the same time someone disabled and enabled the Master Server.	This is just a safe guard.
10913	Invalid GUID found for NetBackup Master Server.	NBSL is not getting the GUID from the NetBackup.	Check the NBSL logs.
10914	NetBackup is not initialized. Please check if the NetBackup services are running and NetBackup is correctly initialized.	NBSL is not passing the Product Name.	Ensure that NBSL service are up and running. Also verify there is no error during start-up of service.
10915	OpsCenter machine is not reachable from the specified Master Server.	This error occurs when OpsCenter is not reachable from NBSL/NetBackup Or there might be firewall configuration blocking OpsCenter- NetBackup communication. This indicates that OpsCenter is able to communicate to NBSL but reverse communication is not working.	Make sure OpsCenter is reachable from NetBackup via ping command. Also check if firewall is configured, check port 1556 is opened on NetBackup machine.
10916	The specified agent already exists.	This error is caused when we try to add same agent host, twice.	Do not add agent host multiple times.
10917	The specified data collector already exists.	Each agent is associated with one or more data collector that user can create. This error occurs when data collector with existing data collector name is created.	Save each data collector with a unique name.

Table E-1 OpsCenter Error codes with Description *(continued)*

Error Code	Description	Root Cause	Solution
10925	The specified agent is already deleted.	This occurs when one user is editing the agent and another user deleted the same agent from another session. Basically one user is working on stale data.	User will see the refreshed list by again accessing the agent home page.
10926	The specified data collector is already deleted. Come back to agent home page and user will see the refreshed list.	This occurs when one user is editing the data collector and another user has deleted the same data collector from another session. Basically one user is working on stale data.	User will see the refreshed list by again accessing the agent home page.
10927	The specified agent has been updated by other user. Please try again.	While updating agent information, there are chances that multiple users try to modify the same agent at the same time. This can make database inconsistent and hence the error message.	Try updating after some time assuming that other user has completed updating.
10928	The specified data collector has been updated by other user. Please try again.	While updating data collector information, there are chances that multiple users try to modify the same data collector at the same time. This can make database inconsistent and hence the error message.	Try updating after some time assuming that other user has completed updating.
10929	The specified platform is not supported. Agent is supported on Windows platform.	This error signifies that agent is not installed on the supported platform.	Install agent on Windows platform.
10930	Unable to connect with specified target host.	This error occurs while adding a point product host which is not reachable from OpsCenter. Or there might be firewall configuration blocking OpsCenter,-NetBackup communication.	Make sure Point Product host is reachable from OpsCenter and vice-a-versa via ping command.
10931	The specified product is not licensed.	This occurs when product is not licensed for data collection.	Install the appropriate license for point product data collection.
10932	Unable to connect with agent. Please check if the machine is reachable and the agent service is running.	This error occurs when OpsCenter is unable to connect with agent host.	Make sure that agent host is reachable from OpsCenter host and vice-a-versa.

Table E-1 OpsCenter Error codes with Description *(continued)*

Error Code	Description	Root Cause	Solution
10934	The specified data collector is disabled.	This is only in case of reconnection server task is present and at the same time someone disabled and enabled the Master Server.	This is just a safe guard.
10935	Deletion is already in progress for the specified data collector.	This error occurs when deleting the agent data collector while another delete request is already in progress.	Wait till the previous delete request is completed.
10936	The specified install or volume directory is invalid.	This error occurs when an invalid path to “Volume Manager Directory” or “Install Directory” is specified while defining Advanced Data Collection Properties in Add Master Server.	While defining advanced data collection properties, make sure you specify proper path of NetBackup install directory and volume manager directory.
10937	The specified install directory of the product does not exist.	This error occurs when “Install Directory” path (under Configuring Advanced data collection properties of Add Master Server) is incorrect or does not exist on the NetBackup host.	Make sure NetBackup is installed on the host and specify proper path of NetB ackup home directory.
10938	The specified volume directory of the product does not exist.	This error occurs when “Volume Manager Directory” path (under Configuring Advanced data collection properties of Add Master Server) is incorrect or does not exist on the NetBackup host.	Correct the Remote Admin Console installed path (installed on Agent box). Or install the NetBackup Remote Admin Console on the Agent.
10939	The specified username or password is not valid.	This occurs when UserName/Password is not valid to connect to Master Server through BPJava.	Provide correct user name and password of Master Server.
10943	A database error has occurred. Please contact your system administrator.	This error occurs when any database related exception occurs.	Log file helps in finding the exact root cause.
10944	Deletion is in progress for the same Master Server. Connection to this master server will occur once deletion is completed.	This error occurs when a Master Server delete request is in progress and user tries to add/locate Master Server at the same time.	Before you add/locate Master Server, make sure that the previous request for delete Master Server is complete.
Messages related to Schedules			

Table E-1 OpsCenter Error codes with Description *(continued)*

Error Code	Description	Root Cause	Solution
20800	Failed to get the next schedule time for schedule {0}. The schedule information in the database might be corrupted. Please re-create the schedule and try again.	For each schedule, the next schedule time is calculated based on the type of schedule (daily, weekly, monthly, etc). The problem can occur when data for schedule in database is corrupted.	You can delete the schedule for which you are facing the problem and re-create it so that proper data is stored for schedule. Such problem may occur in case of upgraded schedule where data is not migrated properly for schedule.
20801	Failed to execute the query at the database.	This error can occur when Time schedule crud operations such as add/delete/update/fetch are performed. This error is due to a problem at the database level when the corresponding query is fired.	Log helps in finding the cause of failure at the database level.
20802	Schedule cannot be deleted as it is referred in one or more report schedules.	When Time schedule is referred by one or more Report Schedules, then user cannot delete the Time schedule since it is in use.	If you want to delete the Time Schedule, make sure it is not referred in any of the Report Schedule.
20803	Schedule {0} already exists. Please save the schedule with a different name.	You cannot save a Time schedule with same name that already exists.	Save the schedule with a different name.
Messages related to Chargeback			
20850	Failed to load the chargeback definition file {0}. Chargeback definitions are stored in XML format.	If any problem exists in XMLfile, then this error message is shown.	Make sure reports.zip file present in {OPS_INSTALL_DIR}/definitions folder is not corrupt. If problem still persists, escalate to CFT/Engineers.
20851	Failed to execute the query at the database.	This error can occur when chargeback crud operations such as add/delete/update/fetch chargeback variable, chargeback formula or chargeback currency are performed. This error is due to problem at the database level when we fire the corresponding query.	Log helps in finding the cause of failure at the database level.

Table E-1 OpsCenter Error codes with Description *(continued)*

Error Code	Description	Root Cause	Solution
20852	Cannot delete the formula as it is referred in one or more chargeback reports.	Chargeback formula created can be used in chargeback based reports. If such reports are saved with a given formula, then that formula cannot be deleted until we remove the reference of the formula from all the saved reports.	Before you delete chargeback formula, make sure you remove all references to the formulae from all saved report.
20853	Cannot delete the variable as it is referred in one or more chargeback reports or chargeback formulae.	Chargeback variable created can be used in chargeback based reports and in chargeback formula. If such reports/formulae are saved with a given variable, then that variable cannot be deleted until we remove the reference of the variable from all saved reports/formulae.	Before you delete a chargeback variable, make sure you remove all references to the variable from all saved report and all saved formulae.
20854	Chargeback variable {0} already exists. Please save the variable with a different name.	This error occurs due to saving chargeback variable with the same name that already exists.	Save the variable with a different name.
20855	Chargeback formula {0} already exists. Please save the formula with a different name.	This error occurs due to saving chargeback formula with the same name that already exists.	Save the formula with a different name.

Glossary

application	A program or group of programs designed to perform a specific task. Oracle Database and Veritas NetBackup are examples of applications.
OpsCenter Database	A Sybase SQL Anywhere database management system that resides on the OpsCenter Server. The OpsCenter database gathers data that is related to monitoring, reports, alerts, cost metrics, chargeback formulae, and so on. It is installed silently when you install OpsCenter Service.
Data Collector	Data collector is a part of Veritas NetBackup OpsCenter Agent that collects data from various products.
event	A notification that indicates when an action, such as an alert or a change in state, has occurred for one or more objects on the storage network.
OpsCenter Analytics	The licensed version of OpsCenter is called OpsCenter Analytics. OpsCenter Analytics lets you do advanced business-level reporting.
Views	Veritas NetBackup OpsCenter views are logical groups of IT assets (hosts or file systems) organized in a hierarchical manner. You can create views in Java View Builder and make them available in the Veritas NetBackup OpsCenter console. The following view details appear in the Veritas NetBackup OpsCenter console.

Index

A

about OpsCenter 19
about OpsCenter Analytics 20
access OpsCenter console 34
ActiveX 32
add
    master server 285, 290–291
    NetBackup master server 286
add email recipient
    options 245
add email recipient options 245
Add Master Server options 290
add SNMP trap recipient
    options 247
add SNMP trap recipient options 247
adding
    existing user 236, 238
    new user 236, 238
adding AD / LDAP domain in OpsCenter 228
adding users 226
Agent
    overview 27
agent
    delete 266
    modify 266
Agent options 264
agent.conf file 29
alert policies
    alert conditions 421
    Open Storage alert condition 512
alerts
    filtering by type 386
    responding to 387
    view by master server 391
application logs 199

B

backing up
    OpsCenter database 184
Backup Exec 293
bookmarks
    using with OpsCenter 67
breakup jobs 280–281
    viewing 280
Breakup Jobs option 276
business planning 23

C

capacity license 506
Change Job Priority dialog box
    options 337
Change Job Priority dialog box options 337
changedbpassword 629
chargeback
    cost variables 252, 254
    formulae 255
    modeling 256
cluster
    installing OpsCenter server
        Windows 144, 147
    limitations
        Windows 143
    OpsCenter server
        Windows 143
    prerequisites
        Windows 143
    uninstalling OpsCenter server
        Windows 151
color use
    in OpsCenter 59
compliance reporting 23
configure
    session timeout interval 47
configure SMTP 216
configurePorts 630
Content pane
    enlarging 59
    Summary and Hierarchical views 57
control OpsCenter logging
    on UNIX 198
    on Windows 198

controlling OpsCenter services and processes 168
copy user profile
    options 222
copy user profile options 222
copying
    user profile 221
correlation reports 551
cost
    formulae 255
cost estimation 256
    options 257
cost estimation options 257
cost variable
    options 251
cost variable options 251
costs variables 252
Create Agent options 265
create alert policy 428
Create Time Schedule options 590
creating
    cost formulae 255
    cost variables 252
    custom report 559
    custom reports 566
    custom SQL query 573
    email recipients 245
    SNMP trap recipients 246
    views 307
currency settings
    options 250
currency settings options 250
Custom Report Wizard
    columns parameters
        populating table columns 572
    data parameters 569
    filter parameters
        selecting 568
        using 568
    filtering parameters 573
    time frame parameters 566
custom reports 546, 566
    data 569
    table columns 572
    time frame 566
custom SQL query 547
customizing
    alert settings 539
    OpsCenter login page 46

D

data
    in graphical reports 551
    parameters 569
data collection 288
data collection status 280–281
    view 283
Data Collection view 274
Data Collector
    configuring 268, 271
    deleting 271
data collector
    Backup Exec 293
Data Collector configuration 270
Data Collector status
    viewing 267
Data Collector Wizard 269
data purge
    configure 214
database
    see (OpsCenter database) 171
dbbackup 631
dbdefrag 633
    OpsCenter cluster 140
deduplication 295
deduplication to the cloud 20, 405
default admin user login 42
defining
    cost formulae 255
    cost variables 252
delete
    master server 292
Deleting
    user group 242
deleting
    alert recipients 248
    cost formulae 255
    views 309
deleting user 236, 238
dependency of OpsCenter services 169
disable security warnings
    on Mozilla 35
documentation
    for Sybase 171
    HTTPS ports 192
    NBSL 78
    NetBackup 30
    SymcOpsCenterWebServer 72
    VxUL 72

E

edit
    master server 292
Edit Agent options 265
edit currency list
    options 251
edit currency list options 251
Edit Time Schedule options 590
editing
    currency list 250
editing user profile 236, 238
editing users 226
email
    options 243
    report 556
email options 243
email recipients
    creating 245
exporting
    report 554

F

file formats 555
filtering
    parameters 573
firewall considerations 188
firewalls
    Veritas Private Branch Exchange 25
forecast
    reports 551

G

getting started with typical OpsCenter tasks 65
Guided Recovery 487
    Destination host and login screen 492
    Job Details screen 494
    metadata 488, 495
    Performing a cloning operation 489
    Post-clone operations 494
    Pre-clone check screen 494
    Pre-operation checks 488
    Select Control File Backup screen 492
    Select Destination Parameters screen 493
    Select Master Server dialog 491
    Select Source Database 491
    Selection summary screen 494
    Troubleshooting 495

H

host alias
    adding 218
    viewing 218

I

icons for managed server status 59
install
    clustering. *See* cluster
    OpsCenter DVD 76
install and upgrade checklist 82
install OpsCenter
    on UNIX 94
    on Windows 88
Installing OpsCenter 87

J

JavaScript 32
Jobs List View
    options 329
Jobs List View options 329
JRE (Java Run Time Environment) 71

L

license
    viewing 212
license keys 74
    adding 213
    deleting 214
    viewing 213
license report issues 505, 510
licensed OpsCenter features 75
licenses
    adding 212
    managing 212
licensing model 73
licensing page 509
log files
    on UNIX servers 202–203
    on Windows servers 200
logging
    on to OpsCenter 42
    out of OpsCenter 46

M

Manage Folders options 580

Manage views
controlling scope 416
manage alert policies 418
manage devices 443
manage storage 438
managed master server considerations 77
managed server icons 59
Management Information Base (MIB) 522
managing
folders 580
master server 288
add 285
details 281
general details 282
modeling
chargeback 256
modifying
alert recipients 248
cost formulae 255
cost variables 254
report export location 222
views 308
Monitor views
controlling scope 320
monitor views
monitoring alerts 381
monitoring appliance hardware
Deduplication 405
master server 395
media server 398
NetBackup 401
monitoring cloud 413
monitoring devices 369
monitoring hosts 377
monitoring jobs 329, 337
monitoring media 358
monitoring policies 349
monitoring services 347
My Dashboard options 578
My Dashboard tab 578
My Reports tab 575

N

nbfindfile command 634
nbproxy process 170
NetBackup Data Collection
concept 275
NetBackup data collection
adding a master server 285
NetBackup data collection *(continued)*
deleting a master server 292
editing a master server 292
enabling or disabling data collection 293
supported data types and collection status 283
NetBackup licensing 498
NetBackup master server
add 286
NetBackup master server state
disabled 285
not connected 285
NetBackup master server states
connected 285
NetBackup options 273
NetBackup PureDisk data collector
configuring 297
NetBackup Service Layer (NBSL) 78, 192, 275
Network Address Translation (NAT) network
considerations 77
numeric data
viewing 551

O

object merger
options 220
object type
add 224
add attribute 225
delete 224
delete attribute 225
modify 225
options 223
object type options 223
object types 223
objects (hosts)
merging 219
operational restore
backup timelines 472
browse a client 467
browse files and directories 477
restore cart 478
simple or advanced search 468
opsadmin 638
OpsCenter 516–518
color use 59
database 79
installing
UNIX 94
Windows 88

OpsCenter *(continued)*
sanity check after installing 135
sizing 79
status bar 59
store database and logs on separate disk 174
Sybase database used 72
tasks performed on startup 137
uninstalling
UNIX 138
Windows 137
OpsCenter alerts
about alert policies 417
alert conditions 420
creating alert policy 420
managing alert policy 436
understanding alert counts 435
OpsCenter Analytics and OpsCenter 73
OpsCenter Analytics XML
DTD 665
DTD elements 666
OpsCenter AnalyticsXML
example files 670
OpsCenter architecture
database 26
OpsCenter back up and restore procedures 184
OpsCenter cluster 139
OpsCenter console
alert summary pane 56
content pane 57
description 48
quick links 56
tabs and subtabs 51
title bar 50
View pane 52
OpsCenter context-sensitive help
locating 30
OpsCenter database
back up using backupDB script 184
backing up 184
restoring 186
OpsCenter database utilities
change database administrator password 172
OpsCenter documentation 68
OpsCenter DVD layout 76
OpsCenter installation
hardware requirements 79
install checklist 82
master server considerations 77
web browser considerations 31
OpsCenter login page
customizing 46
OpsCenter post-installation
starting to use OpsCenter 136
OpsCenter processes
on UNIX 165
OpsCenter reports 543
OpsCenter Server 24
OpsCenter server scripts
on Windows and UNIX 166
OpsCenter services on Windows 164
OpsCenter start-up tasks 137
OpsCenter system requirements
see OpsCenter 79
OpsCenter upgrade procedures 115
OpsCenter user profiles 185
OpsCenter View Builder 30
OpsCenter views
managing 306–307
overview 299–300
opsCenterAgentSupport 640
opsCenterSupport 641
originator ID 197

P

parameters
Custom Report Wizard 566
password
changing 211
PBX 25
PDOS 295
pie chart reports 551
policy
filtering by type 353
port numbers
backup and archive products 191
HTTPS 192
key OpsCenter components 188
ports
Veritas Private Branch Exchange 25
product ID 197
PureDisk reports
table columns 572

Q

quick links
minimizing 56
quick start for OpsCenter tasks 65

R

ranking reports 551
refresh OpsCenter console 51
report export 223
report export location
    options 223
report export location options 223
report formats 550
report schedules 585
report templates 545
reports
    conditions 573
    custom
        creating 566
    formats 551
    graphical
        formats 551
        numeric data 551
    notification
        condition parameters 573
    ToolTips in 551
reports custom
    filtering parameters 573
restore cart
    about 478
    using 479
restoring
    OpsCenter 186
runstoredquery 644

S

saving
    report 554
schedules 582
Schedules options 584
scripts
    runstoredquery 644
search files
    using OpsCenter 460
services
    controlling 348
    filtering by type 348
setting
    default currency 249
Simple Network Management Protocol (SNMP) 521
    configuring community name 537
    configuring SNMP version 538
    SNMP traps 522
    supported SNMP versions 522
Single Instance Storage
    SIS 295
SIS
    single instance storage 572
SMTP server options 217
    options 217
SNMP port 193
SNMP trap recipient
    options 244
SNMP trap recipient options 244
SNMP trap recipients
    creating 246
software components used by OpsCenter 71
start-up tasks
    OpsCenter server 137
startagent 645
startdb 646
startgui 647
starting
    runstoredquery 644
startserver 648
status icons 59
stopagent 649
stopdb 650
stopgui 651
stopserver 652
storage lifecycle policies
    reporting 518
storage unit groups
    reporting 518
storage units
    reporting 518
supported backup products 23
supported platforms for cluster solutions 140
supported upgrade paths 79

T

tables in OpsCenter
    applying filters 64
    creating custom filters 64
    customizing 61
    selecting rows 63
    using filters 64
    viewing hidden columns 61
    viewing multiple pages 63
tape library
    modifying 220
thresholds
    report 573

time frames
parameters 566
time schedule 590
tool tips 59
ToolTips 551
trending reports
format 551
troubleshooting
accessing OpsCenter 36
OpsCenter console logon issues 43
OpsCenter server issues 47
support script in OpsCenter 193

U

unified logging (VxUL) 197
uninstalling
OpsCenter
UNIX 138
OpsCenter on Windows 137
UNIX
installing
OpsCenter 94
upgrading 129
upgrading
OpsCenter
UNIX 129
Windows 121
user access rights 231
user groups
creating 241
options 241
user groups options 241
user preferences
options 208
user preferences options 208
user profiles
viewing 235

V

Veritas Java Web Server
(SymcOpsCenterWebServer) 72
Veritas NetBackup PureDisk
PDOS 295
Veritas Private Branch Exchange 25
port number configuration 71
Veritas Private Branch Exchange (PBX) 71
Veritas Technical Support
OpsCenter custom reports 547
Veritas Technical Support *(continued)*
OpsCenter custom SQL queries 547
Veritas Unified Logging (VxUL) 72
log files 197
originator IDs used by OpsCenter 197
view
accessing 304
level 305
view OpsCenter alerts
using HP OV NNM 541
using HP OV NNM 7.50/7.51 on Windows 541
view OpsCenteralerts
using SCOM 2007 541
View pane
making selections 53
using 52
view_exportimport.bat 653
viewing
alerts by master server 391
email recipients 243
viewing alerts
using List View 382
using Summary View 390
viewing alerts by NetBackup Master Server 391
views
view type 302
Views options 300
visual keys
in the OpsCenter console 59

W

web browser
book marks 67
pop-up blockers 31
UTF-8 32
Windows
installing
OpsCenter 88
uninstalling
OpsCenter 137
upgrading OpsCenter 121
wizards
Custom Report Wizard 566

X

XML
DTD 665
examples for importing 670

XML *(continued)*
importing 665