

NetBackup™ Web UI Administrator's Guide

Release 10.3.0.1



NetBackup™ Web UI Administrator's Guide

Last updated: 2024-01-12

Legal Notice

Copyright © 2024 Veritas Technologies LLC. All rights reserved.

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

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

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

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

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

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

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

<http://www.veritas.com>

Technical Support

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

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

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

<https://my.veritas.com>

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

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

Documentation

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

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

Documentation feedback

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

NB.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Section 1	About NetBackup	18
Chapter 1	Introducing NetBackup	19
	About NetBackup	19
	NetBackup documentation	21
	NetBackup web UI features	21
	NetBackup administration interfaces	24
	Terminology	24
	First-time sign in to the NetBackup web UI	26
	Sign in to the NetBackup web UI	27
	Sign out of the NetBackup web UI	29
	Documentation for catalog recovery, disk pools, disk array hosts, and host properties in the NetBackup web UI	30
Chapter 2	Administering NetBackup licenses	31
	About NetBackup licenses	31
	Add licenses	32
	View licenses	33
	Renew licenses	33
	Remove licenses	33
Chapter 3	Registering the data collector	35
	About the data collector	35
	Register the data collector with Veritas Alta View	36
	Register the data collector with Veritas NetBackup IT Analytics	36
	Unregister the data collector	37
Section 2	Monitoring and notifications	38
Chapter 4	Monitoring NetBackup activity	39
	The NetBackup dashboard	39
	Activity monitor	40
	Monitor NetBackup daemons	41

	Monitor NetBackup processes	41
	Job monitoring	42
	Workloads that require a custom RBAC role for specific job permissions	43
	View a job	44
	View the jobs in the List view	45
	View the jobs in the Hierarchy view	45
	Jobs: cancel, suspend, restart, resume, delete	45
	Search for or filter jobs in the jobs list	46
	Create a jobs filter	47
	Edit, copy, or delete a jobs filter	49
	Import or export job filters	51
	View the status of a redirected restore	51
	Troubleshooting the viewing and managing of jobs	52
Chapter 5	Device monitor	55
	About the Device Monitor	55
	About media mount errors	56
	About pending requests and actions	57
	About pending requests for storage units	58
	Resolve a pending request	58
	Resolve a pending action	59
	Resubmit a pending request	60
	Deny a pending request	60
Chapter 6	Notifications	61
	Job notifications	61
	Send email notifications for job failures	61
	Send notifications to the backup administrator about failed backups	64
	Send notifications to a host administrator about backups	65
	Configure the nbmail.cmd script on the Windows hosts	65
	NetBackup event notifications	67
	View notifications	68
	Modify or disable NetBackup event notifications in the web UI	68
	NetBackup event types supported with notifications	70
	About configuring automatic notification cleanup tasks	75

Section 3	Configuring hosts	77
Chapter 7	Managing host properties	78
	Overview of host properties	78
	View or edit the host properties of a server or client	79
	Host information and settings in Host properties	80
	Reset a host's attributes	81
Chapter 8	Managing credentials for workloads and systems that NetBackup accesses	83
	Overview of credential management in NetBackup	84
	Add a credential in NetBackup	85
	Add a credential for an external KMS	85
	Add a credential for NetBackup Callhome Proxy	86
	Edit or delete a named credential	87
	Add a credential for CyberArk	88
	Certificate revocation lists for CyberArk server	89
	Configure external credentials	90
	Add a configuration for an external CMS server	91
	Edit or delete the configuration for an external CMS server	92
	Add a credential for Network Data Management Protocol (NDMP)	93
	Edit or delete Network Data Management Protocol (NDMP) credentials in NetBackup	93
	Troubleshooting the external CMS server issue	94
Chapter 9	Managing deployment	95
	Managing the NetBackup Package repository	95
	Update host	96
	Deployment policies	97
Section 4	Configuring storage	98
Chapter 10	Overview of storage options	99
	About storage configuration	99
Chapter 11	Configuring storage units	101
	Overview of storage units	101
	Create a storage unit	102

	Edit storage unit settings	103
	Copy a storage unit	104
	Delete a storage unit	104
	About universal shares	105
	Create a universal share	105
	Using instant access for MS-Windows and Standard policies	107
	View or edit a universal share	108
	Delete a universal share	109
Chapter 12	Configuring disk storage	110
	About configuring BasicDisk storage	110
	About configuring disk pool storage	111
	Create a disk pool	111
	Editing a disk pool	112
	Create a Media Server Deduplication Pool (MSDP, MSDP Cloud)	
	storage server	113
	Editing a storage server	115
	Integrating MSDP Cloud and CMS	116
	Migrating or upgrading MSDP Cloud and CMS	119
	Create a Media Server Deduplication Pool (MSDP) storage server for	
	image sharing	120
	Create an AdvancedDisk, OpenStorage (OST), or Cloud Connector	
	storage server	121
	Using image sharing from the NetBackup web UI	123
Chapter 13	Managing media servers	125
	Add a media server	125
	Activate or deactivate a media server	126
	Stop or restart the media manager device	127
	About NetBackup server groups	127
	Add a server group	128
	Delete a server group	128
Chapter 14	Managing tape drives	130
	Change a drive comment	130
	About downed drives	131
	Change a drive operating mode	131
	Change a tape drive path	132
	Change the operating mode for a drive path	132
	Change tape drive properties	133
	Change a tape drive to a shared drive	133

	Clean a tape drive	134
	Delete a drive	134
	Reset a drive	135
	Reset the mount time of a drive	135
	Set the drive cleaning frequency	136
	View drive details	136
Chapter 15	Staging backups	137
	About staging backups	137
	About basic disk staging	138
	Create a BasicDisk storage unit with disk staging	139
	Disk staging storage unit size and capacity	140
	Finding potential free space on a BasicDisk disk staging storage unit	141
	Schedule settings for disk staging	143
Chapter 16	Troubleshooting storage configuration	147
	Registering a media server	147
	Storage configuration issues	148
	Troubleshooting universal share configuration issues	149
Section 5	Configuring backups	152
Chapter 17	Overview of backups in the NetBackup web UI	153
	Backups methods supported in the NetBackup web UI	153
	Protection plan vs. policy FAQs	154
	Supported protection plan types	154
	Support for NetBackup classic policies	155
Chapter 18	Managing protection plans	156
	Create a protection plan	156
	Customizing protection plans	162
	Edit or delete a protection plan	163
	Subscribe an asset or an asset group to a protection plan	164
	Unsubscribe an asset from a protection plan	165
	View protection plan overrides	166
	About Backup Now	166

Chapter 19	Managing classic policies	168
	Add a policy	168
	Example policy - Exchange Server DAG backup	169
	Example policy - Sharded MongoDB cluster	170
	Edit, copy, or delete a policy	171
	Deactivate or activate a policy	172
	Edit or delete a client	173
	Edit or delete a backup selection	174
	Edit or delete a schedule	174
	Perform manual backups	175
 Chapter 20	 Protecting the NetBackup catalog	 176
	About the NetBackup catalog	176
	Catalog backups	177
	The catalog backup process	177
	Prerequisites for backing up the NetBackup catalog	178
	Configuring catalog backups	179
	Backing up NetBackup catalogs manually	180
	Concurrently running catalog backups with other backups	181
	Catalog policy schedule considerations	181
	How catalog incrementals and standard backups interact on UNIX	182
	Determining whether or not a catalog backup succeeded	182
	Strategies that ensure successful NetBackup catalog backups	182
	Disaster recovery emails and the disaster recovery files	183
	Disaster recovery packages	184
	About disaster recovery settings	185
	Setting the passphrase to encrypt disaster recovery packages	186
	Recovering the catalog	189
 Chapter 21	 Managing backup images	 190
	About the Catalog utility	190
	Catalog utility search criteria and backup image details	191
	Verify backup images	193
	Promote a copy to a primary copy	194
	Duplicate backup images	195
	Multiplexed duplication considerations	199
	Jobs that appear while making multiple copies	199
	Expire backup images	199
	About importing backup images	200

	About importing expired images	200
	Import backup images, Phase I	201
	Import backup images, Phase II	202
Chapter 22	Pausing data protection activity	204
	Pause backups and other activity	204
	Allow the automatic pause of data protection activity	205
	Pause backups and other activity on a client	205
	View paused backups and other paused activities	205
	Resume data protection activity	206
Section 6	Managing security	207
Chapter 23	Security events and audit logs	208
	View security events and audit logs	208
	About NetBackup auditing	209
	User identity in the audit report	212
	Audit retention period and catalog backups of audit records	213
	Viewing the detailed NetBackup audit report	213
	Send audit events to system logs	216
	Send audit events to log forwarding endpoints	216
Chapter 24	Managing security certificates	218
	About security management and certificates in NetBackup	218
	NetBackup host IDs and host ID-based certificates	219
	Managing NetBackup security certificates	220
	Reissue a NetBackup certificate	221
	Managing NetBackup certificate authorization tokens	223
	Using external security certificates with NetBackup	224
	Configure an external certificate for the NetBackup web server	225
	Remove the external certificate configured for the web server	226
	Update or renew the external certificate for the web server	227
	View external certificate information for the NetBackup hosts in the domain	227

Chapter 25	Managing host mappings	229
	View host security and mapping information	229
	Approve or add mappings for a host that has multiple host names	230
	Example host mappings	232
	Remove mappings for a host that has multiple host names	235
Chapter 26	Configuring multi-person authorization	237
	About multi-person authorization	237
	Workflow to configure multi-person authorization for NetBackup operations	238
	RBAC roles and permissions for multi-person authorization	240
	Multi-person authorization process with respect to roles	240
	NetBackup operations that need multi-person authorization	243
	Configure multi-person authorization	244
	View multi-person authorization tickets	244
	Manage multi-person authorization tickets	244
	Add exempted users	245
	Schedule expiration and purging of multi-person authorization tickets	245
	Disable multi-person authorization	246
Chapter 27	Managing user sessions	247
	Terminate a NetBackup user session	247
	Unlock a NetBackup user	248
	Configure when idle sessions should time out	249
	Configure the maximum of concurrent user sessions	249
	Configure the maximum of failed sign-in attempts	249
	Display a banner to users when they sign in	250
Chapter 28	Configuring multi-factor authentication	252
	About multi-factor authentication	252
	Configure multi-factor authentication for your user account	253
	Disable multi-factor authentication for your user account	253
	Enforce multi-factor authentication for all users	254
	Configure multi-factor authentication for your user account when it is enforced in the domain	254
	Reset multi-factor authentication for a user	255

Chapter 29	Managing the global security settings for the primary server	256
	Certificate authority for secure communication	256
	Disable communication with NetBackup 8.0 and earlier hosts	257
	Disable automatic mapping of NetBackup host names	258
	Configure the global data-in-transit encryption setting	258
	About NetBackup certificate deployment security levels	259
	Select a security level for NetBackup certificate deployment	261
	About TLS session resumption	262
	Set a passphrase for disaster recovery	262
	About trusted primary servers	263
	Add a trusted primary server	264
	Remove a trusted primary server	265
Chapter 30	Using access keys, API keys, and access codes	266
	Access keys	266
	API keys	266
	Add an API key or view API key details (Administrators)	267
	Edit, reissue, or delete an API key (Administrators)	268
	Add an API key or view your API key details	269
	Edit, reissue, or delete your API key	270
	Use an API key with NetBackup REST APIs	271
	Access codes	271
	Request CLI access through web UI authentication	272
	Approve the CLI access request of another user	273
	Edit the settings for command-line access	273
Chapter 31	Configuring authentication options	275
	Sign-in options for the NetBackup web UI	275
	Configure user authentication with smart cards or digital certificates	276
	Configure smart card authentication with a domain	276
	Configure smart card authentication without a domain	277
	Edit the configuration for smart card authentication	278
	Add or delete a CA certificate that is used for smart card authentication	279
	Disable or temporarily disable smart card authentication	280
	About single sign-on (SSO) configuration	280
	Configure NetBackup for single sign-on (SSO)	282
	Configure the SAML KeyStore	283

Configure the SAML keystore and add and enable the IDP configuration	286
Enroll the NetBackup primary server with the IDP	288
Manage an IDP configuration	289
Video: Configure single sign-on in NetBackup	291
Troubleshooting SSO	292
Redirection issues	292
Unable to sign in due to authorization-related issues	294

Chapter 32 Managing role-based access control 296

RBAC features	296
Authorized users	297
Configuring RBAC	297
Notes for using NetBackup RBAC	298
Add AD or LDAP domains	299
View users in RBAC	299
Add a user to a role (non-SAML)	299
Add a smart card user to a role (non-SAML, without AD/LDAP)	300
Add a user to a role (SAML)	301
Remove a user from a role	302
Default RBAC roles	302
Add a custom RBAC role	305
Edit or remove a role a custom role	306
Add a custom RBAC role to restore Azure-managed instances	307
Add a custom RBAC role for a PaaS administrator	308
Add a custom RBAC role for a Malware administrator	309
Role permissions	310
Manage access permission	311
View access definitions	312

Chapter 33 Disabling access to NetBackup interfaces for OS Administrators 314

Disable command-line (CLI) access for operating system (OS) administrators	314
Disable web UI access for operating system (OS) administrators	315

Section 7	Detection and reporting	316
Chapter 34	Malware scanning	317
	About malware scanning	317
	Workflow for malware scanning	318
	Configurations	323
	Configuring scan host pool	323
	Managing scan host	325
	Configure resource limits	328
	Perform a malware scan	329
	Backup images	331
	Assets by policy type	333
	Assets by workload type	335
	Managing scan tasks	336
	View the malware scan status	336
	Actions for malware scanned images	337
	Recover from malware-affected images (clients protected by policies)	341
	Recover from malware-affected images (clients protected by protection plan)	342
	Single file restore	343
Chapter 35	Detecting anomalies	345
	About backup anomaly detection	345
	How a backup anomaly is detected	346
	Configure backup anomaly detection settings	347
	View backup anomalies	348
	About system anomaly detection	349
	Configure system anomaly detection settings	350
	View system anomalies	351
Chapter 36	Usage reporting and capacity licensing	352
	Track protected data size on your primary servers	352
	Add a local primary server	353
	Select license types to display in usage reporting	354
	Scheduling reports for capacity licensing	354
	Other configuration for incremental reporting	357
	Troubleshooting failures for usage reporting and incremental reporting	359

Section 8	NetBackup workloads and NetBackup Flex Scale	361
Chapter 37	NetBackup SaaS Protection	362
	Overview of NetBackup for SaaS	362
	Adding NetBackup SaaS Protection Hubs	364
	Configuring the autodiscovery frequency	365
	Proxy configuration for autodiscovery	365
	Viewing asset details	366
	Configuring permissions	367
	Troubleshooting SaaS workload issues	368
Chapter 38	NetBackup Flex Scale	370
	Managing NetBackup Flex Scale	370
	Access NetBackup from the Flex Scale infrastructure management console	371
	Manage NetBackup and the NetBackup Flex Scale cluster management from the NetBackup Flex Scale web UI	372
	Access NetBackup Flex Scale from the NetBackup web UI	373
Chapter 39	NetBackup workloads	375
	Protection of other asset types and clients	375
Section 9	Disaster recovery and troubleshooting	376
Chapter 40	Managing Resiliency Platforms	377
	About Resiliency Platform in NetBackup	377
	Understanding the terms	378
	Configuring a Resiliency Platform	379
	Add a Resiliency Platform	379
	Configure a third-party CA certificate	380
	Edit or delete a Resiliency Platform	380
	View the automated or not-automated VMs	381
	Troubleshooting NetBackup and Resiliency Platform issues	383

Chapter 41	Managing Bare Metal Restore (BMR)	385
	About Bare Metal Restore (BMR)	385
	Add a custom role for a Bare Metal Restore (BMR) administrator	386
Chapter 42	Troubleshooting the NetBackup Web UI	388
	Tips for accessing the NetBackup web UI	388
	If a user doesn't have the correct permissions or access in the NetBackup web UI	390
	Unable to validate the user or group when configuring LDAP server	390
Section 10	Other topics	391
Chapter 43	Additional NetBackup catalog information	392
	Parts of the NetBackup catalog	392
	NetBackup databases and configuration files	393
	About the NetBackup image database	395
	About the catalog backup of cloud configuration files	397
	Archiving the catalog and restoring from the catalog archive	398
	Enabling intelligent catalog archiving (ICA) to reduce the number of .f files	401
	Creating a catalog archiving policy	405
	Catalog archiving commands	406
	Catalog archiving considerations	408
	Extracting images from the catalog archives	409
	Estimating catalog space requirements	409
	NetBackup file size considerations on UNIX systems	411
	Moving the image catalog	411
	About image catalog compression	413
Chapter 44	About the NetBackup database	417
	About the NetBackup database installation	417
	About NetBackup primary server installed directories and files	417
	NetBackup configuration entry	420
	NetBackup database server management	421
	The NetBackup database and clustered environments	422
	Post-installation tasks	422
	Changing the NetBackup database password	423
	Moving a database after installation	424

Copying the NetBackup databases	426
Creating the NBDB database manually	426
Using the NetBackup Database Administration utility on Windows	
4 2 8	
.....	429
.....	430
Using the NetBackup Database Administration utility on UNIX	433
Select/Restart Database and Change Password menu options	
.....	434
Database Space Management menu options	435
Database Validation Check and Rebuild menu options	436
Move Database menu options	437
Unload Database menu options	438
Backup and Restore Database menu options	438

About NetBackup

- [Chapter 1. Introducing NetBackup](#)
- [Chapter 2. Administering NetBackup licenses](#)

Introducing NetBackup

This chapter includes the following topics:

- [About NetBackup](#)
- [NetBackup documentation](#)
- [NetBackup web UI features](#)
- [NetBackup administration interfaces](#)
- [Terminology](#)
- [First-time sign in to the NetBackup web UI](#)
- [Sign in to the NetBackup web UI](#)
- [Sign out of the NetBackup web UI](#)
- [Documentation for catalog recovery, disk pools, disk array hosts, and host properties in the NetBackup web UI](#)

About NetBackup

NetBackup provides a complete, flexible data protection solution for a variety of platforms. The platforms include Windows, UNIX, and Linux systems.

NetBackup administrators can set up periodic or calendar-based schedules to perform automatic, unattended backups for clients across a network. An administrator can carefully schedule backups to achieve systematic and complete backups over a period of time, and optimize network traffic during off-peak hours. The backups can be full or incremental: Full backups back up all indicated client files, while incremental backups back up only the files that have changed since the last backup.

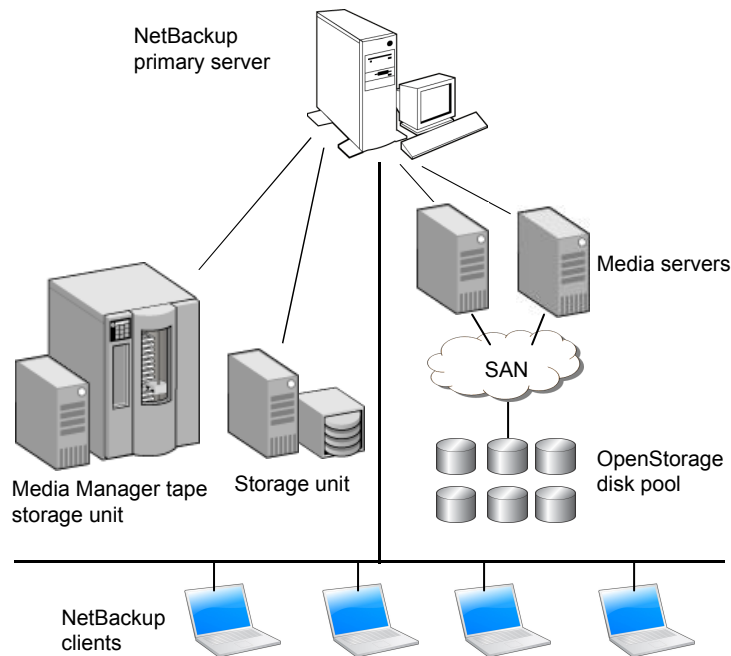
The NetBackup administrator can allow users to back up, restore, or archive the files from their computer. (An archive operation backs up a file, then deletes it from the local disk if the backup is successful.)

NetBackup includes both the server and the client software as follows:

- Server software resides on the computer that manages the storage devices.
- Client software resides on computers that contain data to back up. (Servers also contain client software and can be backed up.)

Figure 1-1 shows an example of a NetBackup storage domain.

Figure 1-1 NetBackup storage domain example



NetBackup accommodates multiple servers that work together under the administrative control of one NetBackup primary server in the following ways:

- The primary server manages backups, archives, and restores. The primary server is responsible for media and device selection for NetBackup. Typically, the primary server contains the NetBackup catalog. The catalog contains the internal databases that contain information about NetBackup backups and configuration.
- Media servers provide additional storage by allowing NetBackup to use the storage devices that are attached to them. Media servers can also increase

performance by distributing the network load. Media servers can also be referred to by using the following terms:

- Device hosts (when tape devices are present)
- Storage servers (when I/O is directly to disk)
- Data movers (when data is sent to independent, external disk devices like OpenStorage appliances)

During a backup or archive, the client sends backup data across the network to a NetBackup server. The NetBackup server manages the type of storage that is specified in the backup policy.

During a restore, users can browse, then select the files and directories to recover. NetBackup finds the selected files and directories and restores them to the disk on the client.

NetBackup documentation

For a complete list of NetBackup technical documents for each supported release, see the *NetBackup Documentation Landing Page* at the following URL:

<https://www.veritas.com/docs/DOC5332>

No responsibility is assumed for the installation and use of the Adobe Acrobat Reader.

NetBackup web UI features

The NetBackup web user interface provides the following features:

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

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

- A dashboard that displays a quick overview of the information that is important to you.
- Role-based access control (RBAC) that lets the administrator configure user access to NetBackup and to delegate the tasks such as security, storage management, or workload protection.

- Management of NetBackup security settings, certificates, API keys, and user sessions.
- Management of NetBackup host properties.
- Data protection is achieved through protection plans or policies. (Policy support is limited at this time. Additional policy types will be added in future releases.)
- Detection and reporting features provide for the detection of malware and anomalies and provide usage reporting to track the size of backup data on your primary servers. You can also easily connect to Veritas NetInsights Console to view and manage NetBackup licensing.

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

Access control in the NetBackup web UI

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

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

Monitor NetBackup jobs and events

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

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

Protection plans: One place to configure schedules and storage

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

See [“Supported protection plan types”](#) on page 154.

Protection plans offer the following benefits:

- A workload administrator can create and manage protection plans, including the backup schedules and storage that is used. This administrator selects the protection plans that protect assets.
See [“Role permissions”](#) on page 310.
- In addition to schedules for backups, a protection plan can also include a schedule for replication and long-term retention.
- When you select from your available storage, you can see any additional features available for that storage.
- Users with a workload administrator role can create protection plans, manage credentials, subscribe assets to the protection plans that meet the SLO, and monitor protection status.

Backup policies

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

See [“Support for NetBackup classic policies”](#) on page 155.

Server-directed and self-service recovery

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

BigData	Hyper-V	NDMP
Cloud-Object-Store	Hypervisor – Nutanix	Standard
FlashBackup		Universal-Share
FlashBackup-Windows	MS-Windows	VMware (agent-based recovery)
	NAS-Data-Protection	

Restore types in addition to “Normal backups” are available for certain policy types. For example: Archived backups, Optimized backups (MS-Windows), Point-in-time rollback (Standard), Raw partition backups, True image backups, Virtual disk restore (VMware), and Virtual machine backups (Hypervisor-Nutanix).

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

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

NetBackup administration interfaces

NetBackup can be administered with several interfaces. The best choice depends on personal preference and the systems that are available to the administrator.

Table 1-1 NetBackup administration interfaces

Name of interface	Description
NetBackup web user interface	<p>With the NetBackup web user interface (UI), you can view NetBackup activities and manage NetBackup configuration, from a primary server.</p> <p>To start the NetBackup web UI:</p> <ul style="list-style-type: none">■ Users must have a role that is configured for them in NetBackup RBAC.■ Open a web browser and go to the following URL: <code>https://primaryserver/webui/login</code>
Character-based, menu interface	<p>Run the <code>tpconfig</code> command to start a character-based, menu interface for device management.</p> <p>Use the <code>tpconfig</code> interface from any terminal (or terminal emulation window) that has a <code>termcap</code> or a <code>terminfo</code> definition.</p>
Command line	<p>NetBackup commands are available on both Windows and UNIX platforms. Enter NetBackup commands at the system prompt or use the commands in scripts.</p> <p>All NetBackup administrator programs and commands require root or administrator user privileges by default.</p>

Terminology

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

Table 1-2 Web user interface terminology and concepts

Term	Definition
Administrator	Also see <i>role</i> .
Asset group	See <i>intelligent group</i> .
Asset	The data to be protected, such as physical clients, virtual machines, and database applications.
Backup now	An immediate backup of an asset. NetBackup performs a one-time, full backup of an asset using the selected protection plan. This backup does not affect any scheduled backups.
Classic policy	In the NetBackup web UI, indicates that a legacy policy protects the asset.
External certificate	A security certificate that is issued from any CA other than NetBackup.
Intelligent group	<p>Allows NetBackup to automatically select assets for protection based on the criteria (queries) that you specify. An intelligent group automatically stays up-to-date with changes in the production environment. These groups are also referred to as asset groups.</p> <p>These groups appear under the tab Intelligent VM groups or Intelligent groups.</p>
NetBackup certificate	A security certificate that is issued from the NetBackup CA.
Protection plan	A protection plan defines when backups are performed, how long the backups are retained, and the type of storage to use. Once a protection plan is set up, assets can be subscribed to the protection plan.
RBAC	Role-based access control. The role administrator can delegate or limit access to the NetBackup web UI through the roles that are configured in RBAC.
Role	For RBAC, defines the operations that a user can perform and the assets or objects that they can access. For example, you can configure a role to manage recovery of specific databases and the credentials that are needed for backups and restores.
Storage	The storage to which the data is backed up, replicated, or duplicated (for long-term retention).

Table 1-2 Web user interface terminology and concepts (*continued*)

Term	Definition
Subscribe, to a protection plan	The action of selecting an asset or an asset group to subscribe to a protection plan. The asset is then protected according to the schedule in the plan. The web UI also refers to <i>Subscribe</i> as <i>Add protection</i> .
Unsubscribe, from a protection plan	<i>Unsubscribe</i> refers to the action of removing protection or removing an asset or asset group from a plan.
Workload	The type of asset. For example: VMware, Microsoft SQL Server, or Cloud.

First-time sign in to the NetBackup web UI

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

See [“Authorized users”](#) on page 297.

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

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

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

`https://primaryserver/webui/login`

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

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

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

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

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

See [“Configuring RBAC”](#) on page 297.

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

Support and additional configuration

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

- Ensure that you are an authorized user.
See [“Authorized users”](#) on page 297.
- For details on supported browsers for the web UI, see the [NetBackup Software Compatibility List](#).
- If port 443 is blocked or in use, you can [configure and use a custom port](#).
- If you want to use an external certificate with the web browser, see the following topic.
See [“Configure an external certificate for the NetBackup web server”](#) on page 225.
- See other tips for accessing the web UI.
See [“Tips for accessing the NetBackup web UI”](#) on page 388.

Sign in to the NetBackup web UI

Authorized users can sign in to a NetBackup primary server from a web browser, using the NetBackup web UI. The NetBackup web user interface (web UI) is available for NetBackup 8.1.2 and later. This interface is available on the primary server and supports the version of NetBackup on that server.

Users should contact their NetBackup security administrator for information on how to sign in.

The following sign-in options are available:

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

Sign in with a username and password

You can sign in to NetBackup web UI with your username and password.

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

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

`https://primaryserver/webui/login`

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

- 2 Depending on the sign-in options that are available, choose from the following:

- Enter your credentials and click **Sign in**.
- [Conditional] If your user account is configured for multi-factor authentication, you are prompted to enter the one-time password.
Enter the one-time password on the **Login** pop-up screen and click **Confirm**.
See [“About multi-factor authentication”](#) on page 252.
- If the default method is not username and password, click **Sign in with username and password**. Then enter your credentials.

The following are example credentials:

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

Sign in with a certificate or smart card

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

To sign in with a certificate or smart card

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

`https://primaryserver/webui/login`

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

- 2 Click **Sign in with certificate or smart card**.
- 3 When your browser prompts you, select the certificate.

Sign in with single sign-on (SSO)

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

To sign in to a NetBackup primary server using SSO

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

`https://primaryserver/webui/login`

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

- 2 Click **Sign in with single sign-on**.
- 3 Follow the steps as provided by your administrator.

On subsequent logons, NetBackup signs you in automatically to the primary server.

Sign out of the NetBackup web UI

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

To sign out of the NetBackup web UI

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

Documentation for catalog recovery, disk pools, disk array hosts, and host properties in the NetBackup web UI

The NetBackup web UI includes some functions that are not documented in this guide. Refer to the following guides for details about these functions:

- Catalog recovery
[NetBackup Troubleshooting Guide](#)
- Disk array hosts
[NetBackup Snapshot Manager for Data Center Administrator's Guide](#)
- Disk pools. Refer to the following guides.
[NetBackup Cloud Administrator's Guide](#)
[NetBackup Deduplication Guide](#)
[NetBackup OpenStorage Solutions Guide for Disk](#)
[NetBackup Replication Director Solutions Guide](#)
[NetBackup Administrator's Guide, Volume I](#)
- Host properties
[NetBackup Administrator's Guide, Volume I](#)

Administering NetBackup licenses

This chapter includes the following topics:

- [About NetBackup licenses](#)
- [Add licenses](#)
- [View licenses](#)
- [Renew licenses](#)
- [Remove licenses](#)

About NetBackup licenses

NetBackup uses a common license system that other Veritas products also use. However, the common license system provides flexibility in the license features that each product implements.

For example, NetBackup does not have a node-locked license system, but some other products do.

Licenses for all purchased NetBackup SKUs must be entered on the primary server. Enter licenses by using one of the following methods:

- During NetBackup primary server installation
The installer prompts you to enter the licenses for all NetBackup products that you plan to install.
You must add either a NetBackup license file or use an in-built evaluation or a temporary production license during primary server installation. For more information, refer to the *NetBackup Installation Guide* or the following article:
https://www.veritas.com/support/en_US/article.100058779

- NetBackup web UI (recommended)
After NetBackup primary server installation, in the NetBackup web UI, click **Settings > License Management > Add license**.
- Command-line interface
After NetBackup primary server installation, use the following command:

```
/usr/opensv/netbackup/bin/admincmd/get_license_key
```


Use the `bpminlicense` command to manage licenses.
Refer to the *NetBackup Commands Reference Guide* for more details.
On UNIX, you can also use the following command:

```
/usr/opensv/netbackup/bin/admincmd/get_license_key
```

Note: Veritas recommends the use of a browser and the NetBackup web UI to manage licenses remotely.

Add licenses

You can add licenses after primary server installation using the NetBackup web UI.

To add licenses after primary server installation

- 1 In the NetBackup web UI, click **Settings > License Management**.
- 2 On the **License management** screen, click **Add license**.
- 3 Add license file using one of the following methods:
 - **Veritas Entitlement Management System (VEMS)** - Use this method to add the license from the VEMS portal.
 - Sign in to your Veritas account by specifying the **Username** and **Password**.
 - Select the entitlement that you want to add.
For more information, refer to the [VEMS User Guide](#).
 - **File system** - Use this method to add a license file that you have already downloaded on your local host.
 - Click **Browse** to select the `.slf` license file that you want to add.
- 4 Click **Add**.

View licenses

You can view the NetBackup licenses that you have already added, using the web UI.

To view NetBackup licenses

- 1 In the NetBackup web UI, click **Settings > License Management**.
- 2 You can see the following license details:
 - **Name** - Name of the license
 - **Status** - Status of the license, such as Active
 - **License type** - Type of license such as Perpetual, Subscription
 - **Activation** - Date when the license was activated
 - **Expiration** - Date when the license will be expired
 - **Entitlement ID** - Unique identification number of each license with respect to the product features it offers and the customer account that is entitled to use it

Renew licenses

You can renew subscription type of licenses.

To renew licenses

- 1 In the NetBackup web UI, click **Settings > License Management**.
- 2 Click the **Actions** option for the license that you want to renew.
- 3 Click **Renew**.
- 4 For the VEMS option, enter the username and password.
For the File system option, select the license file.
- 5 Click **Sign in**.
- 6 Click **Renew**.

Remove licenses

You can remove licenses.

To remove licenses

- 1** In the NetBackup web UI, click **Settings > License Management**.
- 2** Click the **Actions** option for the license that you want to remove.
- 3** Click **Remove**.

Registering the data collector

This chapter includes the following topics:

- [About the data collector](#)
- [Register the data collector with Veritas Alta View](#)
- [Register the data collector with Veritas NetBackup IT Analytics](#)
- [Unregister the data collector](#)

About the data collector

The data collector collects metadata from NetBackup and sends information such as policies, jobs, image records to Veritas Alta View or Veritas NetBackup IT Analytics. Based on the information that the data collector has sent, these applications monitor, manage, and report on NetBackup domains.

See [“Register the data collector with Veritas Alta View”](#) on page 36.

See [“Register the data collector with Veritas NetBackup IT Analytics”](#) on page 36.

To receive data from the data collector, you need to register Veritas Alta View or Veritas NetBackup IT Analytics with the data collector.

Note: Either Veritas Alta View or Veritas NetBackup IT Analytics can be registered with a single data collector at a time.

Register the data collector with Veritas Alta View

Veritas Alta View is a centralized management platform to manage multiple NetBackup domains. It provides global enterprise data protection visibility and operations. It is a cloud-based management console unifying the protection and management of on-premises and cloud workloads from a single interface, delivering simplified policy management, centralized visibility, and flexible protection strategies.

For more information, refer to the *Veritas Alta View Help*.

To enable Veritas Alta View to collect data from NetBackup, you must register the data collector that you have on your primary server with Veritas Alta View using the NetBackup web UI.

To register the data collector with Veritas Alta View

- 1 On the top right, click **Settings > Data collector registration**.
- 2 Click **Register with Veritas Alta View**.
- 3 Click **Choose file** to select the registration file (JSON) that you have downloaded using the Veritas Alta View UI earlier.

See the 'Complete domain registration for NetBackup 10.1.1 and later' topic in the *Veritas Alta View Help*.

- 4 Select the **Use proxy server** option and specify the proxy server settings.

This is an optional step.

- 5 Click **Register**.

After the registration with the data collector, you can monitor, manage, and report on NetBackup domains using the Veritas Alta View UI and the Veritas Alta View Reports UI.

After the registration, you can access Veritas Alta View using the NetBackup web UI. The Veritas Alta View option is added on the left pane in the UI.

Register the data collector with Veritas NetBackup IT Analytics

Veritas NetBackup IT Analytics is the storage resource management platform that enables IT organizations to integrate storage and backup solutions to address rapid growth and declining budgets.

For more information, see the *NetBackup IT Analytics User Guide*.

To enable NetBackup IT Analytics to collect data from NetBackup, you must register the data collector that you have on your primary server with NetBackup IT Analytics using the NetBackup web UI.

If NetBackup IT Analytics portal is hosted on on-premise, you must register the data collector with the portal.

To register the data collector with NetBackup IT Analytics

- 1** On the top right, click **Settings > Data collector registration**.
- 2** Click **Register with NetBackup IT Analytics**.
- 3** Click **Choose file** to select the registration file (JSON) that you have downloaded using the NetBackup IT Analytics portal earlier.

See the 'Add/Edit Data Collectors' topic in the *NetBackup IT Analytics User Guide*.

- 4** Select the **Use proxy server** option and specify the proxy server settings.

This is an optional step.

- 5** Click **Register**.

After the registration with the data collector, you can monitor, manage, and report on NetBackup domains using NetBackup IT Analytics.

Unregister the data collector

To stop collecting data from NetBackup, you must unregister the data collector that you have registered earlier with Veritas Alta View or NetBackup IT Analytics.

If you want to change registration from Veritas Alta View to NetBackup IT Analytics portal or from NetBackup IT Analytics portal to Veritas Alta View, you must first unregister the existing configuration.

To unregister the data collector

- 1** On the top right, click **Settings > Data collector registration**.
- 2** Click **Unregister data collector**.

Monitoring and notifications

- [Chapter 4. Monitoring NetBackup activity](#)
- [Chapter 5. Device monitor](#)
- [Chapter 6. Notifications](#)

Monitoring NetBackup activity

This chapter includes the following topics:

- [The NetBackup dashboard](#)
- [Activity monitor](#)
- [Job monitoring](#)

The NetBackup dashboard

Table 4-1 The NetBackup dashboard

Dashboard widget	Description
Jobs	Lists job information, including the number of active and queued jobs and the status of attempted and completed jobs.
Malware detection	Displays the malware scan result status for the images including Impacted, Not impacted, Failed, In progress, and Pending.
Anomaly detection	<p>Displays the total anomalies that are reported so far.</p> <p>See “View backup anomalies” on page 348.</p> <p>Note: An anomalies count of 0 indicates there are no anomalies generated or that the anomaly detection services are not running.</p>

Table 4-1 The NetBackup dashboard (*continued*)

Dashboard widget	Description
Paused protection activities	<p>Lists any paused protection activities for clients. These activities include new backups, duplication, and image expiration. NetBackup pauses protection if it detects malware in backup images.</p> <p>Automatic indicates the activities that are automatically paused by NetBackup. User-initiated indicates an activity that was paused manually by a user.</p> <p>See “Pause backups and other activity” on page 204.</p>
Tokens	<p>Displays the information about the authorization tokens in your environment.</p>
Certificates	<p>Displays the information about the NetBackup host ID-based security certificates or the external certificates in your environment.</p> <p>For external certificates, the following information is shown for NetBackup 8.2 and later hosts:</p> <ul style="list-style-type: none">■ Total hosts. The total number of hosts. The hosts must be online and able to communicate with NetBackup primary server.■ Missing. The number of hosts that do not have an external certificate enrolled.■ Valid. The number of hosts that have an external certificate enrolled.■ Expired. The number of hosts with expired external certificates. <p>More details are available in Certificates > External certificates.</p> <p>See “About security management and certificates in NetBackup” on page 218.</p>
Security events	<p>The Access history view includes a record of logon events. The Audit events view includes the events that users initiate on the NetBackup primary server.</p>
Usage reporting	<p>Lists the size of the backup data for the NetBackup primary servers in your organization. This reporting is useful to track capacity licensing. Use the drop-down lists in the top right to select the time period and the view that you want to display. Click on a server name to see specific details for that server.</p> <p>Additional details are available for how to configure NetBackup to display primary server information in this widget.</p> <p>See “Track protected data size on your primary servers” on page 352.</p>

Activity monitor

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

Jobs	Displays in-process or completed jobs for the primary server. The Jobs tab also displays details about the jobs. See “ Job monitoring ” on page 42.
Daemons	Displays the status of NetBackup daemons on the primary server. Click Change server to display daemons on a media server in the environment.
Processes	Displays the NetBackup processes that run on the primary server. Click Change server to display processes on a media server in the environment.

Monitor NetBackup daemons

The Activity monitor displays the status of NetBackup daemons on primary and media servers. To start or stop daemons, you must have the applicable RBAC role or similar permissions on the primary or the media server.

Note that not all daemons can be stopped from the NetBackup web UI. On back-level servers, you can still stop and start some services that you cannot in 10.2 and later releases.

To view, stop, or start NetBackup daemons

- 1 On the left, click **Activity monitor**. Then click the **Daemons** tab.
- 2 (Conditional) To manage daemons for a media server in the environment, click **Change server**.
- 3 Locate the daemon.
- 4 On the right, click **Actions**. Then choose from the following actions.

Stop	Stop the selected daemon.
Start	Start the selected daemon.

Monitor NetBackup processes

The Activity monitor displays the status of NetBackup processes on the primary server and the media servers.

To view NetBackup processes

- 1 On the left, click **Activity monitor**. Then click the **Processes** tab.
- 2 (Conditional) To manage processes for a media server in the environment, click **Change server**.

Job monitoring

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

List view

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

Hierarchy view

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

RBAC permissions for jobs

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

See [“Workloads that require a custom RBAC role for specific job permissions”](#) on page 43.

Job hierarchy view

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

See [“Default RBAC roles”](#) on page 302.

Workloads that require a custom RBAC role for specific job permissions

The NetBackup web UI offers granular job access for certain workloads. This functionality lets you create a custom RBAC role with job permissions for a particular workload.

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

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

To create a custom role with job permissions

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

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

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

For example:

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

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

RBAC job permissions for BigData workloads

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

To configure job permissions

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

View a job

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

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

See [“Job monitoring”](#) on page 42.

To view a job and the job details

- 1 On the left, click **Activity monitor**. Then click the **Jobs** tab.
- 2 Click the job name that you want to view.

If you want to open the job in a separate window, at the top right click **Open in new window**.



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

- 4 Click the **Details** tab to view the logged details about a job. You can filter the logs by error type using the drop-down menu.
See [“Search for or filter jobs in the jobs list”](#) on page 46.
- 5 Click the **Job hierarchy** tab to view the complete hierarchy for the job, including any ancestor and any child jobs.
See [“View the jobs in the Hierarchy view”](#) on page 45.

View the jobs in the List view

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

To view the jobs in the List view

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



View the jobs in the Hierarchy view

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

To view the jobs in the Hierarchy view

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



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

Jobs: cancel, suspend, restart, resume, delete

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

To manage a job

- 1 On the left, click **Activity monitor**. Then click the **Jobs** tab.
- 2 Select one or more jobs.
- 3 The top menu shows the actions that you can perform for the selected jobs.

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

Search for or filter jobs in the jobs list

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

Search for jobs in the jobs list

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

Search for jobs in the jobs list

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

Filter the job list

To filter the job list

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

Create a jobs filter

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

To create a jobs filter

- 1 On the left, click **Activity monitor**. Then click the **Jobs** tab.
- 2 In the toolbar, click the **Filter** icon.
- 3 If you have not created any filters yet, on the left click **Create filter**.
Otherwise, click **Actions > Create**.
- 4 Enter a name and an optional description for the filter.
- 5 Choose if you want the filter to be **Private** or **Public**.

Private

All new filters are private by default. These filters appear in “My list” in the **Manage filters** page. Only the owner can view a private filter.

Public

Public filters are available to all NetBackup users. Any user can view, copy, export, or pin a public filter.

- 6 In the **Query** pane, use the drop-down lists to create a condition.
For example, to view all jobs with the VMware policy type, **Policy type = VMware**.

Query

The screenshot shows a 'Query' pane with a toolbar at the top containing '+ Condition' and '+ Sub-query' buttons. Below the toolbar is a single condition row with three dropdown menus: 'Policy Type', '=', and 'VMware'. A trash icon is located at the end of the row.

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

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

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

Query

AND OR + Condition + Sub-query

State = Done

AND OR + Condition + Sub-query

Status code = 196

Status code = 239

- 8 Choose from the following options:

- To save this query and return to the **Jobs** list, click **Save**.
- To save this query and apply the filter you just created, click **Save and apply**.

Example 1. Query filter for all jobs with the VMware policy type.

Activity monitor

Jobs Daemons Processes Background tasks

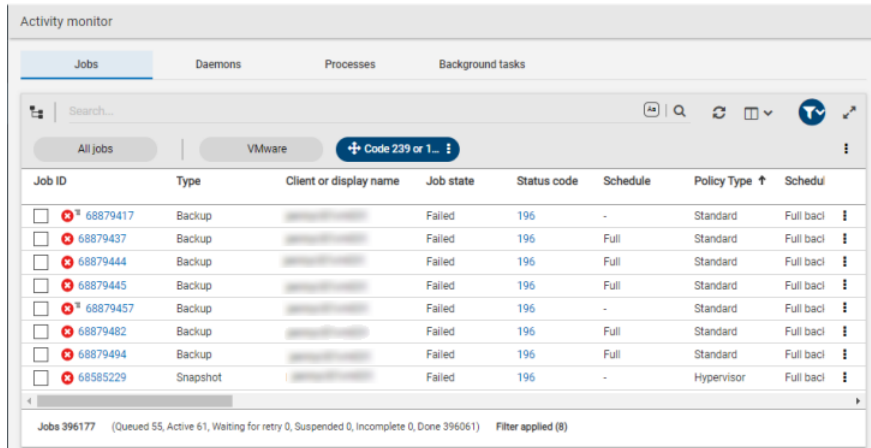
Search...

All jobs + VMware

Job ID	Type	Client or display name	Job state	Status code	Schedule	Policy Type	Sche
68564587	Backup	appliance-10-10-10-10-10-10	Done	0	-	VMware	Full t
68564692	Snapshot	appliance-10-10-10-10-10-10	Done	0	-	VMware	Full t
68564702	Snapshot	appliance-10-10-10-10-10-10	Done	0	-	VMware	Full t
68564707	Snapshot	appliance-10-10-10-10-10-10	Done	0	-	VMware	Full t
68564708	Snapshot	appliance-10-10-10-10-10-10	Done	0	-	VMware	Full t

Jobs 394546 (Queued 125, Active 130, Waiting for retry 0, Suspended 0, Incomplete 0, Done 394291) Filter applied (788)

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



The screenshot shows the 'Activity monitor' window with the 'Jobs' tab selected. A search filter is applied: 'Code 239 or 196'. The table below lists several failed backup jobs.

Job ID	Type	Client or display name	Job state	Status code	Schedule	Policy Type	Schedule
68879417	Backup	client1	Failed	196	-	Standard	Full back
68879437	Backup	client1	Failed	196	Full	Standard	Full back
68879444	Backup	client1	Failed	196	Full	Standard	Full back
68879445	Backup	client1	Failed	196	Full	Standard	Full back
68879457	Backup	client1	Failed	196	-	Standard	Full back
68879482	Backup	client1	Failed	196	Full	Standard	Full back
68879494	Backup	client1	Failed	196	Full	Standard	Full back
68585229	Snapshot	client1	Failed	196	-	Hypervisor	Full back

Jobs 396177 (Queued 55, Active 61, Waiting for retry 0, Suspended 0, Incomplete 0, Done 396061) Filter applied (8)

Edit, copy, or delete a jobs filter

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

Edit a jobs filter

To edit a jobs filter

- 1 On the left, click **Activity monitor**. Then click the **Jobs** tab.
- 2 In the toolbar, click **Filter** icon.
- 3 Click **Actions > Manage filters**.
- 4 Click **My list** or **Shared**.

- 5 Select from the following options.

Options with an asterisk (*) are available for any filters that you own.

View	View the details of a filter that you do not own.
Edit*	Edit the filter properties or filter query.
Export	Export the filter to share with another NetBackup user or import the filter into another NetBackup domain.
Make private*	Make a public filter a private filter.
Make public*	Make a private filter a public filter.
Pin	Pin the filter to the jobs filter toolbar.
Delete*	Delete a filter.

- 6 Make the changes that you want to the filter and click **Save**.

Copy a jobs filter

To copy a jobs filter

- 1 On the left, click **Activity monitor**. Then click the **Jobs** tab.
- 2 In the toolbar, click the **Filter** icon.
- 3 Click **Actions > Manage filters**.
- 4 Click **My list** or **Shared**.
- 5 Select the filter that you want to copy.
- 6 Click **View** or **Edit**.
- 7 Make any changes that you want to the filter.
- 8 Click **Copy**.

Delete a jobs filter

To delete a jobs filter

- 1 On the left, click **Activity monitor**. Then click the **Jobs** tab.
- 2 In the toolbar, click the **Filter** icon.
- 3 Click **Actions > Manage filters**.

- 4 Click **My list**.
- 5 Locate the filter that you want to delete and click **Delete > Yes**.

Import or export job filters

The job filter export and import features allow users to share job filters between users or other NetBackup domains.

Import a jobs filter

To import a jobs filter

- 1 On the left, click **Activity monitor**. Then click the **Jobs** tab.
- 2 In the toolbar, click **Filter** icon.
- 3 Click **Actions > Manage filters**.
- 4 Click **My list**.
- 5 Click **Add > Import**.
- 6 Select the filter that you want to import.

Export a jobs filter

To export a jobs filter

- 1 On the left, click **Activity monitor**. Then click the **Jobs** tab.
- 2 In the toolbar, click **Filter** icon.
- 3 Click **Actions > Manage filters**.
- 4 Click **My list** or **Shared**.
- 5 Select the filter that you want to export.
- 6 Click **Export**.

NetBackup exports the filter as a .json file. Note that changing the name of the file does not change the filter name. You can change the filter name after it is imported.

View the status of a redirected restore

A redirected restore may not produce a progress log if the restoring server has no access to write the log files to the requesting server. The name of the requesting server must appear in the server list for the server that performs the restore. (A progress log is an entry on the **Details** tab for a job in the NetBackup web UI.

Progress logs also display in the **View status** dialog box in the **Backup, Archive, and Restore** client interface.)

Consider the following example. `server1` requests a redirected restore from `server2`. To write a log to `server1`, `server1` must appear in the servers list on `server2`.

To add a server requesting a redirected restore to the server list on the restoring server

- 1 In the web UI, sign in to the server that will perform the restore.
For example, sign in to `server2`.
- 2 On the left, select **Hosts > Host properties**.
- 3 Select the primary server.
For example, select `server2`.
- 4 If necessary, click **Connect**. Then click **Edit primary server**.
- 5 Click **Servers**.
- 6 On the **Additional servers** or the **Media servers** tab, click **Add**.
- 7 Enter the name of the server that is requesting the redirected restore.
For example, `server1`.
- 8 Click **Add**.
- 9 Click **Save**.
- 10 Sign into to the requesting server.
For example, `server1`.
Check the **Activity monitor** to determine the success of the restore operation.

Troubleshooting the viewing and managing of jobs

You may see no job results because:

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

If you cannot expand a parent job and see its child jobs, try closing any additional Jobs tabs that you have open.

Some job actions may not be available to workload administrators with limited RBAC permissions on certain assets.

See [“Job actions not available for workload administrators with limited RBAC permissions on assets”](#) on page 53.

Job actions not available for workload administrators with limited RBAC permissions on assets

Note following issues for view and managing jobs with the NetBackup web UI:

- A job does not receive an asset ID until it runs, which means a queued job does not have an asset ID. Users that have roles with more granular asset permissions for a workload are not able to view or cancel queued jobs.
This behavior does not affect users with an RBAC role that has full job permissions or a role that can manage all assets for a particular workload.
- A job does not receive an asset ID if the asset is not yet discovered. Users that have roles with more granular asset permissions for a workload are not able to cancel or restart a job for the asset.
This behavior does not affect users with an RBAC role that has full job permissions or a role that can manage all assets for a particular workload.

Example 1 - VMware administrator with limited asset permissions cannot cancel any queued jobs

Consider a user that has RBAC permissions only for a VMware vCenter or one or more VMs.

- The user cannot see queued jobs for the vCenter or for the VMs.
- Similarly, the user is not able to cancel any queued jobs for the vCenter or for the VMs.

Example 2 - VMware or RHV administrator with limited asset permissions cannot cancel or restart jobs for undiscovered assets

Consider a user that has RBAC permissions only for a VMware vCenter or an RHV server. This user also has one or more job permissions for these assets, but does not have job permissions for all workload assets.

- A new asset is added to the environment, but the discovery process hasn't run yet.
- An existing intelligent group is configured so it includes the new asset.
- When the backup runs, it includes the new asset in the backup.
- The user is not able to cancel or restart a job for the new asset.

Device monitor

This chapter includes the following topics:

- [About the Device Monitor](#)
- [About media mount errors](#)
- [About pending requests and actions](#)

About the Device Monitor

Use the **Device monitor** to manage your tape drives, disk pools, and service requests for operators, as follows:

Media mounts	See “About media mount errors” on page 56.
Pending requests and actions	See “About pending requests and actions” on page 57. See “About pending requests for storage units” on page 58. See “Resubmit a pending request” on page 60. See “Resolve a pending action” on page 59. See “Deny a pending request” on page 60.

Tape drives	<p>See “Change a drive comment” on page 130.</p> <p>See “About downed drives” on page 131.</p> <p>See “Change a drive operating mode” on page 131.</p> <p>See “Clean a tape drive” on page 134.</p> <p>See “Reset a drive” on page 135.</p> <p>See “Reset the mount time of a drive” on page 135.</p> <p>See “Set the drive cleaning frequency” on page 136.</p> <p>See “View drive details” on page 136.</p> <p>See “Deny a pending request” on page 60.</p>
Disk pools	<p>More information about disk pools is available in the NetBackup guide for your disk storage option:</p> <ul style="list-style-type: none"> ■ The <i>NetBackup AdvancedDisk Storage Solutions Guide</i>. ■ The <i>NetBackup Cloud Administrator's Guide</i>. ■ The <i>NetBackup Deduplication Guide</i>. ■ The <i>NetBackup OpenStorage Solutions Guide for Disk</i>. ■ The <i>NetBackup Replication Director Solutions Guide</i>.

About media mount errors

Errors can occur when media is mounted for NetBackup jobs. Depending on the type of error, NetBackup adds the mount request to the pending requests queue or cancels the mount request, as follows:

Adds to the pending requests queue	<p>When NetBackup adds the mount request to the queue, NetBackup creates an operator-pending action. The action appears in the Device monitor. A queued mount request leads to one of the following actions:</p> <ul style="list-style-type: none"> ■ The mount request is suspended until the condition is resolved. ■ The operator denies the request. ■ The media mount time out is reached.
Cancels the request	<p>When a mount request is automatically canceled, NetBackup tries to select other media to use for backups. (Selection applies only in the case of backup requests.)</p> <p>Many conditions lead to a mount request being automatically canceled instead of queued. When a media mount is canceled, NetBackup selects different media so that the backup is not held up.</p>

When NetBackup selects different media

The following conditions can lead to automatic media reselection:

- The requested media is in a DOWN drive.
- The requested media is misplaced.
- The requested media is write protected.
- The requested media is in a drive not accessible to the media server.
- The requested media is in an offline ACS LSM (Automated Cartridge System Library Storage Module). (ACS robot type only.)
- The requested media has an unreadable barcode. (ACS robot type only.)
- The requested media is in an ACS that is not accessible. (ACS robot type only.)
- The requested media is determined to be unmountable.

About pending requests and actions

In the **NetBackup web UI** click **Storage > Device Monitor**. Then click on the **Device monitor** tab. If requests await action or if NetBackup acts on a request, the request displays in the **Pending requests** pane. For example, if a tape mount requires a specific volume, the request displays in the **Pending requests** pane. If NetBackup requires a specific volume for a restore operation, NetBackup loads or requests the volume.

If NetBackup cannot service a media-specific mount request automatically, it changes the request or action to a pending state.

Table 5-1 Pending states

Pending state	Description
Pending request	<p>Specifies that a pending request is for a tape mount that NetBackup cannot service automatically. Operator assistance is required to complete the request. NetBackup displays the request in the Pending requests pane.</p> <p>NetBackup assigns pending status to a mount request when it cannot determine the following:</p> <ul style="list-style-type: none">■ Which standalone drive to use for a job.■ Which drive in a robot is in Automatic Volume Recognition (AVR) mode.

Table 5-1 Pending states (*continued*)

Pending state	Description
Pending action	Specifies that a tape mount request becomes a pending action when the mount operation encounters problems, and the tape cannot be mounted. Operator assistance is required to complete the request, and NetBackup displays an action request in the Pending requests pane. Pending actions usually occur with drives in robotic libraries.

About pending requests for storage units

In the **NetBackup web UI**, click **Storage > Device Monitor**. Then click on the **Device monitor** tab.

The following tape mount requests do not appear in the **Pending requests** pane:

- Requests for backups
- Requests for a tape that is required as the target of a duplication operation

These requests are for resources in a storage unit and therefore are not for a specific volume. NetBackup does not assign a mount request for one storage unit to the drives of another storage unit automatically. Also, you cannot reassign the mount request to another storage unit.

If the storage unit is not available, NetBackup tries to select another storage unit that has a working robot. If NetBackup cannot find a storage unit for the job, NetBackup queues the job (a **Queued** state appears in the Activity monitor).

You can configure NetBackup so that storage unit mount requests are displayed in the **Device monitor** if the robot or drive is down. Pending requests display in the **Device monitor**, and you can assign these mount requests to drives manually.

Resolve a pending request

Use the following procedure to resolve a pending request.

To resolve a pending request

- 1** Insert the requested volume in a drive that matches the density of the volume that was requested.
- 2** Open the NetBackup web UI.
- 3** On the left, click **Storage > Tape storage**. Then click on the **Device monitor** tab.
- 4** In the **Pending requests** pane, select the request and note the contents of the following columns of the request:

- Density
 - Recorded media ID
 - Mode
- 5 Find a drive type that matches the density for the pending request.
 - 6 Verify that the drive is up and not assigned to another request.
 - 7 Locate the drive. Then ensure that the drive and the pending request are on the same host.
 - 8 If necessary, get the media, write-enable it, and insert it into the drive.
 - 9 Wait for the drive to become ready, as explained in the vendor's drive equipment manual.
 - 10 Locate the request. Then click **Actions > Assign request**.
 - 11 Verify that the request was removed from the **Pending requests** pane.
 - 12 Click on the drive name, then click on the **Drive status** tab.
 Verify that the job request ID appears in the Request ID column for the drive.

Resolve a pending action

A pending action is similar to a pending request. For a pending action, NetBackup determines the cause of the problem and issues an instruction to the operator to resolve the problem.

Use the following procedure to resolve a pending action.

To resolve a pending action

- 1 Open the NetBackup web UI.
- 2 On the left, click **Storage > Tape storage**. Then click on the **Device monitor** tab.
- 3 In the **Pending requests** pane, locate the pending action.
- 4 Click **Actions > Display pending action**.
- 5 Review the list of possible actions and click **OK**.
- 6 Correct the error condition and either resubmit the request or deny the request.

See ["Resubmit a pending request"](#) on page 60.

See ["Deny a pending request"](#) on page 60.

Resubmit a pending request

After you correct a problem with a pending action, you can resubmit the request.

If the problem is a volume missing from a robot, first locate the volume, insert it into the robot, and then update the volume configuration. Usually, a missing volume was removed from a robot and then requested by NetBackup.

To resubmit a request

- 1 Open the NetBackup web UI.
- 2 On the left, click **Storage > Tape storage**. Then click on the **Device monitor** tab.
- 3 In the **Pending requests** pane, locate the request.
- 4 Click **Actions > Resubmit request**.

Deny a pending request

Some situations may require that you deny requests for service. For example, when a drive is not available, you cannot find the volume, or the user is not authorized to use the volume. When you deny a request, NetBackup sends an appropriate status message to the user.

To deny a request

- 1 Open the NetBackup web UI.
- 2 On the left, click **Storage > Tape storage**. Then click on the **Device monitor** tab.
- 3 In the **Pending requests** pane, locate the request.
- 4 Then click **Actions > Deny request**.

Notifications

This chapter includes the following topics:

- [Job notifications](#)
- [NetBackup event notifications](#)

Job notifications

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

- Notifications when job failures occur. NetBackup supports the ticketing systems that use inbound email service for ticket creation.
See [“Send email notifications for job failures”](#) on page 61.
- Notifications to the backup administrator about backups with a non-zero status.
See [“Send notifications to the backup administrator about failed backups”](#) on page 64.
- Notifications to the host administrator about successful and failed backups for a specific host.
See [“Send notifications to a host administrator about backups”](#) on page 65.

Send email notifications for job failures

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

See [“Status codes that generate alerts”](#) on page 63.

NetBackup generates alerts based on certain job failure conditions or NetBackup status codes. Alerts that are similar or have a similar reason for failure are marked as duplicates. Email notifications for duplicate alerts are not sent for the next 24

hours. If a notification cannot be sent, NetBackup retries every 2 hours, up to three attempts.

NetBackup audits an event if changes are made to the alert settings or when it cannot generate an alert or send an email notification. See [“About NetBackup auditing”](#) on page 209.

Prerequisites

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

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

To configure email notifications

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

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

Exclude specific status codes from email notifications

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

To exclude specific status codes

- 1 At the top right, click **Settings > Email notifications**.
- 2 Locate **Exclude status codes**.

- 3 Enter the status codes or a range of status codes (separated by commas) for which you do not want to receive email notifications.
- 4 Click **Save**.

Sample email notification for an alert

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

Example email notification:

```
Primary Server: primary1.example.com
Client Name: client1.example.com
Job ID: 50
Job Start Time: 2018-05-17 14:43:52.0
Job End Time: 2018-05-17 15:01:27.0
Job Type: BACKUP
Parent Job ID: 49
Policy Name: Win_policy
Policy Type: WINDOWS_NT
Schedule Name: schedule1
Schedule Type: FULL
Status Code: 2074
Error Message: Disk volume is down
```

Status codes that generate alerts

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

[Table 6-1](#) lists some of the conditions or status codes for which alerts are generated. These alerts are sent to the ticketing system through email notifications.

Table 6-1 Examples of status codes that generate alerts

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

Send notifications to the backup administrator about failed backups

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

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

See [“Configure the nbmail.cmd script on the Windows hosts”](#) on page 65.

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

See [“Send notifications to a host administrator about backups”](#) on page 65.

To send notifications to the backup administrator about failed backups

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

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

Send notifications to a host administrator about backups

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

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

See [“Configure the nbmail.cmd script on the Windows hosts”](#) on page 65.

To send notifications for backups of a specific host

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

Configure the nbmail.cmd script on the Windows hosts

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

To configure the nbmail.cmd script on the Windows hosts

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

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

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

The following options are used in the script:

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

5 Adjust the lines as follows:

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

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

6 Save `nbmail.cmd`.

NetBackup event notifications

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

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

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

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

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

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

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

View notifications

To view notifications

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

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

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

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

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

Modify or disable NetBackup event notifications in the web UI

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

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

Disable event notifications

To disable event notifications

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

```
DISABLE.NotificationType = true
```

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

```
Or DISABLE.namespace
```

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

See [“NetBackup event types supported with notifications”](#) on page 70.

For example:

- To disable notifications about all storage unit events:

```
DISABLE.StorageUnit = true
```

- To disable only notifications about create storage unit events:

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

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

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

Modify event notifications

To modify the priority or severity of event notifications

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

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

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

Valid priority values are: LOW, MEDIUM, HIGH

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

For example:

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

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

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

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

NetBackup event types supported with notifications

The following NetBackup event types support event notifications in the NetBackup web UI.

Table 6-2 NetBackup event types supported with notifications

Event type and notification type value	Action	Severity	Sample notification message
Autodiscovery and Discover Now <code>AutoDiscoveryEvent</code>	no actions	INFO	An appropriate notification is generated when an autodiscovery action or a Discover Now action is performed for VMWare, RHV, or Cloud servers.
	no actions	CRITICAL	<p>Note: An appropriate notification is generated when an autodiscovery action or a Discover Now action fails for VMWare, RHV, Nutanix, or Cloud servers.</p> <p>Note: An appropriate notification is generated when an autodiscovery action or a Discover Now action fails for VMWare, RHV, or Cloud servers.</p>
CRL Health	Not applicable	CRITICAL	The CRL on host \$ {hostName} is not refreshed.
Catalog Backup Health	Not applicable	CRITICAL	One or more users who can access the identity files that need to be backed up as part of the disaster recovery (DR) package, do not exist on the system.
Catalog Image Expiration <code>Catalog</code> Note: Also applicable for manual image expiration.	Not applicable	CRITICAL	<p>Event for Catalog Image received. No additional details found.</p> <p>Catalog Image <i>Image_Name</i> was modified.</p> <p>Catalog Image <i>Image_Name</i> expired.</p>
cDOT Client <code>cDOTClientEvent</code>	CREATE	INFO	<i>{Cluster_Data_ONTAP_Client_Name}</i> was added as a cDOT client.
	DELETE	CRITICAL	<i>{Cluster_Data_ONTAP_Client_Name}</i> was deleted as a cDOT client.
Certificate Health	Not applicable	CRITICAL	The certificate for host \$ {hostName} is going to expire soon.

Table 6-2 NetBackup event types supported with notifications (*continued*)

Event type and notification type value	Action	Severity	Sample notification message
Client <i>ClientEvent</i>	CREATE	INFO	The client { <i>Client_Name</i> } was created.
	DELETE	CRITICAL	The client { <i>Client_Name</i> } was deleted.
	UPDATE	INFO	The client { <i>Client_Name</i> } was updated.
NetBackup Configuration Health	Not applicable	CRITICAL	The NetBackup configuration file contains multiple <i>CLIENT_NAME</i> entries.
NetBackup Configuration Health	Not applicable	CRITICAL	<p>The service user does not have the required permissions on one or more links or junction target directories. Run the '<i>Install_Path\NetBackup\bin\goodies\nbserviceusercmd.exe -addAcl</i>' command to assign the correct permissions.</p> <p>The service user does not have the required permissions on one or more soft link target directories.</p> <p>The service user does not have the required permissions on ALTPATH directories that are configured for one or more clients. Run the '<i>Install_Path\NetBackup\bin\goodies\nbserviceusercmd.exe -addAcl</i>' command to assign the correct permissions.</p>
NetBackup Configuration Health	Not applicable	INFO	Assigned the execute permission to the service user on one or more NetBackup directories.
NetBackup Configuration Health	Not applicable	WARNING	Could not assign the execute permission to the service user on one or more NetBackup directories.
DBPaaS Operation RCA	Not applicable	CRITICAL	Cannot complete backup. See the Root Cause Identifier (RCA) link for more information.
Drive <i>DriveChange</i>	CREATE	INFO	The drive { <i>Drive_Name</i> } was created for host { <i>Host_Name</i> }.
	DELETE	CRITICAL	The drive { <i>Drive_Name</i> } was deleted for host { <i>Host_Name</i> }.
	UPDATE	INFO	<p>The drive {<i>Drive_Name</i>} was updated for host {<i>Host_Name</i>}.</p> <p>Note: A notification message like this one is generated when a drive is updated for a particular host or when a drive state is changed to UP or DOWN.</p>

Table 6-2 NetBackup event types supported with notifications (*continued*)

Event type and notification type value	Action	Severity	Sample notification message
Isilon Client IsilonClientEvent	CREATE	INFO	<i>{Isilon_Filer_Client_Name}</i> was added as an Isilon client.
	DELETE	CRITICAL	<i>{Isilon_Filer_Client_Name}</i> was deleted as an Isilon client.
KMS Certificate Expiration KMSCredentialStatus	EXPIRY	WARNING	The certificate that is used to communicate with the KMS server <i>{KMS_Server_Name}</i> is about to expire in <i>{days_to_expiration}</i> . If the certificate is not renewed on time, communication with the KMS server fails.
Library Event - Robot Library	CREATE	INFO	The library <i>{Library_Name}</i> was created for host <i>{Host_Name}</i> .
	DELETE	CRITICAL	The library <i>{Library_Name}</i> was deleted for host <i>{Host_Name}</i> .
	UPDATE	INFO	The library <i>{Library_Name}</i> was updated for host <i>{Host_Name}</i> .
Machine [Primary/Media/Cluster] Machine	CREATE	INFO	The host <i>{Host_Name}</i> was created.
	DELETE	CRITICAL	The host <i>{Host_Name}</i> was deleted.
Media Media	CREATE	INFO	The media <i>{Media_ID}</i> was created.
	DELETE	CRITICAL	The media <i>{Media_ID}</i> was deleted.
	UPDATE	INFO	The media <i>{Media_ID}</i> was updated.
Media Group MediaGroup	CREATE	INFO	The media group <i>{Media_Group_ID}</i> was created.
	DELETE	CRITICAL	The media group <i>{Media_Group_ID}</i> was deleted.
	UPDATE	INFO	The media group <i>{Media_Group_ID}</i> was updated.
Media Pool MediaPool	CREATE	INFO	The media pool <i>{Media_Pool_ID}</i> was created.
	DELETE	CRITICAL	The media pool <i>{Media_Pool_ID}</i> was deleted.

Table 6-2 NetBackup event types supported with notifications (*continued*)

Event type and notification type value	Action	Severity	Sample notification message
	UPDATE	INFO	The media pool <i>{Media_Pool_ID}</i> was updated.
Message Broker Service Status <i>ServiceStatus</i>	RUNNING	INFO	The NetBackup Messaging Broker service is running. NetBackup internal notifications are now enabled.
	STOPPED	INFO	The NetBackup Messaging Broker service is stopped. NetBackup internal notifications are now disabled.
Policy <i>Policy</i> Note: When possible, an aggregated policy event for two or more policy actions is created.	Create	INFO	The policy <i>{Policy_Name}</i> was created. Event for Policy received. No additional details found.
	Update	INFO or CRITICAL	The policy <i>{Policy_Name}</i> was activated. The policy <i>{Policy_Name}</i> was deactivated. The policy <i>{Policy_Name}</i> was updated. The client <i>{Policy_Name}</i> was added to the policy <i>\$_{policyName}</i> . The client <i>{Policy_Name}</i> was removed from the policy <i>{Policy_Name}</i> . The schedule <i>{Policy_Name}</i> was added to the policy <i>\$_{Policy_Name}</i> . The schedule <i>{Policy_Name}</i> was removed from the policy <i>{Policy_Name}</i> .
	Delete	CRITICAL	The policy <i>{Policy_Name}</i> was deleted.
Protection Plan <i>ProtectionPlan</i>	Create	INFO	Received an event for protection plan. The protection plan <i>Protection_Plan_Name</i> is created. The protection plan <i>Protection_Plan_Name</i> is created from existing NetBackup policy.
	Update	INFO	The protection plan <i>Protection_Plan_Name</i> is updated.
	Delete	CRITICAL	The protection plan <i>Protection_Plan_Name</i> is deleted.

Table 6-2 NetBackup event types supported with notifications (*continued*)

Event type and notification type value	Action	Severity	Sample notification message
Protection Plan Subscription ProtectionPlanSubscription	Create	INFO	Received an event for protection plan subscription. The Asset_Class Asset_Display_Name is subscribed to protection plan Protection_Plan_Name.
	Update	INFO	The Asset_Class Asset_Display_Name subscription with protection plan Protection_Plan_Name is updated.
	Delete	CRITICAL	The Asset_Class Asset_Display_Name is unsubscribed from protection plan Protection_Plan_Name.
Retention Event RetentionEvent	UPDATE	INFO	Retention level has been changed.
Storage life cycle policy SLP	Create	INFO	Event for Storage Lifecycle Policy received. No additional details found. The Storage Lifecycle Policy {Policy_Name} was created.
	Delete	CRITICAL	The Storage Lifecycle Policy {Policy_Name} was deleted. The Storage Lifecycle Policy {Policy_Name} with version Version_Number was deleted.
Storage life cycle policy state change SlpVersionActInactEvent	UPDATE	INFO	The SLP version {Version} was changed.
Storage Unit StorageUnit Note: Any change to a basic disk staging schedule (DSSU), such as adding, deleting, or modifying, generates relevant storage unit notifications. With those notifications, some additional policy notifications are also generated with policy name __DSSU_POLICY_{Storage_Unit_Name}.	CREATE	INFO	The storage unit {Storage_Unit_Name} was created.
	DELETE	CRITICAL	The storage unit {Storage_Unit_Name} was deleted.
	UPDATE	INFO	The storage unit {Storage_Unit_Name} was updated.

Table 6-2 NetBackup event types supported with notifications (continued)

Event type and notification type value	Action	Severity	Sample notification message
Storage Unit Group StorageUnitGroup	CREATE	INFO	The storage unit group {Storage_Unit_Group_Name} was created.
	DELETE	CRITICAL	The storage unit group {Storage_Unit_Group_Name} was deleted.
	UPDATE	INFO	The storage unit group {Storage_Unit_Group_Name} was updated.
	UPDATE	INFO	The storage service {Storage_Service_Name} was updated.
Usage Reporting UsageReportingEvent	No actions	INFO or ERROR	The usage report generation has started. The usage report is generated successfully. Failed to generate the usage report. For more details, refer to the gather and report logs in the parent directory.
VMware Discovery TAGSDISCOVERYEVENT	no actions	INFO	VMware tags cannot be retrieved.
Web Truststore Health	Not applicable	CRITICAL	One or more files and / or directories do not have appropriate web service user permissions.

About configuring automatic notification cleanup tasks

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

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

From a command line, use `bpsetconfig` or `bpgetconfig` to change the parameter values listed in [Table 6-3](#). See the *NetBackup Command Reference Guide* for more information about these commands.

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

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

See the *NetBackup 10.3.0.1 API Reference* on [SORT](#) for more information about these APIs.

Table 6-3 Configurable parameters for automatic notification cleanup tasks

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

Configuring hosts

- [Chapter 7. Managing host properties](#)
- [Chapter 8. Managing credentials for workloads and systems that NetBackup accesses](#)
- [Chapter 9. Managing deployment](#)

Managing host properties

This chapter includes the following topics:

- [Overview of host properties](#)
- [View or edit the host properties of a server or client](#)
- [Host information and settings in Host properties](#)
- [Reset a host's attributes](#)

Overview of host properties

The configuration options within the **Host properties** let an administrator customize NetBackup to meet specific site preferences and requirements.

To change the properties of another client or server, the NetBackup server that you signed in to must be in the **Servers** list on the other system.

For example, if you logged on to *server_1* and want to change a setting on *client_2*, *client_2* must include *server_1* in its **Servers** list.

For example, if you logged on to *server_1* and want to change a setting on *client_2*, *client_2* must include *server_1* in its **Servers** list.

Some options cannot be configured by using the **NetBackup web UI**. See the *NetBackup Administrator's Guide, Volume I* for details on other configuration options.

A NetBackup administrator can use one of the following methods to read or set the default configuration options.

Table 7-1 NetBackup Host properties configuration methods

Method	Description
NetBackup Web UI interface	Most properties are listed in the NetBackup web UI in Hosts > Host properties . Depending on the host to be configured, select the Primary server , Media server , or Client .
Command line	Use the <code>nbgetconfig</code> command or <code>bpgetconfig</code> command to obtain a list of configuration entries. Then use <code>nbsetconfig</code> or <code>bpsetconfig</code> to change the options as needed. These commands update the appropriate configuration files on both Windows (registry) and UNIX (<code>bp.conf</code> file) primary servers and clients. Use the <code>nbemmcmd</code> command to modify some options on hosts.
<code>vm.conf</code> file	The <code>vm.conf</code> file contains configuration entries for media and device management.
Backup, Archive, and Restore client interface	Administrators can specify configuration options for NetBackup clients.

View or edit the host properties of a server or client

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

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

View or edit the host properties of the primary server

To view or edit the host properties of the primary server

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

View or edit the host properties of a media server

To view or edit the host properties of a media server

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

View or edit the host properties of a client

To view or edit the host properties of a client

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

Host information and settings in Host properties

In **Hosts > Host properties** you can view the information and certain settings for each host in the NetBackup environment.

Table 7-2 Host properties for hosts

Property name	Description	Host type
Host	The NetBackup client name of the host.	Primary server, Media server, Client
Operating system	The operating system and OS version on which the host is installed.	Primary server, Media server, Client
OS type	The type of OS.	Primary server, Media server, Client
Host type	The type of host: Primary server, media server, or client.	Primary server, Media server, Client
IP address	The IP address of the host.	Primary server, Media server, Client

Table 7-2 Host properties for hosts (*continued*)

Property name	Description	Host type
Version	This property is available on the main Host properties page. The NetBackup version of the host.	Primary server, Media server, Client
Status	This property is available on the main Host properties page. Indicates if the host is connected and available for a user to update its host properties. If necessary, select the host and click Connect .	Primary server, Media server, Client
Resiliency	This property is available on the main Host properties page. Indicates if Resilient network settings are configured on the primary server.	Primary server, Media server, Client When a job runs, the primary server updates the media server and the client with the current properties.
Host mappings	This property is available on the main Host properties page. Lists any host mappings that are configured for the host. See “Approve or add mappings for a host that has multiple host names” on page 230.	Primary server, Media server, Client

Reset a host's attributes

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

When you reset a host's attributes:

- NetBackup resets the host ID to host name mapping information, the host's communication status and so on. It does not reset the host ID, host name, or security certificates of the host.

- The connection status is set to the insecure state. The next time the primary server communicates with the host, the connection status is updated appropriately.

To reset the attributes for a host

- 1** On the left, select **Security > Host mappings**.
- 2** Locate the host and click **Actions > Reset attributes**.
- 3** Choose if you want to communicate insecurely with 8.0 and earlier hosts.
NetBackup can communicate with a 8.0 or earlier host when the **Allow communication with NetBackup 8.0 and earlier hosts** option is enabled in the **Global Security Settings**. This option is enabled by default.

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

Managing credentials for workloads and systems that NetBackup accesses

This chapter includes the following topics:

- [Overview of credential management in NetBackup](#)
- [Add a credential in NetBackup](#)
- [Add a credential for an external KMS](#)
- [Add a credential for NetBackup Callhome Proxy](#)
- [Edit or delete a named credential](#)
- [Add a credential for CyberArk](#)
- [Configure external credentials](#)
- [Add a configuration for an external CMS server](#)
- [Edit or delete the configuration for an external CMS server](#)
- [Add a credential for Network Data Management Protocol \(NDMP\)](#)
- [Edit or delete Network Data Management Protocol \(NDMP\) credentials in NetBackup](#)
- [Troubleshooting the external CMS server issue](#)

Overview of credential management in NetBackup

Credential management lets you centrally manage the credentials that NetBackup uses to access systems and the workloads that it protects. You can manage NetBackup credentials and External CMS server configurations from **Credential management**.

Credentials can be managed for the following workloads:

- Cassandra
- Cloud (for a cloud instance)
- Cloud object store
- Kubernetes
- Microsoft SQL Server
- MySQL Server
- Nutanix AHV
- Nutanix AHV Prism Central
- Oracle
- PaaS database
- PostgreSQL Server
- SaaS

Credentials can also be managed for the following systems:

- A Call Home proxy server
- CyberArk
- Disk arrays
- External Key Management Services (KMS)
- Malware detection (Malware scan host)
- Microsoft Sentinel
- NDMP
- VMware guest VM

More information

See [“Add a credential for NetBackup Callhome Proxy”](#) on page 86.

See [“Add a credential for an external KMS”](#) on page 85.

See [“Add a credential for Network Data Management Protocol \(NDMP\)”](#) on page 93.

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

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

Add a credential in NetBackup

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

- See [“Add a credential for NetBackup Callhome Proxy”](#) on page 86.
- See [“Add a credential for an external KMS”](#) on page 85.
- See [“Add a credential for Network Data Management Protocol \(NDMP\)”](#) on page 93.
- See [“Add a credential for CyberArk”](#) on page 88.
- See [“Configure external credentials”](#) on page 90.
- See [“Add a configuration for an external CMS server”](#) on page 91.

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

[NetBackup documentation portal](#)

Add a credential for an external KMS

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

To add a credential for an external KMS

- 1 On the left, click **Credential management**.
- 2 On the **Named credentials** tab, click **Add** and provide the following properties:
 - Credential name
 - Tag
 - Description (for example: This credential is used to access the external KMS.)
- 3 Click **Next**.

- 4** Select **External KMS**.
- 5** Provide the credential details that are needed for authentication.
These details are used to authenticate the communication between the NetBackup primary server and the external KMS server:
 - Certificate - Specify the certificate file contents.
 - Private key - Specify the private key file contents.
 - CA Certificate - Specify the CA certificate file contents.
 - Passphrase - Enter the passphrase of the private key file.
 - CRL check level - Select the revocation check level for the external KMS server certificate.
CHAIN - The revocation status of all the certificates from the certificate chain are validated against the CRL.
DISABLE - Revocation check is disabled. The revocation status of the certificate is not validated against the CRL during host communication.
LEAF - The revocation status of the leaf certificate is validated against the CRL.
- See the [NetBackup Security and Encryption Guide](#) for more information on external KMS configuration.
- 6** Click **Next**.
- 7** Add a role that you want to have access to the credential.
 - Click **Add**.
 - Select the role.
 - Select the credential permissions that you want the role to have.
- 8** Click **Next** and follow the prompts to complete the wizard.

Add a credential for NetBackup Callhome Proxy

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

To add a credential for NetBackup Callhome Proxy

- 1** On the left, click **Credential management**.
- 2** On the **Named credentials** tab, click **Add** and provide the following properties:
 - Credential name
 - Tag

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

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

Edit or delete a named credential

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

Edit a named credential

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

To edit a named credential

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

Delete a named credential

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

To delete a named credential

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

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

Add a credential for CyberArk

This type of credential allows you to access an external CMS server.

To add a credential for an external CMS server

- 1 On the left, click **Credential management**.
- 2 On the **Named credentials** tab, click **Add**.
- 3 Select **NetBackup** and click **Start**.

On **Add a credential** page, provide the following properties:

- Credential name
- Tag
- Description (for example: This credential is used to access the external CMS.)

- 4 Click **Next**.
- 5 Select **CyberArk** as the category.
- 6 Provide the credential details for CyberArk server:

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

- Certificate - Specify the certificate file contents.
- Private key - Specify the private key file contents.

- CA Certificate - Specify the CA certificate file contents.
 - Passphrase - Enter the passphrase of the private key file.
 - CRL check level - Select the revocation check level for the external CMS server certificate.
 - CHAIN - The revocation status of all the certificates from the certificate chain are validated against the CRL.
 - DISABLE - Revocation check is disabled. The revocation status of the certificate is not validated against the CRL during host communication.
 - LEAF - The revocation status of the leaf certificate is validated against the CRL.
- 7 Click **Next**.
- 8 Add a role that you want to have access to the credential.
- Click **Add**.
 - Select the role.
 - Select the credential permissions that you want the role to have.
- 9 Click **Next** and follow the prompts to complete the wizard.

Certificate revocation lists for CyberArk server

Certificate revocation list (CRL) for an external certificate authority (CA) contains a list of digital certificates that the external CA has revoked before the scheduled expiration date and should no longer be trusted. NetBackup supports PEM and DER formats for CRLs for external CA. CRL's for all CRL issuers or external CA's are stored in the NetBackup CRL cache that resides on each host. During secure communication, NetBackup host verifies the revocation status of the peer host's external certificate with the CRL that is available in the NetBackup CRL cache, based on the CRL check level configuration option. For external CMS server, NetBackup supports CDP based server certificates.

NetBackup downloads the CRLs from the URLs that are specified in the peer host certificate's CDP and caches them in the NetBackup CRL cache.

To use CRL's from CDP:

- Ensure that the host can access the URLs that are specified in the peer host's CDP.
- Ensure that the **CRL check level** configuration option is set to a value other than **DISABLE**.

By default, CRLs are downloaded from the CDP after every 24 hours and updated in the CRL cache. To change the time interval, set the

ECA_CRL_REFRESH_HOURS configuration option to a different value. To manually delete the CRL's from the CRL cache, run the `nbcertcmd -cleanupCRLCache` command. The NetBackup CRL cache contains only the latest copy of a CRL for each CA (including root and intermediate CAs). The `bpcintcmd -crl_download` service updates the CRL cache during host communication in the following scenarios irrespective of the time interval set for the **ECA_CRL_REFRESH_HOURS** options:

- When CRLs in the CRL cache are expired.
- If CRLs are available in the CRL source, but they are missing from the CRL cache.

For details of **ECA_CRL_REFRESH_HOURS**, refer to **ECA_CRL_REFRESH_HOURS** for NetBackup servers and clients section from *Veritas NetBackup™ Security and Encryption Guide*.

Note: By default, the **ECMS_HOSTS_SECURE_CONNECT_ENABLED** flag is enabled (set to true). If this flag is enabled, the certificate deployed on the external CMS server must have Common Name or Subject Alternative Name that matches the host name of the external CMS server. Else, the connection to the external CMS server fails. For more information, see the **ECMS_HOSTS_SECURE_CONNECT_ENABLED** section in *NetBackup™ Administrator's Guide, Volume I*.

Configure external credentials

This type of credential allows you to configure an external CMS server.

An **External** credential can only be created if an external CMS server configuration exists.

To configure external credentials

- 1 On the left, click **Credential management**.
- 2 On the **Named credentials** tab, click **Add**.
- 3 Select **External** and click **Start**.

On **Add a credential** page, provide the following properties:

- Credential name
- Tag
- Description

- 4 Select the appropriate **Category** to assign the credential.

5 Search and select the **External CMS configuration**.

Provide the following parameter details for CyberArk Server:

- Application ID - Unique ID of the application issuing the password request.
- Object - Name of the password object to retrieve.
- Safe - Name of the Safe where the password is stored.

For more information on the parameters for CyberArk server, see [Call the Web Service using REST](#).

6 Click **Next**.

7 Add a role that you want to have access to the credential.

- Click **Add**.
- Select the role.
- Select the credential permissions that you want the role to have.

8 Click **Next** and follow the prompts to complete the wizard.

Add a configuration for an external CMS server

This section provides you the procedure for adding a configuration for an external CMS server.

To add a configuration for an external CMS server

1 On the left, click **Credential management**.

2 On the **External CMS servers** tab, click **Add** and provide the following properties:

- Configuration name
- Description (for example: This configuration is used to access the external CMS.)
- External CMS provider
- Host name
- Port number: Default port number 443 would be considered (if not provided by the user).

Note: While configuring the external CMS server for CyberArk server, user can use the DNS hostname or IPV4 address. However it is recommended to use the DNS hostname for connecting to the host. CyberArk configuration fails if IPV6 address is used.

- 3 Click **Next**.
- 4 On the Associate credentials page, **Select existing credential** or **Add a new credential**.

 More information is available on how to add a new credential.

 See [“Add a credential for CyberArk”](#) on page 88.
- 5 Click **Next** and follow the prompts to complete the wizard.

Edit or delete the configuration for an external CMS server

You can edit the properties of the configuration or delete the configuration from the **Credential management**.

Edit the configuration

You can edit the configuration to change the Description only. You cannot change the following properties: Configuration name, External CMS provider, Host name and Port number.

To edit the configuration

- 1 On the left, click **Credential management**.
- 2 On the **External CMS servers** tab, locate and click on the configuration that you want to edit.
- 3 Click **Edit** and update the properties as needed.
- 4 Review the changes and click **Next**.
- 5 Select an existing credential or add a new credential and click **Next**.
- 6 Review the changes and click **Finish**.

Delete the configuration

You can delete the configuration that you no longer need to use with NetBackup.

To delete the configuration

- 1 On the left, click **Credential management**.
- 2 On the **External CMS servers** tab, locate and click on the configuration that you want to delete.
- 3 Click **Delete**.
- 4 Confirm the deletion by clicking on **Remove**.

Add a credential for Network Data Management Protocol (NDMP)

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

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

To add an NDMP credential

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

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

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

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

Edit an NDMP credential

To edit an NDMP credential

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

Delete an NDMP credential

To delete an NDMP credential

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

Troubleshooting the external CMS server issue

If the CyberArk Application ID contains internationalized characters and CyberArk server does not have the appropriate language pack installed, then the NetBackup user encounters a failure in adding the workload credentials from CyberArk.

Recommended action:

If the CyberArk Application Id contains internationalized characters, then install the corresponding language pack on the CyberArk server.

Managing deployment

This chapter includes the following topics:

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

Managing the NetBackup Package repository

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

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

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

- Add new packages.
- Delete existing packages.

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

To add packages

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

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

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

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

To delete packages

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

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

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

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

Update host

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

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

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

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

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

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

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

Deployment policies

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

To add a new policy:

- 1 Navigate to **Hosts > Deployment management > Deployment policies** and select **Add**.
- 2 Enter the required information for deployment policies.
The required deployment policy information is similar to the update host information.
See [“Update host”](#) on page 96.
- 3 Select **Save**.

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

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

Configuring storage

- [Chapter 10. Overview of storage options](#)
- [Chapter 11. Configuring storage units](#)
- [Chapter 12. Configuring disk storage](#)
- [Chapter 13. Managing media servers](#)
- [Chapter 14. Managing tape drives](#)
- [Chapter 15. Staging backups](#)
- [Chapter 16. Troubleshooting storage configuration](#)

Overview of storage options

This chapter includes the following topics:

- [About storage configuration](#)

About storage configuration

NetBackup lets you configure storage options for all protection plans and policies. To set up storage options, on the left click **Storage**.

You can configure the following types of storage:

- Storage units
- Storage lifecycle policies (SLPs)
- Disk storage
- Tape storage
- Snapshot Manager
See the [NetBackup Snapshot Manager for Data Center Administrator's Guide](#) for details.
- Media servers

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

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

Use the following command to update the storage server:

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

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

Configuring storage units

This chapter includes the following topics:

- [Overview of storage units](#)
- [Create a storage unit](#)
- [Edit storage unit settings](#)
- [Copy a storage unit](#)
- [Delete a storage unit](#)
- [About universal shares](#)
- [Create a universal share](#)
- [View or edit a universal share](#)
- [Delete a universal share](#)

Overview of storage units

A storage unit is a label that NetBackup associates with physical storage or cloud storage. The label can identify a path to a volume or a disk pool. Storage units can be included as part of a storage lifecycle policy.

The following types of storage units are available in the NetBackup web UI.

Table 11-1 Storage unit types

Storage unit type	Storage type or location	Option required
Media Server Deduplication Pool (MSDP)	Points to local or cloud storage.	Data Protection Optimization Option

Table 11-1 Storage unit types (*continued*)

Storage unit type	Storage type or location	Option required
AdvancedDisk	Points to a disk pool (storage directly attached to a media server).	Data Protection Optimization Option
OpenStorage Technology (OST))	Points to a disk pool of the type <i>StorageName</i> .	OpenStorage Disk Option
Cloud Connector	Points to a disk pool of the type <i>VendorName</i> , where <i>VendorName</i> can be the name of a cloud storage provider.	
BasicDisk	Points to a directory.	

Create a storage unit

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

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

To create a storage unit

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

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

- 2 In the **Storage type** drop-down, select the option you want to use.
- 3 Select the storage unit from the list and click **Start**.
- 4 In **Basic properties**, enter all required information and click **Next**.

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

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

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

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

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

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

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

See [“Create a disk pool”](#) on page 111.

See [“Create a Media Server Deduplication Pool \(MSDP, MSDP Cloud\) storage server”](#) on page 113.

See [“Create an AdvancedDisk, OpenStorage \(OST\), or Cloud Connector storage server”](#) on page 121.

See [“Create a protection plan”](#) on page 156.

Edit storage unit settings

This option is only available for then **Disk** storage unit type.

Only make changes to a storage unit during periods when no backup activity is expected. This way backups are not affected for the policies or protection plans that use the affected storage units.

To edit storage unit settings

- 1 Click **Storage units**.
- 2 Click on the storage unit that you want to edit.
- 3 Select **Edit** and make the required changes.

For example, you can edit the following settings:

- The basic properties of the storage unit.
- Disk pool

- Media server
- Staging schedule

Copy a storage unit

You can copy a storage unit to create a new storage unit with the same settings. This option is only available for **Disk** storage unit type.

To copy a storage unit

- 1
- 2 Click **Storage units**.
- 3 Select the storage unit that you want to copy and click **Copy storage unit**.
- 4 Type a unique name for the new storage unit. For example, describe the type of storage. Use this name to specify a storage unit for policies and schedules.
- 5 Edit the other properties and disk pool as necessary.
- 6 After reviewing the changes, click **Save**.

Delete a storage unit

To delete a storage unit from a NetBackup configuration means to delete the label that NetBackup associates with the physical storage.

Deleting a storage unit does not prevent files from being restored that were written to that storage unit. (As long as the storage was not physically removed and the backup image has not expired.)

To delete a storage unit

- 1 Open the NetBackup web UI.
- 2 Use the **Catalog** utility to expire any images that exist on the storage unit. This action removes the image from the NetBackup catalog.

See [“Expire backup images”](#) on page 199.

- Do not manually remove images from a BasicDisk or a Media Manager storage unit.
- After the images are expired, they cannot be restored unless the images are imported.

See [“About importing backup images”](#) on page 200.

NetBackup automatically deletes any image fragments from a disk storage unit or a disk pool. This deletion generally occurs within seconds of expiring an

image. However, to make sure that all of the fragments are deleted, confirm that the directory is empty on the storage unit.

- 3 Select the storage unit that you want to delete.
 - 4 Click **Delete > Yes**.
 - 5 Modify any policy that uses a deleted storage unit to use another storage unit.
- If a storage unit points to disk pool, you can delete the storage unit without affecting the disk pool.

About universal shares

The universal share feature provides data ingest into an existing NetBackup deduplication pool (MSDP) or a supported Veritas appliance using an NFS or a CIFS (SMB) share. Space efficiency is achieved by storing this data directly into an existing NetBackup-based Media Server Deduplication Pool.

For more information about universal shares, see the following guides:

Create a universal share

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

You can manage universal shares across NetBackup Appliance, Flex Appliance, Flex Scale, Flex WORM/non-WORM, MSDP AKS/EKS deployment, build-your-own (BYO) and BYO-In-Cloud servers.

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

If you want to view specific storage servers containing universal shares, click on **Select storage server** in the top right. Then, select the storage servers that contain universal shares, and they are displayed in the table.

To create a universal share in the NetBackup web UI

- 1 If necessary, configure an MSDP storage server.
See [“Create a Media Server Deduplication Pool \(MSDP, MSDP Cloud\) storage server”](#) on page 113.
- 2 On the left, click **Storage > Disk storage**.

- 3 Click on the **Universal shares** tab. Then click **Add**.
- 4 Provide the following required information:
 - Enter a **Display name**. This name is used in the universal share path.
 - Select a **Type**. If you want to set up **Cloud cache properties**, you must select **Regular**. If **Accelerator** type is selected, you must specify the **Disk volume**.
 - Select the **Storage server**.
 - Select the **Disk volume**.

When **Accelerator** is selected in **Type**, you can only select a cloud disk volume in the pop-up.

Click the search icon to get the volume list, and select the disk volume.

PureDiskVolume is selected by default.

This option is available only if universal share with object storage in cloud feature is enabled. For more information, see the *NetBackup Deduplication Guide*.
 - In **Cloud cache properties**, specify the size of the local disk cache in the **Request cloud cache disk space**.

The **Request cloud cache disk space** can only be set here on initial setup. Any subsequent changes must be made on the storage server properties page.

Note: When you update the **Cloud cache properties** setting in storage server properties page, there is an interruption of the current shared mounts. When you click **Save**, the `vpfsd` process restarts to apply the new value.

In addition, new universal shares cannot be created if the available size is less than 128GB.

 - Select the **Protocol**: **NFS** or **SMB** (CIFS)
 - Specify a **Host** that is allowed to mount the share and then click **Add to list**. You can use the host name, IP address, short name, or the FQDN to specify the **Host**. You can enter multiple hosts for each share.

When **Accelerator** is selected in **Type**, the **Host** can only be FQDN.
- 5 At this point, continue to enter values in the remaining fields or click **Save** to save the universal share. You can update the remaining fields later from the universal share's details page:
 - Select a **Quota** type: **Unlimited** or **Custom**. If you select **Custom**, also specify the quota in MB, GB, or TB units.

The **Custom** quota value limits the amount of data that is ingested into the share. Quotas are enforced using the front-end terabyte (FETB) calculation method. They are implemented per share and can be modified at any time. You do not need to remount the share for the change to take effect.

To update the quote type or value from the universal share's details page, click **Edit** in the Quota section.

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

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

- Specify Kerberos security methods if the selected protocol is NFS and the Kerberos service is supported on the selected Storage server.
If you select more than one Kerberos security methods, you can specify any method as mount command option to the share from client host.
 - Kerberos 5
Uses Kerberos V5 instead of local UNIX UIDs and GIDs to authenticate the users.
 - Kerberos 5i
Uses Kerberos V5 for user authentication and performs integrity checking of NFS operations using the secure checksums to prevent tampering of the data.
 - Kerberos 5p
Uses Kerberos V5 for user authentication and integrity checking. It encrypts NFS traffic to prevent traffic sniffing. This option is the most secure setting but it also involves the most performance overhead.

Using instant access for MS-Windows and Standard policies

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

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

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

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

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

View or edit a universal share

You can view the details of a universal share or edit certain attributes of the universal share.

View details of a universal share

To view the details of a universal share

- 1 On the left, click **Storage > Disk storage**. Then click on the **Universal shares** tab.

- 2 Locate the universal share and click on its name.

Use the **Filters** to display specific universal shares. For example, universal shares with the **SMB** protocol or universal shares whose state is **Exported**.

The **ID** is the UUID of the universal share.

The **Export path** is the path is used in a universal share backup policy.

The **Mount path** is the path that is used to connect from the client.

Edit a universal share

You can edit the quota for the share and the hosts that can mount the share.

To edit a universal share

- 1 On the left, click **Storage > Disk storage**. Then click on the **Universal shares** tab.
- 2 Locate the universal share and click on its name.
- 3 You can edit the following details for the universal share.

Quota	Click Edit to change the quota for the share.
Hosts	Click Edit to add or delete the hosts that can mount the share.
Kerberos	<p>Click Edit to change the Kerberos security method if the selected protocol is NFS and the Kerberos service is supported on the selected storage server.</p> <p>For more information about the Kerberos support for universal shares, see the <i>NetBackup Deduplication Guide</i>.</p> <p>Note: When the Kerberos security method is updated, it affects the ability to connect NFS server from the clients configured in the current universal share. Use the Kerberos security method you have updated as a mount command parameter to mount NFS server again.</p>

Delete a universal share

You can delete a universal share from NetBackup storage.

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

To delete a universal share

- 1 On the left, click **Storage > Disk storage**. Then click on the **Universal shares** tab.
- 2 Select the universal share that you want to delete and click **Delete > Delete**.

Configuring disk storage

This chapter includes the following topics:

- [About configuring BasicDisk storage](#)
- [About configuring disk pool storage](#)
- [Create a disk pool](#)
- [Editing a disk pool](#)
- [Create a Media Server Deduplication Pool \(MSDP, MSDP Cloud\) storage server](#)
- [Editing a storage server](#)
- [Integrating MSDP Cloud and CMS](#)
- [Create a Media Server Deduplication Pool \(MSDP\) storage server for image sharing](#)
- [Create an AdvancedDisk, OpenStorage \(OST\), or Cloud Connector storage server](#)
- [Using image sharing from the NetBackup web UI](#)

About configuring BasicDisk storage

A **BasicDisk** type storage unit consists of a directory on locally-attached disk or network-attached disk. The disk storage is exposed as a file system to a NetBackup media server. NetBackup stores backup data in the specified directory.

No special configuration is required for **BasicDisk** storage. You specify the directory for the storage when you configure the storage unit.

About configuring disk pool storage

You can configure disk pools if you license a NetBackup feature that uses disk pools.

For more information, see the following guides:

- *The NetBackup AdvancedDisk Storage Solutions Guide.*
- *The NetBackup Cloud Administrator's Guide.*
- *The NetBackup Deduplication Guide.*
- *The NetBackup OpenStorage Solutions Guide for Disk.*
- *The NetBackup Replication Director Solutions Guide.*
- *The NetBackup Administrator's Guide, Volume I.*

Create a disk pool

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

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

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

To create a disk pool

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

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

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

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

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

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

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

Note: Veritas Alta Recovery Vault supports multiple options. For Veritas Alta Recovery Vault Amazon and Amazon Government options in the web UI, you must contact your Veritas NetBackup account manager for credentials or with any questions.

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

For more information about Veritas Alta Recovery Vault Azure options, refer to *About Veritas Alta Recovery Vault Azure* in the [NetBackup Deduplication Guide](#).

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

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

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

Replication is supported only on MSDP.

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

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

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

Editing a disk pool

This procedure tells you how to edit a disk pool.

To edit a disk pool

- 1 On the left, click **Storage > Disk storage**. Click the **Disk pools** tab.
- 2 Click on the **Name** of the disk pool you want to edit.
- 3 On the disk pool details page, Click **Edit** to edit the following parameters of the disk pool:
 - Disk pool options
 - Cloud cache properties
 - Associated cloud credentials
 - General settings
 - Proxy settings
- 4 Under Replication targets, click **Add** to add the replication targets.

Create a Media Server Deduplication Pool (MSDP, MSDP Cloud) storage server

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

To add an MSDP storage server

- 1 Sign in to the NetBackup web UI.
- 2 On the left, click **Storage > Storage units**. Click the **Storage units** tab, then click **Add**.
- 3 In the **Storage type** drop-down, select the option you want to use.
- 4 Select **Media Server Deduplication Pool (MSDP, MSDP Cloud)** from the list.
- 5 In **Basic properties**, enter all required information and click **Next**.
 You must select your media server by clicking on the field. If you do not see the media server you want to use, you can use **Search** to find it.
- 6 In **Storage server options**, enter all required information and click **Next**.

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

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

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

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

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

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

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

Enter the required information to create a disk pool.

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

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

For more information about the storage API types that NetBackup supports, refer to the *About the cloud storage vendors for NetBackup* section in the [NetBackup Cloud Administrator's Guide](#).

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

Note: For more information on environments and deployment of Veritas Alta Recovery Vault for NetBackup, refer to the following article:

<https://www.veritas.com/docs/100051821>

Before you enable the Veritas Alta Recovery Vault Azure and Azure Government options, review the steps from the *Configuring Veritas Alta Recovery Vault Azure and Azure Government* section in the [NetBackup Deduplication Guide](#).

Veritas Alta Recovery Vault supports multiple options. For Veritas Alta Recovery Vault Azure and Azure Government options in the web UI, you must contact your Veritas NetBackup account manager for credentials or with any questions.

For the cloud logical storage unit, click **Edit** to update the **Cloud cache properties** setting in the corresponding disk pool properties page. You must restart the pdde services for the updated setting to work.

Editing a storage server

This procedure tells you how to edit a storage server.

To edit a storage server

- 1 On the left, click **Storage > Disk storage**.
 - 2 Click the **Storage servers** tab.
 - 3 Click on the **Name** of the storage server you want to edit.
 - 4 On the storage server review page, under **Troubleshooting properties**, click **Edit** to edit the troubleshooting properties.
 - 5 Under **Universal share properties**, click **Edit** to edit the universal share properties.
 - 6 Under **Media servers**, click **Add** to add the load balancing media servers.
- For more information see the *Adding an MSDP load balancing server* topic in the *NetBackup Deduplication Guide*.
- 7 Under *Isolated recovery environment*, you can configure isolated recovery environment on the storage server if required.

For more information see the *Configuring an isolated recovery environment using the web UI* topic in the *NetBackup Deduplication Guide*.

Integrating MSDP Cloud and CMS

To integrate MSDP Cloud and CMS

- 1 If you haven't already, create an MSDP storage server. See the *Configuring MSDP server-side deduplication* section in the *NetBackup Deduplication Guide*.
- 2 Add a disk pool.
 - On the left, click **Disk storage**, click the **Disk pools** tab, and then click **Add**.
 - In **Disk pool options**, click **Change** to select a storage server.
 - Select a storage server from the list and click **Select**.
 - Enter the **Disk pool name**.
 - If **Limit I/O streams** is left cleared, the default value is Unlimited and may cause performance issues.
 - After all required information is added, click **Next**.
 - In **Volumes**, use the **Volume** drop down and select **Add volume**.
 - Provide a unique volume name that gives adequate description of the volume.

- In the **Cloud storage provider** section, select Microsoft Azure, Amazon, or any other cloud provider of S3 and Azure types.
- In the **Region** section, select the appropriate region.
- In the **Associate Credentials** section, select **Add a New Credential**.
- Enter a **Credential name** which should be a valid name and should only contain alphanumeric characters, hyphen, colon, and underscore.

Note: For details of authentication types like AWS IAM Role Anywhere and Azure Service Principal, see *NetBackup™ Deduplication Guide*.

- In **Access details for the account**, select **AWS S3 compatible** or **Azure Blob** and enter the access information.
- Alternatively, you can use **Select existing credential** but the credentials must have a Category of MSDP-C and proper credentials for the chosen supported cloud provider.
- In the **Cloud bucket** section, you can create a cloud bucket by clicking **Retrieve list** to select a predefined bucket from the list. If the cloud credentials in use do not have the permissions to list buckets, use **Enter an existing cloud bucket name**.
- Click **Next**.

3 In **Replication**, click **Next**.

4 On the **Details** page, verify that all settings and information are correct. Click **Finish**.

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

In the **Volumes** step, you can now use **Retrieve List** (list buckets) or create a bucket depending on what you want to accomplish.

Note: CMS is now supported for all S3 and Azure cloud vendor types.

Updating credentials

To update credentials

- 1 Create a disk pool.
- 2 After you have selected **Add volume**, **Volume name**, select **Cloud storage**, and select a **Region** then click **Select existing credential**.
- 3 Click on the **Actions** menu to the right of the **Credential name**.
- 4 Click **Edit** and in the **Edit credential** screen, make the changes as necessary.
- 5 In the **Permissions** window, add or change as necessary and click **Save**.
- 6 Finish adding the disk pool.

nbclutil changes

- The CLI now has a new parameter `cmscredname` that should be used instead of `username` from 10.3 and newer. However, the support for `username` is not removed, you can still use `username` for older media servers.
- **Validate credentials** - `nbclutil -validatecreds -storage_server mystorage_server -cmscredname mycmscredentialname`
- **Create bucket** - `nbclutil -createbucket -storage_server mystorage_server -cmscredname mycmscredentialname -bucket_name bucketname`

nbdevconfig changes

- You need to provide `lsuCmsCredName` in the configuration file for Veritas Alta Recovery Vault Azure and Veritas Alta Recovery Vault Azure Gov.
- Instead of using the storage account name for `lsuCmsCredName`, use the name of the credentials that are created when you use **Credential management**.
- The configuration file for `nbdevconfig` CLI now uses a new Key `cmsCredName` instead of user `lsuCloudUser` and `lsuCloudPassword`. The file should look like the following:

```
[root@vramsingh7134 openv]# cat /add_lsu.txt
V7.5 "operation" "add-lsu-cloud" string
V7.5 "lsuName" "ms-lsu-cli" string
V7.5 "lsuCloudBucketName" "ms-mybucket-cli" string
V7.5 "lsuCloudBucketSubName" "ms-lsu-cli" string
V7.5 "cmsCredName" "aws-creds" string
V7.5 "requestCloudCacheCapacity" "4" string
```

Note: For regular Azure and AWS from this 10.3 and newer: If you use the `createdv` option to create a cloud bucket either on the primary server, media server, or older media server, you see a message that tells you to use `nbclutil`.

Note: Some browsers like Firefox may auto-populate the fields to store the credentials in CMS with credentials the browser saves. You must turn off a setting in Firefox so that the credentials do not auto-populate.

Migrating or upgrading MSDP Cloud and CMS

You can upgrade only Access key credentials to CMS. You cannot upgrade the configured credentials for an older disk pool to CMS to use other authentication types. Upgraded credentials to use in CMS must be Access key based.

To migrate or upgrade MSDP Cloud

- 1 If using an MSDP on an old NetBackup version, configure MSDP cloud for any cloud provider by providing credentials in the **Access details for account** section.
- 2 Run a backup and restore.
- 3 Upgrade the MSDP to the newest version.
- 4 Click on the MSDP cloud disk pool that was configured in the previous release.
- 5 In the **Associate credentials** box, to the right and click on the action menu and select **Replace**.
- 6 Click **Continue**.
- 7 Click on **Use existing account access credentials**, if credentials are already in CMS.
- 8 Click on **Add a new credential**.
- 9 Follow the steps from Credential Management.
- 10 Click **Save**.
- 11 Restart NetBackup services on primary server and media server.

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

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

To configure cloud recovery server:

- 1 On the left, click **Storage > Disk storage**. Click the **Storage servers** tab, then click **Add**.

- 2 In the Storage type drop-down, select the option you want to use.

- 3 Select **Media Server Deduplication Pool (MSDP) for image sharing** from the list.

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

You must select your media server by clicking on the field. If you do not see the media server you want to use, use the search option.

- 5 In the storage server options, enter all the required information except for **Encryption options** and **Encryption for local storage** and click **Next**.

If KMS encryption is enabled for the on-premises side, Key Management Service (KMS) must be configured before you can configure cloud recovery server. In the cloud recovery host, you must not configure KMS encryption when you set up a storage server. The KMS options from the on-premises side are selected and configured automatically in the cloud recovery host.

- 6 (Optional) In Media servers, click **Next**. As the cloud recovery server is an all-in-one NetBackup server, no additional media servers are added.

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

If the MSDP with the image sharing creation is unsuccessful, follow the prompts on the screen to correct the issue.

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

You can also create a disk pool as follows:

On the left, click **Disk storage**. Click the **Disk pools** tab, then click **Add**.

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

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

- 10** In **Volumes**, use the **Volume** drop down to add a new volume. Enter all the required information based on the selection and click **Next**.

The volume name must be same as the volume name that is on the on-premises side or the sub bucket name.
 - 11** In **Replication**, click **Next** to continue without adding any primary server.
 - 12** On the **Review** page, verify that all settings and information are correct. Click **Save**.
- See [“Using image sharing from the NetBackup web UI ”](#) on page 123.

Create an AdvancedDisk, OpenStorage (OST), or Cloud Connector storage server

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

Create an AdvancedDisk storage server

Follow this procedure to create an AdvancedDisk storage server.

To create an AdvancedDisk storage server

- 1** On the left, click **Storage > Storage units**. Click the **Storage servers** tab, then click **Add..**
- 2** Select **AdvancedDisk** from the list.
- 3** Select a media server list and enter a **Storage server name** click **Select**.

Create an OpenStorage (OST) storage server

Follow this procedure to create an OpenStorage (OST) storage server.

To create an OpenStorage (OST) storage server

- 1** On the left, click **Storage > Storage units**. Click the **Storage servers** tab, then click **Add..**
- 2** Select **OpenStorage (OST)** from the list.
- 3** In **Basic properties**, enter all required information and click **Next**.

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

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

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

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

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

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

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

Create a Cloud Connector server

Follow this procedure to create a Cloud storage server.

To create a Cloud storage server

- On the left, click **Storage > Storage units**. Click the **Storage servers** tab, then click **Add**..

- Select **Cloud connector** from the list.

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

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

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

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

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

If you use `SOCKS4`, `SOCKS5`, or `SOCKS4A`, some of the options in the **Advanced** section are not available.

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

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

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

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

- 7 On the **Review** page, confirm that all options are correct and click **Save**.
- 8 (Optional) At the top, click on **Create disk pool**.

Using image sharing from the NetBackup web UI

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

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

About image sharing using MSDP cloud

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

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

Importing the images.

1. On the left, click **Storage > Disk storage**.. Then click **Disk pools** tab.
2. Select the volume pools that contain the images that you want to share.
3. In the Disk pool options, locate the disk pool name and click **Actions > Fast Import**.

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

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

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

1. On the left select **VMware** and then select the imported VMware image to convert.
2. On the **Recovery point** tab, select the recovery date.

3. For the recovery point date, choose the required recovery point, click **Actions > Convert**.

For Veritas Alta Recovery Vault, it may take time to get the disk volume and the credentials information.

Provide the credentials of Azure general-purpose storage accounts or AWS account with IAM and EC2 related permissions.

For more information on the permission, see *Recover the VM as an AWS EC2 AMI or VHD in Azure* topic of the *NetBackup Deduplication Guide*.

4. Once the conversion is complete, an AMI ID or VHD URL is generated.
5. Use the AMI ID to locate the image in AWS and then use the AWS console to start the EC2 instance. Or use VHD URL to create virtual machine.

Managing media servers

This chapter includes the following topics:

- [Add a media server](#)
- [Activate or deactivate a media server](#)
- [Stop or restart the media manager device](#)
- [About NetBackup server groups](#)
- [Add a server group](#)
- [Delete a server group](#)

Add a media server

The following table describes an overview of how to add a media server to an existing NetBackup environment.

Note: The NetBackup Enterprise Media Manager service must be active when a media server is added, devices and volumes are configured, and clients are backed up or restored.

Table 13-1 Adding a media server

Step	Procedure	Section
Step 1	On the new media server host, attach the devices and install any software that is required to drive the storage devices.	See the vendor's documentation.
Step 2	On the new media server host, prepare the host's operating system.	See the NetBackup Device Configuration Guide .

Table 13-1 Adding a media server (*continued*)

Step	Procedure	Section
Step 3	<p>On the primary server, add the new media server to the Media servers list of the primary server. Also, add the new media server to the Additional servers list of the clients that the new media server backs up.</p> <p>If the new media server is part of a server group, add it to the Additional servers list on all media servers in the group.</p> <p>Note: Ensure that the name you use in NetBackup is the same as the host name in the TCP/IP configuration.</p>	See the <i>Servers properties</i> topic in the NetBackup Administrator's Guide, Volume I .
Step 4	Install the NetBackup media server software on the new host.	See the NetBackup Installation Guide .
Step 5	On the primary server, configure the robots and drives that are attached to the media server.	See the <i>Configuring robots and tape drives by using the wizard</i> topic in the NetBackup Administrator's Guide, Volume I .
Step 6	On the primary server, configure the volumes.	See the <i>About adding volumes</i> topic in the NetBackup Administrator's Guide, Volume I .
Step 7	On the primary server, add storage units to the media server. Always specify the media server as the media server for the storage unit.	See "Create a storage unit" on page 102.
Step 8	On the primary server, configure the NetBackup policies and schedules to use the storage units that are configured on the media server.	See "Add a policy" on page 168.
Step 9	Test the configuration by performing a user backup or a manual backup that uses a schedule that specifies a storage unit on the media server.	See "Perform manual backups" on page 175.

Activate or deactivate a media server

When you activate a media server, NetBackup can use it for backup and restore jobs. You can deactivate a media server. A common reason to do so is to perform maintenance. When a media server is deactivated, NetBackup does not send job requests to it.

When you deactivate a media server, the following things occur:

- Current jobs are allowed to complete.
- If the host is part of a shared drive configuration, it does not scan drives.

Stop or restart the media manager device

Use the following procedure to stop and restart the NetBackup media manager device.

To start or stop the media manager device

- 1 Open the NetBackup web UI.
- 2 On the left, click **Storage > Media servers**. Then click the **Media servers** tab.
- 3 Select the media server and click **Stop/Restart media manager device daemon**.
- 4 Locate **Action** and select the action that you want to take.

Note: The actions that are available depend on the state of the media manager device.

- 5 Select any of the **Options** that you want.
 - **Eject media from standalone drives**
 - **Enable verbose logging**
- 6 Click **Apply**.

Note: NetBackup shows a notification after the selected action is completed.

About NetBackup server groups

A server group is a group of NetBackup servers that are used for a common purpose.

A NetBackup **Media sharing** group is a server group that shares tape media for write purposes (backups). All members of a **Media sharing** server group must have the same NetBackup primary server.

A **Media sharing** group can contain the following:

- NetBackup primary server
- NetBackup media servers
- NDMP tape servers

Add a server group

A server group is a group of NetBackup servers that are used for a common purpose. Servers can be in more than one group.

Caution: NetBackup allows a server group name to be the same as the name of a media server. To avoid confusion, do not use same name for a server group and a media server.

To add a server group

- 1 On the left, click **Storage > Media servers**.
- 2 Click **Server groups**.
- 3 Click **Add server group**.
- 4 Provide the information for the server group.

Server group name	Provide a unique name for the server group. Do not use the name for an existing media server or other host. You cannot change the name of an existing server group.
Server group type	Select the type of server group.
State	Active. The server group is available for use. Inactive. The server group is not available for use.
Description	Provide a description of the group.

- 5 To add a server to the group, click **Add**, select the server, then click **Add**.
To remove a server from the group, select the server and click **Remove**.
- 6 Click **Save**.

Delete a server group

You can delete a server group if it is no longer in use. Or, if the purpose of the servers in the group has changed.

To delete a server group

- 1** On the left, click **Storage > Media servers**.
- 2** Click **Server groups**.
- 3** Select the group to delete. Then click **Delete > Delete**.

Managing tape drives

This chapter includes the following topics:

- [Change a drive comment](#)
- [About downed drives](#)
- [Change a drive operating mode](#)
- [Change a tape drive path](#)
- [Change the operating mode for a drive path](#)
- [Change tape drive properties](#)
- [Change a tape drive to a shared drive](#)
- [Clean a tape drive](#)
- [Delete a drive](#)
- [Reset a drive](#)
- [Reset the mount time of a drive](#)
- [Set the drive cleaning frequency](#)
- [View drive details](#)

Change a drive comment

You can change the comment that is associated with a drive.

To change a drive comment

- 1 Open the NetBackup web UI.
- 2 On the left, click **Storage > Tape storage**. Then click the **> Device monitor** tab.
- 3 Select a drive.
- 4 Click **Actions > Change drive comment**.
- 5 Add a comment or change the current drive comment.
- 6 Click **Save**.

About downed drives

NetBackup downs a drive automatically when there are read or write errors that surpass the threshold within the time window. The default drive error threshold is 2. That is, NetBackup downs a drive on the third drive error in the default time window (12 hours).

Common reasons for write failures are dirty write heads or old media. The reason for the action is logged in the NetBackup error catalog (view the Media Logs report or the All Log Entries report). If NetBackup downs a device, it is logged in the system log.

You can use the NetBackup `nbemmcmd` command with the `-drive_error_threshold` and `-time_window` options to change the default values.

See [“Change a drive operating mode”](#) on page 131.

Change a drive operating mode

Usually you do not need to change the operating mode of a drive. When you add a drive, NetBackup sets the drive state to UP in Automatic Volume Recognition (AVR) mode. Other operating mode settings are used for special purposes.

The drive operating mode is displayed and changed on the **Device monitor** tab.

To change the mode of a drive

- 1 Open the web UI.
- 2 On the left, click **Storage > Tape storage**. Click the **Device monitor** tab.

- 3 Click on the drive name.
- 4 Select the path or paths. Then click the **Actions** menu and choose the command for the new drive operating mode.

If the drive is configured with multiple device paths or is a shared drive (Shared Storage Option), click **Paths** tab to see a list of all device paths to the drive. Select the path or paths to change.

Change a tape drive path

Use the following procedure to change a drive path.

See [“Change the operating mode for a drive path”](#) on page 132.

To change a drive path

- 1 In the **NetBackup Administration Console**, expand **Media and Device Management > Devices > Drives**. Double-click the drive that you want to change.
- 2 In the **Change Tape Drive** dialog box, select the drive path in the **Host and Path information** list. Click **Change**.
- 3 In the **Change Path** dialog box, configure the properties for the drive path.
The properties you can change depend on drive type, server platform, or NetBackup server type.
- 4 Click **OK** to save the changes.

Change the operating mode for a drive path

The Device monitor shows path information for drives, including the following:

- Multiple (redundant) paths to a drive are configured
- Any drives are configured as shared drives (Shared Storage Option)

To change the operating mode for a drive path

- 1 Open the web UI.
- 2 On the left, click **Storage > Tape storage**. Click the **Device monitor** tab.
- 3 On the **Paths** tab, select a path or select multiple paths.
- 4 Click **Actions**, then choose a command for the path action, as follows:
 - **Up path**
 - **Down path**

- **Reset path**

Change tape drive properties

Use the following procedure to change the configuration information for a drive.

To change drive properties

- 1 In the **NetBackup Administration Console**, expand **Media and Device Management > Devices > Drives**.
- 2 In the details pane, select the drive you want to change.
- 3 Click **Edit > Change**.
- 4 In the **Change Tape Drive** or the **Change Drive** dialog box, change the properties of the drive.

The properties depend on the drive type and host server type.
- 5 If the device changes are complete, select **Yes** on the **Restart Device Manager** dialog box or the **Media and Device Management** dialog box to restart the Device Manager or the device daemon.

If you intend to make other changes, click **No**; you can restart the Device Manager or the device daemon after you make the final change.

If you restart the Device Manager or the device daemon, any backups, archives, or restores that are in progress also may be stopped.

The initial drive status is UP, so the drive is available as soon as you restart the device daemon.
- 6 After you change the properties, click **OK**.

Change a tape drive to a shared drive

Change a drive to a shared drive by adding paths to a currently configured drive.

To configure and use a shared drive, a Shared Storage Option license is required on each primary server and media server.

To change a drive to a shared drive

- 1 In the **NetBackup Administration Console**, expand **Media and Device Management > Devices**.
- 2 Select **Drives** in the tree pane.
- 3 Select the drive you want to change in the **Drives** pane.
- 4 Click **Edit > Change**.

- 5 In the **Change Tape Drive** dialog box, click **Add**.
- 6 In the **Add Path** dialog box, configure the properties for the hosts and paths that share the drive.

Clean a tape drive

When you add a drive to NetBackup, you can configure the automatic, frequency-based cleaning interval.

You can also perform an operator-initiated cleaning of a drive regardless of the cleaning frequency or accumulated mount time of the drive. However, appropriate cleaning media must be added to NetBackup.

After you clean a drive, reset the mount time.

See [“Reset the mount time of a drive”](#) on page 135.

To clean a tape drive

- 1 Open the web UI.
- 2 On the left, click **Storage > Tape storage**. Click the **Device monitor** tab.
- 3 Select the drive to clean.
- 4 Click **Actions > Clean now**. NetBackup initiates drive cleaning regardless of the cleaning frequency or accumulated mount time.

The **Clean now** option resets the mount time to zero, but the cleaning frequency value remains the same. If the drive is a standalone drive and it contains a cleaning tape, NetBackup issues a mount request.

Delete a drive

Use the following procedure to delete a drive or drives when the media server is up and running.

If the media server is down or the host has failed and cannot be recovered, you can delete its drives by using a different procedure.

To delete a drive

- 1 In the **NetBackup Administration Console**, expand **Media and Device Management > Devices**.
- 2 Select **Drives** in the tree pane.
- 3 Select the drive or drives that you want to delete from the **Drives** pane.

- 4 On the **Edit** menu, select **Delete**.
- 5 At the prompt, click **Yes**.

Reset a drive

Resetting a drive changes the state of the drive.

Usually you reset a drive when its state is unknown, which occurs if an application other than NetBackup uses the drive. When you reset the drive, it returns to a known state before use with NetBackup. If a SCSI reservation exists on the drive, a reset operation from the host that owns the reservation can help the SCSI reservation.

If the drive is in use by NetBackup, the reset action fails. If the drive is not in use by NetBackup, NetBackup tries to unload the drive and set its run-time attributes to default values.

Note that a drive reset does not perform any SCSI bus or SCSI device resets.

Use the following procedure to reset a drive.

To reset a drive

- 1 Open the web UI.
- 2 On the left, click **Storage > Tape storage**. Click the **Device monitor** tab.
- 3 Select a drive or select multiple drives.
- 4 Select **Actions > Reset drive**.
- 5 If the drive is in use by NetBackup and cannot be reset, restart the NetBackup Job Manager (nbjmgr) to free up the drive.
- 6 Determine which job controls the drive (that is, which job writes to or reads from the drive).
On the left, click **Activity monitor**. Then on the **Jobs** tab, cancel the job.
- 7 In the **Activity monitor**, restart the NetBackup Job Manager, which cancels all NetBackup jobs in progress.

Reset the mount time of a drive

You can reset the mount time of the drive. Reset the mount time to zero after you perform a manual cleaning.

To reset the mount time

- 1 Open the web UI.
- 2 On the left, click **Storage > Tape storage**. Click the **Device monitor** tab.

- 3 Select a drive.
- 4 Select **Actions > Reset mount time**. The mount time for the selected drive is set to zero.

Set the drive cleaning frequency

When you add a drive to NetBackup, you configure the automatic, frequency-based cleaning interval. From the **Device monitor** you can change the cleaning frequency that was configured when you added the drive.

To set the cleaning frequency

- 1 Open the web UI.
- 2 On the left, click **Storage > Tape storage**. Click the **Device monitor** tab.
- 3 Select a drive.
- 4 Click **Actions > Set cleaning frequency**.
- 5 Enter a time (hours) or use the arrow controls to select the number of mount hours between drive cleaning.

The **Cleaning frequency** option is not available for the drives that do not support frequency-based cleaning. This function is not available for shared drives.

The drive cleaning interval appears in the **Drive properties**.

View drive details

You can obtain detailed information about drives (or shared drives), such as drive cleaning, drive properties, drive status, host, and robotic library information.

To view the drive details

- 1 Open the web UI.
- 2 On the left, click **Storage > Tape storage**. Click the **Device monitor** tab.
- 3 Many drive details are displayed on this tab. For additional details, click on a drive name.

For shared drives, you can see the drive **Control** mode and **Drive index** for each host that shares a drive. Click on the **Shared drive hosts** tab to view a list of hosts that share a drive.

Staging backups

This chapter includes the following topics:

- [About staging backups](#)
- [About basic disk staging](#)
- [Create a BasicDisk storage unit with disk staging](#)
- [Disk staging storage unit size and capacity](#)
- [Finding potential free space on a BasicDisk disk staging storage unit](#)
- [Schedule settings for disk staging](#)

About staging backups

In the staged backups process, NetBackup writes a backup to a storage unit and then duplicates it to a second storage unit. Eligible backups are deleted on the initial storage unit when space is needed for more backups.

This two-stage process allows a NetBackup environment to leverage the advantages of disk-based backups for recovery in the short term.

Staging also meets the following objectives:

- Allows for faster restores from disk.
- Allows the backups to run when tape drives are scarce.
- Allows the data to be streamed to tape without image multiplexing.

NetBackup offers the following methods for staging backups.

Table 15-1 Methods for staging backups

Staging method	Description
Basic disk staging	<p>Basic disk staging consists of two stages. First, data is stored on the initial storage unit (disk staging storage unit). Then, per a configurable relocation schedule, data is copied to the final location. Having the images on the final destination storage unit frees the space on the disk staging storage unit as needed.</p> <p>See “About basic disk staging” on page 138.</p> <p>The following storage unit types are available for basic disk staging: BasicDisk and tape.</p>
Staging using the Storage lifecycle policies utility	<p>Staged backups that are configured within the Storage lifecycle policies utility also consist of two stages. Data on the staging storage unit is copied to a final destination. However, the data is not copied per a specific schedule. Instead, the administrator can configure the data to remain on the storage unit until either a fixed retention period is met, or until the disk needs additional space, or until the data is duplicated to the final location.</p> <p>No BasicDisk or disk staging storage unit can be used in an SLP.</p>

About basic disk staging

Basic disk staging is conducted in the following stages.

Table 15-2 Basic disk staging

Stage	Description
Stage I	Clients are backed up by a policy. The Policy storage selection in the policy indicates a storage unit that has a relocation schedule configured. The schedule is configured in the staging schedule settings.
Stage II	Images are copied from the Stage I disk staging storage unit to the Stage II storage unit. The relocation schedule on the disk staging storage unit determines when the images are copied to the final destination. Having the images on the final destination storage unit frees the space on the disk staging storage unit as needed.

The image continues to exist on both the disk staging storage unit and the final destination storage units until the image expires or until space is needed on the disk staging storage unit.

When the relocation schedule runs, NetBackup creates a data management job. The job looks for any data that can be copied from the disk staging storage unit to the final destination. The job details in the Activity monitor identify the job as one associated with basic disk staging. The jobs list displays Disk Staging in the job’s **Data movement** field.

When NetBackup detects a disk staging storage unit that is full, it pauses the backup. Then, NetBackup finds the oldest images on the storage unit that successfully copied onto the final destination. NetBackup expires the images on the disk staging storage unit to create space.

Note: The basic disk staging method does not support backup images that span disk storage units.

To avoid spanning storage units, do not use Checkpoint restart on a backup policy that writes to a storage unit group that contains multiple disk staging storage units.

Create a BasicDisk storage unit with disk staging

When you configure a BasicDisk storage unit with disk staging, data is stored on the initial storage unit (disk staging storage unit). Then, per a configurable relocation schedule, data is copied to the final location. Having the images on the final destination storage unit frees the space on the disk staging storage unit as needed.

To create a BasicDisk storage unit with disk staging

- 1 Click **Storage > Storage units**.
- 2 Click **Add**.
- 3 Select **BasicDisk**. Then click **Start**.
- 4 Select the basic properties for the storage unit.

Type a **Name** for the storage unit.

Enter the number of **Maximum concurrent jobs** that are allowed to write to this storage unit at one time.

Enter a **High water mark** value.

The high water mark works differently for the BasicDisk disk type. NetBackup assigns new jobs to a BasicDisk disk staging storage unit, even if it is over the indicated high water mark. For BasicDisk, the high water mark is used to prompt the deletion of images that have been relocated.

Note: The **Low water mark** setting does not apply to disk staging storage units.

- 5 Click **Next**.

- 6 For the staging schedule, select the option **Enable temporary staging area**.
- 7 Below **Staging schedule**, click **Add**.

The schedule name defaults to the storage unit name.

Configure the schedule settings.

See [“Schedule settings for disk staging”](#) on page 143.
- 8 Click **Save** to save the disk staging schedule.
- 9 Click **Next**.
- 10 Select a media server.
- 11 Browse or specify the absolute path to the directory to be used for storage.
- 12 Select whether this directory can reside on the root file system or system disk.
- 13 Click **Next**.
- 14 Review the settings for the storage unit and then click **Save**.

Disk staging storage unit size and capacity

To take advantage of basic disk staging requires that the NetBackup administrator understand the life expectancy of the image on the Stage I storage unit.

The size and use of the file system of the Stage I storage unit directly affects the life expectancy of the image before it is copied to the Stage II storage unit. It is recommended a dedicated file system for each disk staging storage unit.

Consider the following example: A NetBackup administrator wants incremental backups to be available on disk for one week.

Incremental backups are done Monday through Saturday, with full backups done on Sunday. The full backups are sent directly to tape and do not use basic disk staging.

Each night's total incremental backups are sent to a disk staging storage unit and average from 300 MB to 500 MB. Occasionally a backup is 700 MB. Each following day the relocation schedule runs on the disk staging storage unit and copies the previous night's incremental backups to the final destination, a Media Manager (tape) storage unit.

The following items give more information about determining disk size for a basic disk staging storage unit.

Minimum disk size

The minimum disk size is the smallest size that is required for the successful operation of the disk staging logic.

The minimum size must be greater than or equal to the largest combined size of the backups that are placed on the storage unit between runs of the disk staging schedule. (In our example, the disk images remain on the disk for one week.)

In this example, the relocation schedule runs nightly, and the largest nightly backup is 700 MB. It is recommended that you double this value to allow for any problems that may occur when the relocation schedule runs. To double the value gives the administrator an extra schedule cycle (one day) to correct any problems.

To determine the minimum size for the storage unit in this example, use the following formula:

Minimum size = Max data per cycle × (1 cycle + 1 cycle for safety)

For example: 1.4 GB = 700 MB × (1+1)

Average disk size

The average disk size represents a good compromise between the minimum and the maximum sizes.

In this example, the average nightly backup is 400 MB and the NetBackup administrator wants to keep the images for one week.

To determine the average size for the storage unit in this example, use the following formula:

Average size = Average data per cycle × (number of cycles to keep data + 1 cycle for safety)

2.8 GB = 400 MB × (6 + 1)

Maximum disk size

The maximum disk size is the recommended size needed to accommodate a certain level of service. In this example, the level of service is that disk images remain on disk for one week.

To determine the maximum size for the storage unit in this example, use the following formula:

Maximum size = Max data per cycle × (# of cycles to keep data + 1 cycle for safety)

For example: 4.9 GB = 700 MB × (6 + 1)

Finding potential free space on a BasicDisk disk staging storage unit

Potential free space is the amount of space on a disk staging storage unit that NetBackup could free if extra space on the volume is needed. The space is the

total size of the images that are eligible for expiration plus the images ready to be deleted on the volume.

To find the potential free space on a BasicDisk storage unit, use the `bpstulist` and the `nbdevquery` commands as follows:

- Run `bpstulist -label` to find the disk pool name.
Note that the name of the storage unit and disk pools are case-sensitive. In the case of BasicDisk storage units, the name of the disk pool is the same as the name of the BasicDisk storage unit. In the following example, the name of the storage unit is *NameBasic*:

```
bpstulist -label basic
NameBasic 0 server1 0 -1 -1 1 0 "C:\\" 1 1 524288 *NULL* 0 1 0 98 80 0 NameBasic server1
```

- Run the `nbdevquery` command to display the status for the disk pool, including the potential free space.
Use the following options, where:

<code>-stype server_type</code>	Specifies the vendor-specific string that identifies the storage server type. For a BasicDisk storage unit, enter <i>BasicDisk</i> .
<code>-dp</code>	Specifies the disk pool name. For a basic disk type, the disk pool name is the name of the BasicDisk storage unit.

So the complete command might look like the following.

```
nbdevquery -listdv -stype BasicDisk -dp NameBasic -D
```

The value is listed as `potential_free_space`.

```
Disk Volume Dump
name           : <Internal_16>
id             : <C:\>
diskpool       : <NameBasic::server1::BasicDisk>
disk_media_id  : <@aaaaaf>
total_capacity : 0
free_space     : 0
potential_free_space: 0
committed_space : 0
precommitted_space : 0
nbu_state      : 2
sts_state      : 0
```

```

flags                : 0x6
num_read_mounts      : 0
max_read_mounts      : 0
num_write_mounts     : 1
max_write_mounts     : 1
system_tag           : <Generic disk volume>

```

Schedule settings for disk staging

The following settings are available when you create a disk staging schedule.

Table 15-3 The Attributes tab settings

Attribute	Description
Name	The schedule Name defaults to the name of the storage unit.
Priority of relocation jobs started from this schedule	The Priority of relocation jobs started from this schedule field indicates the priority that NetBackup assigns to relocation jobs for this policy. Range: 0 to 99999 (highest priority). The default value that is displayed is the value that is set in the Default job priorities host properties for the Staging job type.
Multiple copies	<p>Creates multiple copies of backups. NetBackup can create up to four copies of a backup simultaneously.</p> <p>When this setting is enabled, Final destination volume pool and Final destination media ownership are disabled.</p>
Final destination storage unit	<p>If the schedule is a relocation schedule, a Final destination storage unit must be indicated. (A relocation schedule is created as part of a basic disk staging storage unit configuration.) A Final destination storage unit is the name of the storage unit where the images reside after a relocation job copies them.</p> <p>To copy images to tape, NetBackup uses all of the drives available in the Final destination storage unit. However, the Maximum concurrent write drives setting for that storage unit must be set to reflect the number of drives. The setting determines how many duplication jobs can be launched to handle the relocation job.</p> <p>NetBackup continues to free space until the Low water mark is reached.</p> <p>See “About staging backups” on page 137.</p>
Final destination volume pool	<p>If the schedule is a relocation schedule, a Final destination volume pool must be indicated. (A relocation schedule is created as part of a basic disk staging storage unit configuration.) A Final destination volume pool is the volume pool where images are swept from the volume pool on the basic disk staging storage unit.</p> <p>See “About staging backups” on page 137.</p>

Table 15-3 The Attributes tab settings (*continued*)

Attribute	Description
Final destination media owner	<p>If the schedule is a relocation schedule, a Final destination media owner must be indicated. (A relocation schedule is created as part of a basic disk staging storage unit configuration.) A Final destination media owner is the media owner where the images reside after a relocation job copies them.</p> <p>Specify one of the following:</p> <ul style="list-style-type: none">■ Any lets NetBackup choose the media owner. NetBackup chooses a media server or a server group (if one is configured).■ None specifies that the media server that writes the image to the media owns the media. No media server is specified explicitly, but you want a media server to own the media.
Schedule type	<p>Calendar</p> <p>Frequency</p> <p>If the backups that use a disk staging storage unit run more frequently than expected, compare the retention level 1 setting with the Frequency setting. Internally, NetBackup uses the retention level 1 setting for scheduling purposes with disk staging storage units.</p> <p>Make sure that the frequency period is set to make the backups occur more frequently than the retention level 1 setting indicates. (The default is two weeks.)</p> <p>For example, a frequency of one day and a retention level 1 of 2 weeks should work well. Retention levels are configured in the Retention periods host properties.</p>

Table 15-3 The Attributes tab settings (*continued*)

Attribute	Description
Use alternate read server	<p>An alternate read server is a server allowed to read a backup image originally written by a different media server.</p> <p>The path to the disk or directory must be identical for each media server that is to access the disk.</p> <p>If the backup image is on tape, the media servers must share the same tape library or the operator must find the media.</p> <p>If the backup image is on a robot that is not shared or a standalone drive, the media must be moved to the new location. An administrator must move the media, inventory the media in the new robot, and run <code>bpmedia -oldserver -newserver</code> or assign a failover media server.</p> <p>To avoid sending data over the network during duplication, specify an alternate read server that meets the following conditions:</p> <ul style="list-style-type: none"> ■ Connected to the storage device that contains the original backups (the source volumes). ■ Connected to the storage device that contains the final destination storage units. <p>If the final destination storage unit is not connected to the alternate read server, data is sent over the network.</p>
Copies	Specify the number of copies to create simultaneously. Range: 1 to 4.
Priority of duplication job	Indicates the priority that NetBackup assigns to duplication jobs for this policy. Range: 0 to 99999 (highest priority).

Table 15-3 The Attributes tab settings (*continued*)

Attribute	Description
Copy #	<p>For each copy you want to create, select the copy settings. Copy 1 is the primary copy. If Copy 1 fails, the first successful copy is the primary copy.</p> <p>Storage unit</p> <p>Specify the storage unit where each copy is stored. If a Media Manager storage unit has multiple drives, it can be used for both the source and the destination.</p> <p>Volume pool</p> <p>Specify the volume pool where each copy is stored.</p> <p>If this copy fails</p> <ul style="list-style-type: none"> ■ Continue Continues making the remaining copies. <p>Note: Note: If Take checkpoints every __ minutes is selected for this policy, only the last failed copy that contains a checkpoint can be resumed.</p> <ul style="list-style-type: none"> ■ Fail all copies Fails the entire job. <p>Media owner</p> <p>For tape media, specify who should own the media onto which NetBackup writes the images.</p> <p>These settings do not affect any images that reside on disk. One media server does not own the images that reside on shared disks. Any media server with access to the shared pool of disk can access the images.</p> <ul style="list-style-type: none"> ■ Any NetBackup selects the media owner, either a media server or server group. ■ None Specifies that the media server that writes to the media owns the media. No media server is specified explicitly, but you want a media server to own the media.

Troubleshooting storage configuration

This chapter includes the following topics:

- [Registering a media server](#)
- [Storage configuration issues](#)
- [Troubleshooting universal share configuration issues](#)

Registering a media server

If the primary server is not running when you install a media server, the media server is not registered. You cannot discover, configure, and manage the devices of that media server. You must register the media server with the primary server.

To register a media server

- 1 Start the EMM service on the primary server.
- 2 On the primary server, run the following command. (For *hostname*, use the host name of the media server.)

On Windows:

```
install_path\NetBackup\bin\admincmd\nbemcmd -addhost -machinename
hostname -machinetype media -masterserver server_name
-operatingsystem os_type -netbackupversion
level.major_level.minor_level
```

On UNIX:

```
/usr/opensv/netbackup/bin/admincmd/nbemcmd -addhost -machinename
hostname -machinetype media -masterserver server_name
-operatingsystem os_type -netbackupversion
level.major_level.minor_level
```

Note: Ensure that the name you use in NetBackup is the same as the host name in the TCP/IP configuration.

Storage configuration issues

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

Table 16-1 Storage configuration troubleshooting

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

Troubleshooting universal share configuration issues

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

How to troubleshoot a failed installation or configuration

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

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

To ensure that instant access is enabled on the storage server

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

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

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

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

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

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

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

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

How to check for universal share capability

To ensure that the storage server has universal share capability

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

```
nbdevquery -liststs -U
```

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

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

- 3 Run the following command:

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

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

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

See [“Create a universal share”](#) on page 105.

How to start or to stop a universal share

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

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

```
netbackup start
```

- Use the following command to stop universal share:

```
netbackup stop
```

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

For example:

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

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

Configuring backups

- [Chapter 17. Overview of backups in the NetBackup web UI](#)
- [Chapter 18. Managing protection plans](#)
- [Chapter 19. Managing classic policies](#)
- [Chapter 20. Protecting the NetBackup catalog](#)
- [Chapter 21. Managing backup images](#)
- [Chapter 22. Pausing data protection activity](#)

Overview of backups in the NetBackup web UI

This chapter includes the following topics:

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

Backups methods supported in the NetBackup web UI

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

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

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

Protection plan vs. policy FAQs

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

Table 17-1 Classic policy FAQ

Question	Answer
In the web UI's Protected by column, what does Classic policy only mean?	The asset is not currently subscribed to a protection plan. However, it was subscribed to a protection plan. Or, it was covered by a classic policy at one time and it has a Last backup status. There may or may not be an active classic policy protecting the asset (contact the NetBackup administrator to find out).
Where can I find the details of a classic policy?	The details of a classic policy are not visible in the web UI, with the exception of a few policy types. See "Support for NetBackup classic policies" on page 155.
How can I manage a classic policy?	Some policy types can be managed in the NetBackup web UI. See "Support for NetBackup classic policies" on page 155.
When should I subscribe an asset to a protection plan versus protecting the asset with a classic policy?	A protection plan lets you easily add and remove assets from the plan and see which assets are protected. A workload administrator can fully control who can view or manage protection plans and assets. Policies offer the classic method of data protection. However, they do not have RBAC control for individual policies or for the data you want to protect.
Can I use both a protection plan and a classic policy to protect an asset?	Yes. The web UI shows the details of the protection plan but not the details of the classic policy. You can contact the NetBackup administrator for the classic policy details.
What action should I take when an asset is unsubscribed from a protection plan and the web UI shows Classic policy only for that asset?	You can ask the NetBackup administrator if a classic policy protects the asset.

Supported protection plan types

The web UI supports protection plans for the following workloads.

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

Support for NetBackup classic policies

The following policy types can be managed in the NetBackup web UI.

Table 17-2 Policy types supported in NetBackup web UI

BigData	Informix-On-BAR	NDMP
Cloud-Object-Store	Lotus Notes	Oracle
DataStore (XBSA)		SAP
DB2	MS-Exchange-Server	Standard
Enterprise Vault	MS-SharePoint	Sybase
FlashBackup	MS-SQL-Server	VMware
FlashBackup-Windows	MS-Windows	Universal-Share
	NAS-Data-Protection	
	NBU-Catalog	

Managing protection plans

This chapter includes the following topics:

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

Create a protection plan

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

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

See [“About storage configuration”](#) on page 99.

To create a protection plan

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

Optional selection:

- **Policy name prefix:**

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

- **Enable Continuous Data Protection**

For VMware workloads, select this option to use Continuous data protection for the workload. Select the **Use universal share** option to use universal share for data storage. Using universal share substantially reduces the staging data storage requirements, thereby greatly reducing the data storage costs. CDP with universal share is supported NetBackup version 10.2 onwards. See the *Continuous data protection* chapter of the *NetBackup Web UI VMware Administrator's Guide* for details.

- **Protect PaaS assets only**

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

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

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

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

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

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

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

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

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

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

In the **Attributes** tab:

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

In the **Start window** tab:

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

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

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

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

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

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

Storage option	Requirements	Description
Snapshot storage only	Snapshot Manager is required for this option.	
Perform snapshot backups	Microsoft SQL Server is required for this option.	For instructions on configuring protection plans for Microsoft SQL Server, see the <i>NetBackup Web UI Microsoft SQL Server Administrator's Guide</i> .
Backup storage	OpenStorage is required for this option. Tape, storage unit groups, and Replication Director not supported.	<p>Click Edit to select the storage target. Click Use selected storage after selecting the storage target.</p> <p>The NetBackup Accelerator feature allows protection plans to run faster than traditional backups, by creating a compact data stream that uses less network bandwidth. If the storage server on the NetBackup primary server supports NetBackup Accelerator, this feature is included in the protection plan. For more details on NetBackup Accelerator, contact the NetBackup administrator or see the NetBackup Administrator's Guide, Volume I or the NetBackup for VMware Administrator's Guide.</p> <p>The Instant access feature allows the plan's recovery points to support the creation of instant access VMs or databases.</p>
Replication target	The backup storage must be a source in a targeted A.I.R. environment.	<p>Click Edit to select the replication target primary server. Select a primary server and then select a storage lifecycle policy. Click Use selected replication target to return to the storage options screen.</p> <p>Cloud workloads support the MSDP and MSDP-C storage units for replication (A.I.R.).</p> <p>If the replication target primary server is not in the list, you must add one in NetBackup. For more information on how to add a replication target primary server, review <i>Adding a trusted primary server</i> in the NetBackup Deduplication Guide.</p>

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

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

For the **Cloud** workload:

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

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

- If you have selected the cloud provider as Google Cloud Platform, select **Enable regional snapshot**, to enable regional snapshots.
If the regional snapshot option is enabled, the snapshot is created in the same region in which the asset exists. Otherwise, the snapshot is created in a multi-regional location.
- (Microsoft Azure or Azure Stack Hub cloud provider) Select **Specify snapshot destination resource group** to associate snapshots to a particular peer resource group. This resource group is within the same

region in which the asset exists. Select a configuration, subscription, and a resource group for a snapshot destination.

- If you have selected **Enable Continuous data protection** for a VMware workload, select a Continuous data protection gateway from the list. Click **Next**. If you are using the universal share option, the gateway version must be NetBackup 10.2 or higher.
- If you create a protection plan for cloud LSU residing on MSDP with NetBackup 10.2 or higher, do not specify a staging path in the backup options. This also needs a media server of version 10.2 or higher. For older NetBackup versions, if you create a protection plan for a cloud LSU that resides on MSDP, and upgrade NetBackup to 10.2, the protection plans are also upgraded to use ushare with accelerator.
- For cloud workloads with PaaS assets, select a **Staging path** in the **Backup options** tab. This should be the export path of the MSDP universal share storage, created on block or cloud storage that is residing on the RHEL media server. Only NFS protocol created universal share is supported for PaaS assets. Note that SMB created universal share is not supported. It is recommended to use MSDP cloud storage as a backup storage unit while creating a protection plan for cloud-scale environment (AKS or EKS). If you use a local MSDP storage unit, you need to attach external media to this configuration and use the same for backup and restore.

Note: For NetBackup deployed in AKS and EKS environments, ensure that this universal share contains the export host that is added to the subnet as the media server or media server pod.

- 6 In **Permissions**, review the roles that have access to protection plans.

To give another role access to this protection plan, click **Add**. Select the **Role** in the table and customize the role by adding or removing permissions in the **Select permissions** section.

- 7 In **Review**, verify that the protection plan details are correct and click **Finish**.

Customizing protection plans

After you create a protection plan, only certain settings are available to change or configure. See [Table 18-1](#).

Table 18-1 Protection plan settings that can be configured and edited

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

Edit or delete a protection plan

Edit a protection plan

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

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

See [“Customizing protection plans”](#) on page 162.

To edit a protection plan

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

Delete a protection plan

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

See [“Unsubscribe an asset from a protection plan”](#) on page 165.

See [“Subscribe an asset or an asset group to a protection plan”](#) on page 164.

See [“Create a protection plan”](#) on page 156.

To delete a protection plan

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

Subscribe an asset or an asset group to a protection plan

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

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

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

See [“Customizing protection plans”](#) on page 162.

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

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

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

- 5 In **Choose a protection plan**, select the name of the protection plan and click **Next**.
- 6 (Optional) Adjust any options in the **Backup options** or **Advanced options**.
 - **Schedules**
Change the backup start window for full or incremental schedules.
For SQL Server transaction log schedules you can change the start window, the recurrence, and the retention period.
 - **Backup options**
Adjust the backup options that were set up in the original protection plan.
The options in this area change depending on workload.
 - **Advanced**
Change or add any options that were set up in the original protection plan.
You need the following permissions to make these changes:
 - **Edit attributes**, to edit **Backup options** and **Advanced** options.
 - **Edit full and incremental schedules**, to edit the start window for these schedule types.
 - **Edit transaction log schedules**, to edit the settings for SQL Server transaction log schedules.
- 7 Click **Protect**.

Unsubscribe an asset from a protection plan

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

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

To unsubscribe a single asset from a protection plan

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

To unsubscribe a group of assets from the protection plan

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

View protection plan overrides

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

To view protection plan overrides

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

About Backup Now

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

Backup Now is supported for the following workloads:

- Cassandra
- Cloud and PaaS

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

- Microsoft SQL
- MySQL
- Nutanix AHV
- PostgreSQL
- RHV
- VMware

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

Immediately back up an asset using Backup Now

You can start Backup Now for an asset from the list of assets. For example, from the list of virtual machines, intelligent groups, or databases. Or, you can start Backup Now from the asset's details. These details display all of the protection plans to which the asset is subscribed. You can choose **Backup now** from any one of these protection plans.

To immediately back up an asset using Backup Now

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

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

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

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

- 4 Click **Start backup**.

Managing classic policies

This chapter includes the following topics:

- [Add a policy](#)
- [Example policy - Exchange Server DAG backup](#)
- [Example policy - Sharded MongoDB cluster](#)
- [Edit, copy, or delete a policy](#)
- [Deactivate or activate a policy](#)
- [Edit or delete a client](#)
- [Edit or delete a backup selection](#)
- [Edit or delete a schedule](#)
- [Perform manual backups](#)

Add a policy

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

See [“Example policy - Exchange Server DAG backup”](#) on page 169.

See [“Example policy - Sharded MongoDB cluster”](#) on page 170.

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

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

To add a policy

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

Example policy - Exchange Server DAG backup

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

To add a policy for an Exchange Server DAG backup

- 1** On the left, select **Protection > Policies**.
- 2** Click **Add**.
- 3** On the **Attributes** tab, select the following:
 - **Policy type:** MS-Exchange-Server
 - **Perform snapshot backups:** Must be enabled.

- **Enable granular recovery:** Optional. Enable this option if you want to restore individual mailbox and public folder objects from the database backup.
 - **Database backup source:** Choose whether to back up the active or the passive copy of the database. Also configure the preferred list, depending on the backup source that you selected.
- 4 On the **Schedules** tab, configure all the necessary schedules. For example, Full and incremental schedules.

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

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

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

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

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

Backup selection list

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

- 7 Click **Create**.

Example policy - Sharded MongoDB cluster

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

To add a policy for a MongoDB cluster backup

- 1 On the left, select **Protection > Policies**.
- 2 Click **Add**.

- 3 On the **Attributes** tab, select the following:
 - **Policy type:** BigData
- 4 On the **Schedules** tab, configure all the necessary schedules. For example, Full and incremental schedules.

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

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

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

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

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

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

- 7 Click **Create**.

Edit, copy, or delete a policy

You can make changes to a policy, copy a policy, or delete a policy that you no longer need.

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

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

Edit a policy

You can make changes to policy attributes, schedules, clients, or backup selections.

To edit a policy

- 1 On the left, select **Protection > Policies**.
- 2 Select the policy that you want to change and click **Edit**.
- 3 Make the changes that you want, then click **Save**.

Copy a policy

You can copy a policy to save time creating new policies. This option is especially useful for the policies that contain many of the same policy attributes, schedules, clients, or backup selections.

To copy a policy

- 1 On the left, select **Protection > Policies**.
- 2 Select the policy that you want to copy and click **Copy policy**.
- 3 Provide a name for the policy and click **Copy**.

Delete a policy

You can delete a policy if you no longer need it. To maintain protection of the clients or hosts, add them to another policy before you delete the current policy.

To delete a policy

- 1 On the left, select **Protection > Policies**.
- 2 Select one or more policies and click **Delete > Delete**.

Deactivate or activate a policy

Active policies are available for NetBackup to use to schedule backups or allow user-backups.

You can also use the **Go into effect at** policy attribute to activate a policy or to deactivate a policy. Or, to select a time for a policy to become active.

Deactivate a policy

You can deactivate a policy to temporarily pause any backup requests for that policy. For example, if you want to perform maintenance on the clients in the policy. Note that manual backups or user-requested backups cannot run if a policy is deactivated.

To deactivate a policy

- 1 On the left, click **Protection > Policies**.
- 2 Select the policy, then click **Deactivate**.

Activate a policy

Activate a policy when you are ready for backup schedules in the policy to run.

To activate a policy

- 1 On the left, click **Protection > Policies**.
- 2 Select the policy, then click **Activate**.

Edit or delete a client

You can edit a client in a policy or delete a client from a policy. For a client to be backed up, it must be included in at least one active backup policy.

Edit a client

You can edit the client name in a policy or change the operating system that is selected for a client. If you select multiple clients, you can only change the operating system.

To edit a client

- 1 On the left, select **Protection > Policies**.
- 2 Select the client and click **Edit**.
- 3 Make any changes that you want and click **Save**.

Delete a client

You can delete a client from a policy. For example, if another policy protects the client or if a client is decommissioned.

When you delete a client from a policy, the NetBackup client software is not deleted or uninstalled from the client. Backups for the client can be recovered until the backups expire.

To delete a client

- 1 On the left, select **Protection > Policies**.
- 2 Select one or more clients and click **Delete > Yes**.

Edit or delete a backup selection

You can edit a backup selection or delete it from a policy. A policy requires at least one backup selection for automated (scheduled) backups. User backups do not require backup selections because the user chooses the items at the time of the backup.

Edit a backup selection**To edit a backup selection**

- 1 On the left, select **Protection > Policies**.
- 2 Select the client and click **Edit**.
- 3 To make a change, do one of the following:
 - To replace the file or the directory name, edit the path, file, or directory name. Then click **Save**.
 - To replace a directive, select the directive from the list and click **+**. Then click **Save**.

Delete a backup selection

You can delete a backup selection from a policy. When you delete a backup selection, the actual file or directory is not deleted from the client.

To delete a backup selection

- 1 On the left, select **Protection > Policies**.
- 2 Select one or more backup selections and click **Delete > Yes**.

Edit or delete a schedule

You can edit the client information in a policy or delete a schedule from a policy. A policy requires schedules to run automated backups. For example, full and incremental schedules. A **User backup** schedule is needed for users to run user-directed backups from the client.

Edit a schedule

You can edit the settings of a schedule for a policy.

To edit a schedule

- 1 On the left, select **Protection > Policies**.
- 2 Select the schedule and click **Edit**.
- 3 Make the changes that you want. Then click **Save**.

Delete a schedule

You can delete a schedule from a policy.

To delete a schedule

- 1 On the left, select **Protection > Policies**.
- 2 Select one or more schedules and click **Delete > Yes**.

Perform manual backups

A manual backup is user-initiated and is based on a policy. For example, you can use a manual backup to prepare for the upcoming events that are outside scheduled backups, such as system maintenance.

In some cases, it may be useful to create a policy and schedule that is used only for manual backups. Create a policy for manual backups by creating a policy with a single schedule that has no backup window. Without a backup window, the policy can never run automatically.

To perform a manual backup

- 1 On the left, select **Protection > Policies**.
- 2 Select the policy name and click **Manual backup**.

To perform a manual backup, you must enable the **Go into effect at** attribute for the policy. If the this attribute is set for a future date and time, the backup does not run.
- 3 Choose from the following options:
 - To back up all the clients and the default schedules for the selected policies, click **Backup all**.
 - To select specific clients and the schedule for each policy, click **Specify**.
- 4 Follow the prompts to continue.

Protecting the NetBackup catalog

This chapter includes the following topics:

- [About the NetBackup catalog](#)
- [Catalog backups](#)
- [Disaster recovery emails and the disaster recovery files](#)
- [Disaster recovery packages](#)
- [About disaster recovery settings](#)
- [Setting the passphrase to encrypt disaster recovery packages](#)
- [Recovering the catalog](#)

About the NetBackup catalog

A NetBackup catalog is the internal database that contains information about NetBackup backups and configuration. Backup information includes records of the files that have been backed up and the media on which the files are stored. The catalogs also contain information about the media and the storage devices.

Configure a disaster recovery pass phrase and a catalog backup before you run any regular backups. NetBackup needs information from the catalog to determine where the backups of files are located. Without a catalog, NetBackup cannot restore data.

See [“Setting the passphrase to encrypt disaster recovery packages”](#) on page 186.

See [“Configuring catalog backups”](#) on page 179.

As additional protection for the catalog, consider archiving the catalog.

See [“Archiving the catalog and restoring from the catalog archive”](#) on page 398.

Catalog backups

Because the catalog plays an integral part in a NetBackup environment, a special type of backup protects the catalog and is separate from regular client backups. A catalog backup policy backs up catalog-specific data as well as produces disaster recovery information. The catalog can be stored on a variety of media.

The catalog backup is designed for active environments in which continual backup activity occurs. It includes all the necessary catalog files, the databases (NBDB, NBAZDB, and BMRDB), and any catalog configuration files. The catalog backup can be performed while regular backup activity occurs. Incremental backups of a large catalog can significantly reduce backup times.

Configure a catalog backup before you run any regular backups. NetBackup needs information from the catalog to determine where the backups of files are located. Without a catalog, NetBackup cannot restore data.

See [“Configuring catalog backups”](#) on page 179.

As additional protection for the catalog, consider archiving the catalog.

See [“Archiving the catalog and restoring from the catalog archive”](#) on page 398.

From a catalog backup an administrator can recover either the entire catalog or pieces of the catalog. (For example, separately recover the databases from the configuration files.) Details about catalog recovery scenarios and procedures are available in the *NetBackup Troubleshooting Guide*.

The catalog backup process

The catalog backup performs the following tasks:

- Backs up the catalog while continual client backups are in progress.
- Performs a full or an incremental catalog backup.
- Runs the scheduled catalog backups.
- Copies the databases to the staging directory and then backs up that directory.
- Creates the disaster recovery package.
- Catalog backups that are made to tape also include the following items:
 - Spans multiple tapes for a catalog backup.
 - Allows for a flexible pool of catalog tapes.

Catalog backups to tape use media from the **CatalogBackup** volume pool only.

- Appends to existing data on tape.
- When an online catalog backup is run, it generates three jobs: A parent job, a child job for NetBackup relational database tables, and a child job for catalog images and configuration data. The child jobs contain the actual backed up data. Consider both child jobs to duplicate, verify, or expire the backup.

Refer to the following topics for information on how to configure a catalog backup:

See [“Prerequisites for backing up the NetBackup catalog”](#) on page 178.

See [“Configuring catalog backups”](#) on page 179.

Prerequisites for backing up the NetBackup catalog

The following prerequisites exist for a catalog backup:

- Set a passphrase for the disaster recovery package.
See [“Disaster recovery packages”](#) on page 184.
See [“Setting the passphrase to encrypt disaster recovery packages”](#) on page 186.
If the passphrase is not set, catalog backups fail.
- The primary server and the media server must both be at the same NetBackup version.
See the [NetBackup Installation Guide](#) for information about mixed version support.
- Catalog backups write only to media in the **CatalogBackup** volume pool. A storage device must be configured and media must be available in the **CatalogBackup** volume pool.
- The following requirements exist if the primary server is configured to use a non-privileged user (or service user) account. For more information on this type of account, refer to the [NetBackup Security and Encryption Guide](#).
 - The service user account must have the write access permissions on the disaster recovery (DR) path.
 - Configure the catalog policy with the credentials for the service account. (This setting is located on the **Disaster recovery** tab.)
 - You cannot use another user account, even if that account has the access to the DR path. The NetBackup Administrator must ensure that the service user can write to any network share without switching the context to another user.

On Windows, this requirement is not applicable if the DR path is a network share.

Configuring catalog backups

To protect the NetBackup catalog, you create a backup policy that is specific for catalog backups.

To configure a catalog backup

- 1 Review the prerequisites for performing catalog backups.
See [“Prerequisites for backing up the NetBackup catalog”](#) on page 178.
- 2 Sign in to the NetBackup web UI.
- 3 Click **Protection > Policies**. Then click **Add**.
- 4 On the **Attributes** tab, complete the following entries:
 - Enter a unique **Policy name**.
 - For the **Policy type**, select **NBU-Catalog**.
 - **Policy storage**
For disk storage units, increase the **Maximum Concurrent Jobs** storage unit setting to ensure that the catalog backup can proceed during regular backup activity.

Note: If your installation contains media servers at various versions, you can select a specific media server for the destination **Policy storage**. Do not select **Any Available**.

- **Policy volume pool**
NetBackup automatically creates a **CatalogBackup** volume pool that is selected by default only for **NBU-Catalog** policy types.
 - For other policy attribute descriptions, see the following topic:
- 5 On the **Schedules** tab, configure the schedules you want for the catalog backup.
See [“Concurrently running catalog backups with other backups”](#) on page 181.
See [“Catalog policy schedule considerations”](#) on page 181.
 - 6 Click the **Disaster recovery** tab.
The tab contains information regarding the location of data crucial to disaster recovery.

- Provide the path where each disaster recovery image file can be saved on disk. Enter the **Network share username** and **Network share password**, if necessary.
It is recommended that you use a network share or a removable device.
Do not save the disaster recovery information to the local computer.
- 7 Select **Send disaster recovery email** and enter one or more email addresses for NetBackup administrators (separated by commas).

After every catalog backup, NetBackup sends disaster recovery information to the administrators that are indicated here.

Make sure that email notification is enabled in your environment.

See [“Disaster recovery emails and the disaster recovery files”](#) on page 183.
- 8 Add the policies that back up any critical data to the **Critical policies** list.

These policies are any that you consider crucial to the recovery of a site in the event of a disaster. The disaster recovery report includes a list of the media that is used for backups of critical policies. The report includes media only for incremental and full backup schedules, so any critical policies should use only incremental or full backup schedules.
- 9 Click **Save**.

Backing up NetBackup catalogs manually

Catalog backups typically run automatically per the **NBU-Catalog** policy. You can also manually start a catalog backup.

A manual catalog backup is useful in the following situations:

- To perform an emergency backup. For example, if the system is scheduled to be moved and you cannot wait for the next scheduled catalog backup.
- If there is only one standalone drive and the standalone drive is used for catalog backups. In this situation, automatic backups are not convenient. The catalog backup tape must be inserted before each catalog backup and removed when the backup is done. (The tape swap is necessary because NetBackup does not mix catalog and regular backups on the same tape.)

To perform a manual catalog backup

- 1 Sign in to the NetBackup web UI.
- 2 Click **Protection > Policies**.
- 3 Select the catalog backup policy that you want to run.
- 4 Click **Manual backup**.

- 5 (Optional) Select the schedule that you want to use.
- 6 Click **Backup**.

Concurrently running catalog backups with other backups

You can schedule catalog backups to run concurrently with other backup types for the primary server.

Make the following adjustments to ensure that the catalog backup can proceed while regular backup activity occurs:

- Set the **Maximum jobs per client** value to greater than one. The property is found in the Global attributes host properties for the primary server.
- Increase the **Maximum concurrent jobs** setting on the storage unit where the backups are sent.

See [“Determining whether or not a catalog backup succeeded”](#) on page 182.

See [“Strategies that ensure successful NetBackup catalog backups”](#) on page 182.

Catalog policy schedule considerations

When you work with catalog policy schedules, consider the following:

- Schedule the catalog backups to occur on a regular basis. Without regular catalog backups, you risk losing regular backups if there is a problem with the disk that contains the catalogs.
- The following backup types are supported:
 - Full
 - Differential incremental
This incremental schedule depends on a full schedule.
 - Cumulative incremental
- The least frequent schedule runs if many schedules are due at the same time.
- One catalog backup policy can contain multiple incremental schedules that are session-based:
 - If one is cumulative and the others are differential, the cumulative runs when the backup session ends.
 - If all are cumulative or all are differential, the first schedule that is found runs when the backup session ends.
- The queued scheduled catalog backup is skipped if a catalog backup job from the same policy is running.

- Session end means that no jobs are running. (This calculation does not include catalog backup jobs.)
- The Vault catalog backup is run whenever triggered from Vault, regardless of whether a catalog backup job is running from the same policy.

How catalog incrementals and standard backups interact on UNIX

A catalog backup policy can include both full catalog backups and incremental catalog backups. However, incremental catalog backups differ from incremental standard backups. Catalog backups use both `mtime` and `ctime` to identify changed data. Standard incremental backups use only `mtime` to identify changed data.

Because of this difference, running a standard policy type backup that includes the `/usr/openv/netbackup/db/images/` directory can adversely affect incremental catalog backups. When standard backups run, they reset the file access time (`atime`). In turn, the reset changes the `ctime` for files and directories. If an incremental catalog backup runs, it sees that the `ctime` has changed and backs up the files. The backup may be unnecessary since the files may not have changed since the last catalog backup.

To avoid additional processing during catalog backups, the following is recommended:

If incremental catalog backups are configured, exclude the NetBackup `/usr/openv/netbackup/db/images/` directory from standard backups.

To exclude that directory, create a `/usr/openv/netbackup/exclude_list` file on the primary server.

See [“About NetBackup primary server installed directories and files”](#) on page 417.

Determining whether or not a catalog backup succeeded

An email message is sent to the address that is indicated in the **Disaster recovery** settings for a catalog backup.

Configure this email with the `mail_dr_info.cmd` (on Windows) or the `mail_dr_info` script (on UNIX).

See the [Administrator's Guide, Volume II](#) for more information on setting up this script.

Strategies that ensure successful NetBackup catalog backups

Use the following strategies to ensure successful catalog backups:

- Use only the methods that are described in this chapter to back up the catalogs. These are the only methods that can track all relevant NetBackup activities and ensure consistency between the catalog files.
- Back up the catalogs often. If catalog backup files are lost, the changes that were made between the last catalog backup and the time of the disk crash are lost.
- If you back up your catalogs to disk, always back up to a different disk than where the catalog files reside. If you back up the catalog to the disk where the actual catalog resides, both catalog backups are lost if the backup disk fails. Recovering the catalog is much more difficult. Also, ensure that the disk has enough space for the catalogs. Backups to a full disk fail.

Note: If a catalog backup is on tape, the tape must be removed when the backup is finished or regular backups cannot proceed. NetBackup does not mix catalog and regular backups on the same tape.

Disaster recovery emails and the disaster recovery files

In a catalog backup policy, you can configure the policy to send the disaster recovery information to an email address. This information appears on the **Disaster recovery** tab.

The disaster recovery email and the accompanying attachments that are sent contain the following important items for a successful catalog recovery:

- A list of the media that contains the catalog backup.
- A list of critical policies.
- Instructions for recovering the catalog.
- The image file as an attachment.

If a catalog backup policy included both full backups and incremental backups, the attached image file can be a full or an incremental catalog backup.

Recovering from an incremental catalog backup completely recovers the entire catalog if the **Automatically recover the entire NetBackup catalog** option is selected on the wizard panel. The entire catalog is recovered because the incremental catalog backup references information from the last full backup.

You do not need to recover the last full catalog backup before you recover the subsequent incremental backups.

- The disaster recovery package (.drpkg file) as an attachment.

Note: If you are not able to receive the disaster recovery packages over emails even after the disaster recovery email configuration, and then ensure the following:

Your email exchange server is configured to have the attachment size equal to or greater than the disaster recovery package size. You can check the size of the package (`.drpkg` file size) on the disaster recovery file location that you have specified in the catalog backup policy.

The firewall and the antivirus software in your environment allows the files with the `.drpkg` extension (which is the extension of a disaster recovery package file).

NetBackup emails the disaster recovery file when the following events occur:

- The catalog is backed up.
- A catalog backup is duplicated or replicated.
- The primary catalog backup or any copy expires automatically or is expired manually.

On Windows: You can tailor the disaster recovery email process by providing the `mail_dr_info.cmd` script in the `install_path\Veritas\NetBackup\bin` directory. This script is similar to the `nbmail.cmd` script. See the comments in the `nbmail.cmd` script for use instructions.

Disaster recovery packages

For increased security, a disaster recovery package is created during each catalog backup. The disaster recovery package file has `.drpkg` extension.

The disaster recovery (DR) package stores the identity of the primary server host. NetBackup requires this package to get the identity of the primary server back after a disaster. Once you have recovered the host identity, you can perform the catalog recovery.

The disaster recovery package contains the following information:

- NetBackup CA-signed certificates and private keys of the primary server certificate and the NetBackup certificate authority (CA) certificate
- Information about the hosts in the domain
- Security settings
- External CA-signed certificates
External CA-signed certificates from Windows certificate store, if applicable

- NetBackup configuration options that are specific to external CA-signed certificates
- Key management service (KMS) configuration

Note: By default, the KMS configuration is not backed up during catalog backup. Set the KMS_CONFIG_IN_CATALOG_BKUP configuration option to 1 to include the KMS configuration as part of the disaster recovery package during catalog backup.

Note: You must set a passphrase for the disaster recovery package for the catalog backups to be successful.

About disaster recovery settings

For increased security, a disaster recovery package is created during each catalog backup.

See [“Disaster recovery packages”](#) on page 184.

During each catalog backup, a disaster recovery package is created and encrypted with the passphrase that you set. You need to provide this encryption passphrase while you install NetBackup on the primary server in a disaster recovery mode after a disaster.

The following options are displayed on the **Disaster Recovery** tab:

Table 20-1 Disaster recovery settings

Setting	Description
Passphrase	<p>Enter the passphrase to encrypt disaster recovery packages.</p> <ul style="list-style-type: none"> By default, the passphrase must contain a minimum of 8 and a maximum of 1024 characters. <p>You can set the passphrase constraints using the <code>nbseccmd -setpassphraseconstraints</code> command option.</p> <ul style="list-style-type: none"> The existing passphrase and the new passphrase must be different. Only the following characters are supported for the passphrase: White spaces, uppercase characters (A to Z), lowercase characters (a to z), numbers (0 to 9), and special characters. Special characters include: ~ ! @ # \$ % ^ & * () _ + - = ` { } [] : ; ' , . / ? < > "
Confirm Passphrase	Re-enter the passphrase for confirmation.

Caution: Ensure that the passphrase contains only the supported characters. If you enter a character that is not supported, you may face problems during disaster recovery package restore. The passphrase may not be validated and you may not be able to restore the disaster recovery package.

Note the following before you modify the passphrase for the disaster recovery packages:

- Subsequent disaster recovery packages are encrypted with the new passphrase that you set.
- If you change the passphrase anytime, it is not changed for the previous disaster recovery packages. Only new disaster recovery packages are associated with the new passphrase.
- Passphrase that you provide while you install NetBackup on the primary server in a disaster recovery mode after a disaster must correspond to the disaster recovery package from which you want to recover the primary server host identity.

Setting the passphrase to encrypt disaster recovery packages

During each catalog backup, a disaster recovery package is created and encrypted with the passphrase that you set.

If you do not set a passphrase before you run a catalog backup, the following points apply:

- NetBackup prevents you from configuring a new catalog backup policy.
- If the catalog backup policy is upgraded from a previous version, catalog backups continue to fail until the passphrase is set.

Note: Catalog backups may fail with status code 144 even though the passphrase is set. This situation occurs because the passphrase may be corrupted. To resolve this issue, you must reset the passphrase.

Caution: Ensure that the passphrase contains only the supported characters. If you enter a character that is not supported, you may face problems during disaster recovery package restore. The passphrase may not be validated and you may not be able to restore the disaster recovery package.

Set or modify the passphrase for disaster recovery packages (NetBackup web UI)

Before you modify the passphrase, review the following information:

See [the section called “Notes for modifying the passphrase for the disaster recovery packages”](#) on page 188.

To set or modify the passphrase (NetBackup web UI)

- 1 Open the NetBackup web UI.
- 2 At the top, click **Settings > Global security**.
- 3 Click **Disaster recovery**.
- 4 Enter and confirm the passphrase.

Review the following password rules:

- The existing passphrase and the new passphrase must be different.
- By default, the passphrase must contain a minimum of 8 and a maximum of 1024 characters.

You can set the passphrase constraints using the `nbseccmd -setpassphraseconstraints` command option.

- Only the following characters are supported for the passphrase: White spaces, uppercase characters (A to Z), lowercase characters (a to z), numbers (0 to 9), and special characters. Special characters include: ~ ! @ # \$ % ^ & * () _ + - = ` { } [] | : ; ' , . / ? < > "

Caution: If you enter a character that is not supported, you may face problems during disaster recovery package restore. The passphrase may not be validated and you may not be able to restore the disaster recovery package.

- 5 Click **Save**. If the passphrase already exists, it is overwritten.

Set or modify the passphrase for disaster recovery packages (command-line interface)

Before you modify the passphrase, review the following information:

See [the section called “Notes for modifying the passphrase for the disaster recovery packages”](#) on page 188.

To set or modify the passphrase using the command-line interface

- 1 The NetBackup administrator must be logged on to the NetBackup Web Management Service to perform this task. Use the following command to log on:

```
bpnbat -login -loginType WEB
```

- 2 Run the following command to set a passphrase to encrypt disaster recovery packages:

```
nbseccmd -drpkgpassphrase
```

- 3 Enter the passphrase.

If a passphrase already exists, it is overwritten.

Notes for modifying the passphrase for the disaster recovery packages

Consider the following points before you modify the passphrase

- Subsequent disaster recovery packages are encrypted with the new passphrase that you set.
- If you change the passphrase anytime, it is not changed for the previous disaster recovery packages. Only new disaster recovery packages are associated with the new passphrase.
- The passphrase that you provide when you install NetBackup on the primary server in a disaster recovery mode after a disaster must correspond to the disaster recovery package from which you want to recover the primary server host identity.

Recovering the catalog

Catalog recovery is discussed in the [NetBackup Troubleshooting Guide](#).

Managing backup images

This chapter includes the following topics:

- [About the Catalog utility](#)
- [Catalog utility search criteria and backup image details](#)
- [Verify backup images](#)
- [Promote a copy to a primary copy](#)
- [Duplicate backup images](#)
- [Expire backup images](#)
- [About importing backup images](#)

About the Catalog utility

Use the **Catalog** utility to search for a backup image to perform the following actions:

- Verify the backup contents with what is recorded in the NetBackup catalog.
See [“Verify backup images”](#) on page 193.
- Duplicate the backup image to create up to 10 copies.
- See [“Duplicate backup images”](#) on page 195.
- Promote a copy of a backup to be the primary backup copy.
- See [“Promote a copy to a primary copy”](#) on page 194.
- Expire backup images.
See [“Expire backup images”](#) on page 199.
- Import expired backup images or images from another NetBackup server.
See [“About importing expired images”](#) on page 200.

Catalog utility search criteria and backup image details

The catalog utility in the NetBackup web UI lets you perform various actions on a catalog image. For example, verify or duplicate an image. The catalog utility is organized as follows:

- **Search tab**
Provides the search criteria you can use to locate backup images. See [Table 21-1](#) for details.
For more details on these actions and on data-in-transit encryption (DTE) in your NetBackup environment, see the [NetBackup Administrator's Guide, Volume I](#) and [NetBackup Security and Encryption Guide](#).
After you search for backup images, the image list displays at the bottom of the page. Click **Show or hide columns** to display additional information about the images. See [Search results properties](#) for additional properties that are displayed in the search results.
- **Activity tab**
Displays the progress of the request to verify, duplicate, expire, or import an image.

Search criteria

The following actions and search criteria are available when you search for catalog images.

Table 21-1 Catalog search criteria

Property		Description
Action		Specifies the action that was used to create the image: Verify, Duplicate, Import . See "Verify backup images" on page 193. See "Duplicate backup images" on page 195. See "Expire backup images" on page 199.
Media		
	Media ID	The media ID for the volume. To search on all media, select <All> .
	Media host	The host name of the media server that produced the originals. To search all hosts, select All media hosts .
	Disk type	The disk type of the storage unit.
	Disk pool	The name of the disk pool. Not enabled if the disk type is BasicDisk.

Table 21-1 Catalog search criteria (*continued*)

Property		Description
	Media server	The name of the media server that produced the original images. To search all media servers, select All media hosts .
	Volume	The ID of the disk volume in the disk pool. Enabled if the disk type is not BasicDisk.
	Path	Searches for an image on a disk storage unit, if the path is entered. Or, searches all of the disk storage on the specified server, if All was selected. Enabled if the disk type is BasicDisk.
Date/time range		The range of dates and times that you want to search. The Global attributes property Policy update interval determines the default range.
Copies, policies, and clients		
	Copies	The copy that you want to search. Select either Primary or the copy number.
	Policy name	The policy under which the selected backups were performed. To search all policies, select All policies .
	Policy type	The purpose of the policy.
	Type of backup	The type of schedule that created the backup. To search all schedule types, select All backup types . Enabled if you select a specific Policy type .
	Client (host name)	The host name of the client that produced the backup. To search all hosts, select All clients .
Job priority		
	Override default job priority	<p>The job priority for the catalog action (verify, duplicate, or import).</p> <p>To change the default, enable Override default priority. Then, select a value for the Job priority.</p> <p>If this option is not enabled, the job runs using the default priority as specified in the Default job priorities host property.</p> <p>Changes that you make affect the priority for the selected job only.</p>
	Job priority	The priority of the catalog job. Enabled if you override the default priority.

Search results properties

In addition to properties that you can select for the search, other properties are displayed for the images.

Table 21-2 Catalog search results properties

Property	Description
Copy DTE mode	Specifies whether the data is transferred over a secure channel when the current image copy is created.
Copy hierarchy DTE mode	Specifies whether the data is transferred over a secure channel when the current image copy and all its parent copies in the hierarchy are created.
Expiration date	The date that the image expires.
Image DTE mode	Indicates the data-in-transit encryption (DTE) mode for the backup image.
Immutable	Indicates if the backup image is read-only and cannot be modified, corrupted, or encrypted.
Indelible	Indicates if the backup image is protected from being deleted before it expires.
Malware scan status	The scan status of the backup image.
Mirror copy	Indicates if the image is a mirror replica or copy.
On hold	<p>Indicates whether the image copy is on hold or not.</p> <p>Yes: The image has only one copy and a hold is set on the copy.</p> <p>No: No hold is set on the copy.</p> <p>A hold is set with the <code>nbholdutil</code> command.</p>
Time	The time that the backup ran.
WORM unlock time	<p>Indicates the time at which the image can be altered or deleted.</p> <p>Applies to the storage units that are WORM capable.</p>

Verify backup images

NetBackup can verify the contents of a backup by reading the volume and comparing its contents to what is recorded in the NetBackup catalog.

This operation does not compare the data on the volume to the contents of the client disk. However, the operation does read each block in the image to verify that the volume is readable. (However, data corruption within a block is possible.)

NetBackup verifies only one backup at a time and tries to minimize media mounts and positioning time.

To verify backup images

- 1 On the left, click **Catalog**.
- 2 From the **Action** list, select **Verify**.
- 3 Select the search criteria to find the image you want to verify. Click **Search**.
Backups that have fragments on another volume are included, as they exist in part on the specified volume.
See [“Catalog utility search criteria and backup image details”](#) on page 191.
- 4 Select the image that you want to verify. Then click **Verify**.
- 5 Click the **Activity** tab to view the job results.

Promote a copy to a primary copy

Each backup is assigned a primary copy. NetBackup uses the primary copy to satisfy restore requests. The first backup image that is created successfully by a NetBackup policy is the primary backup. If the primary copy is unavailable and a duplicate copy exists, select a copy of the backup and set it to be the primary copy.

NetBackup restores from the primary backup, and Vault duplicates from the primary backup. If your Vault profile performs duplication, you can designate one of the duplicates as the primary. In most circumstances, the copy remaining in the robot is the primary backup. When a primary backup expires, the next backup (if it exists) is promoted to primary automatically.

Use one of the following methods to promote a copy to a primary copy:

Promote a backup copy to a primary copy

See [the section called “Promote a backup copy to a primary copy”](#) on page 194.

Promote a copy to a primary copy for many backups using the `bpchangeprimary` command

See [the section called “Promote a copy to a primary copy for many backups”](#) on page 195.

Promote a backup copy to a primary copy

To promote a backup copy to a primary copy

- 1 On the left, click **Catalog**.
- 2 From the **Action** list, select **Duplicate**.

- 3 Select the search criteria to find the image you want to promote. Be sure that you indicate a copy in the **Copies** field and not **Primary copy**.

See “[Catalog utility search criteria and backup image details](#)” on page 191.

- 4 Click **Search**.

- 5 Select the image you want to promote. Then click **Set primary copy**.

After the image is promoted to the primary copy, the **Primary copy** column immediately reads **Yes**.

- 6 Click the **Activity** tab to view the job results.

Promote a copy to a primary copy for many backups

More information on the `bpchangeprimary` is available in the [NetBackup Commands Reference Guide](#).

To promote a copy to a primary copy for many backups

- ◆ You can also promote a copy to be a primary copy for many backups using the `bpchangeprimary` command. For example, the following command promotes all copies on the media that belongs to the `b_pool` volume pool. The copies must have been created after August 8, 2022:

```
bpchangeprimary -pool b_pool -sd 08/01/2022
```

In the next example, the following command promotes copy 2 of all backups of `client_a`. The copies must have been created after January 1, 2022:

```
bpchangeprimary -copy 2 -cl client_a -sd 01/01/2022
```

Duplicate backup images

NetBackup does not verify in advance whether the storage units and the drives that are required for the duplicate operation are available for use. NetBackup verifies that the destination storage units exist. The storage units must be connected to the same media server.

[Table 21-3](#) lists the scenarios in which duplication is or is not possible:

Table 21-3 Backup duplication scenarios

Duplication possible	Duplication not possible
<ul style="list-style-type: none"> ■ From one storage unit to another. ■ From one media density to another. ■ From one server to another. ■ From multiplex to nonmultiplex format. ■ From multiplex format and retain the multiplex format on the duplicate. The duplicate can contain all or any subset of the backups that were included in the original multiplexed group. The duplicate is created with a single pass of the tape. (A multiplexed group is a set of backups that were multiplexed together during a single session.) 	<ul style="list-style-type: none"> ■ While the backup is created (unless making multiple copies concurrently). ■ When the backup has expired. ■ By using NetBackup to schedule duplications automatically (unless you use a Vault policy to schedule duplication) ■ When it is a multiplexed duplicate of the following type: <ul style="list-style-type: none"> ■ FlashBackup ■ NDMP backup ■ Backups from disk type storage units ■ Backups to disk type storage units ■ Nonmultiplexed backups

An alternative to duplicating backups is to create up to four copies simultaneously at backup time. (This option is sometimes referred to as Inline Copy.) Another alternative is to use storage lifecycle policies.

To duplicate backup images

- 1 On the left, click **Catalog**.
- 2 From the **Action** list, select **Duplicate**.
- 3 Select the search criteria to find the image you want to duplicate.
See [“Catalog utility search criteria and backup image details”](#) on page 191.
- 4 Select the images that you want to duplicate and click **Duplicate**.
If you duplicate a catalog backup, select all child jobs that were used to create the catalog backup. All jobs must be duplicated to duplicate the catalog backup.
- 5 Specify the number of copies you want to create. NetBackup can create up to 10 copies of unexpired backups.
If enough drives are available, the copies are created simultaneously. Otherwise, the system may require operator intervention if four copies are to be created using only two drives, for example.

- 6 The primary copy is the copy from which restores are done. Normally, the original backup is the primary copy.

If you want one of the duplicated copies to become the primary copy, select the copy number from the drop-down, otherwise select **Keep current primary copy**.

When the primary expires, a different copy automatically becomes primary. (The copy that is chosen is the one with the smallest copy number. If the primary is copy 1, copy 2 becomes primary when it expires. If the primary is copy 5, copy 1 becomes primary when it expires.)

- 7 Specify the storage unit where each copy is stored. If a storage unit has multiple drives, it can be used for both the source and destination.

All storage units must meet the criteria for creating multiple copies.

- 8 Specify the volume pool where each copy is stored.

The following volume pool selections are based on the policy type setting that was used for the query.

If the Policy type is set to All policy types (default).	Specifies that all volume pools are included in the drop-down list. Both catalog and non-catalog volume pools are included.
--	---

If the Policy type is set to NBU-Catalog .	Specifies that only catalog volume pools are included in the drop-down list.
--	--

If the Policy type is set to a policy type other than NBU-Catalog or All policy types .	Specifies that only non-catalog volume pools are included in the drop-down list.
--	--

NetBackup does not verify that the media ID selected for the duplicate copy is different from the media ID that contains the original backup. Because of this potential deadlock, specify a different volume pool to ensure that a different volume is used.

- 9 Select the retention level for the copy, or select **No change**.

The duplicate copy shares many attributes of the primary copy, including backup ID. Other attributes apply only to the primary. (For example, elapsed time.) NetBackup uses the primary copy to satisfy restore requests.

Consider the following items when selecting the retention level:

- If **No change** is selected for the retention period, the expiration date is the same for the duplicate and the source copies. You can use the `bpxupdate` command to change the expiration date of the duplicate.

- If a retention period is indicated, the expiration date for the copy is the backup date plus the retention period. For example, if a backup was created on November 14, 2022 and its retention period is one week, the new copy's expiration date is November 21, 2022.
- 10 Specify whether the remaining copies should continue or fail if the specified copy fails.
 - 11 Specify who should own the media onto which you duplicate images.
 Select one of the following:

Any	Specifies that NetBackup chooses the media owner, either a media server or server group.
None	Specifies the media server that writes to the media owns the media. No media server is specified explicitly, but you want a media server to own the media.
A server group	Specifies that only those media servers in the group are allowed to write to the media on which backup images for this policy are written. All of the media server groups that are configured in your NetBackup environment appear in the drop-down list.
 - 12 If the selection includes multiplexed backups and the backups are to remain multiplexed in the duplicate, select **Preserve multiplexing**. If you do not duplicate all the backups in a multiplexed group, the duplicate contains a different layout of fragments. (A multiplexed group is a set of backups that were multiplexed together during a single session.)

 By default, duplication is done serially and attempts to minimize media mounts and positioning time. Only one backup is processed at a time. If **Preserved multiplexing** is enabled, NetBackup first duplicates all backups that cannot be multiplex duplicated before the multiplexed backups are duplicated.

 The **Preserve multiplexing** setting does not apply when the destination is a disk storage unit. However, if the source is a tape and the destination is a disk storage unit, select **Preserve multiplexing** to ensure that the tape is read in one pass.
 - 13 Click **Yes** to start duplicating.
 - 14 Click the **Activity** tab, then select the duplication job to view the job results.
 See ["Multiplexed duplication considerations"](#) on page 199.

Multiplexed duplication considerations

Consider the following items about multiplexed duplication.

Table 21-4 Multiplexed duplication considerations

Consideration	Description
Multiplex settings are ignored	When multiplexed backups are duplicated, the multiplex settings of the destination storage unit and the original schedule are ignored. However, if multiple multiplexed groups are duplicated, the grouping within each multiplexed group is maintained. This means that the duplicated groups have a multiplexing factor that is no greater than the factor that was used during the original backup.
Backups in a multiplexed group are duplicated and duplicated group is identical	When backups in a multiplexed group are duplicated to a storage unit, the duplicated group is identical as well. However, the storage unit must have the same characteristics as the unit where the backup was originally performed. The following items are exceptions: <ul style="list-style-type: none">■ If EOM (end of media) is encountered on either the source or the destination media.■ If any of the fragments are zero length in the source backups, the fragments are removed during duplication. A fragment of zero length occurs if many multiplexed backups start at the same time.

Jobs that appear while making multiple copies

When multiple copies are made concurrently, a parent job appears, plus a job for each copy.

The parent job displays the overall status, whereas the copy jobs display the status of a single copy. Viewing the status of individual jobs lets you troubleshoot jobs individually. For example, if one copy fails but the other copy is successful, or if each copy fails for different reasons. If at least one copy is successful, the status of the parent job is successful. Use the **Parent Job ID** filter to display the parent Job ID. Use the **Copy number** filter to display the copy number for a particular copy.

Expire backup images

To expire a backup image means to force the retention period to expire, or information about the backup is deleted. When the retention period expires,

NetBackup deletes information about the backup. The files in the backups are unavailable for restores without first re-importing.

To expire a backup image

- 1 On the left, click **Catalog**.
- 2 Select the search criteria to find the image you want to duplicate.
See [“Catalog utility search criteria and backup image details”](#) on page 191.
- 3 Select the image you want to expire and click **Expire > Expire**.

About importing backup images

NetBackup can import the backups that have expired or the backups from another NetBackup server.

During an import operation, NetBackup recreates NetBackup catalog entries for the backups on the imported volume. The import capability is useful for moving volumes from one site to another and for recreating NetBackup catalog entries.

An image is imported in the following two phases:

Table 21-5 Phases to import an image

Phase	Description
Phase I: Initiate Import	NetBackup creates a list of expired catalog entries for the backups on the imported volume. No actual import occurs in Phase I. See “Import backup images, Phase I” on page 201.
Phase II: Import	Images are selected for importing from the list of expired images that was created in Phase I. See “Import backup images, Phase II” on page 202.

About importing expired images

The expiration date for the imported items is the current date plus the retention period. For example, if a backup is imported on November 14, 2021, and its retention period is one week, the new expiration date is November 21, 2021.

Consider the following items when importing backup images:

- You cannot import a backup if an unexpired copy of it already exists on the server.
- NetBackup does not direct backups to imported volumes.

- If you import a catalog backup, import all the child jobs that were used to create the catalog backup. All jobs must be imported to import the catalog backup.
- To import a volume with the same media ID as an existing volume on a server, use the following example where you want to import a volume with media ID A00001. (A volume with media ID A00001 already exists on the server.)
 - Duplicate the existing volume on the server to another media ID (for example, B00001).
 - Remove information about media ID A00001 from the NetBackup catalog by running the following command:
On Windows:

```
install_path\NetBackup\bin\admincmd\bpexpdate  
-d 0 -m mediaID
```


On UNIX:

```
/usr/opensv/netbackup/bin/admincmd/bpexpdate -d 0 -m  
media_ID
```
 - Delete media ID A00001 from Media Manager on the server.
 - Add the other A00001 to Media Manager on the server.To avoid this problem in the future, use unique prefix characters for media IDs on all servers.

See [“Expire backup images”](#) on page 199.

Import backup images, Phase I

Phase I of the import process creates a list of images from which to select to import in Phase II. No import occurs in Phase I.

Note the following about importing backup images:

- If tape is used, each tape must be mounted and read. It may take some time to read the catalog and build the list of images.
- The backup is not imported if it begins on a media ID that the initiating backup procedure did not process.
- The backup is incomplete if it ends on a media ID that the initiating backup procedure did not process.
- To import a catalog backup, import all of the child jobs that were used to create the catalog backup.

To perform Phase I: initialize import of backup images

- 1 To import the images from tape, make the media accessible to the media server so the images can be imported.
- 2 On the left, click **Catalog**.
- 3 On the **Actions** menu, select **Phase I import**.
- 4 For the **Media server**, specify the name of the host that contains the volume to import. This media server becomes the media owner.
- 5 Indicate the location of the image. For the **Image type**, select whether the images to be imported are located on tape or on disk.

The following table shows the actions to take depending on the location of the image.

If images are on tape	In the Media ID field, enter the Media ID of the volume that contains the backups to import.
If images are on disk	<p>In the Disk type field, select the type of the disk storage unit on which to search for backup images. The disk types depend on which NetBackup options are licensed.</p> <p>If the disk type references a disk pool, enter or select the disk pool and the disk volume ID.</p> <p>For a BasicDisk type, enter or browse to the path to the images in the field provided.</p> <p>For other disk types, select <All> or the specific volume.</p>

- 6 Click **Import** to begin reading the catalog information from the source volume.
- 7 Click on the **Activity** tab to watch as NetBackup looks at each image on the tape. NetBackup determines whether or not each image has expired and can be imported. The job also displays in the Activity monitor as an Image import type. Select the import job log to view the job results.

Import backup images, Phase II

To import the backups, first run the Initiate Import operation (Import Phase I). The first phase reads the catalog to determine all of the media that contain the catalog backup images. After Phase I, start the Import operation (Phase II). If Phase II is run before Phase I, the import fails with a message. For example, Unexpected EOF or Import of backup ID failed, fragments are not consecutive.

To import backup images, Phase II

- 1** On the left, click **Catalog**.
- 2** On the **Actions** menu, select **Phase II import**.
- 3** Set up the search criteria to find images available to import. Be sure to select a date range that includes the images you want to import. Click **Search**.
- 4** Select the images that you want to import. Click **Import** to import the selected images.
- 5** Select whether you'd like to log the names of all of the files that are found in the imported images. Click **OK**.
- 6** Click the **Activity** tab to view the progress of Import phase II.

Pausing data protection activity

This chapter includes the following topics:

- [Pause backups and other activity](#)
- [Allow the automatic pause of data protection activity](#)
- [Pause backups and other activity on a client](#)
- [View paused backups and other paused activities](#)
- [Resume data protection activity](#)

Pause backups and other activity

By default, NetBackup or its users cannot pause data protection activities. Backups and other activities continue even if a scan detects malware in an image or a recovery point. Data protection activity includes backups, duplication, and, image expiration.

You can allow NetBackup and authorized users to pause data protection activities. Then NetBackup can automatically pause activity on specific clients. For example, if a scan detects malware in backup images or recovery points for a specific client. A pause applies to scheduled backups and other automatic activities. It also applies to operations that a user initiates.

Authorized users can manually pause data protection activities. These users have an RBAC role with the necessary security permissions to pause data protection activity.

Allow the automatic pause of data protection activity

You can choose to allow NetBackup and authorized users to pause backups and duplication. Optionally, you can allow also the pause the expiration of backup images.

To allow NetBackup and authorized users to pause data protection activity

- 1 On the left, click **Detection and reporting > Paused protection**.
- 2 Click **Edit settings** and then **Edit**.
- 3 Click **Allow automatic pause**.
- 4 (Conditional) If you want to allow the pause of the expiration of backup images, select **Pause image expiration**.

Pause backups and other activity on a client

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

The following conditions occur when a client is added in the paused protection list:

- Automatic and manual replication of the client is paused.
- If the **Automatic pause protection > Pause image expiration** option is enabled, the automatic image cleanup for the client is paused.

View paused backups and other paused activities

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

To view paused data protection activity

- 1 On the left, click **Detection and reporting > Protection status**.
- 2 The page displays the list of clients where the protection activity is paused. "Automatic" indicates that the pause was applied automatically by NetBackup. "User-initiated" indicates that a user manually applied the pause to the client.

If you have not yet configured the setting, click **Edit settings**.
- 3 To see the details of the pause for a specific client, locate the client name. Then click **Actions > View pause details**.

Resume data protection activity

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

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

To resume data protection activity for a client

- 1 On the left, click **Detection and reporting > Paused protection**.
- 2 Select one or more clients and click **Resume**.

Managing security

- [Chapter 23. Security events and audit logs](#)
- [Chapter 24. Managing security certificates](#)
- [Chapter 25. Managing host mappings](#)
- [Chapter 26. Configuring multi-person authorization](#)
- [Chapter 27. Managing user sessions](#)
- [Chapter 28. Configuring multi-factor authentication](#)
- [Chapter 29. Managing the global security settings for the primary server](#)
- [Chapter 30. Using access keys, API keys, and access codes](#)
- [Chapter 31. Configuring authentication options](#)
- [Chapter 32. Managing role-based access control](#)
- [Chapter 33. Disabling access to NetBackup interfaces for OS Administrators](#)

Security events and audit logs

This chapter includes the following topics:

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

View security events and audit logs

NetBackup audits user-initiated actions in a NetBackup environment to help answer who changed what and when they changed it. For a full audit report, use the `nbauditreport` command. See [“Viewing the detailed NetBackup audit report”](#) on page 213.

To view security events and audit logs

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

About NetBackup auditing

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

Auditing of NetBackup operations provides the following benefits:

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

About the NetBackup Audit Manager

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

An administrator can search specifically for:

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

Note the following:

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

Actions that NetBackup audits

NetBackup records the following user-initiated actions.

Activity monitor actions	Canceling, suspending, resuming, restarting, or deleting any type of job creates an audit record.
Alerts and email notifications	If an alert cannot be generated or an email notification cannot be sent for NetBackup configuration settings. For example, SMTP server configuration and the list of excluded status codes for alerts.

Anomalies	When a user reports an anomaly as false positive, the action is audited and logged for that user.
Asset actions	<p>Deleting an asset, such as a vCenter server, as part of the asset cleanup process is audited and logged.</p> <p>Creating, modifying, or deleting an asset group as well any action on an asset group for which a user is not authorized is audited and logged.</p>
Authorization failure	Authorization failure is audited when you use the NetBackup web UI, or the NetBackup APIs.
Catalog information	<p>This information includes:</p> <ul style="list-style-type: none"> ■ Verifying and expiring images. ■ Read the requests that are sent for the front-end usage data.
Certificate management	Creating, revoking, renewing, and deploying of NetBackup certificates and specific NetBackup certificate failures.
Certificate Verification Failures (CVFs)	<p>Any failed connection attempts that involve SSL handshake errors, revoked certificates, or host name validation failures.</p> <p>For certificate verification failures (CVFs) that involve SSL handshakes and revoked certificates, the timestamp indicates when the audit record is posted to the primary server. (Rather than when an individual certificate verification fails.) A CVF audit record represents a group of CVF events over a time period. The record details provide the start and the end times of the time period as well as the total number of CVFs that occurred in that period.</p>
Disk pools and Volume pools actions	Adding, deleting, or updating disk or volume pools.
Hold operations	Creating, modifying, and deleting hold operations.
Host database	NetBackup operations that are related to the host database.
IRE configuration and states	Adding, updating, and deleting IRE allowed subnets or schedule. IRE external network is opened or closed by IRE schedule or by an administrator.
Logon attempts	Any successful or any failed logon attempts for the NetBackup web UI or the NetBackup APIs.
Policies actions	Adding, deleting, or updating policy attributes, clients, schedules, and backup selections lists.

Restore and browse image user actions	<p>All the restore and browse image content (<code>bplist</code>) operations that a user performs are audited with the user identity.</p> <p>To set an interval to periodically add audit records of the browse image (<code>bplist</code>) operations from the cache into the NetBackup database, use the <code>DATAACCESS_AUDIT_INTERVAL_HOURS</code> configuration option. Setting this configuration option prevents the NetBackup database size from increasing exponentially because of the <code>bplist</code> audit records.</p> <p>See the NetBackup Administrator's Guide Volume I.</p> <p>To add all the <code>bplist</code> audit records from the cache into the NetBackup database, run the following command on the primary server:</p> <pre>nbcertcmd -postAudit -dataAccess</pre>
Security configuration	Information that is related to changes that are made to the security configuration settings.
Starting a restore job	NetBackup does not audit when other types of jobs begin. For example, NetBackup does not audit when a backup job begins.
Starting and stopping the NetBackup Audit Manager (<code>nbaudit</code>).	Starting and stopping of the <code>nbaudit</code> manager is always audited, even if auditing is disabled.
Storage lifecycle policy actions	Attempts to create, modify, or delete a storage lifecycle policy (SLP) are audited and logged. However, activating and suspending an SLP using the command <code>nbstlutil</code> are not audited. These operations are audited only when they are initiated from a NetBackup graphical user interface or API.
Storage servers actions	Adding, deleting, or updating storage servers.
Storage units actions	Adding, deleting, or updating storage units. Note: Actions that are related to storage lifecycle policies are not audited.
Token management	Creating, deleting, and cleanup of tokens and specific token issuing failures.
User action that fails to create an audit record	If auditing is enabled but a user action fails to create an audit record, the audit failure is captured in the <code>nbaudit</code> log. NetBackup status code 108 is returned (<code>Action succeeded but auditing failed</code>). The NetBackup does not return an exit status code 108 when auditing fails.

Actions that NetBackup does not audit

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

Any failed actions.	NetBackup logs failed actions in NetBackup error logs. Failed actions do not display in audit reports because a failed attempt does not bring about a change in the NetBackup system state.
---------------------	---

The effect of a configuration change	The results of a change to the NetBackup configuration are not audited. For example, the creation of a policy is audited, but the jobs that result from its creation are not.
The completion status of a manually initiated restore job	While the act of initiating a restore job is audited, the completion status of the job is not audited. Nor is the completion status of any other job type, whether initiated manually or not. The completion status is displayed in the Activity Monitor.
Internally initiated actions	NetBackup-initiated internal actions are not audited. For example, the scheduled deletion of expired images, scheduled backups, or periodic image database cleanup is not audited.
Rollback operations	Some operations are carried out as multiple steps. For example, creating an MSDP-based storage server consists of multiple steps. Every successful step is audited. Failure in any of the steps results in a rollback, or rather, the successful steps may need to be undone. The audit record does not contain details about rollback operations.
Host properties actions	Changes made with the <code>bpsetconfig</code> or the <code>nbsetconfig</code> commands, or the equivalent property in host properties, are not audited. Changes that are made directly to the <code>bp.conf</code> file or to the registry are not audited.

User identity in the audit report

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

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

Audit retention period and catalog backups of audit records

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

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

To configure the audit retention period

- 1 Log on to the primary server.
- 2 Open the following directory:

Windows: *install_path*\NetBackup\bin\admincmd

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

- 3 Enter the following command:

```
nbemmcmd -changesetting -AUDIT_RETENTION_PERIOD  
number_of_days -machinename primaryserver
```

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

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

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

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

`-AUDIT_RETENTION_PERIOD`.

Viewing the detailed NetBackup audit report

You can view the actions NetBackup audits from a primary server using the NetBackup web UI. You can see full audit event details with the *nbauditreport* command.

To view the full audit report

- 1 Log on to the primary server.
- 2 Enter the following command to display the audit report in the summary format.

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

UNIX: /usr/opensv/netbackup/bin/admincmd\mbauditreport

Or, run the command with the following options.

<code>-sdate</code>	The start date and time of the report data you want to view.
<code><"MM/DD/YY [HH:[MM[:SS]]]"></code>	
<code>-edate</code>	The end date and time of the report data you want to view.
<code><"MM/DD/YY [HH:[MM[:SS]]]"></code>	
<code>-ctgy category</code>	<p>The category of user action that was performed. Categories such as <code>POLICY</code> may contain several sub-categories such as schedules or backup selections. Any modifications to a sub-category are listed as a modification to the primary category.</p> <p>See the NetBackup Commands Guide for <code>-ctgy</code> options.</p>
<code>-user</code>	Use to indicate the name of the user for whom you'd like to display audit information.
<code><username[:domainname]></code>	
<code>-fmt DETAIL</code>	<p>The <code>-fmt DETAIL</code> option displays a comprehensive list of audit information. For example, when a policy is changed, this view lists the name of the attribute, the old value, and the new value. This option has the following sub-options:</p> <ul style="list-style-type: none">■ <code>[-notruncate]</code> . Display the old and new values of a changed attribute on separate lines in the details section of the report.■ <code>[-pagewidth <NNN>]</code> . Set the page width for the details section of the report.

`-fmt PARSABLE`

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

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

3 The audit report contains the following details:

DESCRIPTION	The details of the action that was performed.
USER	The identity of the user who performed the action. See "User identity in the audit report" on page 212.
TIMESTAMP	The time that the action was performed.

The following information only displays if you use the `-fmt DETAIL` or the `-fmt PARSABLE` options.

CATEGORY	The category of user action that was performed.
ACTION	The action that was performed.
REASON	The reason that the action was performed. A reason displays if a reason was specified for the operation that created the change.
DETAILS	An account of all of the changes, listing the old values and the new values.

Example of the audit report:

```
[root@server1 admincmd]# ./nbauditreport
```

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

Audit records fetched: 5

Send audit events to system logs

You can send NetBackup audit events to system logs. You must have the NetBackup Security Administrator role or similar RBAC permissions to perform this task.

To send audit events to system logs

- 1 Open the NetBackup web UI.
- 2 On the left, select **Security > Security events**.
- 3 On the top right, click **Security event settings**.
- 4 Enable the **Send the audit events to the system logs** option.
- 5 Click **Select audit event** categories. Then select the audit categories for which you want to send the audit events to the system logs.

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

- 6 Click **Save**.

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

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

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

Send audit events to log forwarding endpoints

You can send NetBackup audit events to log forwarding endpoints.

To send audit events to log forwarding endpoints

- 1 On the left, select **Security > Security events**.
- 2 On the top right, click **Security events settings**.

- 3 Enable **Send the audit events to log forwarding endpoints** option.
Once you enable the option, the **Select endpoints and categories** option appears.
- 4 Click the **Select endpoints and categories** option to see the log forwarding endpoints that are configured in your environment and the available audit categories.
Example of an endpoint: Azure Sentinel.
- 5 Select the appropriate log forwarding endpoints.
- 6 Click the **Select audit event categories** option.
- 7 On the **Select audit event categories** pop-up screen, select the categories of the audit events that you want to forward to the selected endpoints. For example, Alert, Anomaly and so on.
- 8 Once you select your log forwarding endpoint, options to specify the associated credentials appear. You can either add new credentials for the endpoint or select the existing credentials.

Managing security certificates

This chapter includes the following topics:

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

About security management and certificates in NetBackup

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

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

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

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

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

Security certificates for NetBackup 8.1 and later hosts

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

Security certificates for NetBackup 8.0 hosts

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

NetBackup host IDs and host ID-based certificates

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

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

In some cases a host can have multiple host IDs:

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

Managing NetBackup security certificates

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

See [“Using external security certificates with NetBackup”](#) on page 224.

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

View a NetBackup certificate

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

To view a NetBackup certificate

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

Revoke a NetBackup CA certificate

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

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

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

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

To revoke a NetBackup CA certificate

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

View the NetBackup certificate authority details and fingerprint

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

To view the NetBackup certificate authority details and fingerprint

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

Reissue a NetBackup certificate

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

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

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

Reissue a NetBackup certificate, with a token

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

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

To reissue a NetBackup certificate for a host

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

Allow a NetBackup certificate reissue, without a token

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

To allow a NetBackup certificate reissue, without a token

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

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

Revoke the ability to reissue a NetBackup certificate without a token

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

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

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

Managing NetBackup certificate authorization tokens

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

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

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

Create an authorization token

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

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

See [“Reissue a NetBackup certificate”](#) on page 221.

To create an authorization token

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

To find and copy an authorization token value

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

To find and copy an authorization token value

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

Cleanup tokens

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

To cleanup tokens

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

Delete a token

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

To delete a token

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

Using external security certificates with NetBackup

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

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

See [“Configure an external certificate for the NetBackup web server”](#) on page 225.

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

Configure an external certificate for the NetBackup web server

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

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

To configure an external certificate for the web server

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

- 2 Run the following command:

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

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

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

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

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

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

On UNIX, run the following commands:

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

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

Location of the commands:

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

UNIX `install_path/wmc/bin/install`

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

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

- 4 Restart the NetBackup Messaging Queue Broker (nbmqbroker) service as follows:

On Windows:

Go to the **Services** application in the **Windows Control Panel** and manually restart the NetBackup Messaging Queue Broker service.

On UNIX:

Run the following command:

```
nbmqbroker stop; nbmqbroker start
```

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

Remove the external certificate configured for the web server

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

To remove the external certificate configured for the web server

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

```
configureWebServerCerts -removeExternalCert -nbHost
```

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

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

- 2 Restart the NetBackup Web Management Console service.
 - In a clustered primary server setup, run the following command on the active node to unfreeze the cluster:

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

- 3** Restart the NetBackup Messaging Queue Broker (`nbmqbroker`) service as follows:

On Windows:

Go to the **Services** application in the **Windows Control Panel** and manually restart the NetBackup Messaging Queue Broker service.

On UNIX:

Run the following command:

```
nbmqbroker stop; nbmqbroker start
```

Update or renew the external certificate for the web server

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

To update or renew the external certificate for the web server

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

```
configureWebServerCerts -addExternalCert -nbHost -certPath  
certificate path -privateKeyPath private key path -trustStorePath  
CA bundle path
```

View external certificate information for the NetBackup hosts in the domain

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

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

To view external certificate information for the hosts

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

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

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

View details for a host's external certificate

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

To view details for a host's external certificate

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

The list of external certificates displays for the primary server.

- 3 To view additional certificate details for a host, click on a host name.

Managing host mappings

This chapter includes the following topics:

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

View host security and mapping information

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

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

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

To view NetBackup host information

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

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

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

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

See [“Disable automatic mapping of NetBackup host names”](#) on page 258.

See [“Example host mappings”](#) on page 232.

Approve the host mappings that NetBackup discovers

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

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

To approve the host names that NetBackup discovers

- 1 On the left, select **Security > Host mappings**.
- 2 Click the **Mappings to approve** tab.
- 3 Click the name of the host.
- 4 Review the mappings for the host and click **Approve** if you want to use the discovered mapping.

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

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

- 5 Click **Save**.

Map other host names to a host

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

To map a host name to a host

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

Map shared or cluster names to multiple NetBackup hosts

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

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

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

To map shared or cluster names to multiple NetBackup hosts

- 1 On the left, select **Security > Host mappings**.
- 2 Click **Add shared or cluster mappings**.
- 3 Enter a **Shared host name or cluster name** that you want to map to two or more NetBackup hosts.

For example, enter a cluster name that is associated with NetBackup hosts in your environment.

- 4 On the right, click **Add**.

- 5 Select the NetBackup hosts that you want to add and click **Add to list**.
For example, if you entered a cluster name in step 3 select the nodes in the cluster here.
- 6 Click **Save**.

Example host mappings

The following examples describe scenarios where you may want to create host mappings to consolidate host names or to ensure successful communication between hosts.

- See [the section called “Examples of auto-discovered mappings for a cluster”](#) on page 232.
- See [the section called “Example of host names that are displayed for a multiple NIC environment”](#) on page 233.
- See [the section called “Example of auto-discovered mappings for a cluster in a multiple NIC environment”](#) on page 234.
- See [the section called “Examples of auto-discovered mappings for SQL Server environments”](#) on page 234.

Examples of auto-discovered mappings for a cluster

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

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

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

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

Example of host names that are displayed for a multiple NIC environment

In some advanced NetBackup configurations like a multi-NIC environment, a NetBackup host may display under two host names in the **Host properties**. One name reflects the operating system (OS) name and the other name reflects the name that was specified when NetBackup was installed. This behavior does not affect the ability to connect to the host or to view or edit the host's properties.

For example, you may see the following entries for *Host 1* that is in a multi-NIC environment.

Table 25-1 Multiple host name entries for a host in a multi-NIC environment

Host	Mapped host names
osname-host1.domain.com	OS name of <i>Host 1</i>
clientname-host1.domain.com	Client name of <i>Host 1</i>

To consolidate these host names, to the host `clientname-host1.domain.com` add a mapping for `osname-host1.domain.com`. After you add the mapping, you see only one entry for the host in host properties.

Table 25-2 Host mapping for a multi-NIC environment

Host	Mapped host names
client01-name.domain.com	clientname-host1.domain.com, osname-host1.domain.com

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

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

Table 25-3 Mapping host names for a cluster in a multi-NIC environment

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

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

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

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

Host	Mapped host names or IP addresses
client01-bk.lab04.com	clustername-bk.lab04.com
client02-bk.lab04.com	clustername-bk.lab04.com

Examples of auto-discovered mappings for SQL Server environments

In [Table 25-4](#), FCI is a SQL Server failover cluster instance. WSFC is Windows Server Failover Cluster.

Table 25-4 Example mapped host names for SQL Server environments

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

Remove mappings for a host that has multiple host names

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

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

See [“Reset a host’s attributes”](#) on page 81.

To remove a host name that NetBackup discovers

- 1 On the left, select **Security > Host mappings**.
- 2 Locate the host that you want to update.

- 3** Click **Actions > Manage mappings**.
- 4** Locate the mapping you want to remove and click **Delete > Save**.

Configuring multi-person authorization

This chapter includes the following topics:

- [About multi-person authorization](#)
- [Workflow to configure multi-person authorization for NetBackup operations](#)
- [RBAC roles and permissions for multi-person authorization](#)
- [Multi-person authorization process with respect to roles](#)
- [NetBackup operations that need multi-person authorization](#)
- [Configure multi-person authorization](#)
- [View multi-person authorization tickets](#)
- [Manage multi-person authorization tickets](#)
- [Add exempted users](#)
- [Schedule expiration and purging of multi-person authorization tickets](#)
- [Disable multi-person authorization](#)

About multi-person authorization

NetBackup Security Administrator can configure multi-person authorization. It proactively protects NetBackup primary servers from an undesirable or a malicious act by ensuring that a second authorized user approves that action before it is allowed to take place. If you configure multi-person authorization for a certain operation, you can perform the associated operation only using the NetBackup web

UI or REST APIs. You cannot perform the operation using the NetBackup Administration Console.

To bypass multi-person authorization, you can add the associated users as exempted users who do not require approval for performing the required operations.

To configure multi-person authorization in NetBackup, you need to have two users: one is the requester and other is the approver.

A requester cannot be an approver of his or her own tickets.

Terminologies

- Ticket - Ticket is a multi-person authorization request to perform a critical operation.
- Requester - Requester is an end user who wants to perform a critical operation that requires multi-person authorization.
- Approver - Approver is an individual who reviews and allows an operation that requires multi-person authorization by approving a ticket.
- Exempted user - An exempted user is not required to go through the multi-person authorization process, and must be used only when an automation user wants to perform critical operations.
For enhanced security, it is suggested that there should not be any exempted users.

Workflow to configure multi-person authorization for NetBackup operations

Here are the high-level steps to configure multi-person authorization for NetBackup operations:

Table 26-1

Step	Description
Step 1	Identify critical NetBackup operations that require multi-person authorization. See “NetBackup operations that need multi-person authorization” on page 243.
Step 2	Identify the approvers who can approve requests or multi-person authorization tickets.

Table 26-1 (continued)

Step	Description
Step 3	Assign the Default multi-person authorization approver RBAC role to the approvers. See "RBAC roles and permissions for multi-person authorization" on page 240.
Step 4	Configure multi-person authorization using the NetBackup web UI. See "Configure multi-person authorization" on page 244.
Step 5	When a user or a requester tries to perform an operation that requires multi-person authorization (for example, expiring an image), a ticket is generated. Initially, the ticket is in the pending state.
Step 6	The ticket is visible to all multi-person authorization approvers in the NetBackup web UI where they can review the ticket information and approve or reject the ticket.
Step 7	When the approver approves or rejects the ticket, the requester is notified.

Multi-person authorization configuration begins when the Administrator or the Security Administrator enables critical operations that require multi-person authorization and specifies other settings like expiration period and purge period. A multi-person authorization configuration ticket is generated. After the approver approves the ticket, multi-person authorization configuration comes into effect.

Initial multi-person authorization configuration

Configuring multi-person authorization for the first time involves adding users to the Default Multi-Person Authorization Approver role. To start using the multi-person authorization for additional data security, the Security Administrator must enable the multi-person authorization for critical pre-defined operations that require an additional approval from a user with the Default Multi-Person Authorization Approver role.

Initially, the Security Administrator should configure multi-person authorization that results into a multi-person authorization ticket. After the approver approves the ticket, multi-person authorization becomes mandatory for the specified NetBackup operation (such as image expiry). The Administrator or Security Administrator can add users to the Default Multi-Person Authorization Approver role at any point in time.

RBAC roles and permissions for multi-person authorization

Multi-person authorization configuration requires the users to be assigned to the following RBAC roles:

- Administrator
- Default Security Administrator
- Default Multi-Person Authorization Approver

Users with these RBAC roles should have the following permissions.

Table 26-2

RBAC role	Permissions
Administrator	View, update multi-person authorization configuration, and delegate the configuration permissions to other users. View, update tickets, and delegate ticket permissions to other users.
Default Security Administrator	View, update multi-person authorization configuration, and delegate the configuration permissions to other users.
Default Multi-person Authorization Approver	View and update tickets.
Default Operator	View all NetBackup entities.

Multi-person authorization process with respect to roles

Users can be requesters and approvers at the same time, however they cannot approve their own tickets.

The multi-person authorization process flow with respect to roles is as follows:

Table 26-3

Component	Description
Multi-person authorization ticket	<p>When a requester performs a critical NetBackup operation that is protected by multi-person authorization, a ticket is generated that requires an approval from the approver before a specific action can be executed.</p> <p>This ticket is used within NetBackup to ensure that critical actions undergo thorough review process by multiple people before they are executed.</p> <p>The following sample flow is for the image expiry operation that requires multi-person authorization:</p> <ol style="list-style-type: none"> 1 A requester expires an image using the NetBackup web UI. 2 A ticket is created. 3 The ticket is pending for approval. 4 Approvers review the ticket. 5 Approvers either approve or reject the ticket. 6 After the approval, the ticket is scheduled by NetBackup and finally marked Done after the execution. 7 The ticket activity log, request, and response details can be viewed by the approver or the requester using the web UI, on the Ticket details page. 8 A ticket is expired after it ages beyond the expiration period. Such tickets cannot be approved unless they are renewed by the Requester. 9 Tickets in the Done, Rejected, Expired, and Canceled states are purged when no action is performed on them for the specified purge period in days.

Table 26-3 (continued)

Component	Description
Requester role	<ol style="list-style-type: none"> 1 A requester is a user who initiates an operation that requires multi-person authorization. 2 A ticket is created for the operation if the user is not in the exempted users' list. 3 The ticket requires an approval from an approver before the operation is performed. 4 A requester is not allowed to self approve even if the requester is also an approver, an Administrator, or a Security Administrator. 5 Once the ticket is created it is in the Pending state. 6 The requester can cancel a ticket only if it is in the Pending state. 7 If the ticket ages beyond the expiry period, the ticket is moved to the Expired state. 8 Only the requester can renew such tickets. A new expiry period is calculated for the renewed ticket based on the configuration settings multi-person authorization.
Approver role	<ol style="list-style-type: none"> 1 An approver is an authorized individual who reviews and provides approval for tickets. 2 The approver evaluates the details of the ticket and either approves or rejects the ticket based on the assessment. 3 After the approval, the ticket is scheduled for execution. 4 To be an approver, the user should have RBAC permissions like Update Ticket, View Ticket or the user should have the Default Multi-Person Authorization Approver role. 5 When a ticket is in the Pending State, it can be approved or rejected.

Table 26-3 (continued)

Component	Description
Exempted users	<ol style="list-style-type: none"> 1 An exempted user is an individual who is not subjected to the multi-person authorization workflow. 2 This eliminates the necessity for any approvals, however it must be used with caution. 3 If the exempted user account is hacked, the multi-person authorization process can be of no use as it is bypassed for this user. 4 For instance, if Alice is designated as an exempted user and she attempts to expire an image (an operation subjected to multi-person authorization), the image automatically expires without ticket generation and additional approvals.

NetBackup operations that need multi-person authorization

The following operations require multi-person authorization and therefore a ticket is generated for these operations:

- Configuring multi-person authorization
- Enabling and disabling operations that require multi-person authorization
- Adding exempted users
- Changing any multi-person authorization settings generates a ticket
- Expiring images
- Deleting images

Even if multi-person authorization is configured for image expiry, the following operations do not require multi-person authorization:

- Changing values for image retention level
- Modifying retention levels in policy and SLP
- Canceling incomplete SLPs using the `nbstlutil` command:
Refer to the *NetBackup Commands Reference Guide*.

Configure multi-person authorization

Configuring multi-person authorization for NetBackup operations is supported only from the NetBackup web UI. Administrator or Security Administrator can configure multi-person authorization for critical NetBackup operations.

To configure multi-person authorization for NetBackup operations

- 1 On the left pane, click **Security > Multi-person authorization**.
- 2 Click the **Configure multi-person authorization** option.
- 3 Select critical operations for which you want to configure multi-person authorization.
- 4 Select users to be exempted from multi-person authorization.
- 5 Click **Save**.
- 6 Click **Configure**.

A multi-person authorization ticket is created for the associated operation. After the approver approves the ticket, the operation is subjected the MPA.

View multi-person authorization tickets

Users can view their own multi-person authorization tickets.

- ◆ On the left pane, click **Security > Multi-person authorization**. The list of multi-person authorization tickets is displayed.

Click the ticket ID to see more details.

Manage multi-person authorization tickets

Users with the approver role can approve or reject the multi-person authorization tickets.

To manage multi-person authorization tickets

- 1 On the left pane, click **Security > Multi-person authorization**. The list of multi-person authorization tickets is displayed.
- 2 Click the ticket ID to view the request details.
- 3 Click **Approve** or **Reject**. Based on the selected action, the respective dialog box appears.
- 4 Add comments and click **Approve** or **Reject**.

Add exempted users

You can exempt certain users from the multi-person authorization process.

An exempted user is generally an automation user or a script that does not require multi-person authorization. The multi-person authorization configuration has default settings with no exempted users and is the recommended security setting. If there is need in your organization to add exemption for some user account to proceed any critical data operation without a secondary approval, add such users to the exempted users' list.

Note: User groups cannot be added to the exempted list.

To add exempted users

- 1 On the left pane, click **Security > Multi-person authorization**.
- 2 On the top right, click **Configure multi-person authorization**.
- 3 In the **Exempted users** section, click **Add**.
- 4 Specify the name of the user whom you want to exempt from the multi-person authorization process.
- 5 Click **Add to list** and then **Save**.
- 6 Click **Save**.

Schedule expiration and purging of multi-person authorization tickets

Expiration period is configurable option defines the duration for which a multi-person authorization ticket can be in the Pending state. A ticket expires if it is in the Pending state for more than the configured expiry period.

For multi-person authorization configuration, expiration period can vary from minimum 24 hours to 168 hours. By default, tickets expire after 72 hours.

Purge period is a configurable option defines the duration for which a ticket resides in the tickets database. Purging a ticket ensures that the database does not grow exponentially. Purge period can vary from minimum 3 days to 30 days.

By default, tickets purge after 72 hours. All the Done, Expired, Rejected, and Canceled tickets are purged after the given purge period.

To schedule expiration and purging of tickets

- 1 On the left pane, click **Security > Multi-person authorization**.
- 2 On the top right, click **Configure multi-person authorization**.
- 3 In the **Schedules** section, click **Edit**.
- 4 Specify the expiration period (in hours) for the **Expire ticket after** option.
Specify the purge period (in days) for the **Purge ticket after** option.
- 5 Click **Save**.
- 6 Click **Save**.

Disable multi-person authorization

In certain cases, you may need to temporarily disable multi-person authorization for the associated operations.

To disable multi-person authorization for all the associated operations, run the following command after `bpnbat -login -loginType WEB` using the root or Administrator account.

```
nbseccmd -disableMPA
```

You can disable multi-person authorization for a specific operation using the NetBackup web UI

To disable multi-person authorization for a specific operation

- 1 On the left pane, click **Security > Multi-person authorization**.
- 2 On the top right, click **Configure multi-person authorization**.
- 3 In the **Operations for multi-person authorization** section, click **Edit**.
- 4 Clear the check box for the operation for which you want to disable multi-person authorization.
- 5 Click **Save**.
- 6 Click **Save**.

This generates a ticket that is shown on the ticket details page with the operation name as MPA Configuration.

Multi-person authorization will be disabled for the associated operation only after the approval of the respective ticket.

Managing user sessions

This chapter includes the following topics:

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

Terminate a NetBackup user session

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

See [“Configure when idle sessions should time out”](#) on page 249.

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

To sign out a user session

- 1 On the left, click **Security > User sessions**.
- 2 At the top right, click **User account settings**.
- 3 Click the **Active sessions** tab.

- 4 Select the user session that you want to sign out.
- 5 Click **Terminate session**.

To sign out all user sessions

- 1 On the left, click **Security > User sessions**.
- 2 At the top right, click **User account settings**.
- 3 Click the **Active sessions** tab.
- 4 Click **Terminate all sessions**.

Unlock a NetBackup user

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

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

See [“Configure the maximum of failed sign-in attempts”](#) on page 249.

To unlock out a locked user account

- 1 On the left, click **Security > User sessions**.
- 2 At the top right, click **User account settings**.
- 3 Click the **Locked users** tab.
- 4 Select the user account that you want to unlock.
- 5 Click **Unlock**.

To unlock all locked user accounts

- 1 On the left, click **Security > User sessions**.
- 2 At the top right, click **User account settings**.
- 3 Click the **Locked users** tab.
- 4 Click **Unlock all users**.

Configure when idle sessions should time out

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

To configure when idle sessions should time out

- 1 On the left, click **Security > User sessions**.
- 2 At the top right, click **User account settings**.
- 3 Turn on **Session idle timeout** and click **Edit**.
- 4 Select the number of minutes and click **Save**.

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

Configure the maximum of concurrent user sessions

This setting limits the number of concurrent API sessions that a user can have active. This setting does not apply to API key sessions or to other applications like the NetBackup Backup, Archive, and Restore interface.

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

To configure the maximum of concurrent user sessions

- 1 On the left, click **Security > User sessions**.
- 2 At the top right, click **User account settings**.
- 3 Turn on **Maximum concurrent sessions** and click **Edit**.
- 4 Select the **Number of concurrent sessions per user** and click **Save**.

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

Configure the maximum of failed sign-in attempts

You can automatically lock a user account if the user exceeds a maximum number of failed sign-in attempts. The user account remains locked until the account lockout period passes.

If there is an immediate need to access NetBackup, the administrator can unlock the account.

See [“Unlock a NetBackup user”](#) on page 248.

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

To configure the maximum of failed sign-in attempts

- 1 On the left, click **Security > User sessions**.
- 2 At the top right, click **User account settings**.
- 3 Turn on **User account lockout** and click **Edit**.
- 4 Select the number of failed sign-in attempts that you want to allow before an account is locked.
- 5 To unlock a locked account after a period of time, select the number of minutes for **Unlock locked accounts after**.
- 6 Click **Save**.

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

Display a banner to users when they sign in

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

To display a banner to users when they sign in

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

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

To remove the sign-in banner

- 1** On the left, click **Security > User sessions**.
- 2** At the top right, click **User account settings**.
- 3** Turn off **Sign-in banner configuration**
- 4** Click **Save**.

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

Configuring multi-factor authentication

This chapter includes the following topics:

- [About multi-factor authentication](#)
- [Configure multi-factor authentication for your user account](#)
- [Disable multi-factor authentication for your user account](#)
- [Enforce multi-factor authentication for all users](#)
- [Configure multi-factor authentication for your user account when it is enforced in the domain](#)
- [Reset multi-factor authentication for a user](#)

About multi-factor authentication

Multi-factor authentication is a multiple-step account login process that requires you to enter a 6-digit one-time password along with your password.

It is strongly recommended that you configure multi-factor authentication to protect the security of your account.

See [“Configure multi-factor authentication for your user account”](#) on page 253.

If multi-factor authentication is enforced in the NetBackup domain, all users must configure multi-factor authentication for their user accounts for successful sign-in.

See [“Configure multi-factor authentication for your user account when it is enforced in the domain”](#) on page 254.

Configure multi-factor authentication for your user account

For enhanced security, you can configure multi-factor authentication for your user account. You must first install and configure authenticator application on your smart device that provides you with the one-time password.

Configuring multi-factor authentication in NetBackup does not require internet connectivity on your smart device.

If the NetBackup administrator has enforced multi-factor authentication in the NetBackup domain, you must configure it for your user account for successful sign-in.

See [“Disable multi-factor authentication for your user account”](#) on page 253.

To configure multi-factor authentication for your user account

- 1 On the top right, click the profile icon and click **Configure multi-factor authentication**.
- 2 On the **Configure multi-factor authentication** screen, click **Configure**.
- 3 On the next screen, follow the given steps.
Install and configure authenticator application on your smart device. It generates one-time password and sends it on your smart device.
[Supported authenticator applications](#)
- 4 Scan the QR code with the authenticator application or enter the key manually.
- 5 Enter the one-time password that you see in the authenticator application on your smart device.
- 6 Click **Configure**.

At the time of next sign-in, you need to enter the one-time password along with the username and password.

Disable multi-factor authentication for your user account

If multi-factor authentication is not enforced, you can disable it for your user account. However, it is strongly recommended that you configure multi-factor authentication to protect the security of your account.

See [“Configure multi-factor authentication for your user account”](#) on page 253.

To disable multi-factor authentication for your user account

- 1 On the top right, click the profile icon and select **Configure multi-factor authentication**.
- 2 If you have already configured multi-factor authentication for your user account, you can see the **Disable** option.
- 3 Click **Disable**.
- 4 Enter the one-time password and click **Confirm**.

Enforce multi-factor authentication for all users

Only the NetBackup administrator can enforce multi-factor authentication for all NetBackup users.

To enforce multi-factor authentication for all users

- 1 On the top right, click **Settings > Global security**.
- 2 On the **Security controls** tab, turn on **Enforce multi-factor authentication**.
 Click **Confirm** to enforce multi-factor authentication for all NetBackup users.
 Notify all users that they must configure multi-factor authentication for their user accounts to be able to successfully sign in.
 See [“Configure multi-factor authentication for your user account”](#) on page 253.

Configure multi-factor authentication for your user account when it is enforced in the domain

After multi-factor authentication is enforced in the domain, you must configure it for your user account if you have not already configured it. If you do not configure multi-factor authentication for your account after the enforcement, you cannot sign-in.

To configure multi-factor authentication after the enforcement

- 1 Open a web browser and go to the following URL.
 https://primaryserver/webui/login
 The *primaryserver* is the host name or IP address of the NetBackup primary server that you want to sign in to.
- 2 Go to the NetBackup sign-in screen.
- 3 Enter the **Username** and **Password**.

See [“Sign in to the NetBackup web UI”](#) on page 27.

4 Click **Sign in**. The **Configure multi-factor authentication** screen is displayed.

5 On the next screen, follow the given steps.

Install and configure an authenticator application on your smart device. It generates a one-time password and sends it to your smart device.

[Supported authenticator applications](#)

6 Scan the QR code with the authenticator application or enter the key manually.

7 Enter the one-time password that you see in the authenticator application on your smart device.

8 Click **Configure**.

Successful configuration takes you back to the sign-in screen.

Enter the username, password, and one-time password for successful sign-in.

Reset multi-factor authentication for a user

Only the NetBackup administrator can reset multi-factor authentication for other NetBackup users.

To reset multi-factor authentication for a NetBackup user

1 On the top right, click **Settings > Global security**.

2 Click the **Security controls** tab.

3 **Reset multi-factor authentication for a user** section, click **Reset**.

4 Select the user for whom you want to reset multi-factor authentication.

5 Click **Reset**.

6 When prompted, enter the one-time password and click **Confirm**.

Managing the global security settings for the primary server

This chapter includes the following topics:

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

Certificate authority for secure communication

In the global security settings, the **Certificate authority** information indicates the type certificate authorities that the NetBackup domain supports.

NetBackup hosts in the domain can use certificates as follows:

- NetBackup certificates.

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

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

To view the certificate authorities that a NetBackup domain supports

- 1 Open the NetBackup web UI.
- 2 Open **Settings > Global security**.
- 3 Click on the **Secure communication** tab.

Disable communication with NetBackup 8.0 and earlier hosts

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

To disable communication with NetBackup 8.0 and earlier hosts

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

Disable automatic mapping of NetBackup host names

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

To disable automatic mapping of NetBackup host names

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

Configure the global data-in-transit encryption setting

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

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

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

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

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

RESTful API to be used for the global DTE configuration:

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

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

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

About NetBackup certificate deployment security levels

Security levels for certificate deployment are specific to NetBackup CA-signed certificates. If the NetBackup web server is not configured to use NetBackup certificates for secure communication, the security levels cannot be accessed.

The NetBackup certificate deployment level determines the checks that are performed before the NetBackup CA issues a certificate to a NetBackup host. It also determines how frequently the NetBackup Certificate Revocation List (CRL) is refreshed on the host.

NetBackup certificates are deployed on hosts during installation (after the host administrator confirms the primary server fingerprint) or with the `nbcertcmd` command. Choose a deployment level that corresponds to the security requirements of your NetBackup environment.

Note: During NetBackup certificate deployment on a NAT client, you must provide an authorization token irrespective of the certificate deployment security level that is set on the primary server. This is because, the primary server cannot resolve the host name to the IP address from which the request is sent.

For more information about NAT support in NetBackup, refer to the [NetBackup Administrator's Guide, Volume I](#).

Table 29-1 Description of NetBackup certificate deployment security levels

Security level	Description	CRL refresh
Very High	An authorization token is required for every new NetBackup certificate request.	The CRL that is present on the host is refreshed every hour.
High (default)	<p>No authorization token is required if the host is known to the primary server. A host is considered to be known to the primary server if the host can be found in the following entities:</p> <ol style="list-style-type: none"> 1 The host is listed for any of the following options in the NetBackup configuration file (Windows registry or the <code>bp.conf</code> file on UNIX): <ul style="list-style-type: none"> ■ APP_PROXY_SERVER ■ DISK_CLIENT ■ ENTERPRISE_VAULT_REDIRECT_ALLOWED ■ MEDIA_SERVER ■ NDMP_CLIENT ■ SERVER ■ SPS_REDIRECT_ALLOWED ■ TRUSTED_MASTER ■ VM_PROXY_SERVER ■ MSDP_SERVER <p>For more details on the NetBackup configuration options, refer to the NetBackup Administrator's Guide, Volume I.</p> 2 The host is listed as a client name in the <code>altnames</code> file (<code>ALTNAMESEDB_PATH</code>). 3 The host appears in the EMM database of the primary server. 4 At least one catalog image of the client exists. The image must not be older than 6 months. 5 The client is listed in at least one backup policy. 6 The client is a legacy client. This is a client that was added using the Client Attributes host properties. 	The CRL that is present on the host is refreshed every 4 hours.
Medium	The certificates are issued without an authorization token if the primary server can resolve the host name to the IP address from which the request was originated.	The CRL that is present on the host is refreshed every 8 hours.

Select a security level for NetBackup certificate deployment

NetBackup offers several security levels for the NetBackup certificate deployment. The security level determines what security checks the NetBackup certificate authority (CA) performs before it issues a certificate to a NetBackup host. The level also determines how frequently the Certificate Revocation List (CRL) for the NetBackup CA is refreshed on the host.

More details are available for security levels, NetBackup certificate deployment, and the NetBackup CRL:

- See [“About NetBackup certificate deployment security levels”](#) on page 259.
- See the [NetBackup Security and Encryption Guide](#).

To select a security level for NetBackup certificate deployment

- 1 At the top, click **Settings > Global security**.
- 2 Click **Secure communication**.
- 3 For **Security level for NetBackup certificate deployment**, select a security level.

If you choose to use NetBackup certificates, they are deployed on hosts during installation, after the host’s administrator confirms the primary server fingerprint. The security level determines if an authorization token is required or not for a host.

Very high	NetBackup requires an authorization token for every new NetBackup certificate request.
High (Default)	NetBackup does not require an authorization token if the host is known to the primary server, which means the host appears in a NetBackup configuration file, the EMM database, a backup policy, or the host is a legacy client.
Medium	NetBackup issues NetBackup certificates without an authorization token if the primary server can resolve the host name to the IP address from which the request was originated.

- 4 Click **Save**.

About TLS session resumption

NetBackup uses TLS (Transport Layer Security) to secure communications between NetBackup hosts and is enabled by default. Each new TCP connection between NetBackup hosts must perform a TLS handshake and verify the peer identity before NetBackup sends traffic across that connection.

TLS session resumption is an open standards optimization that allows a TLS client and server to reuse a secure session that is generated during a previous connection. Reusing a secure session allows NetBackup to use a streamlined handshake instead of a full handshake. Performing this action reduces both the host CPU and time that is required to establish the new connection.

At TLS version 1.2 (used by current NetBackup versions), this version reduces forward security for the interval between full handshakes. To limit this window while still benefitting from session reuse, NetBackup allows global configuration of the maximum interval between full TLS handshakes.

To use the options for **TLS session resumption**, navigate to **Settings > Global security > Secure communication**. You can use the **Perform full handshake every** option to set the security level as follows:

- **Default for current security level** – If you use this option, NetBackup defaults to the security setting as follows:
 - Very high - 10 minutes
 - High - 30 minutes
 - Medium - 60 minutes
- **Custom (overrides the security level settings)** - The value of this interval can be configured at a minute granularity, within the range of 1 minute to 720 minutes.

Note: If strict forward security is a concern, NetBackup also allows session resumption to be globally disabled.

Note: This feature currently only applies to NBQA. ECA to be supported in a future release.

Set a passphrase for disaster recovery

During a catalog backup, NetBackup creates a disaster recovery package and encrypts the backup with a passphrase that you set. The constraints for the

passphrase can be changed with the NetBackup APIs or the CLIs (`nbseccmd -setpassphraseconstraints`).

See the information for disaster recovery settings in the [NetBackup Security and Encryption Guide](#).

To set a passphrase for disaster recovery

- 1 At the top, click **Settings > Global security**.
- 2 Click **Disaster recovery**.
- 3 Enter and confirm a passphrase.

Note: The passphrase should meet additional constraints that you may have set. You can check the additional constraints using the `nbseccmd` command or the passphrase-constraints web API.

- 4 Click **Save**.

About trusted primary servers

A trust relationship between NetBackup domains lets you do the following:

- Select specific domains as a target for replication. This type of Auto Image Replication is known as targeted A.I.R.
Without a trust relationship, NetBackup replicates to all defined target storage servers. A trust relationship is optional for Media Server Deduplication Pool and PureDisk Deduplication Pool as a target storage. To use a Cloud Catalyst storage server, a trust relationship is required.
- Include usage reporting for multiple primary servers.

Primary servers can use a NetBackup certificate authority (CA) certificate or an external CA certificate. NetBackup determines the CAs used by the source and the target domains and selects the appropriate CA to use for communication between the servers. If the target primary server is configured for both CA types, NetBackup prompts you to select the CA that you want to use. To establish trust with a remote primary server using the NetBackup CA, the current primary and the remote primary must have NetBackup version 8.1 or later. To establish trust with a remote primary server using an external CA, the current primary and the remote primary must have NetBackup version 8.2 or later.

Table 29-2 Determining the certificate authority (CA) to use for a trust relationship between servers

Source primary server CA or CAs	Target primary server CA or CAs	Certificate authority that is selected
NetBackup CA and external CA	External CA	External CA
	NetBackup CA	NetBackup CA
	External CA and NetBackup CA	NetBackup prompts you to select the CA.
NetBackup CA	External CA	No trust is established.
	NetBackup CA	NetBackup CA
	External CA and NetBackup CA	NetBackup CA

Add a trusted primary server

Replication operations require that a trust relationship exists between the NetBackup servers in the different domains. You can create a trust relationship between the primary servers that both use the NetBackup CA or that both use an external CA.

To add a trusted primary server

- 1 Open the NetBackup web UI.
- 2 Identify the NetBackup versions that are installed and the certificate types that are used on the source and the target servers.

The NetBackup web UI does not support adding a trusted primary that uses NetBackup version 8.0 or earlier. Both servers must use the same certificate type.

- 3 For the servers that use the NetBackup certificate authority (CA), obtain an authorization token for the remote server.

See [“Managing NetBackup certificate authorization tokens”](#) on page 223.

- 4 For the servers that use the NetBackup certificate authority (CA), obtain the fingerprint for each server.

See [“Managing NetBackup security certificates”](#) on page 220.

- 5 At the top, select **Settings > Global security**.
- 6 Select **Trusted primary servers**.
- 7 Click **Add**.

- 8 Follow the prompts in the wizard.
- 9 Repeat these steps on the remote primary server.

More information

For more information on using an external CA with NetBackup, see the [NetBackup Security and Encryption Guide](#).

Remove a trusted primary server

Note: Any trusted primary servers at NetBackup version 8.0 or earlier must be removed using the NetBackup Administration Console or the NetBackup CLI.

You can remove a trusted primary server, which removes the trust relationship between primary servers. Note the following implications:

- Any replication operations fail that require the trust relationship.
- A remote primary server is not included in any usage reporting after you remove the trust relationship.

To remove a trusted primary server, you must perform the following procedure on both the source and the target server.

To remove a trusted primary server

- 1 Open the NetBackup web UI.
- 2 Ensure that all replication jobs to the target primary server are complete.
- 3 Delete all storage lifecycle policies (SLPs) that use the trusted primary as a destination. Before deleting an SLP, ensure that there are no backup policies or protection plans that use the SLP for storage.
- 4 At the top, select **Settings > Global security**.
- 5 Select **Trusted primary servers**.
- 6 Select **Actions > Remove**.
- 7 Click **Remove trust**.

Using access keys, API keys, and access codes

This chapter includes the following topics:

- [Access keys](#)
- [API keys](#)
- [Access codes](#)

Access keys

NetBackup access keys provide access the NetBackup interfaces through API keys and access codes.

See [“API keys”](#) on page 266.

See [“Access codes”](#) on page 271.

API keys

A NetBackup API key is a pre-authenticated token that identifies a NetBackup user to NetBackup RESTful APIs. The user can use the API key in an API request header when a NetBackup API requires authentication. API keys can be created for authenticated NetBackup users (groups are not supported). A specific API key is only created one time and cannot be recreated. Each API key has a unique key value and API key tag. NetBackup audits operations that are performed with that key with the full identity of the user.

The 'View' RBAC permission is required to create an API key.

The following actions are available for administrators and API key users.

- Administrators with the applicable role or RBAC permissions can manage API keys for all users. These roles are the Administrator, the Default Security Administrator, or a role with RBAC permissions for API keys.
- An authenticated NetBackup user can add and manage their own API key in the NetBackup web UI. If a user does not have access to the web UI, they can use the NetBackup APIs to add or manage a key.

More information

See [“User identity in the audit report”](#) on page 212.

See the [NetBackup Security and Encryption Guide](#) for information on using API keys with the `bpnbat` command.

Add an API key or view API key details (Administrators)

The API key administrator can manage the keys that are associated with all NetBackup users.

Add an API key

Note: Only one API key can be associated with a specific user at a time. If a user requires a new API key, the user or administrator must delete the key for that user. An expired API key can be reissued. The 'View' RBAC permission is required to create an API key.

To add an API key

- 1 On the left, select **Security > Access keys > API keys**.
- 2 On left, click **Add**.
- 3 Enter a **Username** for which you want to create the API key.
- 4 (Conditional) If the API key is for a SAML user, select **SAML authentication**.
A new API key for a SAML user remains inactive until the user signs into the web UI.
- 5 Indicate how long you want the API key to be valid, from today's date.
NetBackup calculates the expiration date and displays it.
- 6 Click **Add**.
- 7 To copy the API key, click **Copy and close**.

Store this key in a safe place. After you click **Copy and close**, the key cannot be retrieved again. If this API key replaces a previous key for your account, you must update any scripts, etc. to reflect the new API key.

View API key details

An API key administrator can view the API key details that are associated with all NetBackup users.

To view API key details

- 1 On the left, select **Security > Access keys > API keys**.
- 2 Locate the API key that you want to view.
- 3 Click **Actions > Edit** to edit the date or description for the key.

Edit, reissue, or delete an API key (Administrators)

As an API key administrator, you can edit API key details and reissue or delete API keys.

Edit the expiration date or description for an API key

Note: For SAML users, avoid selecting an expiration date for the API key that occurs after the SAML session expires. If the date occurs after the session expires, this action can introduce a security risk with that API key.

You can edit the description of an API key or change the expiration date of an active API key.

To edit the expiration date or description for an API key

- 1 On the left, select **Security > Access keys > API keys**.
- 2 Locate the API key that you want to edit.
- 3 Click **Actions > Edit**.
- 4 Note the current expiration date for the key and extend the date as wanted.
- 5 Make any wanted changes to the description.
- 6 Click **Save**.

Reissue an API key after it expires

Note: For SAML users, avoid selecting an expiration date for the API key that occurs after the SAML session expires. If the date occurs after the session expires, this action can introduce a security risk with that API key.

When an API key expires you can reissue the API key. This action creates a new API key for the user.

To reissue an API key

- 1 On the left, select **Security > Access keys > API keys**.
- 2 Locate the API key that you want to edit.
- 3 Click the **Actions** menu. Then select **Reissue > Reissue**.

Delete an API key

You can delete an API key to remove access for the user or when the key is no longer used. The key is permanently deleted, meaning that the associated user can no longer use that key for authentication.

To delete an API key

- 1 On the left, select **Security > Access keys > API keys**.
- 2 Locate the API key that you want to view.
- 3 Click the **Actions** menu. Then click **Delete > Delete**.

Add an API key or view your API key details

You can create an API key to authenticate your NetBackup user account when using NetBackup RESTful APIs.

Add an API key

As a NetBackup web UI user you can use the web UI to add or view the details for your own API key.

To add an API key

- 1 If your API key has expired you can reissue the key.
See [the section called “Reissue your API key after it expires”](#) on page 270.
- 2 On the top right, click the profile icon and click **Add API key**.
- 3 (Non-SAML users) Indicate how long you want the API key to be valid, from today's date.
NetBackup calculates the expiration date and displays it.
- 4 (SAML users) After NetBackup validates the token from the SAML session, then the expiration date for the API key can be determined.

- 5 Click **Add**.
- 6 To copy the API key, click **Copy and close**.

Store this key in a safe place. After you click **Copy and close**, the key cannot be retrieved again. If this API key replaces a previous key for your account, you must update any scripts, etc. to reflect the new API key.

View your API key details

To view your API key details

- ◆ On the top right, click the profile icon and select **View my API key details**.

Edit, reissue, or delete your API key

You can manage your own API key from the NetBackup web UI.

Edit the expiration date or description for your API key (non-SAML users)

Non-SAML users can change the expiration date for an active API key. After an API key expires, you can reissue the key.

To edit your API key details

- 1 On the top right, click the profile icon and click **View my API key details**.
Note: If your API key is expired, you can click **Reissue** to reissue the key.
See [the section called “Reissue your API key after it expires”](#) on page 270.
- 2 Click **Edit**.
- 3 Note the current expiration date for the key and extend the date as wanted.
- 4 Make any wanted changes to the description.
- 5 Click **Save**.

Reissue your API key after it expires

When your API key expires you can reissue the API key. This action creates a new API key for you.

To reissue your API key

- 1 On the top right, click the profile icon and click **View my API key details**.
- 2 On the top right, click **Reissue**.

- 3 (Non-SAML users) Note the current expiration date for the key and extend the date as wanted.
- 4 Make any wanted changes to the description.
- 5 Click **Reissue**.

Delete your API key

You can delete an API key if you no longer have access to the key or no longer use it. When you delete an API key, that key is permanently deleted. You can no longer use that key for authentication or with the NetBackup APIs.

To delete your API key

- 1 On the top right, click the profile icon and click **View my API key details**.
- 2 On the top right, click **Delete**. Then click **Delete**.

Use an API key with NetBackup REST APIs

After a key is created, the user can pass the API key in the API request headers. For example:

```
curl -X GET https://primaryservername.domain.com/netbackup/admin/jobs/5 \
-H 'Accept: application/vnd.netbackup+json;version=3.0' \
-H 'Authorization: <API key value>'
```

Access codes

To run certain NetBackup administrator commands, for example `bperor`, you need to authenticate through the web UI. You need to generate an access code through the command-line interface, get the access request approved from the administrator, and then access the command.

With the web UI authentication for CLI access, NetBackup administrators can delegate the associated privileges to other users. By default, only a root administrator or an administrator can perform NetBackup operations through the command-line interface. The web UI authentication support allows non-root users to administer NetBackup who have CLI access that the Security Administrator has granted. You can also administer NetBackup with a non-RBAC user role (such as Operating System Administrator) even though you are not registered as a NetBackup user. Each time you need to generate a new access code to access CLIs.

Request CLI access through web UI authentication

To run NetBackup commands using the NetBackup CLI, the following requirements exist for the user:

- The user must have the RBAC role Default NetBackup Command Line (CLI) Administrator or a role with similar permissions.
- The user must submit a request for temporary access to the CLI. By default, a CLI access session is valid for 24 hours.

The command that the user runs for the request depends on whether or not they have access to the NetBackup web UI.

See [the section called “Request CLI access when you have access to the NetBackup web UI”](#) on page 272.

See [the section called “Request CLI access from the security administrator”](#) on page 272.

Request CLI access when you have access to the NetBackup web UI

If you have access to the NetBackup web UI, you can use the web UI to approve a CLI access request using the access code from the `bnpbat` command.

To request CLI access

- 1 Run the following command:

```
bnpbat -login -logintype webui
```

An access code is generated.

- 2 Open the NetBackup web UI.
- 3 On the top right, click the profile icon.
- 4 Click **Approve access request**.
- 5 Enter the CLI access code that was created when you ran the `bnpbat` command. Then click **Review**.
- 6 Review the access request details.
- 7 Click **Approve**.
- 8 After you approve the request, you can use the command-line interface to run the wanted commands.

Request CLI access from the security administrator

If you do not have access to the NetBackup web UI, you must submit a request for a CLI access to the security administrator. A user with the Default Security Administrator role or a role with similar permissions must approve the request.

To request CLI access from the security administrator

- 1 Run the following command:

```
bpnbat -login -logintype webui -requestApproval
```

An access code is generated.
- 2 Contact the security administrator and give them the access code to approve the CLI access request.

See [“Approve the CLI access request of another user”](#) on page 273.
- 3 After the request is approved, you can use the command-line interface to run the wanted commands.

Approve the CLI access request of another user

If you have the Default Security Administrator role or a role with similar permissions, you can approve the request of another user who needs CLI access. Note that to run commands, that user must also have the RBAC role Default NetBackup Command Line (CLI) Administrator or a role with similar permissions.

To approve the CLI access request of another user

- 1 The user that requires CLI access must first run the following command to request approval:

```
bpnbat -login -logintype webui -requestApproval
```
- 2 Sign in to the NetBackup web UI.
- 3 On the left, select **Security > Access keys**. Then click the **Access codes** tab.
- 4 Enter the CLI access code that you have received from the user who requires CLI access and click **Review**.
- 5 Review the access request details.
- 6 (Optional) Provide any comments.
- 7 Click **Approve**.

Edit the settings for command-line access

You can configure the default time that is set for a CLI session when a user requests CLI access.

To edit the settings for command-line access

- 1 On the left, select **Security > Access keys**.
- 2 On the right, select **Access settings**.

- 3** Click **Edit**.
- 4** Enter the time in minutes or hours that you want the CLI access session to be valid. 1 minute is the minimum value and 24 hours is the maximum value.

Configuring authentication options

This chapter includes the following topics:

- [Sign-in options for the NetBackup web UI](#)
- [Configure user authentication with smart cards or digital certificates](#)
- [About single sign-on \(SSO\) configuration](#)
- [Configure NetBackup for single sign-on \(SSO\)](#)
- [Troubleshooting SSO](#)

Sign-in options for the NetBackup web UI

NetBackup supports authentication of local domain users and Active Directory (AD) or LDAP domain users. AD and LDAP domains, smart card, and single sign-on (SSO with SAML) requires separate configuration for each primary server domain where you want to use the authentication method.

NetBackup supports the following types of user authentication:

- Username and password
- Digital certificate or smart card, including CAC and PIV
This authentication method only supports one AD or LDAP domain for each primary server domain and is not available for local domain users.
See [“Configure user authentication with smart cards or digital certificates”](#) on page 276.
- Single sign-on, with SAML
Note the following requirements and limitations.

- To use SSO, you must have a SAML 2.0 compliant identity provider configured in your environment.
- Only one AD or LDAP domain is supported for each primary server domain. This feature is not available for local domain users.
- Configuration of the IDP requires the NetBackup APIs or the NetBackup command `nbidpcmd`.
- API keys are used to authenticate a user or a group and cannot be used with SAML-authenticated users or groups.
- Global logout is not supported.

See [“Configure NetBackup for single sign-on \(SSO\)”](#) on page 282.

Configure user authentication with smart cards or digital certificates

You can map a smart card or certificate with an AD or an LDAP domain for user validation. Alternatively, you can configure a smart card or certificate without an AD or an LDAP domain.

See [“Configure smart card authentication with a domain”](#) on page 276.

See [“Configure smart card authentication without a domain”](#) on page 277.

Configure smart card authentication with a domain

You can configure NetBackup to validate users with smart cards or certificates with an AD or an LDAP domain.

Note the following prerequisites:

- Before you add the authentication method you must add the domain that is associated with your NetBackup users. See the [NetBackup Security & Encryption Guide](#).
- Ensure that you complete the role-based access control (RBAC) configuration for the NetBackup users before you configure smart card or certificate authentication.

See [“Configuring RBAC”](#) on page 297.

To configure smart card authentication with a domain

- 1 At the top right, select **Settings > Smart card authentication**.
- 2 Turn on **Smart card authentication**.
- 3 Select the required AD or LDAP domain from the **Select the domain** option.

- 4** Select a **Certificate mapping attribute**: Common name (CN) or Universal principal name (UPN).
- 5** Optionally, enter the **OCSP URI**.
If you do not provide the OCSP URI, the URI in the user certificate is used.
- 6** Click **Save**.
- 7** To the right of **CA certificates**, click **Add**.
- 8** Browse for or drag and drop the **CA certificates** and click **Add**.

Smart card authentication requires a list of trusted root or intermediate CA certificates. Add the CA certificates that are associated with the user digital certificates or the user smart cards.

Certificate file types must be .crt, .cer, .der, .pem, or PKCS #7 format and less than 64KB in size.
- 9** On the **Smart card authentication** page, verify the configuration information.
- 10** Before users can use a digital certificate that is not installed on a smart card, the certificate must be uploaded to the browser's certificate manager.

See the browser documentation for instructions or contact your certificate administrator for more information.
- 11** When users sign in, they now see an option to **Sign in with certificate or smart card**.

If you do not want users to have this sign-in option yet, turn off **Smart card authentication**. (For example, if all users do not yet have their certificates configured on their hosts.). The settings that you configured are retained even if you turn off smart card authentication.

For such users, the domain name and domain type are smart card.

Configure smart card authentication without a domain

You can configure NetBackup to validate users with smart cards or certificates without an associated AD or LDAP domain. Only users are supported for this configuration. User groups are not supported.

To configure smart card authentication without a domain

- 1** At the top right, select **Settings > Smart card authentication**.
- 2** Turn on **Smart card authentication**.
- 3** (Conditional step) If AD or LDAP domain is configured in your environment, select **Continue without the domain** option.

- 4 Select a **Certificate mapping attribute**: Common name (CN) or Universal principal name (UPN).
- 5 Optionally, enter the **OCSP URI**.
If you do not provide the OCSP URI, the URI in the user certificate is used.
- 6 Click **Save**.
- 7 To the right of **CA certificates**, click **Add**.
- 8 Browse for or drag and drop the **CA certificates** and click **Add**.
- 9 Smart card authentication requires a list of trusted root or intermediate CA certificates. Add the CA certificates that are associated with the user digital certificates or the user smart cards.

Certificate file types must be .crt, .cer, .der, .pem, or PKCS #7 format and less than 64KB in size.
- 10 On the **Smart card authentication** page, verify the configuration information.
Before users can use a digital certificate that is not installed on a smart card, the certificate must be uploaded to the browser's certificate manager.
- 11 When users sign in, they now see an option to **Sign in with certificate or smart card**.

If you do not want users to have this sign-in option yet, turn off **Smart card authentication**. (For example, if all users do not yet have their certificates configured on their hosts.). The settings that you configured are retained even if you turn off smart card authentication.

Edit the configuration for smart card authentication

If the configuration changes for smart card authentication, you can edit the configuration details.

To edit user authentication configuration with domain

- 1 At the top right, select **Settings > Smart card authentication**.
 - 2 You may want to edit the AD or LDAP domain selection in the following cases:
 - To select a domain that is different than the existing one
 - The existing domain is deleted and you want to select a new domain
 - You want to continue without the domain
- Click **Edit**.

- 3 Select a domain.
 Only the domains that are configured for NetBackup display in this list.
 If you do not want to validate the users with domain, you can select **Continue without the domain**.
- 4 Edit the **Certificate mapping attribute**.
- 5 Leave the **OCSP URI** field empty if you want to use the **URI** value from the user certificate. Or, provide the URI that you want to use.

Add or delete a CA certificate that is used for smart card authentication

Add a CA certificate

Smart card authentication requires a list of trusted root or intermediate CA certificates. Add the CA certificates that are associated with the user digital certificates or the user smart cards.

To add a CA certificate

- 1 At the top right, select **Settings > Smart card authentication**.
- 2 Click **Add**.
- 3 Browse for or drag and drop the **CA certificates**. Then click **Add**.

Smart card authentication requires a list of trusted root or intermediate CA certificates. Add the CA certificates that are associated with the user digital certificates or the user smart cards.

Certificate file types must be in DER, PEM, or PKCS #7 format and no more than 1 MB in size.

Delete a CA certificate

You can delete a CA certificate if it is no longer used for smart card authentication. Note that if a user attempts to use the associated digital certificate or smart card certificate, they are not able to sign in to NetBackup.

To delete a CA certificate

- 1 At the top right, select **Settings > Smart card authentication**.
- 2 Select the CA certificates that you want to delete.
- 3 Click **Delete > Delete**.

Disable or temporarily disable smart card authentication

You can disable smart card authentication if you no longer want to use that authentication method for the primary server. Or, if you need to complete other configuration before users can use smart cards.

To disable smart card authentication

- 1 At the top right, select **Settings > Smart card authentication**.
- 2 Turn off **Smart card authentication**.

The settings that you configured are retained even if you turn off smart card authentication.

About single sign-on (SSO) configuration

You can configure single sign-on (SSO) with any identity provider (IDP) that uses the SAML 2.0 protocol for exchanging authentication and authorization information. Note that you can configure an IDP with more than one Veritas product. For example, the same IDP can be configured with NetBackup and with APTARE.

Note the following requirements and limitations:

- To use SSO, you must have a SAML 2.0 compliant identity provider configured in your environment.
- Only identity providers that use AD or LDAP directory services are supported.
- Configuration of the IDP requires the NetBackup APIs or the NetBackup command `nbidpcmd`.
- SAML users cannot use the APIs. API keys are used to authenticate a user and therefore cannot be used with a SAML-authenticated user.
- Global logout is not supported.

Figure 31-1 Example NAT configuration: Identity provider in a private network

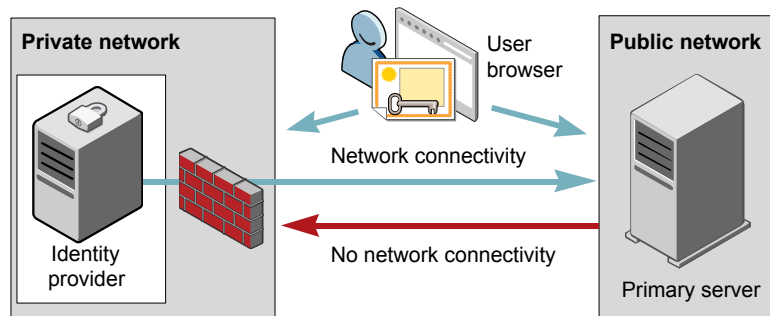


Figure 31-2 Example NAT configuration: Primary server in a private network

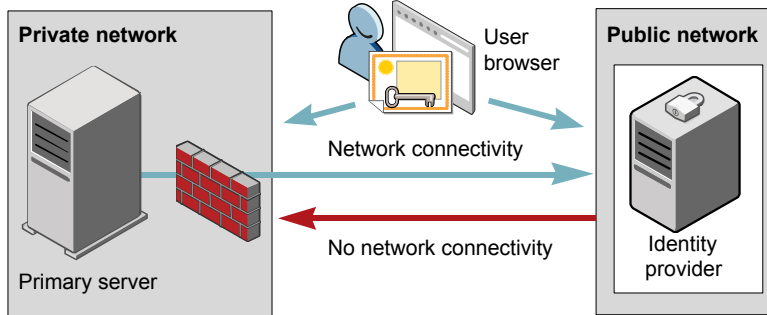


Figure 31-3 Example configuration: Primary server and identity provider in same network

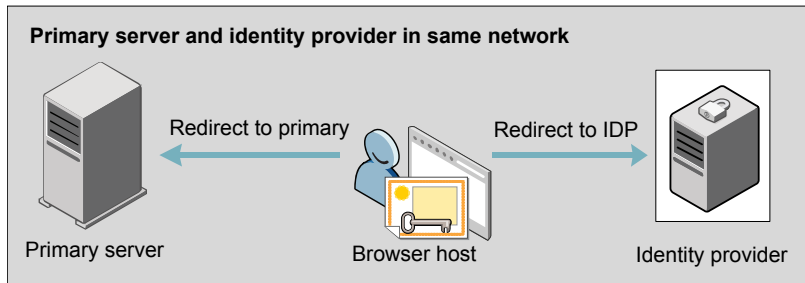
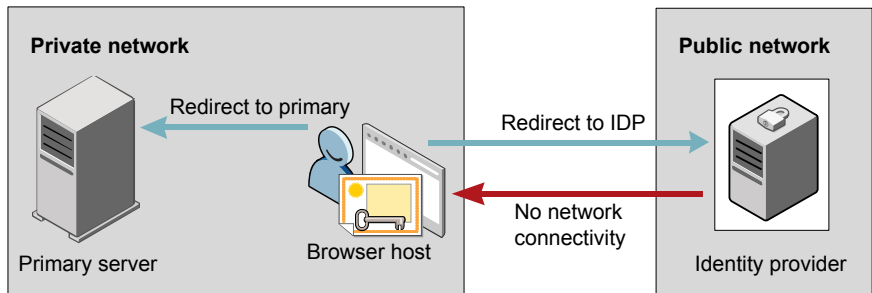


Figure 31-4 Example configuration: Primary server in private network and identity provider in public network



Configure NetBackup for single sign-on (SSO)

This section provides steps to set up trust and exchange configuration information between the IDP and the NetBackup primary server. Before proceeding with the steps, ensure that the following prerequisites are met in your environment:

- An IDP is set up and deployed in your environment.
- The IDP is configured to authenticate domain users of Active Directory (AD) or Lightweight Directory Access Protocol (LDAP).

Table 31-1 Steps to configure NetBackup for single sign-on

Step	Action	Description
1.	Download the IDP metadata XML file	<p>Download and save the IDP metadata XML file from the IDP.</p> <p>SAML metadata that is stored in XML files is used to share configuration information between the IDP and the NetBackup primary server. The IDP metadata XML file is used to add the IDP configuration to the NetBackup primary server.</p>
2.	Configure the SAML keystore, and add and enable the IDP configuration on the NetBackup primary server	<p>See “Configure the SAML KeyStore” on page 283.</p> <p>See “Configure the SAML keystore and add and enable the IDP configuration” on page 286.</p>
3.	Download the service provider (SP) metadata XML file	<p>The NetBackup primary server is the SP in the NetBackup environment. You can access the SP metadata XML file from the NetBackup primary server by entering the following URL in your browser:</p> <p><code>https://<i>masterserver</i>/netbackup/sso/saml2/metadata</code></p> <p>Where <i>masterserver</i> is the IP address or host name of the NetBackup primary server.</p>
4.	Enroll the NetBackup primary server as a service provider (SP) with the IDP	<p>See “Enroll the NetBackup primary server with the IDP” on page 288.</p>

Table 31-1 Steps to configure NetBackup for single sign-on (*continued*)

Step	Action	Description
5.	Add SAML users and the SAML groups that use SSO to the necessary RBAC roles	SAML users and SAML user groups are available in RBAC only if the IDP is configured and enabled on the NetBackup primary server. For steps on adding RBAC roles, see the following topic. See “Add a user to a role (non-SAML)” on page 299.

After the initial setup, you can choose to enable, update, disable, or delete the IDP configuration.

See [“Manage an IDP configuration”](#) on page 289.

After the initial setup, you can choose to update, renew, or delete the NetBackup CA SAML keystore . You can also configure and manage the ECA SAML keystore.

Configure the SAML KeyStore

To establish a trust between the NetBackup primary server and the IDP server, you must configure an SAML KeyStore on the NetBackup primary server. Depending on whether you are using the NetBackup CA or an external certificate authority (ECA), refer to either of the following sections:

Note: If you are using a combination of an ECA and NetBackup CA in your environment, by default, the ECA is considered while establishing trust with the IDP server.

Note: The SAML KeyStore configuration using batch files, such as `configureCerts.bat`, `configureCerts`, `configureSAMLECACert.bat`, `configureSAMLECACert` and their corresponding options is deprecated.

Configure a NetBackup CA KeyStore

If you are using the NetBackup CA, create the NetBackup CA KeyStore on the NetBackup primary server.

To create a NetBackup CA KeyStore

- 1 Log on to the NetBackup primary server as root or administrator.
- 2 Run the following command:

```
nbidpcmd -cCert -M master_server -f
```

`-f` is optional. Use the option for the forceful update.

Once the NetBackup CA KeyStore is created, ensure that you update the NetBackup CA KeyStore every time the NetBackup CA certificate is renewed.

To renew the NetBackup CA KeyStore

- 1 Log on to the NetBackup primary server as root or administrator.
- 2 Run the following command:

```
nbidpcmd -rCert -M master_server
```

- 3 Download the new SP metadata XML file from the NetBackup primary server by entering the following URL in your browser:

<https://primaryserver/netbackup/sso/saml2/metadata>

Where *primaryserver* is the IP address or host name of the NetBackup primary server.

- 4 Upload the new SP metadata XML file to the IDP.

See [“Enroll the NetBackup primary server with the IDP”](#) on page 288.

To remove the NetBackup CA KeyStore

- 1 Log on to the NetBackup primary server as root or administrator.
- 2 Run the following command

```
nbidpcmd -dCert -M master_server
```

- 3 Download the new SP metadata XML file from the NetBackup primary server by entering the following URL in your browser:

<https://primaryserver/netbackup/sso/saml2/metadata>

Where *primaryserver* is the IP address or host name of the NetBackup primary server.

- 4 Upload the new SP metadata XML file to the IDP.

- 5 See [“Enroll the NetBackup primary server with the IDP”](#) on page 288.

Configure an ECA KeyStore

If you are using an ECA, import the ECA KeyStore to the NetBackup primary server.

Note: If you are using a combination of an ECA and the NetBackup CA in your environment, by default, the ECA is considered while establishing trust with the IDP server. To use the NetBackup CA, you must first remove the ECA KeyStore.

To configure an ECA KeyStore

- 1 Log on to the primary server as root or administrator.
- 2 Depending on whether you want to configure SAML ECA keystore using the configured NetBackup ECA KeyStore or you want to provide the ECA certificate chain and private key, run the following commands:

- Run the following command to use NetBackup ECA configured KeyStore:

```
nbidpcmd -cECACert -uECA existing ECA configuration [-f] [-M  

primary_server]
```

- Run the following command to use ECA certificate chain and private key provided by the user:

```
nbidpcmd -cECACert -certPEM certificate chain file -privKeyPath  

private key file [-ksPassPath Keystore Passkey File] [-f] [-M  

<master_server>]
```

- Certificate chain file specifies the certificate chain file path. The file must be in PEM format and must be accessible to the primary server on which the configuration is being performed.
- Private key file specifies the private key file path. The file must be in PEM format and must be accessible to the primary server on which the configuration is being performed.
- KeyStore passkey file specifies the KeyStore password file path and must be accessible to the primary server on which the configuration is being performed.
- Primary server is the host name or IP address of primary server on which you want to perform SAML ECA KeyStore configuration. The NetBackup primary server where you run the command is selected by default.

To remove the ECA KeyStore

- 1 Log on to the primary server as root or administrator.
- 2 Download the new SP metadata XML file from the NetBackup primary server by entering the following URL in your browser:

<https://primaryserver/netbackup/sso/saml2/metadata>

Where *primaryserver* is the IP address or host name of the NetBackup primary server.

- 3 Upload the new SP metadata XML file to the IDP.

See [“Enroll the NetBackup primary server with the IDP”](#) on page 288.

Configure the SAML keystore and add and enable the IDP configuration

Before proceeding with the following steps, ensure that you have downloaded the IDP metadata XML file and saved it on the NetBackup primary server.

To configure SAML keystore and add and enable an IDP configuration

- 1 Log on to the primary server as root or administrator.
- 2 Run the following command.

For IDP and NetBackup CA SAML KeyStore configuration:

```
nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata file
[-t SAML2] [-e true | false] [-u IDP user field] [-g IDP user
group field] [-cCert] [-f] [-M primary server]
```

Alternatively for IDP and ECA SAML KeyStore configuration:

Depending on whether you want to configure SAML ECA KeyStore using the configured NetBackup ECA KeyStore or you want to provide the ECA certificate chain and private key, run the following commands:

- Use NetBackup ECA configured keystore:

```
nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata
file[-t SAML2] [-e true | false] [-u IDP user field] [-g IDP
user group field] -cECACert -uECA existing ECA configuration
[-f] [-M Primary Server]
```

- Use ECA certificate chain and private key provided by the user:

```
nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata
file[-t SAML2] [-e true | false] [-u IDP user field] [-g IDP
user group field] -cECACert -certPEM certificate chain file
-privKeyPath private key file [-ksPassPath KeyStore passkey
file] [-f] [-M primary server]
```

Replace the variables as follows:

- *IDP configuration name* is a unique name provided to the IDP configuration.
- *IDP XML metadata file* is the path to the XML metadata file, which contains the configuration details of the IDP in Base64URL-encoded format.
- *-e true | false* enables or disables the IDP configuration. An IDP configuration must be added and enabled, otherwise users cannot sign in with the single sign-on (SSO) option. Even though you can add multiple IDP configurations on a NetBackup primary server, only one IDP configuration can be enabled at a time.

- The SAML attribute names *IDP user field* and *IDP user group field* are used to map user identity information and group information in the Identity Provider. These fields are optional, and if not provided, they are mapped to the `userPrincipalName` and `memberOf` SAML attributes by default. For instance, if you have customized the attribute mapping in the Identity Provider to use attributes like email and groups, when configuring the SAML configuration, you need to provide the `-u` option for email and `-g` option for groups.

If you have not provided values for these attributes during configuration, ensure that the Identity Provider returns the values against the `userPrincipalName` and `memberOf` attributes.

For Example:

If SAML response is as follows:

```
saml:AttributeStatement <saml:Attribute Name="userPrincipalName">
<saml:AttributeValue>username@domainname</saml:AttributeValue>
</saml:Attribute> <saml:Attribute Name="memberOf">
<saml:AttributeValue>CN=group name,
DC=domainname</saml:AttributeValue> </saml:Attribute>
</saml:AttributeStatement>
```

It implies that you need to map the `-u` and `-g` options against the fields "saml:Attribute Name".

Note: Ensure that the SAML attribute values are returned in the format of *username@domainname* for the field mapped to the `-u` option that defaults to `userPrincipalName`. If you include the domain name when returning group information, it should follow the format "(CN=group name, DC=domainname)" or "(domainname\groupname)".

However, if you return the group name as plain text without domain information, it should be mapped without the domain name in the SAML RBAC group.

- *primary Server* is the host name or IP address of primary server to which you want to add or modify the IDP configuration. The NetBackup primary server where you run the command is selected by default.
- *Certificate Chain File* is the certificate chain file path. The file must be in PEM format and must be accessible to the primary server on which the configuration is being performed.
Private Key File is the private key file path. The file must be in PEM format and must be accessible to the primary server on which the configuration is being performed.

KeyStore Passkey File is the KeyStore passkey file path and must be accessible to the primary server on which the configuration is being performed.

If your Identity Provider is already configured with SAML attribute names as `userPrincipalName` and `memberOf`, you do not have to provide the `-u` and `-g` option while configuration. If you are using any other custom attributes name, provide those names against `-u` and `-g` as follows:

For example:

If the Identity Provider SAML attribute names are mapped as "email" and "groups", use the following command for configuration:

```
nbidpcmd -ac -n veritas_configuration -mxp file.xml -t SAML2 -e true -u email -g groups -cCert -Mprimary_server.abc.com
```

`-u` and `-g` are optional and it depends on the Identity Provider configuration. Ensure that you specify the same parameter values that you have provided at the time of configuration.

Enroll the NetBackup primary server with the IDP

The NetBackup primary server must be enrolled with the IDP as a service provider (SP). For step-by-step procedures that are specific to a particular IDP, see the following table:

Table 31-2 IDP-specific steps for enrolling the NetBackup primary server

IDP name	Link to steps
ADFS	https://www.veritas.com/docs/100047744
Okta	https://www.veritas.com/docs/100047745
PingFederate	https://www.veritas.com/docs/100047746
Azure	https://www.veritas.com/docs/100047748
Shibboleth	https://www.veritas.com/docs/00047747

Enrolling an SP with an IDP typically involves the following operations:

Uploading the SP metadata XML file to the IDP

The SP metadata XML file contains the SP certificate, the entity ID, the Assertion Consumer Service URL (ACS URL), and a log out URL (SingleLogoutService). The SP metadata XML file is required by the IDP to establish trust, and exchange authentication and authorization information with the SP.

Mapping the SAML attributes to their AD or LDAP attributes

Attribute mappings are used to map SAML attributes in the SSO with its corresponding attributes in the AD or LDAP directory. The SAML attribute mappings are used for generating SAML responses, which are sent to the NetBackup primary server. Ensure that you define SAML attributes that map to the `userPrincipalName` and the `memberOf` attributes in the AD or LDAP directory. The SAML attributes must adhere to the following formats:

Table 31-3

Corresponding AD or LDAP attribute	SAML attribute format
<code>userPrincipalName</code>	<code>username@domainname</code>
<code>memberOf</code>	<code>(CN=group name, DC=domainname)</code>

Note: While adding the IDP configuration to the NetBackup primary server, the values entered for the user (`-u`) and user group (`-g`) options must match the SAML attribute names that are mapped to the `userPrincipalName` and the `memberOf` attributes in the AD or LDAP.

See [“Configure the SAML keystore and add and enable the IDP configuration”](#) on page 286.

Manage an IDP configuration

You can manage the identity provider (IDP) configurations on the NetBackup primary server by using the enable (`-e true`), update (`-uc`), disable (`-e false`), and delete (`-dc`) options of the `nbidpcmd` command.

Enable an IDP configuration

By default, an IDP configuration is not enabled in the product environment. If you did not enable the IDP when you added it, you can use the `-uc -e true` options to update and enable the IDP configuration.

To enable an IDP configuration

- 1 Log on to the primary server as root or administrator.
- 2 Run the following command:

```
nbidpcmd -uc -n IDP configuration name -e true
```

Where *IDP configuration name* is a unique name provided to the IDP configuration.

Note: Even though you can configure multiple IDPs on a NetBackup primary server, only one IDP can be enabled at a time.

Update an IDP configuration

You can update the XML metadata file associated with an IDP configuration.

To update the IDP XML metadata file in an IDP configuration

- 1 Log on to the primary server as root or administrator.
- 2 Run the following command:

```
nbidpcmd -uc -n IDP configuration name -mxp IDP XML metadata file
```

Replace the variables as described below:

- *IDP configuration name* is a unique name provided to the IDP configuration.
- *IDP XML metadata file* is the path to the XML metadata file, which contains the configuration details of the IDP in Base64URL-encoded format.

If you want to update the IDP user or IDP user group values in an IDP configuration, you must first delete the configuration. The single sign-on (SSO) option is not available for users until you re-add the configuration with the updated IDP user or IDP user group values.

To update IDP user or IDP user group in an IDP configuration

- 1 Log on to the primary server as root or administrator.
- 2 Delete the IDP configuration.

```
nbidpcmd -dc -n IDP configuration name
```

Where *IDP configuration name* is a unique name provided to the IDP configuration.

- 3 To add and enable the configuration again, run the following command:

```
nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata file  
[-t SAML2] [-e true | false] [-u IDP user] [-g IDP user group  
field] [-M Master Server]
```

Replace the variables as described below:

- *IDP configuration name* is a unique name provided to the IDP configuration.
- *IDP XML metadata file* is the path to the XML metadata file, which contains the configuration details of the IDP in Base64URL-encoded format.

- `-e true | false` enables or disables the IDP configuration. An IDP must be available and enabled otherwise users cannot sign in with the single sign-on (SSO) option. Even though you can add multiple IDP configurations on a NetBackup primary server, only one IDP configuration can be enabled at a time.
- *Master Server* is the host name or IP address of the primary server to which you want to add or modify the IDP configuration. The NetBackup primary server where you run the command is selected by default.

Disable an IDP configuration

If an IDP configuration is disabled in the product environment, the single sign-on (SSO) option of that IDP is not available for users when they sign in.

To disable an IDP configuration

- 1 Log on to the primary server as root or administrator.
- 2 Run the following command:

```
nbidpcmd -uc -n IDP configuration name -e false
```

Where *IDP configuration name* is a unique name provided to the IDP configuration.

Delete an IDP configuration

If an IDP configuration is deleted, the single sign-on (SSO) option of that IDP is not available for users when they sign in.

To delete an IDP configuration

- 1 Log on to the primary server as root or administrator.
- 2 Run the following command:

```
nbidpcmd -dc -n IDP configuration name
```

Where *IDP configuration name* is a unique name provided to the IDP configuration.

Video: Configure single sign-on in NetBackup

In this video, you will see an overview of how to configure single sign-on (SSO) in NetBackup.

[Video link](#)

Depending on which IDP you are using, see the following articles for steps on downloading the IDP metadata XML file and enrolling the NetBackup primary server with the IDP:

- ADFS: <https://www.veritas.com/docs/100047744>
- Okta: <https://www.veritas.com/docs/100047745>
- PingFederate: <https://www.veritas.com/docs/100047746>
- Azure: <https://www.veritas.com/docs/100047748>
- Shibboleth: <https://www.veritas.com/docs/100047747>

More information is available about SSO in NetBackup.

See “[Configure NetBackup for single sign-on \(SSO\)](#)” on page 282.

Troubleshooting SSO

This section provides steps for troubleshooting issues related to SSO.

Redirection issues

If you are facing issues with redirection, check the error messages in web services log files to narrow down the cause of the issue. NetBackup creates logs for the NetBackup web server and for the web server applications. These logs are written to the following location:

- UNIX: `/usr/opensv/logs/nbwebbservice`
- Windows: `install_path\NetBackup\logs\nbwebbservice`

NetBackup web UI does not redirect to the IDP sign in page

The IDP metadata XML file contains the IDP certificate, the entity ID, the redirect URL, and the logout URL. The NetBackup web UI can fail to redirect to the IDP sign in page, if the IDP XML metadata file is outdated or corrupted. The following message is added to the web service log:

```
Failed to redirect to the IDP server.
```

To ensure that the latest configuration details are available to the NetBackup primary server, download the latest copy of the XML metadata file from the IDP. Use the IDP XML metadata file to add and enable the latest IDP configuration on the NetBackup primary server. See “[Configure the SAML keystore and add and enable the IDP configuration](#)” on page 286.

IDP sign in page does not redirect to the NetBackup web UI

When you enter your credentials in the IDP sign in page, your browser might display an **Authentication failed** error, instead of redirecting to the NetBackup web UI.

Refer to the following table for resolution steps based on the error found in the web service log.

Table 31-4

Web Service log error message	Explanation and recommended action
<code>userPrincipalName not found in response.</code>	While adding the IDP configuration to the NetBackup primary server, the value entered for the user (-u) option must match the SAML attribute name, which is mapped to the <code>userPrincipalName</code> attribute in AD or LDAP. For more information, See “Configure the SAML keystore and add and enable the IDP configuration” on page 286.
<code>userPrincipalName is not in expected format</code>	<p>The IDP sends SAML responses to the NetBackup primary server, which contains SAML user and SAML user group information. To enable the IDP to successfully send this information, ensure the value of <code>userPrincipalName</code> attribute sent by the IDP is defined in the format of <code>username@domainname</code>.</p> <p>For more information, See “Enroll the NetBackup primary server with the IDP” on page 288.</p>
<code>Authentication issue instant is too old or in the future</code>	<p>This error can occur because of the following reasons:</p> <ul style="list-style-type: none"> ■ The date and time of IDP server and the NetBackup primary server is not synchronized. ■ By default, the NetBackup primary server allows a user to remain authenticated for a period of 24 hours. You might encounter this error, If an IDP allows a user to remain authenticated for a period longer than 24 hours. To resolve this error, you can update the SAML authentication lifetime of the NetBackup primary server to match that of the IDP. Specify the new SAML authentication lifetime in the <code><installpath>\var\global\wsl\config\web.conf</code> file on the NetBackup primary server. <p>For example, If your IDP has an authentication lifetime as 36 hours, update the entry in the <code>web.conf</code> file as follows:</p> <pre>SAML_ASSERTION_LIFETIME_IN_SECS=129600</pre>
<code>Response is not success</code>	<p>This error can occur because of the following reasons:</p> <ul style="list-style-type: none"> ■ The IDP metadata XML file contains an IDP certificate. If you are using a NetBackup CA, ensure that the IDP certificate is updated with latest NetBackup CA certificate information. For more information, See “Configure the SAML KeyStore” on page 283. ■ The Certificate Revocation List (CRL) must be disabled in the IDP if you are using a NetBackup CA keystore.

Unable to sign in due to authorization-related issues

To sign in with SSO, you must add SAML users and the SAML user groups to the necessary RBAC roles. If the RBAC roles are not correctly assigned, you might encounter the following error while signing into NetBackup web UI.

You are not authorized to access this application. Contact your NetBackup security administrator to request RBAC permissions for the NetBackup web user interface.

Refer to the table below to troubleshoot authorization-related issues:

Table 31-5

Cause	Explanation and recommended action
RBAC roles are not assigned to the SAML users and the SAML groups.	<p>After an IDP configuration is added and enabled on the NetBackup primary server, ensure that necessary RBAC roles are assigned to SAML users and SAML user groups that use SSO. Note that SAML users and SAML user groups are available in RBAC only after the IDP configuration is added and enabled on the NetBackup primary server.</p> <p>For steps on adding users, See “Add a user to a role (non-SAML)” on page 299.</p>
RBAC roles are assigned to SAML users and SAML user groups associated with an IDP configuration that is not currently added and enabled.	<p>When you add a SAML users or SAML user group in RBAC, the SAML user or SAML user group entry is associated with the IDP configuration that is added and enabled at that time.</p> <p>If you add and enable a new IDP configuration, ensure that you also add another entry for the SAML user or SAML user group. The new entry is associated with the new IDP configuration.</p> <p>For example, NBU_user is added to RBAC and assigned the necessary permissions, while an ADFS IDP configuration is added and enabled. If you add and enable an Okta IDP configuration, you must add a new user entry for NBU_user. Assign the necessary RBAC roles to the new user entry, which is associated with the Okta IDP configuration.</p> <p>For steps on adding users, See “Add a user to a role (non-SAML)” on page 299.</p>

Table 31-5 (continued)

Cause	Explanation and recommended action
RBAC roles are assigned to local domain users or Active Directory (AD) or LDAP domain users (instead of SAML users and SAML user groups).	<p>SAML user or SAML user group records might appear similar to corresponding local domain users or AD or LDAP domain users already added in the RBAC.</p> <p>After an IDP configuration is added and enabled on the NetBackup primary server, ensure that you add SAML users and SAML user groups in RBAC and assign the necessary permissions. Note that SAML users and SAML user groups are available in RBAC only after the IDP configuration is added and enabled on the NetBackup primary server.</p> <p>For steps on adding SAML users and user groups, See “Add a user to a role (non-SAML)” on page 299.</p>
The NetBackup primary server is unable to retrieve user group information from the IDP	<p>The IDP sends SAML responses to the NetBackup primary server, which contains SAML user and SAML user group information. To enable the IDP to successfully send this information, ensure the following:</p> <ul style="list-style-type: none">■ The IDP is configured to authenticate domain users from AD or LDAP.■ The value of <code>memberOf</code> attribute sent by the IDP is in the X.500 distinguished format, that is, {cn=groupname,dc=domain}.■ While adding the IDP configuration to the NetBackup primary server, the values entered for the user group (-g) option matches the SAML attribute name, which is mapped to the <code>memberOf</code> attribute in AD or LDAP. For more information, See “Configure the SAML keystore and add and enable the IDP configuration” on page 286.

Managing role-based access control

This chapter includes the following topics:

- [RBAC features](#)
- [Authorized users](#)
- [Configuring RBAC](#)
- [Default RBAC roles](#)
- [Add a custom RBAC role](#)
- [Role permissions](#)
- [Manage access permission](#)
- [View access definitions](#)

RBAC features

The NetBackup web user interface provides the ability to apply role-based access control in your NetBackup environment. Use RBAC to provide access for the users that do not currently have access to NetBackup. Or, for current NetBackup users with administrator access you can provide limited access and permissions, based on their role in your organization.

For information on access control and auditing information for root users and administrators, refer to the [NetBackup Security and Encryption Guide](#).

Table 32-1 RBAC features

Feature	Description
Roles allow users to perform specific tasks	Add users to one or more default RBAC roles or create custom roles to fit the role of your users. Add a user to the Administrator role to give full NetBackup permissions to that user. See “ Default RBAC roles ” on page 302.
Users can access NetBackup areas and the features that fit their role	RBAC users can perform common tasks for their business role, but are restricted from accessing other NetBackup areas and features. RBAC also controls the assets that users can view or manage.
Auditing of RBAC events	NetBackup audits RBAC events.
DR ready	RBAC settings are protected with the NetBackup catalog.

Authorized users

The following users are authorized to sign in to and use the NetBackup web UI.

Table 32-2 Users that are authorized to use the NetBackup web UI

User	Access	Notes
Root OS administrators Users with the RBAC Administrator role	Full	You can disable automatic access for OS administrators. See “ Disable web UI access for operating system (OS) administrators ” on page 315.
nbasesadmin Appliance user appadmin Flex Appliance user	Default Security Administrator role	This role can grant access to other appliance users. The default admin user for the NetBackup appliance does not have access to the web UI.
Users that have an RBAC role that gives access to the web UI	Varies	See “ Configuring RBAC ” on page 297.

Configuring RBAC

To configure role-based access control for the NetBackup web UI, perform the following steps.

Table 32-3 Steps to configure role-based access control

Step	Action	Description
1	Configure any Active Directory or LDAP domains.	Before you can add domain users, Active Directory or LDAP domains must be authenticated with NetBackup. See the NetBackup Security & Encryption Guide .
2	Determine the permissions that your users need.	Determine the permissions that your users need to perform their daily tasks. You can use the default RBAC roles or use a default role as a template to create a new role. Or, you can create a completely custom role to fit your needs. See "Role permissions" on page 310. See "Default RBAC roles" on page 302. See "Add a custom RBAC role" on page 305.
3	Add users to the appropriate roles.	See "Add a user to a role (non-SAML)" on page 299. See "Add a user to a role (SAML)" on page 301. See "Add a smart card user to a role (non-SAML, without AD/LDAP)" on page 300.
4	Determine the permissions that you want for OS administrators	See "Disable web UI access for operating system (OS) administrators" on page 315. See "Disable command-line (CLI) access for operating system (OS) administrators" on page 314.

Notes for using NetBackup RBAC

Note the following when you configure the permissions for RBAC roles:

- When you create roles, be sure to enable the minimal number of permissions so the user can sign in to and use the web UI. Some individual permissions do not have a direct correlation with a screen in the web UI. Users that attempt to sign in but that only have a permission of this kind receive an "Unauthorized" message.
- If a user is added to or removed from a role, the user must sign out and sign in again before the user's permissions are updated.
- Most permissions are not implicit.
In most cases a **Create** permission does not give a user **View** permission. A **Recovery** permission does not give a user **View** permission or other recovery options like **Overwrite**.

- Not all RBAC-controlled operations can be used from the NetBackup web UI. These types of operations are included in RBAC so a role administrator can create roles for API users as well as for web UI users.
- Some tasks require a user to have permissions in multiple RBAC categories. For example, to establish a trust relationship with a remote primary server, a user must have permissions for both **Remote primary servers** and **Trusted primary servers**.

Add AD or LDAP domains

NetBackup supports Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) domain users. Before you can add domain users to RBAC roles, you must add the AD or the LDAP domain. A domain also must be added before you can configure that domain for smart card authentication.

You can use the `POST /security/domains/vxat` API or the `vssat` command to configure domains.

For more information on the `vssat` command and more of its options, see the [NetBackup Command Reference Guide](#). For troubleshooting information, see the [NetBackup Security & Encryption Guide](#).

View users in RBAC

You can view the users that have been added to RBAC and the roles that they are assigned to. The **Users** list is view-only. To edit the users that are assigned to a role, you must edit the role.

To view the users in RBAC

- 1 On the left, click **Security > RBAC**.
- 2 Click on the **Users** tab.
- 3 The **Roles** column indicates each role to which the user is assigned.

Add a user to a role (non-SAML)

This topic describes how to add a non-SAML user or group to a role.

Non-SAML users use one of the following sign-in methods: **Sign in with username and password** or **Sign in with smart card**.

To add a user to a role (non-SAML)

- 1 On the left, click **Security > RBAC**.
- 2 Click the **Roles** tab.

- 3 Click on the role name, then click on the **Users** tab.
- 4 (Conditional) From the **Sign-in type** list, select from the following:
 - **Default sign-in.** For a user that signs into NetBackup with their username and password.
 - **Smart card user.** For a user that uses a smart card to sign into NetBackup.

Note: The **Sign-in type** list is only available if there is an IDP configuration available for NetBackup.

- 5 Enter the user or the group name that you want to add.

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

- 6 Click **Add to list**.
- 7 The user must sign out and sign in again before the user's permissions are updated.

Add a smart card user to a role (non-SAML, without AD/LDAP)

This topic describes how to add a smart card user to a role. In this case the user is a non-SAML user and there is no AD or no LDAP domain association or mapping. User groups are not supported with this type of configuration.

This type of user uses the following sign-in method: **Sign in with smart card**.

To add a smart card user to a role (non-SAML, without AD/LDAP)

- 1 On the left, click **Security > RBAC**.
- 2 Click the **Roles** tab.
- 3 Click on the role name, then click on the **Users** tab.

- 4 (Conditional) From the **Sign-in type** list, select **Smart card user**.

Note: The **Sign-in type** list is available only if there is an IDP configuration available for NetBackup. The smart card user option in the **Sign-in type** list is available when the smart card configuration is done without AD or LDAP domain mapping.

- 5 Enter the username that you want to add.
Provide the exact common name (CN) or the universal principal name (UPN) that is available in the certificate.
- 6 Click **Add to list**.
- 7 The user must sign out and sign in again before the user's permissions are updated.

Add a user to a role (SAML)

This topic describes how to add a SAML user or group to a role.

SAML users use one of the following sign-in methods: **SAML user** or **SAML group**.

To add a user to a role (SAML)

- 1 On the left, click **Security > RBAC**.
- 2 Click the **Roles** tab.
- 3 Click on the role name, then click on the **Users** tab.
- 4 From the **Sign-in type** list, select the sign-in method **SAML user** or **SAML group**.
- 5 Enter the user or the group name that you want to add.

For example, nbuadmin@my.host.com.

If your Identity Provider (IDP) returns group information in the format of (CN=groupname, DC=domainname) or domainname\groupname, you should add the group using the format groupname@domainname. However, it is also possible to configure SAML Groups in Role-Based Access Control (RBAC) without including the domain name. If your IDP returns group names without domain information, you can add those groups as plain text. Please note that using the email format is not mandatory for SAML groups.

- 6 Click **Add to list**.
- 7 The user must sign out and sign in again before the user's permissions are updated.

Remove a user from a role

You can remove a user from a role when you want to remove permissions for that user.

If a user is removed from a role, the user must sign out and sign in again before the user's permissions are updated.

To remove a user from a role

- 1 On the left, click **Security > RBAC**.
- 2 Click the **Roles** tab.
- 3 Click on the role that you want to edit, select the **Users** tab.
- 4 Locate the user you want to remove and click **Actions > Remove > Remove**.

Default RBAC roles

The NetBackup web UI provides the following default RBAC roles with preconfigured permissions and settings.

Table 32-4 Default RBAC roles in the NetBackup web UI

Role name	Description
Administrator	The Administrator role has full permissions for NetBackup and can manage all aspects of NetBackup.
Default Apache Cassandra Administrator	This role has all the permissions that are necessary to manage and protect Apache Cassandra assets with protection plans.
Default AHV Administrator	This role has all the permissions that are necessary to manage Nutanix Acropolis Hypervisor and to back up those assets with protection plans.
Default Cloud Administrator	<p>This role has all the permissions that are necessary to manage cloud assets and to back up those assets with protection plans.</p> <p>Note that a PaaS administrator requires some additional permissions that you can add to a custom role.</p> <p>Cloud administrators also need additional permissions to manage cloud and PaaS assets using intelligent groups.</p> <p>See “Add a custom RBAC role for a PaaS administrator” on page 308.</p>
Default Cloud Object Store Administrator	This role has all the permissions to manage the protection for cloud objects using classic policies.
Default IRE SLP Administrator	Manages IRE (Isolated Recovery Environment) SLP (Storage lifecycle policies) functionalities.

Table 32-4 Default RBAC roles in the NetBackup web UI (*continued*)

Role name	Description
Default Kubernetes Administrator	This role has all the permissions that are necessary to manage Kubernetes and to back up those assets with protection plans. The permissions for this role give a user the ability to view and manage jobs for Kubernetes assets. To view all jobs for this asset type, a user must have the default role for that workload. Or, a similar custom role must have the following option applied when the role is created: Apply selected permissions to all existing and future workload assets.
Default Microsoft Sentinel Administrator	This role has all the permissions necessary to add Microsoft Sentinel credentials in NetBackup and to send NetBackup audit events to Microsoft Sentinel.
Default Microsoft SQL Server Administrator	This role has all the permissions that are necessary to manage SQL Server databases and to back up those assets with protection plans. In addition to this role, the NetBackup user must meet the following requirements: <ul style="list-style-type: none"> ■ Member of the Windows administrator group. ■ Have the SQL Server “sysadmin” role.
Default Multi-Person Authorization (MPA) Approver	This role has permissions to manage MPA tickets.
Default MySQL Administrator	This role has all the permissions that are necessary to manage MySQL instances and databases and to back up those assets with protection plans.
Default NAS Administrator	This role has all the permissions that are necessary to perform the backup and restore of NAS volumes using a NAS-Data-Protection policy. To view all jobs for the backups and restores of a NAS volume, a user must have this role. Or, the user must have a custom role with same permissions applied when the role was created.
Default NetBackup Command Line (CLI) Administrator	This role has all the permissions that are necessary to manage NetBackup using the NetBackup command line (CLI). With this role a user can run most of the NetBackup commands with a non-root account. Note: A user that has only this role cannot sign into the web UI.
Default Oracle Administrator	This role has all the permissions that are necessary to manage Oracle databases and to back up those assets with protection plans.
Default PostgreSQL Administrator	This role has all the permissions that are necessary to manage PostgreSQL instances and databases and to back up those assets with protection plans.
Default Resiliency Administrator	This role has all the permissions to protect the Veritas Resiliency Platform (VRP) for VMware assets.

Table 32-4 Default RBAC roles in the NetBackup web UI (*continued*)

Role name	Description
Default RHV Administrator	<p>This role has all the permissions that are necessary to manage Red Hat Virtualization computers and to back up those assets with protection plans. This role gives a user the ability to view and manage jobs for RHV assets.</p> <p>To view all jobs for RHV assets, a user must have this role. Or, the user must have a similar custom role with following option applied when the role was created: Apply selected permissions to all existing and future RHV assets.</p>
Default SaaS Administrator	This role has all the permissions to view and manage SaaS assets.
Default Security Administrator	This role has permissions to manage NetBackup security including role-based access control (RBAC), certificates, hosts, identity providers and domains, global security settings, and other permissions. This role can also view settings and assets in most areas of NetBackup: workloads, storage, licensing, and other areas.
Default Storage Administrator	This role has permissions to configure disk-based storage and storage lifecycle policies. SLP settings are managed with the Administrator role.
Default Universal Share Administrator	This role has the permissions to manage policies and storage servers. It can also manage the assets for Windows and Standard client types and for universal shares.
Default Veritas Alta View Administrator	This role has all the permissions that are necessary to manage Veritas Alta View functionalities.
Default VMware Administrator	<p>This role has all the permissions that are necessary to manage VMware virtual machines and to back up those assets with protection plans. To view all jobs for VMware assets, a user must have this role. Or, the user must have a similar custom role with following option applied when the role was created: Apply selected permissions to all existing and future VMware assets.</p>
NetBackup Read-Only Operator	Provides read-only permissions to the IT Analytics Operator, Multi-Person Authorization Approver, and other operators in NetBackup, with no permissions for security.

Note: Veritas reserves the right to update the RBAC permissions for default roles in future releases. Any revised permissions are automatically applied to users of these roles when NetBackup is upgraded. If you have copies of default roles these roles are not updated automatically. (Or, if you have any custom roles that are based on default roles.) If you want these custom roles to include changes to default roles, you must manually apply the changes or recreate the custom roles.

Add a custom RBAC role

Create a custom RBAC role if you want to manually define the permissions and the access that users have to workload assets, protection plans, or credentials.

Note: Veritas reserves the right to update the RBAC permissions for default roles in future releases. Any revised permissions are automatically applied to users of these roles when NetBackup is upgraded. Any copies of default roles (or any custom roles that are based on default roles) are not automatically updated.

To add a custom RBAC role

- 1 On the left, select **Security > RBAC** and click **Add**.
- 2 Select the type of role that you want to create.

You can make a copy of a default role that contains all the preconfigured permissions and settings for that type of role. Or, select **Custom role** to manually configure all the permissions for a role.
- 3 Provide a **Role name** and a description.

For example, you may want to indicate that role is for any users that are backup administrators for a particular department or region.
- 4 Under **Permissions**, click **Assign**.

The permissions that you select determine the other settings that you can configure for the role.

If you select a default role type, certain permissions are enabled only if they are required for that type of role. (For example, the **Default Storage Administrator** does not require permissions for protection plans. The **Default Microsoft SQL Server Administrator** requires credentials.)

 - **Workloads** are enabled when you select **Asset** permissions.
 - **Protection plans** are enabled when you select **Protection plans** permissions.
 - **Credentials** are enabled when you select **Credentials** permissions.
- 5 Configure the permissions for the role.

See [“Role permissions”](#) on page 310.

See [“Notes for using NetBackup RBAC”](#) on page 298.

- 6
- Under **Users**, click **Assign**.
- 7
- When you are done configuring the role, click **Save**.
- Note: After a role is created, you must edit permissions for assets, protection plans, or credentials directly from the applicable node in the web UI. For example, to edit permissions for VMware, go to **Workloads > VMware** and then select **VMware settings > Manage permissions**. Or, open the details for a VM and click on the **Permissions** tab.

Edit or remove a role a custom role

You can edit or remove a custom role when you want to change or remove permissions for users with that role. Default roles cannot be edited or removed. You can only add or remove users from default roles.

Edit a custom role

Note: When you change permissions for a custom role, the changes affect all users that are assigned to that role.

To edit a custom role

- 1
- On the left, click **Security > RBAC**.
- 2
- On the **Roles** tab, locate and click on the custom role that you want to edit.
- 3
- To edit the role description, click **Edit name and description**.
- 4
- Edit the permissions for the role. You can edit the following details for a role:

Global permissions for the role	On the Global permissions tab, click Edit .
Users for the role	Click the Users tab.
Access definitions for the role	Click the Access definitions tab.

See [“Role permissions”](#) on page 310.

See [“Notes for using NetBackup RBAC”](#) on page 298.

- 5
- To add or remove users for the role, click the **Users** tab.
- See [“Add a user to a role \(non-SAML\)”](#) on page 299.
- See [“Remove a user from a role”](#) on page 302.
- 6
- Permissions for assets, protection plans, and credentials must be edited directly in the applicable node in the web UI.

Remove a custom role

Note: When you remove a role, any users that are assigned to that role lose the permissions that the role provided.

To remove a custom role

- 1 On the left, click **Security > RBAC**.
- 2 Click the **Roles** tab.
- 3 Locate the custom role that you want to remove and select the check box for it.
- 4 Click **Remove > Yes**.

Add a custom RBAC role to restore Azure-managed instances

To restore Azure-managed instances, users must have the view permission for these instances. Administrators and similar users can provide other users with a custom role and this permission.

To assign the view permission for Azure-managed instances

- 1 To get the access control ID of the managed instance, enter the following command:

```
GET /asset-service/workloads/cloud/assets?filter=extendedAttributes/managedInstanceName eq 'managedInstanceName'
```

Search for *accessControlId* field in the response. Note down the value of this field.

- 2 To get the role ID, enter the following command:

```
GET /access-control/roles
```

Search for the *id* field in the response. Note down the value of this field.

- 3 Create an access definition, as follows:

```
POST /access-control/managed-objects/{objectId}/access-definitions
```

Request payload

```
{
  "data": {
    "type": "accessDefinition",
    "attributes": {
```

```

        "propagation": "OBJECT_AND_CHILDREN"
    },
    "relationships": {
        "role": {
            "data": {
                "id": "<roleId>",
                "type": "accessControlRole"
            }
        },
        "operations": {
            "data": [
                {
                    "id": "|OPERATIONS|VIEW|",
                    "type": "accessControlOperation"
                }
            ]
        },
        "managedObject": {
            "data": {
                "id": "<objectId>",
                "type": "managedObject"
            }
        }
    }
}

```

Use the following values:

- `objectId`: Use the value of *accessControlId* obtained from step 1.
- `roleId`: Use the value of *id* obtained from step 2.

Note: For an alternate restore, provide the `|OPERATIONS|ASSETS|CLOUD|RESTORE_DESTINATION|` permission in the *operations* list.

Add a custom RBAC role for a PaaS administrator

A PaaS administrator needs additional storage permissions. You can use the **Default Cloud Administrator** role as a template to create a custom role.

To add a custom RBAC role

- 1 On the left, select **Security > RBAC** and click **Add**.
- 2 Select **Default Cloud Administrator**.
- 3 Provide a **Role name** and a description.
 For example, you may want to indicate that the role is for any users that are PaaS administrators.
- 4 Under **Permissions**, click **Assign**.
- 5 On the **Global** tab, expand the **Storage** section. Select the following permissions.

Disk pools	View
Storage servers	View
Storage universal shares	View, Create
- 6 On the **Assets** tab, under desired policy type / workload section select the following permissions:
 - Instant access
 - Restore from malware-infected images (Required to restore from malware infected images)
- 7 Click **Assign**.
- 8 Under **Users**, click **Assign**. Then add each user that you want to have access to this custom role.
- 9 When you are done configuring the role, click **Add role**.

Add a custom RBAC role for a Malware administrator

You can use the Default Workload Administrator (of supported workload) role as a template to create a custom role.

To add a custom RBAC role

- 1 On the left, select **Security > RBAC** and click **Add**.
- 2 Select **Default Workload Administrator** or **Custom Role**.
- 3 Provide a **Role name** and a description.
 For example, you may want to indicate that the role is for any users that are Malware administrators.

- 4 Under **Permissions**, click **Assign**.
- 5 On the **Global** tab, expand the **NetBackup management** section. Select the following permissions.

Malware	Scan for malware, View scan results
Scan host pools	View, Create, Update, Delete
Scan hosts	View, Create, Update, Delete
Malware tools	View
- 6 Click **Assign**.
- 7 Under **Users**, click **Assign**. Then add each user that you want to have access to this custom role.
- 8 When you are done configuring the role, click **Add role**.

Role permissions

Role permissions define the operations that roles users have permission to perform.

For details on individual RBAC permissions and dependencies, refer to the NetBackup API documentation.

<http://sort.veritas.com>

Table 32-5 Role permissions for NetBackup RBAC

Category	Description
Global	<p>Global permissions apply to all assets or objects.</p> <p>BMR - Configuration and management of BMR.</p> <p>NetBackup Web Management Console Administration - With guidance from Veritas Support, create diagnostic files to troubleshoot NetBackup and perform JVM garbage collection.</p> <p>These operations are only available from the NetBackup APIs. Refer to the following guides for information on JVM tuning options: NetBackup Installation Guide, NetBackup Upgrade Guide.</p> <p>NetBackup management - Configuration and management of NetBackup.</p> <p>Protection - NetBackup backup policies and storage lifecycle policies.</p> <p>Security - NetBackup security settings.</p> <p>Storage - Manage backup storage settings.</p>

Table 32-5 Role permissions for NetBackup RBAC (*continued*)

Category	Description
Assets	Manage one or types of assets. For example, VMware assets.
Protection plans	Manage how backups are performed with protection plans.
Credentials	Manage credentials for assets and for other features of NetBackup.

Manage access permission

The **Manage access** permission allows a user to manage who can access a specific part of NetBackup. Users that manage access also need **Access control** permissions. This permission is available for each permission category. However, for some categories the **Manage access** functionality is only available from the NetBackup APIs and not the NetBackup web UI.

For example, a user that has **Manage access** on VMware assets can add or remove the custom roles that have access to VMware assets. This user can also add or remove the specific permissions that a custom role has on VMware assets.

Add the manage access permission to a custom role

If a default role does not have the **Manage access** permission that a user needs, you can create a custom role with that permission. Also give the user the permissions for **User** and **Roles**. These permissions allow the user to view and add users to roles and to add and manage roles.

Assign permissions [Learn about permissions](#)

Global

Assets

Protection plans

Credentials

RHV assets

All | None

☐ View

☐ Create

☐ Update

☐ Delete

☐ Manage access

☐ Protect

☐ View restore targets

☐ Restore

☐ Allow restore to overwrite

☐ Cancel Jobs

☐ Restart Jobs

☐ View Jobs

VMware assets

All | None

☒ View

☐ Create

☐ Update

☐ Delete

☒ Manage access

☐ Protect

☐ View restore targets

☐ Restore to cloud

☐ Granular restore

☐ Instant access - Download files

☐ Instant access - Restore files

☐ Instant access

☐ Restore

☐ Allow restore to overwrite

☐ Cancel Jobs

☐ Restart Jobs

☐ View Jobs

Assign permissions

Global

Assets

Protection plans

Credentials

NetBackup management

Protection

Security

Access control

Users

☒ View
☐ Manage access
☒ Assign to role

Roles

☒ Create
☒ Update
☒ Delete
☐ Manage access

Remove access for a custom role

You can remove access to an area of the web UI for a custom role. For each category for which you want to remove the manage access permission, clear the **Manage access** permission. You must edit permissions for assets, protection plans, or credentials directly from the applicable node in the web UI.

For example, to remove manage access permissions for VMware, go to **Workloads > VMware** and then select **VMware settings > Manage permissions**. Or, open the details for a VM and click on the **Permissions** tab.

View access definitions

Access definitions describe the permissions that are part of an RBAC role.

View access definitions

To view access definitions for a role in the web UI, you must have the **View** permission on the role.

To view access definitions

- 1 On the left, select **Security > RBAC** and click on the **Roles** tab.
- 2 Click on the role.
- 3 Click on the **Access definitions** tab.
- 4 Expand the namespace to see the permissions that are assigned to that namespace.

Disabling access to NetBackup interfaces for OS Administrators

This chapter includes the following topics:

- [Disable command-line \(CLI\) access for operating system \(OS\) administrators](#)
- [Disable web UI access for operating system \(OS\) administrators](#)

Disable command-line (CLI) access for operating system (OS) administrators

By default, an OS administrator (user or group member) has access to the NetBackup CLI and does not need to be a member of an RBAC role.

This option prevents OS administrators from accidentally running NetBackup CLIs. A malicious user with the OS administrator access of the primary server can still bypass this restriction.

After you can disable the option, the OS administrator must log in with `bpnbat -login` to access the CLI.

To disable CLI access for OS administrators

- 1 On the top right, click **Settings > Global security**.
- 2 On the **Security controls** tab, turn off the **CLI access for Operating System Administrator** option.

Disable web UI access for operating system (OS) administrators

By default, an OS administrator (user or group member) has access to the NetBackup web UI and does not need to be a member of an RBAC role.

If you do not want an OS administrator to automatically have this access, you can disable it. An OS administrator must then have the RBAC Administrator role to be able to access the web UI.

To disable web UI access control for the OS administrators

- 1 On the top right, click **Settings > Global security**.
- 2 On the **Security controls** tab, turn off the **Web UI access for Operating System Administrator** option.

Detection and reporting

- [Chapter 34. Malware scanning](#)
- [Chapter 35. Detecting anomalies](#)
- [Chapter 36. Usage reporting and capacity licensing](#)

Malware scanning

This chapter includes the following topics:

- [About malware scanning](#)
- [Configurations](#)
- [Perform a malware scan](#)
- [Managing scan tasks](#)

About malware scanning

NetBackup finds malware in supported backup images and finds the last good-known image that is malware free. This feature is supported for Standard, MS-Windows, NAS-Data-Protection, Cloud, Universal share and VMware workloads.

Malware scanning provides the following benefits:

- You can select one or more backup images of the supported policy-types for an on-demand scan. You can use a predefined list of scan hosts.
- If malware is detected during the scanning, a notification is generated in the Web UI.
- In case files are skipped due to not being accessible to scanner or failure from malware scanner, then following respective notifications are generated with information about number and list of skipped files:
 - **Critical severity:** In case malware is found in the backup image and some of the files were skipped during scan.
 - **Warning severity:** In case no malware found in the backup image but some of the files were skipped during scan.

This information can be obtained by clicking on **Actions > Export skipped files list**.

Note: During recovery if user starts recovery from a malware-affected backup image, a warning message is shown and confirmation is required for proceeding with recovery. Only users with permission to restore from malware-affected images can proceed with recovery.

Malware scanning before recovery

- User can trigger malware scan of the selected files/folders for recovery as part of recovery flow from Web UI and decide the recovery actions based on malware scan results.
- Catalog entry for the backup image is not updated after recovery time scan as only subset of files are scanned in the backup. Notification would be generated if malware is found as part of recovery time scan.
- During recovery time scan all the images in the start and end date are scanned for malware. Malware scanning of backup image may take long time depending on the number of files selected for recovery. It is recommended to set the Start /End date to include only images which are intended to be used for recovery.
- User can trigger multiple recovery time scan for same backup image.
- Malware scan as part of recovery may take minimum 15-20 minutes for small size backup based on availability of scan host and number of scan jobs in progress. User can track the progress using **Activity monitor > Jobs**. Scan results would be displayed incrementally in the malware detection page. List of backup images in start and end date would be picked up for malware scan incrementally in batches.
- Supported policy types for recovery time scan: Standard, MS-Windows, Universal Share, and NAS-Data-Protection.

Note: For successful recovery time malware scan operation, the media server version must be 10.3.

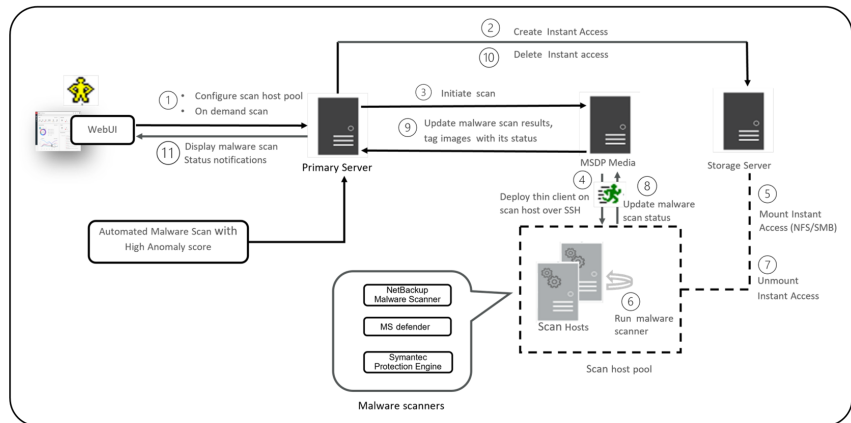
Workflow for malware scanning

This section describes the workflow for malware scanning for the following:

- MSDP backup images
- OST and AdvancedDisk

Malware scanning workflow for MSDP backup images

The following figure displays the workflow of malware scanning for MSDP backup images:



The following steps depict the workflow for malware scanning for MSDP backup images:

- After triggering **On Demand Scan**, primary server will validate backup images and create scan jobs for each eligible backup image and identify available scan host for them. Following are few of the criteria's on which the backup images are validated:
 - Backup image must be supported for malware detection.
 - Backup image must have a valid Instant Access copy.
 - For an on-demand scan, no existing scan must be running for same backup image. For DNAS the related streams are also considered.
 - Malware detection does not support media server associated with storage.
 - Unable to get information for backup image from catalog.
- After the backup images are queued for an on-demand scan, the primary server identifies the storage server. An instant access mount is created on the storage server of the configured share type that is specified in scan host pool.

Note: Currently the primary server starts 50 scan threads at a time. After the thread is available it processes the next job in the queue. Until then the queued jobs are in the pending state.

For NetBackup version 10.3 and later, large backups are scanned in batches of 500K files. Each batch is scanned by a separate scan thread.

For recovery time scan, scan in batches feature is not supported.

3. Primary server identifies available and supported MSDP media server and instructs the media server to initiate the malware scan.
4. MSDP media server deploys the thin client on the scan host over SSH.
5. Thin client mounts the instant access mount on the scan host.
6. Scan is initiated using the malware tool that is configured in the scan host pool.
Media server fetches the progress of scan from scan host and update the primary server.
7. After the scan is completed, the scan host unmounts the instant access mount from the scan host.
8. Malware scan status is updated to the media server over SSH. Scan logs are copied to the media server log directory.
9. Media server updates the scan status and the infected file list along with skipped file list (if any infected files) to the primary server.
10. Primary server updates the scan results and deletes instant access.
11. Malware scan status notification is generated.
12. Malware scan will timeout in case there is no update on scan. Default timeout period is 48 hours.

Malware detection performs an automated cleanup of eligible scan jobs that are older than 30 days.

Note: The infected scan jobs would be cleaned automatically.

Note: You can download a malware scanner from the Microsoft Azure Marketplace and the AWS Marketplace. Follow the instructions on how to install, configure, and use the malware scanner for AWS and Azure.

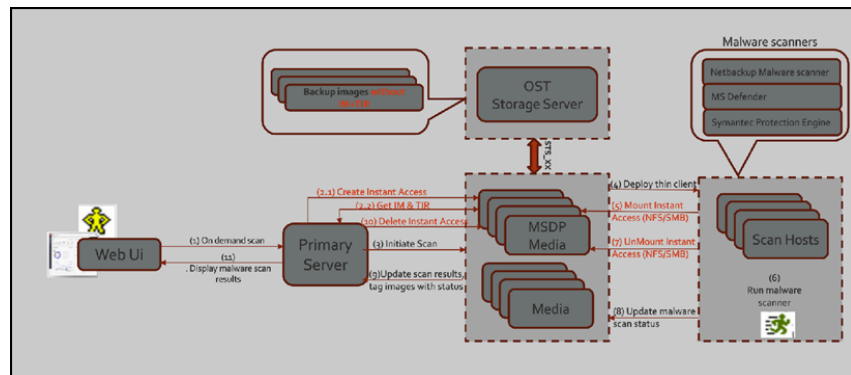
Refer to the following for more information:

AWS: [AWS Marketplace](#) and [NetBackup Marketplace Deployment on AWS Cloud](#)

Microsoft Azure: [Microsoft Azure Marketplace](#) and [Microsoft Azure Marketplace](#)

Malware scanning workflow for OST and AdvancedDisk

The following figure displays the workflow of malware scanning for OST and AdvancedDisk.



The following prerequisites exist for malware scanning of OST and AdvancedDisk:

- MSDP component for example, SPWS, VPFSD are required for an instant access mount. Hence for OST and AdvancedDisk storage, any one of the media servers must be configured as MSDP storage server so that it can serve the instant access API.
- Primary servers and media servers must be upgraded to NetBackup version 10.3.
- Media servers must be accessible to the OST or AdvancedDisk storage server.
- OST plug-in must be deployed on instant access (host with MSDP components) hosts. No new version of OST plug-ins is required.
- Compatible instant access host (RHEL).
- The throttling limit on concurrent instant access from OST and AdvancedDisk STU is same as instant access from MSDP.

For a complete list of supported OST devices, see the *NetBackup Software Compatibility List* or *NetBackup Hardware Compatibility List*.

The following steps depict the workflow for malware scanning for OST and AdvancedDisk.

1. Using the **On Demand Scan** APIs, the backup image is added to the worklist table on Primary server.

Primary server identifies the available scan host from the specified scan host pool.

2. As part of processing the work list:

(2.1) Create media server for instant access:

- From the backup images, it finds out the storage server.
- From the storage server it finds out the eligible media server.
Media server with instant access capability.
Media server with NetBackup version 10.3 or later.
- Sends the instant access API request to the selected media server.
- If multiple media servers are eligible for an instant access mount request, it selects the media server with minimum number of ongoing instant access requests. This way it can distribute the instant access requests and achieve the load balance.

(2.2) Get IM & TIR

- On the selected media server, in the context of instant access API, it fetches the IM and TIR information from the primary server. It stores the information in the same format that the OS requires for mounting the backup image by VPFSD.
- After instant access mount, for IO file, VPFSD uses OST API to read backup image from storage server.
- Update worklist with images for which instant access was performed with `mountId`, `exportPath`, `storageserver`, and `status`.

3. The primary server identifies the available MSDP media server and instructs the media server to initiate the malware scan.

Note: The media server that is selected for the instant access mount and the server that is selected for communication with the scan host can be the same server or a different server.

4. When it receives the **scan** request, the scan manager from the media server initiates the malware scan on the scan host using thin client (`nbmalwareutil`) through remote communication using SSH.
5. Depending on the configuration of scan host, from the scan host it mounts the export using either NFS or SMB from the media server. This media server is where the backup image is mounted using instant access API.
6. Scan is initiated using the malware tool that is configured in the scan host pool.

Note: VPFSD on the media server, uses STS_XXX APIs to open and read the backup images from the OST or AdvancedDisk storage server.

7. After the scan is completed, the scan host unmounts the export path from the media server where backup image is mounted using instant access API.
8. Malware scan status is updated to the media server over SSH. Scan logs are copied to the media server log directory.
9. Media server updates the scan status and the infected file list (if there are any infected files) to the primary server.
10. Primary server updates the scan results and deletes instant access request to the selected media.
11. Malware scan status notification is generated.

Configurations

Configuring scan host pool

Prerequisites for scan host pool

Scan host pool is a group of scan hosts. Scan host pool configurations must be performed from NetBackup Web UI before the scan host configuration is completed.

- All the scan host added in the scan host pool must have same malware tool as that of the scan host pool.
- All the scan host added in the pool must have same share type as that of scan host pool.
- To add scan host in a scan pool, credentials of scan host and RSA key are required. To get the RSA key of the scan host, See [“Managing credentials for malware scanning”](#) on page 327.

- Before performing the scan, ensure that the scan hosts are active and available in scan host pool.

Configuring a new scan host pool

- 1 On left, click **Detection and reporting > Malware detection**.
- 2 On the **Malware detection** page, select **Malware detection settings > Malware scanner host pools** on the top-right corner to go to host pool list page.
For configuration details, see the [NetBackup Security and Encryption Guide](#).
- 3 On the **Malware scanner host pools** page, click **Add** to add a new host pool.
- 4 On the **Add malware scanner host pools** page, enter the details such as **Host pool name**, **Malware scanner**, and **Type of share**.
- 5 Click **Save and add hosts**.

Add a new host in a scan host pool

Use this procedure to add a new scan host in the scan host pool configured.

Note: To configure a new scan host

- 1 On left, click **Detection and reporting > Malware detection**.
- 2 Click **Malware detection** page, click **Malware detection settings** on the top-right corner.
- 3 On the **Malware scanner host pools** page, select the desired scan host pool and click **Manage hosts** from the action menu.
- 4 On the **Manage malware scanner hosts** page, click **Add new**.
- 5 On the **Add malware scanner host** page, enter **Host name**.
- 6 Click on **Select existing credential** or **Add a new credential**. See [“Managing credentials for malware scanning”](#) on page 327.

- 7 Select media server to validate credentials.
- 8 Click **Save** to save the credentials.

Note: To validate the configuration later, See [“Validating the configuration”](#) on page 326.

Or

Click on **Save and validate configuration** simultaneously.

Note: By default three parallel scans are supported per scan host and this limit is configurable. Having more scan hosts in the scan pool will increase the number of parallel scans.

See [“Configure resource limits”](#) on page 328.

Managing scan host

Add an existing scan host

Use this procedure to add a same scan host in another scan host pool of same share type.

To configure an existing scan host

- 1 On left, click **Detection and reporting > Malware detection**.
- 2 On the **Malware detection** page, click **Malware detection settings** on the top right corner.
- 3 On the **Malware scanner host pools** page, select the desired scan host pool and click **Manage hosts** from the action menu.
- 4 On the **Manage malware scanner hosts** page, click **Add existing** to select pre-existing host.

Note: List includes all scan hosts from all scan host pools.

- 5 On the **Add existing malware scanner host** window, select the desired one or more scan hosts.
- 6 Click **Add**.

Validating the configuration

Use this procedure to validate the configuration for the newly added or existing scan host in the configured scan host pool.

- 1 On left, click **Detection and reporting > Malware detection**.
- 2 Click **Malware detection** page, click **Malware detection settings** on the top-right corner.
- 3 After adding a new scan host or an existing scan host, on the **Manage malware scanner hosts** page, select the desired scan host pool and click **Validate configuration** from the action menu.

Note: To add a new scan host, See [“Add a new host in a scan host pool”](#) on page 324.

To add an existing scan host, See [“Add an existing scan host”](#) on page 325.

- 4 On the **Validate configuration** page, enter the details to search and select an image to validate the configuration.
- 5 Select the backups to scan and click on **Validate configuration**.

Note: It is recommended to use backup image with small number of files. For large backups, IA creation may delay and test scan might fail.

- 6 After successful validation, click **Finish**.

The **Malware scanner host pools** page is displayed with the list of added scanner hosts.

Remove the scan host

- 1 On left, click **Detection and reporting > Malware detection**.
- 2 On the **Malware detection** page, click **Malware detection settings** on the top right corner.
- 3 On the **Malware scanner host pools** page, select the desired scan host pool and click **Manage hosts** from the action menu.
- 4 Select the desired host and click **Remove**, to remove scan host from scan host pool.

Deactivate the scan host

- 1 On left, click **Detection and reporting > Malware detection**.
- 2 On the **Malware detection** page, click **Malware detection settings** on the top right corner.
- 3 On the **Malware scanner host pools** page, select the desired scan host pool and click **Manage hosts** from the action menu.
- 4 Select the desired host and click **Deactivate**.

Managing credentials for malware scanning

To add new credentials

- 1 On the **Manage credentials** page, select **Add new credentials** and click **Next**.
- 2 On the **Manage credentials** page, add the details such as **Credential name**, **tag**, **description**.
- 3 On the **Host credentials** tab, add **Host username**, **Host password**, **SSH port**, **RSA key**, and **Share type**.

- Run the following command to ensure that the SSH connection between MDSP media server and host is working:

```
ssh username@remote_host_name
```

- Run the following command to verify that it is listing the RSA key for remote scan host:

```
ssh-keyscan scan_host_name 2>/dev/null | grep ssh-rsa
```

- To obtain the RSA key for the scan host, use the following command from any Linux host with SSH connectivity to scan host (this could be the scan host itself):

```
ssh-keyscan scan_host_name 2>/dev/null | grep ssh-rsa | awk  
'{print $3}' | base64 -d | sha256sum
```

Note: Following host key algorithms are used to connect to scan host in the given order:

```
rsa-sha2-512, rsa-sha2-256, ssh-rsa
```

For example, the output is

```
33f697637ab3f0911c1d462d4bde8be3eec61a33403e8f6a88daecb415a31eef
```

- where the RSA key is

```
33f697637ab3f0911c1d462d4bde8be3eec61a33403e8f6a88daecb415a31eef
```

Note: Ensure that you remove the – character from RSA key when you copy.

- 4 For **SMB** share type, enter the following additional details:
 - **Active directory domain:** A domain to which storage server is connected (used to authenticate mounts on scan host).
 - **Active directory group:** A group name in active directory domain.
 - **Active directory user:** A user added in selected active directory group.
 - **Password**
- 5 Click **Save**.

To add existing credentials

- 1 On the **Manage credentials** page, select **Select existing credentials** and click **Next**.
- 2 On the **Select credentials** tab, select the desired credential and click **Save**.

To validate the scan host credentials

- 1 Once the credentials are provided for scan host on the **Add malware scanner host** page, search and select the Media server to enable the **Validate credential** button.

Note: Only SSH credentials are validated by connecting to scan host from the selected media server. Media server must be Linux media server with NetBackup version 10.3 or above.

- 2 On successful validation of credentials, click **Save**.

Configure resource limits

To configure resource limits

- 1 On left, click **Detection and reporting > Malware detection**.
- 2 On the top right, click **Malware detection settings > Resource limits**.
For configuration details, see the *NetBackup Security and Encryption Guide*.
- 3 Click **Edit** to edit the resource limit of the resource type.

- 4 Set the global limit which would be considered when resource limit is not set for a resource type.

Or, click **Add** to override the global setting.

- 5 Enter the new host name and set the limits.

Note: Resource type scan host: Number of scans per scan host. Default: 3, Minimum: 1, Maximum: 10

Resource type storage server: Number of scans per storage server. Default: 20, Minimum: 1, Maximum: 50

- 6 Click **Save**.

Caution: Setting the Instant Access limit to large value would lead to Storage server resources (memory, CPU, disk) being used for malware scanning purpose. It is advised to set the value based on the existing load on storage server due to backup/duplication operations.

Note: For NetBackup version 10.2 and later, global parallel scans limit configured through **MALWARE_DETECTION_JOBS_PER_SCAN_HOST** configuration option is not applicable. Configure the global parallel scans limit using the Web UI.

Perform a malware scan

To perform a malware scan

- 1 On left, click **Detection and reporting > Malware detection**.
- 2 On the **Malware detection** page, click **Scan for malware**.
- 3 In the **Search by** option, select one of the following:
 - **Backup images**
 - **Assets by policy type**
 - **Assets by workload type**

Note: NetBackup supports VMware assets for malware scan of backup images only with MSDP.

For more information on the options for scanning, refer to the following on-demand scan:

- See “Backup images” on page 331.
- See “Assets by policy type” on page 333.
- See “Assets by workload type” on page 335.

Following steps are applicable for scanning **Assets by policy type** and **Assets by workload type**.

- 4 From the **Client/Asset** table, select a Client/Asset to scan.
- 5 Click **Next**.

Note: (Applicable only if **Search by** option is selected as **Assets by policy type**) If the selected client in the previous step supports multiple policy types, then user has an option of selecting a single policy type for scanning.

- 6 For the **Start date/time** and **End date/time** verify the date and the time range or update it.

Note: According to selection criterion, scan gets initiated to maximum of 100 images.

- 7 In the **Scanner host pool**, **Select** the appropriate host pool name.
- 8 (Applicable only for the **NAS-Data-Protection** policy type) In the **Volume** field, **Select volume** backed up for NAS devices.

Volume-level filtering only fetches the top-level directories of the NAS-Data-Protection volume backup. Volume-level filtering is applicable only if the top-level directory is a volume. In such a case, you can select individual backup images with the **Backup images** option in the **Search by** option.

- 9 From the **Current status of malware scan**, select one of the following:
 - **Not scanned**
 - **Not infected**
 - **Infected**
 - **All**

10 Click **Scan for malware**.

There are more than 100 images in your search. Unable to scan more than 100 images. Adjust the date range and try again.

11 After the scan is initiated, the **Malware Scan Progress** is displayed. Following are the status fields:

- **Not scanned**
- **Not infected**
- **Infected**
- **Failed**

Note: When we hover on failed status, the tool tip displays the reason for failed scan.

The backup images which failed in validation, are ignored. Malware scanning is supported for the backup images that are stored on storage with instant access capability for the supported policy type only.

- **Pending**
- **In progress**

Backup images

This section describes the procedure for scanning policy of client backup images for malware.

To scan a policy client backup images for malware

- 1** On left, click **Detection and reporting > Malware detection**.
- 2** On the **Malware detection** page, click **Scan for malware**.
- 3** In the **Search by** option, select **Backup images**.
- 4** In the search criteria, review and edit the following:
 - **Policy name**
Only supported policy types are listed.
 - **Client name**
Displays the clients that have backup images for a supported policy type.
 - **Policy type**
 - **Type of backup**

Any incremental backup images that do not have the NetBackup Accelerator feature enabled are not supported for the VMware workload.

- **Copies**

If the selected copy does not support instant access, then the backup image is skipped for the malware scan.

(For *NAS-Data-Protection* policy type) Select the **Copies** as **Copy 2**.

- **Disk pool**

MSDP (PureDisk), OST (DataDomain) and AdvancedDisk storage type disk pools are listed.

- **Disk type**

MSDP (PureDisk), OST (DataDomain) and AdvancedDisk disk types are listed.

- **Malware scan status.**

- For the **Select the timeframe of backups**, verify the date and the time range or update it.

5 Click **Search**.

Select the search criteria and ensure that the selected scan host is active and available.

6 From the **Select the backups to scan** table select one or more images for scan.

7 In the **Select a malware scanner host pool**, **Select** the appropriate host pool name.

Note: Scan host from the selected scan host pool must be able to access the instant access mount created on storage server which is configured with NFS/SMB share type.

8 Click **Scan for malware**.

9 After the scan is initiated, the **Malware Scan Progress** is displayed.

The following are the status fields:

- **Not scanned**
- **Not infected**
- **Infected**
- **Failed**

Hover over the status to view the reason for the failed scan.

Note: Any backup images that fail validation are ignored. Malware scanning is supported for the backup images that are stored on storage with instant access capability and for the supported policy types only.

- **In progress**
- **Pending**

Note: You can cancel the malware scan for one or more in progress and pending jobs.

Assets by policy type

NetBackup supports MS-Windows, NAS-Data-Protection, and Standard policy types for malware scan. The following section describes the procedure for scanning NAS-Data-Protection backup images for malware.

NAS-Data-Protection

Each NAS volume or share is read over NFS or SMB, and backed up using a configured number of backup streams. The maximum number of streams per volume determines the number of backup streams that are created to back up each volume. For example, consider a policy that contains 10 volumes and the maximum number of streams is 4. The backup of the policy creates 4 backup streams for each volume, with a total of 40 child backup streams and 10 parent backup streams.

Note: The number of scans depends on the number of batches that were created to perform the scan. Only the parent stream backup image is visible on the Malware detection UI.

For more information on multi stream backups, refer to *NetBackup NAS Administrator's Guide*.

- 1** On left, click **Detection and reporting > Malware detection**.
- 2** On the **Malware detection** page, click **Scan for malware**.
- 3** In the **Search by** option, select **Assets by policy type**.
- 4** From the **Client/Asset** table, select a Client/Asset to scan.
- 5** Click **Next**.

If the selected client in the previous step supports multiple policy types, you can select a single policy type for scanning.

- 6 For the **Start date/time** and **End date/time** verify the date and the time range or update it.

The scan is initiated for a maximum of 100 images.

- 7 In the **Scanner host pool**, **Select** the appropriate host pool name.
- 8 In the **Volume** field, **Select volume** backed up for NAS devices.

Note: Volume level filtering only fetches top-level directories of the NAS-Data-Protection volume backup. Volume level filtering is applicable only if the top-level directory is a volume. In such case, user has the option to select individual backup images by using the **Backup images** option in the **Search by** option.

- 9 From the **Current status of malware scan**, select one of the following:

- **Not scanned**
- **Not infected**
- **Infected**
- **All**

- 10 Click **Scan for malware**.

Warning: There are more than 100 images in your search. Unable to scan more than 100 images. Adjust the date range and try again.

- 11 After the scan is initiated, the **Malware Scan Progress** is displayed. The following are the status fields:

- **Not scanned**
- **Not infected**
- **Infected**
- **Failed**

Note: Hover over the status to view the reason for the failed scan.

Any backup images that fail validation are ignored. Malware scanning is supported for the backup images that are stored on storage with instant access capability and for the supported policy types only.

- **Pending**
- **In progress**

More information is available on the malware scan status.

See [“View the malware scan status”](#) on page 336.

Note: For NAS-Data-Protection any backup images that were created on the previous version of NetBackup 10.3 media server, you must select the **Malware scan status** option as **All**.

Assets by workload type

This section describes the procedure for scanning VMware, Universal share, and Cloud VM assets for malware.

Ensure that you meet the following prerequisites:

- The backups were performed with a storage server at NetBackup 10.1 or later.
- Backup images are stored on MSDP storage only with instant access capability, for the supported policy type only.
- The last backup must be successful.
- You must have an RBAC role with permissions to perform malware scans.

To scan the supported assets for malware, perform the following:

- 1** On left, select the supported workload under **Workloads**.
- 2** Select the resource which has backups completed (for example, VMware/Cloud VM, Universal share and so on).
- 3** Select **Actions > Scan for malware**.
- 4** On the **Malware scan** page, perform the following:
 - Select the date range for the scan by selecting **Start date/time** and **End date/time**.
 - Select **Scanner host pool**
 - From the **Select current status of malware scan** list select one of the following:
 - **Not scanned**
 - **Not infected**
 - **Infected**

- All

5 Click **Scan for malware**.

Note: The malware scanner host can initiate a scan of three images at the same time.

6 After the scan starts, you can see the **Malware Scan Progress** on **Malware Detection**, the following fields are visible:

- Not scanned
- Not infected
- Infected
- Failed

Note: Any backup images that fail validation are ignored.

- In progress
- Pending

Managing scan tasks

View the malware scan status

To view the malware scan status

- ◆ On the left, click **Detection and reporting > Malware detection**.

The following columns are displayed:

- Client - Name of the NetBackup client where the malware is detected.
- Backup time - Time when the backup was performed.
- Scan status - The scan status of the backup image. The different statuses are infected, not infected, failed, in progress, pending, canceled, and cancellation in progress.
- Files infected - Indicates the number of files that were found infected during the scan.
- Scan progress - Indicates the percentage of scan completed.

- **Total files** - Indicates the count of files and folders as recorded in the catalog for the backup image (list of backup images in case of DNAS). For recovery time scan, the **Total files** column would only indicate the count of files selected for recovery.
- **% infected** - Provides the percentage of infected files as compared to **Total files**.

Note: Skipped files during recovery are considered as **Not-infected**.

- **Elapsed time** - Represents the time since scan request was accepted (Date of scan) till the time of completion of scan (End date of Scan). The elapsed time would consist of idle time, time spent in pending state. For resume of failed jobs it would include time spent from failure till the time when the resume operation was triggered.
- **Scanned files** - Indicates the number of files that are scanned.
- **Schedule type** - The backup type of the associated backup job
- **Date of scan** - Date when the scan was performed.
- **Policy type** - Type of the policy that was selected for scanning.
- **Policy name** - Name of the policy that was used for scanning.
- **Malware scanner** - Name of the malware scanner that was used for scanning.
- **Scanner host pool** - Indicates the host pool used for malware scanning.
- **Malware scanner version** - Version of the malware scanner that was used for scanning.

Note:

Actions for malware scanned images

Once you scan the backup images for malware detection, a tabular data is available on the **Malware detection** home page. See "[View the malware scan status](#)" on page 336.

For each backup image, the following quick configuration are available:

Expire all copies

- 1 On the left, select **Detection and reporting > Malware detection**.
- 2 For the desired scan result, from the right, select **Expire all copies**.
- 3 Confirm to expire all the copies of the selected backup image.

Note: This option is available only for infected scan results.

View infected files

- 1 On the left, select **Detection and reporting > Malware detection**.
- 2 For the desired scan result, select **View infected files**.

Note: This option is available only for infected scan results and scan type 'Recovery'.

- 3 In the **Infected files** table, search or the desired file, if needed.
- 4 If needed, click **Export list**.

Note: A list of infected files from the selected malware scanning result is exported in `.csv` format. The file name is of following format:

`backupid_infected_files_timestamp.csv`

Export infected files list

- 1 On the left, select **Detection and reporting > Malware detection**.
- 2 For the desired malware affected , from the right, select **Export Infected files list**.

Note: `.csv` file contains backup time and names of the infected files.

Cancel malware scan

- 1 On the left, select **Detection and reporting > Malware detection**.
- 2 For desired scan result, from actions menu, click **Cancel malware scan**.

Note: You can cancel the malware scan only from in progress and pending states.

- 3 Click **Cancel scan** to confirm.

Note: The status changes to Cancellation in progress.

Note: The **Cancel malware scan** is not supported for scan results with scan type 'Recovery'.

Rescan image

- 1 On the left, select **Detection and reporting > Malware detection**.
- 2 For desired scan result, from actions menu, click **Rescan image**.
- 3 Click **Rescan** to confirm.
- 4 In case of bulk rescan, when you select one or more image with different or empty scanner host pool, you need to select a new scanner host pool.
 - Click **Rescan image**
 - From the **Select a malware scanner host pool** pop-up select a new scan host pool.

Note: New scan host pool is applicable for all the selected images for this rescan.

- Click **Rescan** to confirm.
Rescan (and resume) is not supported for scan results with scan type recovery.
- 5 In case of rescan of failed/cancelled jobs, scanning would be triggered from the point of failure (resumed) instead of complete scan under the following conditions:

- If the value of **Date of scan** is more than 48 hours, then the job would not be resumed and full scan would be initiated. This is to ensure that malware signatures used for scan does not differ significantly.
- Supported for Standard/MS-Windows backup images which has large number of files (>500k) or more than one stream in case of DNAS.
- Instant Access must have succeeded for the failed job.
- Resume would identify first IA capable copy to scan, which can be different from the copy selected for the initial scan request.

Once resumed existing scan result would be moved from failed to pending and subsequently to in-progress state. And progress update could continue from the point of failure. In case of complete rescan new scan result would be displayed. If user needs to perform a complete scan, then it can be triggered using on demand scan options.

Delete scan results

- 1 On the left, select **Detection and reporting > Malware detection**.
- 2 For scan results which are in failed or cancelled state can be deleted manually from UI by clicking the **Delete scan results** option from the actions menu.
- 3 Click **Yes** to confirm the deletion of the selected scan results.

Note: In one go a maximum of 20 scan results can be selected for deletion.

View details

- 1 On the left, select **Detection and reporting > Malware detection**.
- 2 Details for backup images with individual batch level can be viewed by clicking the **View details** option from the actions menu.

Note: The **View details** option is available only for scan results which are in failed or in progress state.

- 3 On the **View details** page, from the action menu, you can **Copy failure details** or **Copy the scan results** to the clipboard.
- 4 Click **Close**.

Recover from malware-affected images (clients protected by policies)

To restore from malware-affected images, you must have the Administrator role or equivalent RBAC permissions. To recover a VMware asset that is affected by malware, see the following topic.

See [“Recover from malware-affected images \(clients protected by protection plan\)”](#) on page 342.

To recover from malware-affected images (clients protected by policies)

- 1
- On the left, click **Recovery**.
- 2
- Under **Regular recovery**, click **Start recovery**.
- 3
- Select the following properties:

Source client	The client that performed the backup.
Destination client	The client to which you want to restore the backup.
Policy type	The type of policy that is associated with the backup you want to restore.
Restore type	The type of restore that you want to perform. The restore types that are available depend on the policy type that you choose.

- 4
- Click **Next**.
- 5
- Select the **Start date** and **End date**.

Or, click **Backup history** to view and select specific images. Click **Select** to add the selected images for recovery.

Note: The table displays all the backup image details for selected time frame. You can filter and sort the images based on the malware scan results, schedule type, policy type or policy name.

- 6
- To include any malware-infected images in the recovery, select **Allow the selection of images that are malware-affected**.

Note: The **Allow the selection of images that are malware-affected** option will be disabled if user selects **Scan for malware before recovery** option.

- 7
- On the left, expand the **Source client** directory. Select any directories that you want to restore. Or in the right pane, select any files or directories. Click **Next**.

- 8 Select the recovery target.
- 9 To restore any files that are malware-infected, click **Allow recovery of files infected by malware**. Otherwise, NetBackup only restores the files that are scanned and free from malware.
- 10 Select any other recovery options that you want. Then click **Next**.
- 11 Review the recovery settings and then click **Start recovery**.

Recover from malware-affected images (clients protected by protection plan)

To restore from malware-affected recovery points, you must have the Administrator role or equivalent RBAC permissions. To recover a specific recovery point that is affected by malware, see the following topic :

See [“Recover from malware-affected images \(clients protected by policies\)”](#) on page 341.

To recover from malware-affected images for clients protected by protection plan

- 1 On left pane select the supported **Workload**.
- 2 Locate the protected resource and click **Actions > Recover**.
- 3 On the **Recovery points** tab you can see **Malware scan** status of each recovery point, as follows:
 - **Not scanned**
 - **Not infected**
 - **Infected**
- 4 Select the recovery point.
- 5 Select **Allow the selection of recovery points that are malware-affected**. This option only displays if there are recovery points that contain malware-affected images.

Note: To restore from malware-affected recovery points, you must have the Administrator role or equivalent RBAC permissions.

- 6 Click **Recover** and select the type of recovery. Then follow the prompts.
For more details on recovering a VM, see the *NetBackup Web UI VMware Administrator's Guide*.

Single file restore

To restore from malware-affected images, you must have the Administrator role or equivalent RBAC permissions.

To recover a VMware asset that is affected by malware, refer to the following procedure:

VMware single file restore from recovery point (with agent and agentless)

- 1 On left pane select **Workload > VMware**.
- 2 Search and click on the virtual machine to be recovered.
- 3 On the **Recovery points** tab, select the date for recovery point.
- 4 Select **Allow the selection of recovery points that are malware-affected**. This option only displays if there are recovery points that contain malware-affected images.

Note: To restore from malware-affected recovery points, you must have the Administrator role or equivalent RBAC permissions.

- 5 Click **Recover** and select the type of recovery as **Restore files and folders**. Then follow the prompts.

Note: NetBackup now provides support for VMware single file restore clean recovery by selecting the **Allow recovery of files infected by malware** option in the **Recovery options**.

For more details on recovering a VM, see the *NetBackup Web UI VMware Administrator's Guide*.

To recover a specific recovery point that is affected by malware, refer to the following procedure:

Single file restore using recovery flow (with agent)

- 1 On the left, click **Recovery**.
- 2 Under **Regular recovery**, click **Start recovery**.

3 Select the following properties:

Source client	The client that performed the backup. Under the Virtual machines search tab, select the virtual machine and click Apply .
Destination client	The client to which you want to restore the backup.
Policy type	The type of policy that is associated with the backup you want to restore.
Restore type	The type of restore that you want to perform. The restore types that are available depend on the policy type that you choose.

4 Click **Next**.

5 Edit the **Date range**.

Or, click **Use backup history** to view and select specific images. Click **Apply** to add the selected images for recovery.

Note: The table displays all the backup image details for selected time frame. You can filter and sort the images based on the malware scan results, schedule type, policy type or policy name.

6 To include any malware-infected images in the recovery, select **Allow the selection of images that are malware-affected**.

7 On the left, expand the **Source client** directory. Select any directories that you want to restore. Or in the right pane, select any files or directories. Click **Next**.

8 Select the recovery target.

9 To restore any files that are malware-infected, click **Allow recovery of files infected by malware**. Otherwise, NetBackup only restores the files that are scanned and free from malware.

10 Select any other recovery options that you want. Then click **Next**.

11 Review the recovery settings and then click **Start recovery**.

Detecting anomalies

This chapter includes the following topics:

- [About backup anomaly detection](#)
- [Configure backup anomaly detection settings](#)
- [View backup anomalies](#)
- [About system anomaly detection](#)
- [Configure system anomaly detection settings](#)
- [View system anomalies](#)

About backup anomaly detection

NetBackup can now detect anomalies in backup metadata. It can detect any unusual job data in the data backup flow. For example, it can detect a file count or a file size that is different than the usual count or size.

Note: By default, the anomaly detection algorithm runs on the NetBackup primary server. If you see any impact on the primary server because of the anomaly detection process, you can configure a media server to detect anomalies.

The following backup job metadata, attributes, or features are verified during backup anomaly detection:

- Backup image size
- Number of backup files
- Data that is transferred in KB
- Deduplication rate

■ Backup job completion time

Any unusual deviation in these backup job attributes is considered to be an anomaly and is notified using the NetBackup web UI.

Workflow of backup anomaly detection and notification

The workflow of the backup anomaly detection and notification is as follows:

Table 35-1 Workflow

Step	Description
Step 1	Install or upgrade NetBackup software on the primary server and the media server. See the NetBackup Installation or Upgrade Guide .
Step 2	Enable the primary server to detect backup anomalies. By default, the anomaly detection algorithm runs on the NetBackup primary server. If you see any impact on the primary server because of the anomaly detection process, you can configure a media server to detect anomalies. See the NetBackup Security and Encryption Guide .
Step 3	Configure anomaly detection settings using the NetBackup web UI. See “ Configure backup anomaly detection settings ” on page 347.
Step 4	View the anomalies using the NetBackup web UI. See “ View backup anomalies ” on page 348.

How a backup anomaly is detected

Consider the following example:

In an organization, around 1 GB of data is backed up every day for a given client and backup policy with the schedule type FULL. On a particular day, 10 GB of data is backed up. This instance is captured as an image size anomaly and notified. The anomaly is detected because the current image size (10 GB) is much greater than the usual image size (1 GB).

Significant deviation in the metadata is termed as an anomaly based on its anomaly score.

An anomaly score is calculated based on how far the current data is from the cluster of similar observations of the data in the past. In this example, a cluster is of 1 GB of data backups. You can determine the severity of anomalies based on their scores.

For example:

Anomaly score of Anomaly_A = 7

Anomaly score of Anomaly_B = 2

Conclusion - Anomaly_A is severer than Anomaly_B

NetBackup takes anomaly detection configuration settings (default and advanced if available) into account during anomaly detection.

See the [NetBackup Security and Encryption Guide](#).

Configure backup anomaly detection settings

Once you enable anomaly detection, anomaly data gathering, detection service, and events are enabled. Basic and advanced backup anomaly detection settings are available to be configured.

See [“About backup anomaly detection”](#) on page 345.

To configure backup anomaly detection settings

- 1 On the left, click **Detection and reporting > Anomaly detection**.
- 2 On the top right, click **Anomaly detection settings > Backup anomaly detection settings**.
- 3 Click **Edit** on the right to configure the following **Anomaly detection > Enable anomaly detection activities** settings:
 - **Disable all**
 - **Enable anomaly data gathering**
 - **Enable anomaly data gathering and detection service**
 - **Enable anomaly data gathering and detection service and events**
- 4 Click **Save**.
- 5 Click **Edit** to modify the following **Basic Settings**:
 - **Anomaly detection sensitivity**
 - **Data retention settings**
 - **Data gathering settings**
 - **Anomaly proxy server settings**
- 6 Click **Save**.
- 7 Expand the **Advanced settings** section and click **Edit** to configure the following settings and click **Save**.
 - **Disable anomaly settings for clients**

- **Disable policy type or specific features for machine learning**

View backup anomalies

NetBackup can now detect anomalies in backup metadata. It can detect any unusual job data in the data backup flow. For example, it can detect a file count or a file size that is different than the usual count or size.

See [“About backup anomaly detection”](#) on page 345.

Note: Anomaly count of 0 indicates there are no anomalies generated or that the anomaly detection services are not running.

To view backup anomalies

- 1 On the left, select **Detection and reporting > Anomaly detection > Backup anomalies**.

The following columns are displayed:

- Job ID - Job ID of the job for which the anomaly is detected
- Client name - Name of the NetBackup client where the anomaly is detected
- Policy type - The policy type of the associated backup job
- Count - The number of anomalies that are detected for this job
- Score - Severity of the anomaly. The score is higher if the severity of the anomaly is more.
- Anomaly severity - Severity of the anomalies that are notified for this job
- Anomaly summary - Summary of the anomalies that are notified for this job
- Received - Date when the anomaly is notified
- Review status - Indicates whether the detected anomaly is reported as a false positive, an actual anomaly, or it can be ignored.
- Policy name - The policy name of the associated backup job
- Schedule name - The schedule name of the associated backup job

- Schedule type - The schedule type of the associated backup job
- 2** Expand a row to see the details of the selected anomaly.
- For each anomaly record, the current value of that feature and its actual range based on the past data are displayed.
- Consider the following example:
- An anomaly of the image size feature is displayed as 100MB (Usual 350MB, 450MB). This information implies that the current image size that is reported as anomaly is 100 MB. However, the usual image size range is 350 MB - 450 MB that is derived from the analysis of past data. Because of the significant difference between the current images size and usual image size range, NetBackup notifies it as an anomaly.
- 3** You can perform the following actions on the anomaly record:
- Click **Mark as ignore** when you can ignore the anomaly condition.
 The **Review status** of the anomaly record appears as *Ignore*.
 - Click **Confirm as anomaly** when you want to take some action on the anomaly condition.
 The **Review status** of the anomaly record appears as *Anomaly*.
 - Click **Report as false positive** if the anomaly is a false positive. Similar anomalies are not shown in the future.
 The **Review status** of the anomaly record appears as *False positive*.

About system anomaly detection

NetBackup can detect system anomalies during critical operations as follows:

- NetBackup clients that are offline under suspicious circumstances
 The 'Client offline' anomaly adds the ability to detect offline clients because of a compromised file system on a NetBackup host. Once the anomaly is detected, NetBackup generates a critical alert for the affected client.
- Any unusual manual NetBackup image expirations or expiry date modifications
 The 'Image expiration' anomaly detects unusual attempts that are made by privileged users to expire backup images. Once the anomaly is detected, NetBackup generates a critical alert and identifies the user.

See [“View system anomalies”](#) on page 351.

Configure system anomaly detection settings

Once you enable anomaly detection, anomaly data gathering, detection service, and events are enabled. Basic and advanced backup anomaly detection settings are available to be configured.

See [“About system anomaly detection”](#) on page 349.

To configure backup anomaly detection settings

- 1 On the left, click **Detection and reporting > Anomaly detection**.
- 2 On the top right, click **Anomaly detection settings > System anomaly detection configuration**.
- 3 On the **System anomaly detection configuration** screen, configure the following **System anomaly detection** settings:
 - Select the **Detect clients that are offline with suspicious error codes** check box to generate an anomaly alert when NetBackup detects that a client is offline under suspicious circumstances.
 - Select the **Detect anomalies for image expiration operations** check box to generate an anomaly when unusual activity occurs with image expiration.
- 4 Configure the following **Rules-based anomaly detection** setting:
 Select the **Detect anomalies using NetBackup anomaly detection rules** check box to list the predefined rules or the criteria for which you want to generate anomalies.

For example: Storage server is set to null STU, Clients removed from the policy, or Token deleted by user.

The following details each of the predefined rules are displayed:

- Rule name
- Description
- Severity
- Version
- Enabled

You need to download the rules that you want to use. Go to the Veritas Download Center to download the rules file (.zip) and store it on your local computer.

Note: NetBackup does not ship any standard rules by default.

Click **Upload rules** to select the rules file that you have downloaded. All the latest rules are listed in the **Rules-based anomaly detection** section.

- 5 Select the rules that you want to enable and for which you want to generate anomalies.

Click **Enable**.

NetBackup generates anomalies that meet the rule criteria.

View system anomalies

NetBackup can detect system anomalies. During a backup operation, NetBackup checks all the file extensions, compares them with the ransomware extension list, and generates an anomaly if there is a match. Anomaly is generated for each ransomware extension that is found in a particular backup. This anomaly detection is enabled by default for all policy types.

To view system anomalies

- 1 On the left, select **Detection and reporting > Anomaly detection > System anomalies**.

The following columns are displayed:

- Anomaly ID - ID of the anomaly record
- Anomaly type - Type of the anomaly
- Severity - Severity of the anomaly
- Description - Additional information about the anomaly
- Detected on - The date when the anomaly is detected
- Review status - Indicates whether the detected anomaly is reported as a false positive, an actual anomaly, or it can be ignored.

- 2 Expand a row to see the details of the selected anomaly.

- 3 You can perform the following actions on the anomaly record:

- Click **Mark as ignore** when you can ignore the anomaly condition.
- Click **Confirm as anomaly** when you want to take some action on the anomaly condition.
- Click **Report as false positive** if the anomaly is a false positive. Similar anomaly conditions are not reported in the future.

Usage reporting and capacity licensing

This chapter includes the following topics:

- [Track protected data size on your primary servers](#)
- [Add a local primary server](#)
- [Select license types to display in usage reporting](#)
- [Scheduling reports for capacity licensing](#)
- [Other configuration for incremental reporting](#)
- [Troubleshooting failures for usage reporting and incremental reporting](#)

Track protected data size on your primary servers

The Usage reporting application displays the primary servers that are configured for capacity licensing and their respective consumption details. This reporting provides the following benefits:

- Ability to plan for capacity licensing.
- On a weekly basis, NetBackup gathers and reports usage and trend information. The `nbdeployutil` utility has scheduled runs to gather data for the report (enabled by default).
- A link to the [Veritas NetInsights Console](#). The Usage Insights tool within the NetInsights Console tool NetBackup customers to proactively manage their license use through near real-time visibility of consumption patterns.
- Reporting is done for all policy types that are used for data protection.

Requirements

NetBackup automatically collects data for the usage reporting, provided the following requirements are met:

- The primary servers (or primary servers) are at NetBackup 8.1.2 or later.
- You use capacity licensing.
- You use automatic, scheduled reports. If you manually generate capacity license reports, the data does not display in the usage report in the NetBackup web UI.
- The following file exists:
UNIX: `/usr/opensv/var/global/incremental/Capacity_Trend.out`
Windows: `install_path\var\global\incremental\Capacity_Trend.out`
The **Usage** tab displays an error if the backup data is not available. Or, if the usage report is not generated (file does not exist).
- If you want one of your primary servers to gather usage reporting data for other remote primary servers, additional configuration is required. You must create a trust relationship between the primary servers. You must also add the local primary server (where you plan to run `nbdeployutil`) to the **Servers** list on each remote primary server.
See [“Add a local primary server”](#) on page 353.
See [“Add a trusted primary server”](#) on page 264.

Additional information

- Details are available on capacity licensing, scheduling, and options for capacity licensing reports.
See [“Scheduling reports for capacity licensing”](#) on page 354.
- *Veritas Usage Insights for NetBackup Getting Started Guide*. Details on how to use [Usage Insights](#) to manage your NetBackup deployment and licensing. This tool provides accurate, near real-time reporting for the total amount of data that is backed up.

Add a local primary server

If you want to add usage reporting information for a primary server but that server does not have an internet connection, you need to add the name of the local primary server to the servers list of the remote primary server. The local primary server is where you plan to run the usage reporting tool.

To add a local primary server

- 1 On the left, click **Hosts > Host Properties**.
- 2 Select the host and click **Connect**.
- 3 Click **Edit primary server**.
- 4 Click **Servers**.
- 5 On the **Additional Servers** tab, click **Add**.
- 6 Enter the name of the primary server where you plan to run `nbdeployutil`.
- 7 Click **Add**.

Select license types to display in usage reporting

You can select the license types for which you want to generate usage reports using the `netbackup_deployment_insights` utility.

Some license types cannot be configured with other types on a primary server. For example, you cannot select traditional licensing if you select any type of capacity licensing. For details, see the NetBackup Licensing Guide.

To select license types to display in usage reporting

- 1 On the left, click **Detection and reporting > Usage**.
- 2 On the top right, click **Usage reporting settings**.

License settings with the license type and license model are displayed for the primary server.

- 3 Click **Edit**.
- 4 Select the license types that you want to use. Then click **Save**.

Scheduling reports for capacity licensing

By default, NetBackup triggers `nbdeployutil` to run on a specified schedule to incrementally gather data and to generate licensing reports. For the first run, the duration of the report uses the frequency that is specified in the configuration file.

For capacity licensing, the report duration is always for the last 90 days based on the availability of the gathered data. Any data older than 90 days is not considered in the report. Each time `nbdeployutil` runs, it gathers information for the time between the latest run of `nbdeployutil` and the previous successful run.

Licensing report location

The current capacity licensing report resides in the following directory:

On Windows: `install_path\NetBackup\var\global\incremental`

On UNIX: `/usr/opensv/var/global/incremental`

It contains the following files:

- The generated report for the latest `nbdeployutil` result.
- Folders containing incrementally gathered data.
- The archive folder that contains the older generated reports.
- `nbdeployutil` log files.

The older reports are placed in the archive folder. Veritas recommends that you retain at least 90 days of reporting data. Data can be kept longer than 90 days, depending on the requirements of your environment. Older reports can help to show how the capacity usage has changed over time. Delete the reports or the folder when they are no longer required.

Use Case I: Using the default values for the licensing report

The `nbdeployutilconfig.txt` file is not required when you use the default parameters. `nbdeployutil` uses the following default values for capacity licensing:

- `FREQUENCY_IN_DAYS=7`
- `MASTER_SERVERS=local_server`
- `PARENTDIR=folder_name`
For Windows: `install_path\NetBackup\var\global\incremental`
For UNIX: `/usr/opensv/var/global/incremental`
- `PURGE_INTERVAL=120` (number of days)
- `MACHINE_TYPE_REQUERY_INTERVAL = 90` (number of days)

Use Case II: Using custom values for the licensing report

If the file `nbdeployutilconfig.txt` is not present, create a file using the following format:

```
[NBDEPLOYUTIL_INCREMENTAL]
MASTER_SERVERS=<server_names>
FREQUENCY_IN_DAYS=7
PARENTDIR=<folder_name_with_path>
PURGE_INTERVAL=120
MACHINE_TYPE_REQUERY_INTERVAL=90
```

To use custom values for the licensing report

- 1 Copy the `nbdeployutilconfig.txt` file to the following location:

For Windows: `install_path\NetBackup\var\global`

For UNIX: `/usr/opensv/var/global`

- 2 Open the `nbdeployutilconfig.txt` file.
- 3 Edit the `FREQUENCY_IN_DAYS` value to reflect how often you want the report to be created.

Default 7
(recommended)

Minimum 1

Parameter deleted `nbdeployutil` uses the default value.

- 4 Edit the `MASTER_SERVERS` value to include a comma-separated list of the primary servers you want to include in the report.

Note: Veritas Usage Insights requires that primary servers be at NetBackup 8.1.2 or later.

No value `nbdeployutil` uses the default value.

Parameter deleted `nbdeployutil` uses the default value.

For example:

- `MASTER_SERVERS=newserver, oldserver`
- `MASTER_SERVERS=newserver, oldserver.domain.com`
- `MASTER_SERVERS=myserver1.somedomain.com, newserver.domain.com`

- 5 Edit the `PARENTDIR` value to include the full path for location where the data is gathered and reported.

No value `nbdeployutil` uses the default value.

Parameter deleted `nbdeployutil` uses the default value.

- 6 Edit the `PURGE_INTERVAL` to indicate the interval (in days) for how often you want to delete the report data. Data that is older than 120 days is automatically purged.

Default	120
Minimum	90
No value	<code>nbdeployutil</code> uses the default value.
Parameter deleted	<code>nbdeployutil</code> uses the default value.

- 7 Edit the `MACHINE_TYPE_REQUERY_INTERVAL` to indicate how often to scan physical clients for updates to the machine type.

Default	90
Minimum	1
No value	<code>nbdeployutil</code> uses the default value.
Parameter deleted	<code>nbdeployutil</code> uses the default value.

Other configuration for incremental reporting

To change the directory of the gathered data and capacity licensing report

- 1 If you have older gathered data and licensing reports, copy the complete directory to the new location.
- 2 Edit `nbdeployutilconfig.txt` and change the location of the gathered data and licensing report in the `PARENTDIR=folder_name` field.

To use the data that was gathered previously to generate a capacity licensing report

- 1 Locate the folder that was generated for the gathered data after the previous run of `nbdeployutil` and copy it to the following location:

On Windows: `install_path\NetBackup\var\global\incremental`

On UNIX: `/usr/openv/var/global/incremental`

- 2 Create the `gather_end.json` file inside the copied folder and add the following text:

```
{"success":0}
```

The next incremental run considers the data inside the copied folder to generate a capacity licensing report.

Note: Delete any other gather folders inside the copied folder to avoid gaps for the period in which data is gathered. The missing data is automatically generated during the next incremental run.

To create a custom interval report using existing gathered data for capacity licensing

- ◆ To create a report for a time interval that is different than the default interval of 90 days, run the following command:

On Windows:

```
nbdeployutil.exe --capacity --incremental --report --inc-settings  
"install_dir\netbackup\var\global\nbdeployutilconfig.txt"  
--hoursago <custom-time-interval>
```

On UNIX:

```
nbdeployutil.exe --capacity --incremental --report --inc-settings  
"/usr/opensv/var/global/nbdeployutilconfig.txt"  
--hoursago <custom-time-interval>
```

The number of hours specified in `--hoursago` must be fewer than the `purge-interval` that is specified in the `nbdeployutilconfig.txt` file.

You can also use `--start` or `--end` options in the `nbdeployutilconfig.txt` file.

```
--start="mm/dd/yyyy HH:MM:SS"
```

```
--end="mm/dd/yyyy HH:MM:SS"
```

If the latest gather operation fails to retrieve front-end data size (FEDS) data, the custom report fails because the required backup information is not available. Let the next scheduled incremental gather run successfully and then try to generate the custom report.

Note: `nbdeployutil` uses existing gathered data to generate the custom interval report. You are not required to use the `--gather` option.

Troubleshooting failures for usage reporting and incremental reporting

- For incremental runs of `nbdeployutil`, notifications are sent to the NetBackup web UI. The notification details include, status of the run, duration, start time, and end time.

- `nbdeployutil` fails to gather data and generate the report for your environment. Refer to the logs to understand when the task failed and the reason for the failure.
- `nbdeployutil` fails with a `bpimagelist` error with status 37 after you run the utility manually. Ensure that you added the primary servers to the additional servers list.
See [“Add a local primary server”](#) on page 353.
- The following error displays because of internal web service communication failures:
Internal Web API error occurred for primary server *SERVER_NAME*. Run `nbdeployutil` again with the gather option on primary server *SERVER_NAME*.
- For VMware or NDMP, when the backup agent fails to post licensing information to the database, a status code 5930 or 26 displays in the Activity Monitor: For more information, see the [NetBackup Status Codes Reference Guide](#).
- `nbdeployutil` may fail with errors related to loading the Perl modules. In such a scenario, it is recommended to refer the Perl documentation related to the reported error.

You can use `netbackup_deployment_insights` with the same troubleshooting points.

NetBackup workloads and NetBackup Flex Scale

- [Chapter 37. NetBackup SaaS Protection](#)
- [Chapter 38. NetBackup Flex Scale](#)
- [Chapter 39. NetBackup workloads](#)

NetBackup SaaS Protection

This chapter includes the following topics:

- [Overview of NetBackup for SaaS](#)
- [Adding NetBackup SaaS Protection Hubs](#)
- [Configuring the autodiscovery frequency](#)
- [Viewing asset details](#)
- [Configuring permissions](#)
- [Troubleshooting SaaS workload issues](#)

Overview of NetBackup for SaaS

The NetBackup web UI provides the capability to view the assets of NetBackup SaaS Protection. The assets configured to protect SaaS applications data are automatically discovered in the NetBackup web UI.

The NetBackup SaaS Protection assets comprise of the assets such as, Hubs, StorSites, Stors, and Services.

The following assets details are displayed:

- Storage size
- Storage tier details
- Number of items in the storage
- WORM details
- Write, delete, stub policies details

- Schedule for the next backup
- Status of the last backup

The NetBackup web UI lets you perform the following operations:

- Add a NetBackup SaaS Protection Hub.
- View assets in the Hub.
- Launch the NetBackup SaaS Protection web UI.
- Delete the added Hub.

Note: If a SaaS asset is deleted from NetBackup SaaS Protection web UI, the deleted asset is not removed from the NetBackup database immediately. The deleted asset remains in the NetBackup database for 30 days.

The following table describes the features of NetBackup for SaaS:

Table 37-1 Features of NetBackup for SaaS

Features	Description
Integration with NetBackup role-based access control (RBAC)	The NetBackup web UI provides RBAC roles, which enable its users to view assets in SaaS workload. The user does not need to be a NetBackup administrator to add a NetBackup SaaS Protection Hub or view assets in the Hub.
NetBackup SaaS Protection-specific credentials	NetBackup SaaS Protection service accounts are used to authenticate the Hubs.
Autodiscovery of assets	NetBackup automatically discovers StorSites, Stors, and Services in the Hubs. You can also perform manual discovery. After the assets are discovered, you can view assets details.
Cross Launch	You can cross launch the NetBackup SaaS Protection web UI. If SSO is configured the user is redirected to the NetBackup SaaS Protection UI without entering the credentials for each login.

About NetBackup SaaS Protection

NetBackup SaaS Protection is a cloud-based data protection solution that is deployed on Microsoft Azure. It is used to protect the data of the on-premises application and SaaS applications.

NetBackup SaaS Protection protects data of the following SaaS applications:

- Box
- Exchange
- Google Drive
- SharePoint sites
- OneDrive sites
- Teams sites and chats
- Slack

NetBackup SaaS Protection supports bulk or granular data restore at the required locations. It also supports restore of the last updated data or any specific point-in-time data.

An account is configured for a customer, which is referred to as a tenant. The assets are configured for the tenant to protect the required data.

For more information, refer to the NetBackup SaaS Protection administrator's guide.

Adding NetBackup SaaS Protection Hubs

You can add NetBackup SaaS Protection Hubs and autodiscover all the assets inside the Hub.

To add NetBackup SaaS Protection Hubs

- 1 On the left, click **Workloads > SaaS**.
- 2 On the **Hubs** tab, click **Add**.
- 3 On the **Add a NetBackup SaaS Protection Hub** page, enter the name of the Hub.
 - To use the existing credential, click **Select existing credentials**.
On the next page, select the required credentials, and click **Select**.
 - To create a new credential, click **Add a new credential**.
On the **Add credential** page, enter the following:
 - **Credentials name**: Enter a name for the credential.
 - **Tag**: Enter a tag to associate with the credential.
 - **Description**: Enter a description of the credential.
 - **Username**: Enter the username, which is configured as a service account in NetBackup SaaS Protection.

- **Password:** Enter the password.
- 4 Click **Add**.
After the credentials are successfully validated, the Hub is added and autodiscovery runs to discover available assets in the Hub.
See [“Configure NetBackup for single sign-on \(SSO\)”](#) on page 282.

Configuring the autodiscovery frequency

Autodiscovery keeps a count of the assets in Hubs. NetBackup web UI refreshes Hubs at intervals to get the updates from NetBackup SaaS Protection for any addition or removal of assets. By default, the interval for refresh is 8 hours.

To configure the autodiscovery frequency

- 1 On the left, click **Workloads > SaaS**.
- 2 On the top-right, click **SaaS settings > Autodiscovery**.
- 3 Click **Edit**.
- 4 Enter the number of hours after which NetBackup should run autodiscovery and click **Save**.

Proxy configuration for autodiscovery

To discover SaaS applications of NetBackup SaaS Protection, you are required to connect the primary server to the NetBackup SaaS Protection server. Direct internet traffic from the primary server must be open, otherwise the discovery fails. To allow discovery of NetBackup SaaS Protection assets, configure a proxy server to reroute the traffic. The discovery plug-in supports proxy server types HTTP and SOCKS.

Configuring the proxy setting on primary server using the bpsetconfig utility

To configure the proxy setting on primary server using the bpsetconfig utility

- 1 Open a command prompt in primary server.
- 2 Change the directory to the following path:
 - For Windows: **C:\Program Files\Veritas\NetBackup\bin\ admincmd**

- For Linux: `/usr/opensv/netbackup/bin/admincmd/`

3 Execute the `bpsetconfig` command and provide the following proxy details.

```
bpsetconfig> SAAS_PROXY_HOST = X.X.X.X
bpsetconfig> SAAS_PROXY_PORT = 3128
bpsetconfig> SAAS_PROXY_TYPE = HTTP
bpsetconfig> SAAS_PROXY_TUNELLING = 1
```

The following are the proxy configuration keys:

Table 37-2 Proxy configuration keys

Proxy configuration keys	Supported values
SAAS_PROXY_TYPE	HTTP, SOCKS, SOCKS4, SOCKS4A, SOCKS5
SAAS_PROXY_HOST	IP address or FQDN of the proxy host
SAAS_PROXY_TUNNELING	0 or 1
SAAS_PROXY_PORT	Any valid port (1- 65535). The default port is 3128.

Viewing asset details

The NetBackup SaaS Protection assets are displayed in two tabs, **Services** tab and **Hubs** tab.

To view asset details

1 On the left, click **Workloads > SaaS**.

The **Services** tab is displayed. It displays the services configured for the Hub.

You can perform the following actions on the tab:

- View the list of services configured for the Hub.
- Search the required service in the list of services.
- Filter the list of services based on the status of the services.
- Sort columns.
- View the following service details:
 - Application type for which the service is configured.
 - Date and time of the last backup and the next scheduled backup.

- Criteria set for write, stub, and delete policy.
- WORM details.

2 Click the **Hubs** tab to view details on Hubs, StorSites, and Stors.

You can navigate to the required asset using the left panel. You can perform the following actions on the **Hubs** tab:

- View a list of the Hubs.
- Search for a Hub in the list.
- Add new Hubs.
- Validate the credentials.
- Sort columns.
- Click **Actions** to perform the following:
 - Edit credentials.
 - Delete the Hub.
 - Manually discover assets in the Hub.
- View the following asset details:
 - Associated Stors, last backup details, and so on for the Services.
 - Version, ID, and state of the Hub.
 - State, tier details, and so on for the StorSite.
 - State, policy details, and so on for the Stors.
 - Launch the NetBackup SaaS Protection web UI. You can cross launch the NetBackup SaaS Protection web UI from Services, Stors, and Hubs page.

For more information, refer to the NetBackup SaaS Protection administrator's guide.

Configuring permissions

Using the NetBackup web UI, you can assign different access privileges to the user roles on the assets. For example, view, update, delete, and manage access.

See [“Manage access permission”](#) on page 311.

Note: The user with access permission on the SaaS workload in NetBackup, and no or limited permissions in NetBackup SaaS Protection can still view the NetBackup SaaS Protection assets on the NetBackup web UI.

Troubleshooting SaaS workload issues

Check the following locations for logs of the SaaS workload:

- PiSaaS
 - Windows: <install path>\Veritas\NetBackup\logs\ncfnbcs
 - UNIX: <install path>/openv/netbackup/logs/ncfnbcs
- bpVMUtil
 - Windows: <install path>\Veritas\NetBackup\logs\bpVMutil
 - UNIX: <install path>/openv/netbackup/logs/bpVMutil
- APIs/nbWebServices
 - Windows: <install path>\Veritas\NetBackup\logs\nbweb service
 - UNIX: <install path>/openv/logs/nbweb service

Use the following information to troubleshoot issues.

Table 37-3 Troubleshooting issues in SaaS Workload

Problems	Recommended actions
Failed to add a Hub due to incorrect Hub name or invalid user credentials.	Enter appropriate Hub name and valid credentials.
Failed to add a Hub due to issue in credential validation.	Check if the credentials are not expired. Also check if the credentials are valid.
Failed to add a Hub due to limited permissions.	Assign appropriate permissions to the user on the SaaS workload. See “Role permissions” on page 310.
Failed to delete a Hub due to limited permissions.	Assign appropriate permissions to the user on the SaaS workload. See “Role permissions” on page 310.

Table 37-3 Troubleshooting issues in SaaS Workload (*continued*)

Problems	Recommended actions
Failed to perform discovery on the Hub due to limited permissions.	Assign appropriate permissions to the user on the SaaS workload. See "Role permissions" on page 310.
The services are not deleted from NetBackup after deleted the associated Connector from NetBackup SaaS Protection.	The services get removed from NetBackup after 30 days from Connector deletion.
Failed to launch the NetBackup SaaS Protection web UI using the Launch NSP option. Credentials are required while launching the NetBackup SaaS Protection web UI.	Check if SSO is configured correctly. If SSO is configured correctly, check if the user has appropriate permissions to access the NetBackup SaaS Protection web UI. See "Configure NetBackup for single sign-on (SSO)" on page 282.
Connecting to the proxy host X.X.X.X on port 3128 with type SOCKS5	Configure proxy settings on the primary server using the bpsetconfig utility.

NetBackup Flex Scale

This chapter includes the following topics:

- [Managing NetBackup Flex Scale](#)

Managing NetBackup Flex Scale

The NetBackup Flex Scale appliance administrator can access Cluster Management in the NetBackup web UI. The Appliance administrator must be assigned the RBAC **Administrator** role for the NetBackup web UI.

For full instructions on managing NetBackup Flex Scale, see the following resources.

NetBackup Flex Scale Installation and Configuration Guide

NetBackup Flex Scale administrator's guide

Table 38-1 Accessing NetBackup Flex Scale and NetBackup

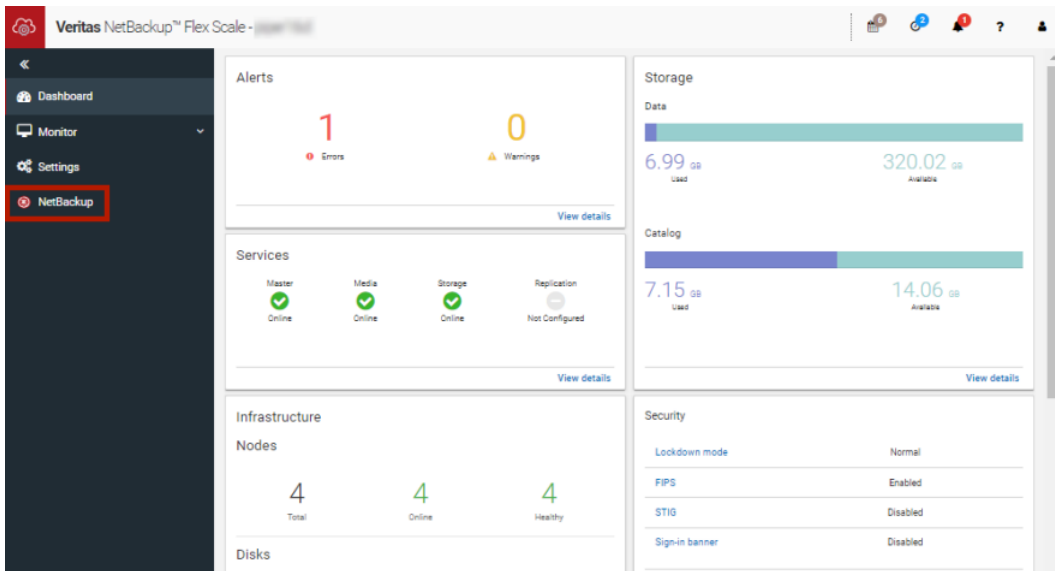
Interface and URL	Access to NetBackup Flex Scale or NetBackup
NetBackup web UI https://primaryserver/webui/login	To open NetBackup Flex Scale, click the Appliance management node. This action opens the NetBackup Flex Scale infrastructure management console in a new browser tab. See “Access NetBackup Flex Scale from the NetBackup web UI” on page 373.
NetBackup Flex Scale web UI https://ManagementServerIPorFQDN/webui	To access the NetBackup Flex Scale features, expand Cluster Management . See “Manage NetBackup and the NetBackup Flex Scale cluster management from the NetBackup Flex Scale web UI” on page 372.

Table 38-1 Accessing NetBackup Flex Scale and NetBackup (*continued*)

Interface and URL	Access to NetBackup Flex Scale or NetBackup
<p>NetBackup Flex Scale infrastructure management console</p> <p>IPv4: <code>https://ManagementServerIPorFQDN:14161/</code></p> <p>IPv6: <code>https://ManagementServerIP:14161/</code></p>	<p>To open NetBackup, click the NetBackup node. This action launches the NetBackup Flex Scale web UI in the same browser tab. To access the NetBackup Flex Scale infrastructure management console again, click Cluster Management.</p> <p>See “Access NetBackup from the Flex Scale infrastructure management console” on page 371.</p>

Access NetBackup from the Flex Scale infrastructure management console

You can open NetBackup from the Flex Scale infrastructure management console when you click on the **NetBackup** node.



To access NetBackup from the Flex Scale infrastructure management console

- 1** In a web browser, enter the URL for the Flex Scale infrastructure management console.

`https://ManagementServerIPorFQDN:14161/`

The *ManagementServerIP* is the public IP address or FQDN that you specified for the NetBackup Flex Scale management server.

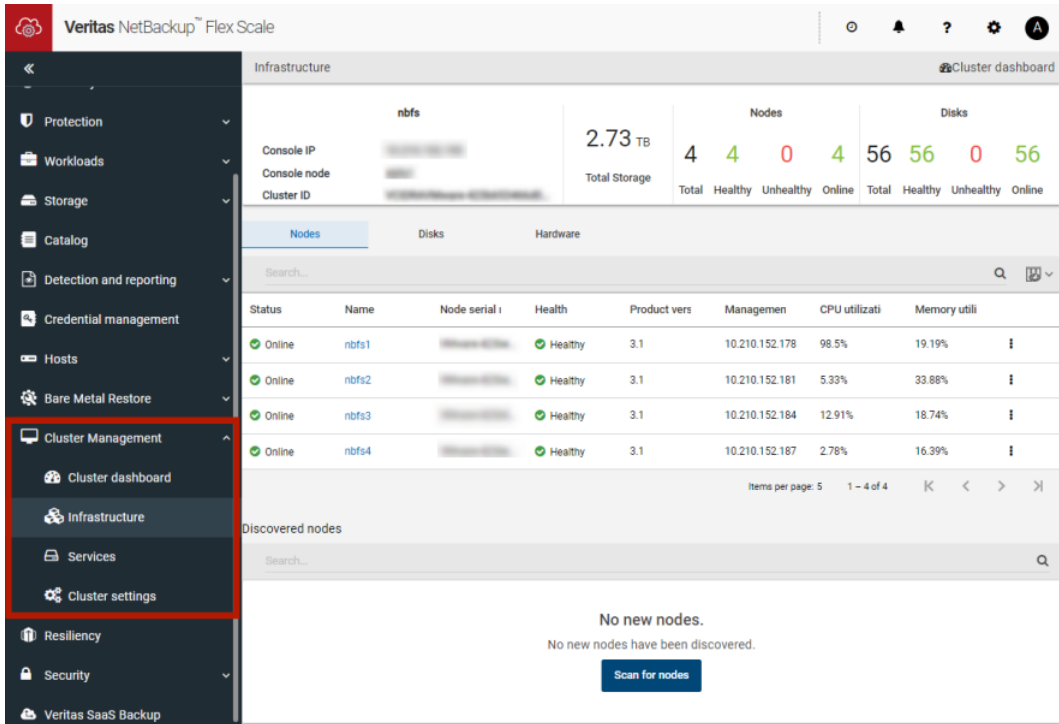
- 2** Enter the credentials for a user with the Appliance administrator role and click **Sign in**.

- 3** On the left, click **NetBackup**.

This action launches the Flex Scale web UI in the same browser tab, where you can manage both NetBackup and Flex Scale.

Manage NetBackup and the NetBackup Flex Scale cluster management from the NetBackup Flex Scale web UI

You can manage both NetBackup and the NetBackup Flex Scale cluster management from the NetBackup Flex Scale web UI.

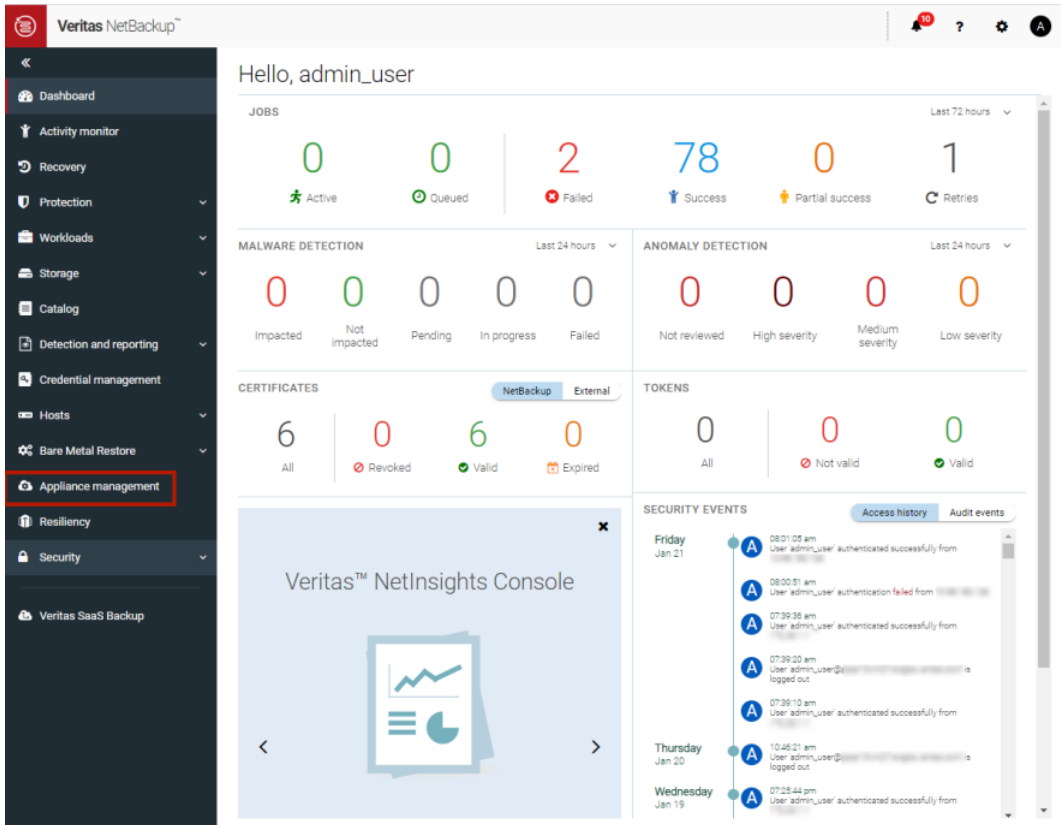


To access NetBackup and Flex Scale cluster management from the NetBackup Flex Scale web UI

- 1 In a web browser, enter the URL for the NetBackup Flex Scale web UI.
`https://ManagementServerIPorFQDN/webui`
The *ManagementServerIPorFQDN* is the host name or IP address of the NetBackup Flex Scale server that you want to sign in to.
- 2 Enter the credentials for a user with the Appliance Administrator role and click **Sign in**.
The web UI displays the NetBackup functionality and the NetBackup Flex Scale **Cluster management** node.

Access NetBackup Flex Scale from the NetBackup web UI

You can open NetBackup Flex Scale from the NetBackup web UI when you click on the **Appliance management** node.



To access Flex Scale from the NetBackup web UI

- 1 In a web browser, enter the URL for the NetBackup web UI.

<https://primaryserver/webui/login>

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

See “Sign in to the NetBackup web UI” on page 27.

- 2 Enter the credentials for a user with the Appliance administrator role and click **Sign in**.
- 3 On the left, click **Appliance management**.

In a new browser window, the NetBackup Flex Scale infrastructure management console opens.

NetBackup workloads

This chapter includes the following topics:

- [Protection of other asset types and clients](#)

Protection of other asset types and clients

The NetBackup web UI protects assets like databases, virtual machines, and clients through either protection plans or policies. Some workloads support both protection plans and policies. For more information on performing backups and restores, refer to the associated guide for that workload or agent. Protection of **Standard** and **MS-Windows** clients are covered in the *NetBackup Administrator's Guide, Volume I*.

Disaster recovery and troubleshooting

- [Chapter 40. Managing Resiliency Platforms](#)
- [Chapter 41. Managing Bare Metal Restore \(BMR\)](#)
- [Chapter 42. Troubleshooting the NetBackup Web UI](#)

Managing Resiliency Platforms

This chapter includes the following topics:

- [About Resiliency Platform in NetBackup](#)
- [Understanding the terms](#)
- [Configuring a Resiliency Platform](#)
- [Troubleshooting NetBackup and Resiliency Platform issues](#)

About Resiliency Platform in NetBackup

You can integrate NetBackup and Veritas Resiliency Platform to manage your disaster recovery operations. Veritas Resiliency Platform provides a single console from which you can proactively maintain business uptime across private, public, and hybrid clouds. Integrating NetBackup and Resiliency Platform lets you leverage the capabilities, such as complete automation, visualizing and monitoring DR specific information for all resiliency operations for the virtual machines in your data center.

Note the following points:

- You can integrate more than one Resiliency Platform with your NetBackup primary server.
- You can have more than one data centers for a Resiliency Platform.
- You can use Resiliency Platform with Veritas Resiliency Platform version 3.5 and later in NetBackup.
- After you add a Resiliency Platform, the assets are automatically discovered and displayed on the **Virtual machines** tab.

- You can view detailed information alerts and error messages in the **Notifications** section.

Understanding the terms

The following table explains the key components related to Veritas Resiliency Platform and NetBackup integration.

Term	Description
Resiliency Platform	The Veritas Resiliency Platform integrated with your NetBackup primary server. The Resiliency Manager provides the services required for protecting assets, such as virtual machines, within a resiliency domain. It also provides workload automation services.
Resiliency manager	The component that provides resiliency capabilities within a resiliency domain. It is composed of loosely coupled services, a distributed data repository, and a management console.
Infrastructure management server (IMS)	The component that discovers, monitors, and manages the asset infrastructure within a data center. The IMS transmits information about the asset infrastructure to the Resiliency Manager. The IMS is deployed as a virtual appliance. To achieve scale, multiple IMSs can be deployed in the same data center.
Data center	The location that contains source data center and a target data center. Each data center has one or more IMSs.
Resiliency group	The unit of management and control in Resiliency Platform. You organize related assets into a resiliency group and manage and monitor them as a single entity.
Automated virtual machines	The assets that are a part of a resiliency group and you can perform actions, such as migrate, recover, and rehearsal.
Recovery readiness	Measured based on migrate, recover or rehearsal operations. <ul style="list-style-type: none">■ Low - If no operations are performed or failed.■ High - If at least one operation is performed successfully in the past 7 days.■ Medium - If the recovery readiness does not fall in either high or low category.

Term	Description
Recovery Point Object (RPO)	<p>Recovery Point Objective is the point in time you can recover to in the event of a disaster.</p> <p>For example, if you have an RPO of 4 hours on your critical virtual machines then you lose 4 hours of data, as 4 hours ago is the last point in time to which you can recover data on your VMs.</p>

Configuring a Resiliency Platform

You can add, edit, delete, or refresh a Resiliency Platform. You can add more than one Resiliency Platform in NetBackup.

Add a Resiliency Platform

You can add one or more than one Resiliency Platforms in NetBackup. The Resiliency Platform lets you add virtual machines and automate protection. If the resiliency manager is using a third-party certificate, see the [NetBackup Web UI Administrator's Guide](#).

To add a Resiliency Platform

- 1 On the left, click **Resiliency**.
- 2 Click the **Resiliency Platform** tab.
- 3 Click **Add Resiliency Platform**.
- 4 Read the instructions on the **Add Resiliency Platform** dialog box and click **Next**.
- 5 In the **Add credentials** dialog box, enter a value in the following fields and click **Next**:
 - **Resiliency manager host name or IP address**
 - **Resiliency Platform API access key**
 - **NetBackup API access key**
- 6 In the **Add data center and Infrastructure management** server dialog box, select a data center.
- 7 In the **Infrastructure management server** section, select a preferred server.
- 8 Click **Add**.

After you add the Resiliency Platform in NetBackup, the NetBackup primary server will be configured automatically in the Resiliency Platform.

Note: If the NetBackup has FIPS mode enabled and you need to fetch the respective certificates, refer *Integrating with NetBackup* topic in *Resiliency Platform* product documentation. You need to install Resiliency Platform certificates in FIPS trust store and then add the Resiliency Platform. (Only done when NetBackup has FIPS mode enabled)

Configure a third-party CA certificate

You can use a self-signed or a third-party certificate to validate your Resiliency manager.

Consider the following points:

- For Windows, you can give a certificate as a file path or install the third-party certificate in the Trusted root certificates authorities.
- To switch from a self-signed certificate to a third-party certificate for an already added Resiliency Platform, you can edit the Resiliency Platform.

To configure a third-party CA certificate

- 1 Copy a PKCS #7 or P7B file having certificates of the trusted root certificates authorities that are bundled together. This file may either be PEM or DER encoded.
- 2 Create a CA file containing the PEM encoded certificates of the trusted root certificate authorities that are concatenated together.
- 3 In the `bp.conf` file, create the following entries, where `/certificate.pem` is the file name:
 - `ECA_TRUST_STORE_PATH = /certificate.pem`
 - Verify that the `nbwebsvc` account has the permissions to access the path that `ECA_TRUST_STORE_PATH` refers.

Edit or delete a Resiliency Platform

After you add a Resiliency Platform, you can edit the Resiliency Platform and NetBackup API access keys. You cannot change or update the Resiliency manager host name or IP address. However, you can delete the Resiliency Platform and add it to NetBackup again. If you refresh the Resiliency Platform, the discovery of assets on the Resiliency Platform is triggered.

To edit a Resiliency Platform

- 1 On the left, click **Resiliency**.
- 2 Click the **Resiliency Platform** tab.

- 3 Click the **Actions** menu for the Resiliency Platform that you want to edit and select **Edit**.
- 4 Enter the updated **Resiliency Platform API access key** and **NetBackup API access key**.
- 5 Click **Next**.
- 6 In the **Edit data center and Infrastructure management server** dialog box, select the **Data center** and then select the preferred infrastructure management server.
- 7 Click **Save**.
- 8 To delete a Resiliency Platform, from the **Actions** menu, select **Delete**.

View the automated or not-automated VMs

The virtual machines that belong to a resiliency group in Veritas Resiliency Platform are discovered and displayed on the **Automated** tab and the VMs that don't belong any resiliency group are displayed on the **Not automated** tab. You can view the status of the assets and perform various actions. You can search for a VM or apply filters too.

The following table lists the columns displayed on the **Automated** and **Not automated** tabs:

Table 40-1

Tab	Column	Description
<ul style="list-style-type: none"> ■ Automated ■ Not automated 	Name	Name of the virtual machine.
<ul style="list-style-type: none"> ■ Automated 	RPO	<p>Recovery Point Objective is the point in time you can recover to in the event of a disaster.</p> <p>For example, if you have an RPO of 4 hours on your critical virtual machines then you lose 4 hours of data, as 4 hours ago is the last point in time to which you can recover data on your VMs.</p>
<ul style="list-style-type: none"> ■ Automated ■ Not automated 	State	Whether the VM is switched on or off.

Table 40-1 (continued)

Tab	Column	Description
<ul style="list-style-type: none"> Automated 	Recovery readiness	<p>Measured based on migrate, recover or rehearsal operations.</p> <ul style="list-style-type: none"> Low - If no operations are performed or failed. High - If at least one operation is performed successfully in the past 7 days. Medium - If the recovery readiness does not fall in either high or low category.
<ul style="list-style-type: none"> Automated Not automated 	Platform	The platform that the VM belongs to.
<ul style="list-style-type: none"> Automated Not automated 	Server	The server name of the VM.
<ul style="list-style-type: none"> Automated 	Protection	Protection status of the VM.
<ul style="list-style-type: none"> Automated 	Resiliency group	Name of the resiliency group to which the VM belongs.
<ul style="list-style-type: none"> Not automated 	Recovery action	Launch the Resiliency Platform to add the VM to a resiliency group.

To view and perform actions on automated VMs

- 1 On the left, click **Resiliency**.
- 2 On the **Virtual machines** tab, click **Automated**.
- 3 To view more details about a VM, in the **Name** column, click a VM.
- 4 To view all VMs that are a part of the same resiliency group, click the preferred resiliency group.

- 5 To perform disaster recovery operation, such as rehearse, restore, or recover, click **Launch Resiliency Platform**.

To enable single-sign, same authentication domain must be configured NetBackup and Veritas Resiliency Platform. If not configured, you must login with username and password to access Veritas Resiliency Platform web console.
- 6 Log on to your Resiliency Platform and perform the preferred action. See the *Veritas Resiliency Platform User Guide*.

To view and perform actions on not automated VMs

- 1 On the left, click **Resiliency**.
- 2 On the **Virtual machines** tab, click **Not automated**.
- 3 To add the VM to a resiliency group, in the **Recovery action** column, click **Automate Recovery**.
- 4 Perform the preferred action for your Resiliency Platform. See the *Veritas Resiliency Platform User Guide*.

Troubleshooting NetBackup and Resiliency Platform issues

Use the following information to troubleshoot issues.

Table 40-2 Troubleshooting issues

Issue	Action
Failed to configure the current NetBackup primary server with the Resiliency Platform.	<div>Check the logs at the following location in Veritas Resiliency Platform's Resiliency manager:</div> <ul style="list-style-type: none">■ /var/opt/VRTSitrp/logs/copydata-service.log■ /var/opt/VRTSitrp/logs/api-service.log
Failed to establish a persistent connection between the current NetBackup primary server and the Resiliency Platform.	<ul style="list-style-type: none">■ Verify that the logged in user has permissions in credentials namespace.■ Check the logs at the following location on the NetBackup primary server:<ul style="list-style-type: none">■ /usr/openv/logs/nbwebbservice/ in NetBackup installation directory■ C:\Program Files\Veritas\NetBackup\logs\nbwebbservice in NetBackup windows

Table 40-2 Troubleshooting issues (*continued*)

Issue	Action
Failed to launch the Veritas Resiliency Platform	Verify that same authentication domain is used to configure Veritas Resiliency Platform and NetBackup.

Managing Bare Metal Restore (BMR)

This chapter includes the following topics:

- [About Bare Metal Restore \(BMR\)](#)
- [Add a custom role for a Bare Metal Restore \(BMR\) administrator](#)

About Bare Metal Restore (BMR)

NetBackup Bare Metal Restore (BMR) is the server recovery option of NetBackup. BMR automates and streamlines the server recovery process so you do not have to reinstall the operating systems or configure the hardware manually. BMR restores the operating system, the system configuration, and all the system files and the data files with the following steps.

For complete information on BMR, refer to the [NetBackup Bare Metal Restore Administrator's Guide](#).

In the NetBackup web UI, you can perform the following BMR operations:

- View and manage the clients that are backed up for VM conversion.
- Convert BMR-enabled backups to a virtual machine using the Virtual Machine Conversion wizard.
- Create point-in-time restore configurations.
- View and manage VM conversion tasks.
- View and manage the BMR clients and configurations.
- Run pre-restore operations on the client configuration and the VM conversion client's configurations. For example, prepare-to-restore, prepare-to-discover, and dissimilar disk restore operations.

- View and manage boot servers.
- View and manage resources like shared resource trees, discovered configurations, and Windows device driver packages.
- View and manage BMR restore or discover tasks.
- View and manage the BMR clients and configurations.
- Run pre-restore operations on the client configuration and the VM conversion client's configurations. For example, prepare-to-restore, prepare-to-discover, and dissimilar disk restore operations.
- View and manage boot servers.
- View and manage resources like shared resource trees, discovered configurations, and Windows device driver packages.
- View and manage BMR restore or discover tasks.

Add a custom role for a Bare Metal Restore (BMR) administrator

To add a custom RBAC role

- 1 On the left, select **Security > RBAC** and click **Add**.
- 2 Select **Custom role** to manually configure all the permissions for the role.
- 3 Provide a **Role name** and a description.

For example, you may want to indicate that the role is for any users that are BMR administrators.
- 4 On the **Global** tab, expand the **BMR** section and select all the permissions for **BMR**.

Boot servers	View, Delete
Clients	View, Create, Update, Delete, Pre restore
VM conversion	View, Delete, VM conversion

- 5 Expand the **NetBackup management** section.
 - Locate the **NetBackup hosts** group.
 - Select the following permissions:

NetBackup hosts	View, Update
-----------------	--------------

- Locate the **NetBackup backup images** group.
- Select the following permissions:

NetBackup backup images	Image Requests > View
NetBackup backup images	View

6 For ESXi servers, additional permissions are needed for **Host properties**.

- On the **Global** tab, expand the **NetBackup management** section.
- Select the following permissions:

Access hosts	View, Create, Update, Delete
--------------	------------------------------

7 On the **Assets** tab, select the following permissions.

VMware assets	View, Update, View restore targets
---------------	------------------------------------

8 Click **Assign**.

9 Under **Workloads**, click **Assign**.

Select the VMware assets that you want the role to have access to.

- To give the role access to all VMware assets and future assets that you add, select **Apply selected permissions to all existing and future VMware assets**.
- To select individual assets, deselect **Apply selected permissions to all existing and future VMware assets** and click **Add**.
 For example, you can select one or more: datastores, datastore clusters, ESXi servers, ESXi clusters, resource pools, vApps.

10 When you have added all the assets, click **Assign**.

11 On the **Users** card, click **Assign**. Then add each user that you want to have access to this custom role.

12 When you are done configuring the role, click **Save**.

Troubleshooting the NetBackup Web UI

This chapter includes the following topics:

- [Tips for accessing the NetBackup web UI](#)
- [If a user doesn't have the correct permissions or access in the NetBackup web UI](#)
- [Unable to validate the user or group when configuring LDAP server](#)

Tips for accessing the NetBackup web UI

When NetBackup is properly configured, a user can access the primary server at the following URL:

`https://primaryserver/webui/login`

If the web UI on a primary server does not display, follow these steps to troubleshoot the issue.

Browser displays an error that the connection was refused or that it cannot connect to the host

Table 42-1 Solutions when the web user interface does not display

Step	Action	Description
Step 1	Check the network connection.	
Step 2	Verify that the firewall is open for port 443.	Refer to the following article: https://www.veritas.com/docs/100042950

Table 42-1 Solutions when the web user interface does not display
(continued)

Step	Action	Description
Step 3	If port 443 is in use, configure another port for the web UI.	Refer to the following article: https://www.veritas.com/docs/100042950
Step 4	Verify that the nbweb service is up.	Check the nbweb service logs for more details.
Step 5	Verify that the vnetd -http_api_tunnel is running.	Verify that the vnetd -http_api_tunnel service is running. For more details, check the vnetd -http_api_tunnel logs with OID 491.
Step 6	Ensure that the external certificate for the NetBackup web server is accessible and has not expired.	<ul style="list-style-type: none"> ■ Use the Java Keytool commands to validate the following file: Windows: <code>install_path\var\global\wsl\credentials\nbweb service.jks</code> UNIX: <code>/usr/opensv/var/global/wsl/credentials nbweb service.jks</code> ■ Check whether the nbweb group has a permission to access the nbweb service.jks file. ■ Contact Veritas Technical Support.

Cannot access web UI when you use a custom port

- Restart the vnetd service.
- Follow the steps in [Table 42-1](#).

Certificate warning displays when you try to access the web UI

The certificate warning displays if the NetBackup web server uses a certificate that is issued by a CA that is not trusted by the web browser. (Including the default NetBackup web server certificate that the NetBackup CA issued.)

To resolve a certificate warning from the browser when you access the web UI

- 1 Configure the external certificate for the NetBackup web server.
See [“Configure an external certificate for the NetBackup web server”](#) on page 225.
- 2 If the problem persists, contact Veritas Technical Support.

If a user doesn't have the correct permissions or access in the NetBackup web UI

Note that only administrators and root users automatically have full access to the web UI. Other users must be configured in RBAC to have access and permissions for the web UI.

See [“Configuring RBAC”](#) on page 297.

If a user does not have the correct permissions or cannot access the workload assets that they should have access to, do the following:

- Verify that the user's credentials match the username (or the username and the domain name) that is specified in the user's role.
- Review the roles for the user in **Security > RBAC**. You may need to change the role permissions. However, be aware that those kinds of changes also affect any other users that belong to those roles.
- Any user account changes with the identity provider are not synchronized with the user's roles. If a user account changes with the identity provider, the user may not have the correct permissions or access. The NetBackup security administrator must edit each role for the user to remove the existing user account and re-add the new account.
- Changes to a user's roles are not immediately reflected in the web UI. A user with an active session must sign out and sign in again before any changes take effect.

Unable to validate the user or group when configuring LDAP server

When the administrator configures the LDAP server, they must specify the `-d DomainName` option. `DomainName` can be the LDAP server name or the domain name. Whatever name is specified for `-d DomainName` is the domain name that an administrator should use when they add users to an RBAC role.

If you specify the incorrect domain, you may see the error `Unable to validate the user or group`. Review the following:

- The username and domain name are typed correctly.
- You specified the correct domain name.
 The domain name that you should specify depends on how the LDAP server is configured in NetBackup. Contact your administrator for help with adding users to RBAC.

Other topics

- [Chapter 43. Additional NetBackup catalog information](#)
- [Chapter 44. About the NetBackup database](#)

Additional NetBackup catalog information

This chapter includes the following topics:

- [Parts of the NetBackup catalog](#)
- [Archiving the catalog and restoring from the catalog archive](#)
- [Estimating catalog space requirements](#)

Parts of the NetBackup catalog

The NetBackup catalog resides on the NetBackup primary server. It manages and controls access to the following types of data:

- Image metadata (information about backup images and copies).
- Backup content data (information about the folders, files, and the objects in a backup (.*z* files)).
- NetBackup backup policies.
- NetBackup licensing data.
- The NetBackup error log.
- The client database.
- Cloud configuration files.

See [“About the catalog backup of cloud configuration files”](#) on page 397.

The catalog consists of the following parts:

- NetBackup stores information in the NetBackup database (NBDB). The metadata includes information about the data that has been backed up, and about where the data is stored.
See [“NetBackup databases and configuration files”](#) on page 393.
- The image database.
The image database contains information about the data that has been backed up.
See [“About the NetBackup image database”](#) on page 395.
- NetBackup configuration files.
- The key management service (KMS) configuration files
For more details on the KMS configuration, see the [NetBackup Security and Encryption Guide](#).

NetBackup is sensitive to the location of the primary server components. Running any part of NetBackup (the binaries, the logs, the database, the images) on a network share (NFS, for example) can affect performance of even normal operations. NetBackup can be CIFS-mounted on SAN or NAS storage as long as the average I/O service times remain less than 20 milliseconds.

The storage must also meet certain conditions to ensure data integrity in the NetBackup catalog.

- The order of file writes must be guaranteed.
- When a write request is issued, the write must complete to the physical storage. The write request must not merely be buffered when the SAN or the NAS returns from the write call.
See the following article for more information:

NetBackup databases and configuration files

The NetBackup catalog backup includes the NetBackup databases and the configuration files, as follows.

Databases

The NetBackup databases include the NBDB database and the NetBackup Authorization database (NBAZDB). If Bare Metal Restore is installed (optionally-licensed) there is also the BMRDB database.

The databases are located in the following directories:

`install_path\NetBackupDB\data`

`/usr/opensv/db/data/`

These directories contain the following subdirectories:

`\bmrdb\` or `/bmrdb/` (if BMR is installed)

`\nbazdb\` or `/nbazdb/` (NetBackup authorization)

`\nbdb\` or `/nbdb/` (contains both the NBDB and the EMM databases)

Configuration files

Warning: Do not edit the configuration files. NetBackup may not start if you change these files.

Note: The catalog backup process copies this data to `/usr/opensv/db/staging` and backs up the copy.

The following configuration files are created:

```
pgbouncer.ini
pg_hba.conf
pg_ident.conf
postgresql.auto.conf
postgresql.conf
userlist.txt
vxdbs.conf
web.conf
```

Most of the configuration files are located in the following directories:

```
install_path\NetBackupDB\data\instance
/usr/opensv/db/data/instance
```

`web.conf` is created in the following directories:

```
/usr/opensv/var/global/wsl/config
install_path\NetBackup\var\global\wsl\config
```

About the Enterprise Media Manager (EMM)

The Enterprise Media Manager (EMM) is a NetBackup service that manages the device and the media information for NetBackup. The Enterprise Media Manager stores its managed information in a database that resides on the primary server.

The NetBackup Resource Broker queries EMM to allocate storage units, drives (including drive paths), and media.

EMM contains the following information:

- Device attributes
- Robotic library and standalone drive residence attributes
- NDMP attributes
- Barcode rule attributes
- Volume pool attributes
- Tape attributes
- Media attributes
- Storage unit attributes
- Storage unit group attributes
- Hosts with assigned tape drives
- Media and device errors
- Disk pool and disk volume attributes
- Storage server attributes
- Log on credentials for storage servers, disk arrays, and NDMP hosts
- Fibre Transport attributes

EMM ensures consistency between drives, robotic libraries, storage units, media, and volume pools across multiple servers. EMM contains information for all media servers that share devices in a multiple server configuration. The NetBackup scheduling components use EMM information to select the server, drive path, and media for jobs.

About the NetBackup image database

The image database contains subdirectories for each client that is backed up by NetBackup, including the primary server and any media servers.

The image database is located in the following location:

- **Windows:** `Program Files\Veritas\Netbackup\db\images`
- **UNIX:** `/usr/opensv/netbackup/db/images`

The image database contains the following files:

Image files	Files that store only backup set summary information.
.lck files	Used to prevent simultaneous updates on images.
Image .f files	Used to store the detailed information about each file backup.
db_marker.txt	Used to ensure that access to the db directory is valid when the NetBackup Database Manager starts up. Do not delete this file.

The image database is the largest part of the NetBackup catalog. It consumes about 99% of the total space that is required for the NetBackup catalog. While most of the subdirectories are relatively small in the NetBackup catalogs, `\images` (Windows) or `/images` (UNIX) can grow to hundreds of gigabytes. The image database on the primary server can grow too large to fit on a single tape. Image database growth depends on the number of clients, policy schedules, and the amount of data that is backed up.

See [“Estimating catalog space requirements”](#) on page 409.

If the image catalog becomes too large for the current location, consider moving it to a file system or disk partition that contains more space.

See [“Moving the image catalog”](#) on page 411.

The catalog conversion utility (`cat_convert`) can be used to convert .f files into a human-readable format.

About NetBackup image .f files

The binary catalog contains one or more image .f files. This type of file is also referred to as a “files” file. The image .f file may be large because it contains the detailed backup selection list for each file backup. Generally, image files range in size from 1 kilobyte to 10 gigabytes.

Note: You can use intelligent catalog archiving (ICA) to reduce the number of catalog .f files based on a specified retention period or file size.

See [“Enabling intelligent catalog archiving \(ICA\) to reduce the number of .f files”](#) on page 401.

ICA applies only to servers running NetBackup 10.3.0.1 and later using MSDP or MSDP Cloud storage.

The .f files are found in the following location:

Windows: `install_path\NetBackup\db\images\clientname\ctime`

UNIX: `/usr/opensv/netbackup/db/images/clientname/ctime/`

The file layout determines whether the catalog contains one `.f` file or many `.f` files. NetBackup configures the file layout automatically, based on the size of the binary catalog. NetBackup uses one of two layouts: single file layout or multiple file layout.

- Image `.f` file single file layout

NetBackup stores file information in a single image `.f` file if the information for the catalog is less than 100 megabytes.

When the backup file of one catalog backup is less than 100 megabytes, NetBackup stores the information in a single image `.f` file. The image `.f` file is always greater than or equal to 72 bytes, but less than 100 megabytes.

The following is a UNIX example of an `.f` file in a single file layout:

```
-rw----- 1 root other  979483 Aug 29 12:23 test_1030638194_FULL.f
```

- Image `.f` file multiple file layout

When the file information for one catalog backup is greater than 100 megabytes, the information is stored in multiple `.f` files: one main image `.f` file plus nine additional `.f` files.

Separating the additional `.f` files from the image `.f` file and storing the files in the `catstore` directory improves performance while writing to the catalog.

The main image `.f` file is always exactly 72 bytes.

```
-rw- 1 root other      72 Aug 30 00:40 test_1030680524_INCR.f
-rw- 1 root other     804 Aug 30 00:08 catstore/test_1030680524_INCR.f-list
-rw- 1 root other 1489728 Aug 30 00:39 catstore/test_1030680524_INCR.f_imgDir0
-rw- 1 root other      0 Aug 30 00:40 catstore/test_1030680524_INCR.f_imgExtraObj0
-rw- 1 root other 1280176 Aug 30 00:39 catstore/test_1030680524_INCR.f_imgFile0
-rw- 1 root other     192 Aug 30 00:40 catstore/test_1030680524_INCR.f_imgHeader0
-rw- 1 root other      0 Aug 30 00:40 catstore/test_1030680524_INCR.f_imgNDMP0
-rw- 1 root other 9112680 Aug 30 00:39 catstore/test_1030680524_INCR.f_imgRecord0
-rw- 1 root other 2111864 Aug 30 00:39 catstore/test_1030680524_INCR.f_imgStrings0
-rw- 1 root other      11 Aug 30 00:40 catstore/test_1030680524_INCR.f_imgUserGroupNames0
```

About the catalog backup of cloud configuration files

The following cloud configuration files are backed up during the NetBackup catalog backup process:

All `.txt` files in the `meter` directory, which contain intermediate metering data

- `CloudInstance.xml`
- `cloudstore.conf`

- `libstspienencrypt.conf`
- `libstspimetering.conf`
- `libstspithrottling.conf`
- `libstspicloud_provider_name.conf`

All `.conf` files that are specific to the cloud providers that NetBackup supports

The cloud configuration files that are backed up during the catalog backup process reside at the following locations:

Windows	<code>install_path\Veritas\NetBackup\var\global\wmc\cloud</code>
UNIX	<code>/usr/opensv/var/global/wmc/cloud</code>

The files `CloudProvider.xml` and `cacert.pem` are at the following location:

Windows	<code><installed-path>\NetBackup\var\global\cloud</code>
UNIX	<code>/usr/opensv/var/global/cloud/</code>

Note: The `cacert.pem` file is not backed up during the NetBackup catalog backup process.

This `cacert.pem` file is a cloud provider-specific file. This file is installed as part of the NetBackup installation. This file includes the well-known public cloud vendor CA certificates used by NetBackup.

Archiving the catalog and restoring from the catalog archive

Catalog archiving helps administrators solve the kinds of problems that large amounts of catalog data can pose: large catalogs require a greater amount of disk space and can be time-consuming to back up.

Catalog archiving reduces the size of online catalog data by relocating the large catalog `.f` files to secondary storage. NetBackup administration continues to require regularly scheduled catalog backups, but the backups are faster without the large amount of online catalog data.

You can also use intelligent catalog archiving (ICA) to reduce the number of catalog `.f` files from secondary storage. When you enable ICA, any catalog `.f` file that is older than the specified retention period value is removed from the catalog disk.

You can also specify a size value so that any catalog .f file that is greater than or equal to the size value is removed from the catalog disk.

See [“Enabling intelligent catalog archiving \(ICA\) to reduce the number of .f files”](#) on page 401.

Catalog archiving should not be used as a method to reclaim disk space when a catalog file system fills up. In that situation, investigate catalog compression or add disk space to grow the file system.

For additional catalog archiving considerations, see the following topic:

See [“Catalog archiving considerations”](#) on page 408.

To archive the catalog and restore the catalog archive

- 1 Use `bpcatlist` to determine what images are available to be archived.

Running `bpcatlist` alone does not modify any catalog images. Only when the `bpcatlist` output is piped to `bpcatarc` are the `.f` files backed up, and only when the output is piped to `bpcatrm` will the `.f` files be deleted from disk.

To determine what images have `.f` files on disk that can be archived, run the following command. The `catarcid` column indicates whether the `.f` file is not currently backed up (0) or the `catarcid` of the backup of that image.

```
/usr/opensv/netbackup/bin/admincmd/bpcatlist -online
```

To determine what images have been previously archived and removed from disk, run the following command.

```
/usr/opensv/netbackup/bin/admincmd/bpcatlist -offline
```

The catalog commands are described in detail in the following topic:

See [“Catalog archiving commands”](#) on page 406.

Note: If catalog archiving has not been previously run, this command should return: `No entity was found.`

For example, to display all images for a specific client before January 1, 2017, run the following command:

```
bpcatlist -client name -before Jan 1 2017
```

To display the help for the `bpcatlist` command run this command.

```
bpcatlist -help
```

Once the `bpcatlist` output correctly lists all the images that are to be archived or deleted, other commands can be added.

2 Running the catalog archive.

Before running the catalog archive, create a backup policy named **catarc**. The policy is required for the `bpcatarc` command to successfully process images. The name of the policy reflects that the purpose of the schedule is for catalog archiving.

See the following topic for details about configuring the **catarc** policy:

See [“Creating a catalog archiving policy”](#) on page 405.

To run the catalog archive, first run the `bpcatlist` command with the same options used in step 1 to display images. Then pipe the output through `bpcatarc` and `bpcatrm`.

```
bpcatlist -client all -before Jan 1 2017 | bpcatarc | bpcatrm
```

A new job appears in the **Activity Monitor**. The command waits until the backup completes before it returns the prompt. The command reports an error only if the catalog archive fails, otherwise the commands return to the prompt.

The **File List**: section of the Job Details in the **Activity Monitor** displays a list of image files that have been processed. When the job completes with a status 0, the `bpcatrm` command removes the corresponding `.f` files. If the job fails, no catalog `.f` files are removed.

If `bpcatlist` is piped to `bpcatarc` but the results are not piped to `bpcatrm`, the backup occurs but the `.f` files are not removed from disk. The same `bpcatlist` command can then be rerun and piped to `bpcatrm` to remove the `.f` files.

3 Restoring the catalog archive.

To restore the catalog archive, first use the `bpcatlist` command to list the files that need to be restored. Once `bpcatlist` displays the proper files to restore, run the `bpcatres` command to restore the actual files.

To restore all the archived files from step 2, run the following command:

```
bpcatlist -client all -before Jan 1 2017 | bpcatres
```

This command restores all of the catalog archive files before January 1, 2017.

Enabling intelligent catalog archiving (ICA) to reduce the number of .f files

Note: Intelligent catalog archiving (ICA) applies only to servers running NetBackup 10.3.0.1 and later using MSDP or MSDP Cloud storage.

You can use intelligent catalog archiving (ICA) to reduce the number of catalog .*fil* files based on a specified retention period or file size. When you enable ICA, any catalog .*fil* file that is older than the specified retention period value is removed from the catalog disk. You can also specify a file size value so that any catalog .*fil* file that is greater than or equal to the size value is removed from the catalog disk.

The main advantage of ICA is that it shortens catalog backup time by reducing the number of .*fil* files that need to be backed up if they meet the required criteria:

- The backup image must be older than the configured ICA retention period.
- The .*fil* file must be larger than or equal to the configured ICA minimum size.
- At least one copy of the backup image must be on MSDP or MSDP Cloud storage and has 1 or more true image restore (TIR) fragments.
- Image catalog .*fil* file has not been recalled in last 24 hours.
- The backup image must be from a completed SLP or from a backup that is not managed by SLP.
- The backup image is not from a catalog backup.
- The image catalog is not archived.

When ICA is enabled, you should notice the following behaviors:

- Initial image cleanup after you enable ICA may take longer than usual.
- Catalog backups will be faster if any of the .*fil* files involved have been intelligently archived.
- Browse and Restore functions will take longer if any of the .*fil* files involved have been intelligently archived.

No additional action is needed to restore the catalog .*fil* file. Catalog .*fil* files are restored from images automatically as follows:

- When an ICA image is browsed.
- When an ICA-eligible copy is expired from an ICA image. Restoring catalog .*fil* files ensures that the remaining copies from that image are accessible and usable.
- When an ICA-eligible image is found but its catalog .*fil* file missing.

More information about .*fil* files is available:

See [“About NetBackup image .*fil* files”](#) on page 396.

To enable intelligent catalog archiving (ICA) and specify retention and file size values

- 1 Run the following command on the primary server:

```
bpconfig -ica_retention seconds
```

When the *seconds* value is between 1 and 2147472000, ICA is enabled. Any image which is older than the value is processed for ICA. The catalog *.f* file from the ICA-eligible image is removed from the catalog disk. Setting this value to 0 (zero) disables ICA. The default value for NetBackup Flex Scale and CloudScale environments is 2592000 (30 days). The default value for all other NetBackup environments is 0 (disabled).

For Accelerator-enabled backups, specify an ICA retention value that is longer than full backup schedules so that the number of *.f* file restores from ICA images goes down.

For example, to set the ICA retention value to 30 days, enter `bpconfig -ica_retention 2592000`.

Use `bpconfig -U` to verify the change:

```
# bpconfig -U
Admin Mail Address:          sasquatch@wapati.edu
Job Retry Delay:             10 minutes
Max Simultaneous Jobs/Client: 1
Backup Tries:                1 time(s) in 12 hour(s)
Keep Error/Debug Logs:      3 days
Max drives this master:      0
Keep TrueImageRecovery Info: 24 days
Compress DB Files:           (not enabled)
Media Mount Timeout:         30 minutes
Display Reports:             24 hours ago
Preprocess Interval:         0 hours
Image DB Cleanup Interval:    12 hours
Image DB Cleanup Wait Time:   10 minutes
Policy Update Interval:       10 minutes
Intelligent Catalog Archiving: Files file larger than 1024 KB
Intelligent Catalog Archiving: Images older than 30 day(s)
```

- 2** **Note:** After you enable ICA, the minimum file size for `.f` files is set to the default value 1024 KB. Use this step to change that value.

To specify a minimum file size, run the following command on the primary server:

```
bpconfig -ica_min_size size
```

When the `size` value is between 0 and 2097151, any catalog `.f` file that is larger than or equal to the `size` value is removed from the catalog disk. The default value is 1024.

For example to set the ICA minimum file size to 2048 KB, enter `bpconfig -ica_min_size 2048`.

Use `bpconfig -U` to verify the change:

```
# bpconfig -U
Admin Mail Address:          sasquatch@wapati.edu
Job Retry Delay:             10 minutes
Max Simultaneous Jobs/Client: 1
Backup Tries:                1 time(s) in 12 hour(s)
Keep Error/Debug Logs:      3 days
Max drives this master:      0
Keep TrueImageRecovery Info: 24 days
Compress DB Files:           (not enabled)
Media Mount Timeout:         30 minutes
Display Reports:             24 hours ago
Preprocess Interval:         0 hours
Image DB Cleanup Interval:   12 hours
Image DB Cleanup Wait Time:  10 minutes
Policy Update Interval:      10 minutes
Intelligent Catalog Archiving: Files file larger than 2048 KB
Intelligent Catalog Archiving: Images older than 30 day(s)
```

To disable intelligent catalog archiving (ICA)

- ◆ Run the following command on the primary server:

```
bpconfig -ica_retention 0
```

Use `bpconfig -U` to verify the change:

```
# bpconfig -U
Admin Mail Address:          sasquatch@wapati.edu
Job Retry Delay:             10 minutes
Max Simultaneous Jobs/Client: 1
Backup Tries:                1 time(s) in 12 hour(s)
Keep Error/Debug Logs:      3 days
Max drives this master:      0
Keep TrueImageRecovery Info: 24 days
Compress DB Files:           (not enabled)
Media Mount Timeout:         30 minutes
Display Reports:             24 hours ago
Preprocess Interval:         0 hours
Image DB Cleanup Interval:   12 hours
Image DB Cleanup Wait Time:  10 minutes
Policy Update Interval:      10 minutes
Intelligent Catalog Archiving: (not enabled)
```

Creating a catalog archiving policy

The catalog archiving feature requires the presence of a policy named **catarc** before the catalog archiving commands can run properly. The policy can be reused for catalog archiving.

To create a catalog archiving policy

- 1 Open the NetBackup web UI.
- 2 On the left, click **Protection > Policies**. Then click **Add**.
- 3 Enter the **Policy name catarc**.

The **catarc** policy waits until `bpcatarc` can activate it. Users do not run this policy. Instead, `bpcatarc` activates this special policy to perform a catalog backup job, then deactivates the policy after the job is done.

- 4 In the **Attributes** policy tab, set the **Policy type** to **Standard** or **MS-Windows**, according to the platform of the primary server.
- 5 In the **Attributes** policy tab, deactivate the catalog archive policy by clearing the **Go into effect at** box.

- 6 Select the **Schedules** tab and click **Add** to create a schedule.
 In the **Attributes** schedule tab, the **Name** of the schedule is not restricted, but the **Type of backup** must be **User backup**.
- 7 Select a **Retention** for the catalog archive. Set the retention level for a time at least as long as the longest retention period of the backups being archived.
 Data can be lost if the retention level of the catalog archive is not long enough.
 You may find it useful to set up and then designate a special retention level for catalog archive images.
- 8 Select the **Start window** tab and define a schedule for the **catarc** policy.
 The schedule must include in its window the time when the `bpcatarc` command is run. If the `bpcatarc` command is run outside of the schedule, the operation fails.
- 9 Click **Add** to save the schedule.
- 10 On the **Clients** tab, enter the name of the primary server as it appears on the NetBackup servers list.
- 11 On the **Backup selections** tab, browse to the directory where catalog backup images are placed:
 On Windows: `install_path\NetBackup\db\images`
 On UNIX: `/usr/openv/netbackup/db/images`
- 12 Click **Create** to save the policy.

Catalog archiving commands

The catalog archiving option relies on three commands to designate a list of catalog `.f` files, then archive the files. A fourth command, `bpcatres`, is used to restore the files if necessary.

Catalog archiving uses the following commands.

Table 43-1 Catalog archiving commands

Command	Description
bpcatlist	<p>The <code>bpcatlist</code> command queries the catalog data. Then, <code>bpcatlist</code> lists the portions of the catalog that are based on selected parameters. For example, date, client, policy, schedule name, backup ID, the age of the backup image, or the date range of the backup image. <code>bpcatlist</code> outputs the formatted image summary information of matched images to standard output.</p> <p>The other catalog archiving commands, <code>bpcatarc</code>, <code>bpcatrm</code>, and <code>bpcatres</code>, all depend on input from <code>bpcatlist</code> by a piped command.</p> <p>For example, to archive (backup and delete) all of the <code>.f</code> files that were created before January 1, 2012, the following would be entered:</p> <pre>bpcatlist -client all -before Jan 1 2012 bpcatarc bpcatrm</pre> <p><code>bpcatlist</code> is also used to provide status information.</p> <p>For each catalog, it lists the following information:</p> <ul style="list-style-type: none"> ■ Backup ID (Backupid) ■ Backup date (Backup Date) ■ Catalog archive ID (catarcid). After one <code>.f</code> file is successfully backed up, a catalog archive ID is entered into the catarcid field in the image file. This field is zero (0) if the image was never archived. ■ Archived status (S). Indicates whether the catalog was archived (2) or was not archived (1). ■ Compressed status (C). Indicates whether the catalog was compressed (<i>positive_value</i>) or was not compressed (0). ■ Catalog file name (Files file) <p>The following is an example of the <code>bpcatlist</code> output, showing all of the backups for client alpha since October 23:</p> <pre># bpcatlist -client alpha -since Oct 23 Backupid Backup Date ...Catarcid S C Files file alpha_097238 Oct 24 10:47:12 2012 ... 973187218 1 0 alpha_097238_UBAK.f alpha_097233 Oct 23 22:32:56 2012 ... 973187218 1 0 alpha_097233_FULL.f alpha_097232 Oct 23 19:53:17 2012 ... 973187218 1 0 alpha_097232_UBAK.f</pre> <p>More information is available in the NetBackup Commands Reference Guide.</p>
bpcatarc	<p>The <code>bpcatarc</code> command reads the output from <code>bpcatlist</code> and backs up the selected list of <code>.f</code> files. After one <code>.f</code> file is successfully backed up, a catalog archive ID is entered into the catarcid field in the image file. For archiving of the <code>.f</code> files to proceed, a policy by the name of catarc is required. The policy is based on a User Backup type schedule. The schedule for catarc must include in its window the time <code>bpcatarc</code> command is run.</p> <p>See “Creating a catalog archiving policy” on page 405.</p>

Table 43-1 Catalog archiving commands (*continued*)

Command	Description
<code>bpcatrm</code>	<p>The <code>bpcatrm</code> command reads the output from <code>bpcatlist</code> or <code>bpcatarc</code>. If the image file has valid catarcid entries, <code>bpcatrm</code> deletes selected image .f files from the online catalog.</p> <p><code>bpcatrm</code> does not remove one .f file unless the file has been previously backed up using the catarc policy.</p>
<code>bpcatres</code>	<p>Use the <code>bpcatres</code> command to restore the catalog. The <code>bpcatres</code> command reads the output from <code>bpcatlist</code> and restores selected archived .f files to the catalog. For example:</p> <pre>bpcatlist -client all -before Jan 1 2012 bpcatres</pre>

Catalog archiving considerations

Consider the following items before catalog archiving:

- Perform catalog archiving operations when NetBackup is in an inactive state (no jobs are running).
- Catalog archiving modifies existing catalog images. As a result, it should never be run when the catalog file system is 100% full.
- To ensure that catalog backup images are not on the same tapes as user backups, create a separate media pool for catalog archives.
- You may find it useful to set up and then designate, a special retention level for catalog archive images.
To specify retention levels, open the NetBackup web UI. On the left click **Hosts > Host properties**. Locate the primary server and click **Edit primary server**. Then click **Retention periods**.
- Additional time is required to mount the tape and perform the restore of archived .f files.
- There is no simple method to determine to which tape the catalog has been archived. The `bpcatlist -offline` command is the only administrative command to determine what images have been archived. This command does not list what tape was used for the archive. As a result, exercise caution to ensure that the tapes used for catalog archiving are available for restoring the archived catalog images. Either create a separate volume pool to use exclusively for catalog archives or find a method to label the tape as a catalog archive tape.

Extracting images from the catalog archives

The situation may arise in which a storage provider needs to extract all of a specific client's records. The storage provider can extract the customer images from the catalog archive by creating the archives that are based on client name.

To extract images from the catalog archives based on a specific client

- 1 Create a volume pool for the client.
- 2 Create a catalog archiving policy. Indicate the volume pool for that client in the **Attributes** tab.
- 3 Run `bpcatlist` so only the `.f` files from that client are listed. For example:

```
bpcatlist -client clientname | bpcatarc | bpcatrm
```
- 4 If you do not want to write more images to the client's volume pool, change the volume pool before you run another archiving catalog.

Estimating catalog space requirements

NetBackup requires disk space to store its error logs and information about the files it backs up.

The disk space that NetBackup needs varies according to the following factors:

- Number of files to be backed up
- Frequency of full and incremental backups
- Number of user backups and archives
- Retention period of backups
- Average length of full path of files
- File information (such as owner permissions)
- Average amount of error log information existing at any given time
- Whether you have enabled the database compression option.

To estimate the disk space that is required for a catalog backup

- 1 Estimate the maximum number of files that each schedule for each policy backs up during a single backup of all its clients.
- 2 Determine the frequency and the retention period of the full and the incremental backups for each policy.

- 3 Use the information from steps 1 and 2 to calculate the maximum number of files that exist at any given time.

For example:

Assume that you schedule full backups to occur every seven days. The full backups have a retention period of four weeks. Differential incremental backups are scheduled to run daily and have a retention period of one week.

The number of file paths you must allow space for is four times the number of files in a full backup. Add to that number one week's worth of incremental backups.

The following formula expresses the maximum number of files that can exist for each type of backup (daily or weekly, for example):

Files per Backup × Backups per Retention Period = Max Files

For example:

A daily differential incremental schedule backs up 1200 files and the retention period for the backup is seven days. Given this information, the maximum number of files that can exist at one time are the following:

$$1200 \times 7 \text{ days} = 8400$$

A weekly full backup schedule backs up 3000 files. The retention period is four weeks. The maximum number of files that can exist at one time are the following:

$$3000 \times 4 \text{ weeks} = 12,000$$

Obtain the total for a server by adding the maximum files for all the schedules together. Add the separate totals to get the maximum number of files that can exist at one time. For example, 20,400.

For the policies that collect true image restore information, an incremental backup collects catalog information on all files (as if it were a full backup). This changes the calculation in the example: the incremental changes from $1200 \times 7 = 8400$ to $3000 \times 7 = 21,000$. After 12,000 is added for the full backups, the total for the two schedules is 33,000 rather than 20,400.

- 4 Obtain the number of bytes by multiplying the number of files by the average number of bytes per file record.

If you are unsure of the average number of bytes per file record, use 132. The results from the examples in step 3 yield:

$$(8400 \times 132) + (12,000 \times 132) = 2692800 \text{ bytes (or about 2630 kilobytes)}$$

- 5 Add between 10 megabytes to 15 megabytes to the total sum that was calculated in step 4. The additional megabytes account for the average space that is required for the error logs. Increase the value if you anticipate problems.
- 6 Allocate space so all the data remains in a single partition.

NetBackup file size considerations on UNIX systems

File system limitations on UNIX include the following:

- Some UNIX systems have a large file support flag. Turn on the flag to enable large file support.
- Set the file size limit for the root user account to unlimited to support large file support.

Moving the image catalog

An image catalog may become too large for its current location. Consider moving the image catalog to a file system or disk partition that contains more available space.

Notes about moving the image catalog

- NetBackup does not support saving the catalog to a remote NFS share. CIFS is supported on some SAN or NAS storage.
See [“Parts of the NetBackup catalog”](#) on page 392.
- NetBackup only supports moving the image catalog to a different file system or disk partition. It does not support moving the other subdirectories that make up the entire NetBackup catalog.
For example, on Windows, do not use the `ALTPATH` mechanism to move `install_path\NetBackup\db\error`.
For example, on UNIX, do not move `/usr/opensv/netbackup/db/error`. The catalog backup only follows the symbolic link when backing up the `/images` directory. So, if symbolic links are used for other parts of the NetBackup catalog, the files in those parts are not included in the catalog backup.
- The directory that is specified in the `ALTPATH` file is not automatically removed if NetBackup is uninstalled. If NetBackup is uninstalled, you must manually remove the contents of this directory.

Moving the image catalog between Windows hosts

To move the image catalog on Windows

- 1 Back up the NetBackup catalogs manually.

A backup of the catalogs ensures that you can recover image information in case something is accidentally lost during the move.

See [“Backing up NetBackup catalogs manually”](#) on page 180.

- 2 Check the **Jobs** tab in the **Activity monitor** and ensure that no backups or restores are running for the client.

If jobs are running, either wait for them to end or stop them by using the **Jobs** tab in the Activity monitor.

- 3 Use the **Daemons** tab in the **Activity monitor** to stop the Request Manager and the Database Manager daemons. These services are stopped to prevent jobs from starting. Do not modify the database while this procedure is performed.

- 4 Create a file named `ALTPATH` in the image catalog directory.

For example, if NetBackup is installed in the default location and the client name is *mars*, the path to the image catalog is:

```
C:\Program Files\Veritas\NetBackup\db\images\mars\ALTPATH
```

- 5 Create the directory to which you intend to move the image information. For example:

```
E:\NetBackup\alternate_db\images\client_name
```

- 6 On the first line of the `ALTPATH` file, specify the path to the directory where you intend to move the client's image information. For example:

```
E:\NetBackup\alternate_db\images\client_name
```

The path is the only entry in the `ALTPATH` file.

- 7 Move all files and directories (except the `ALTPATH` file) that are in the current client directory to the new directory.

For example, if the images are currently in

```
C:\Program Files\Veritas\NetBackup\db\images\mars
```

and the `ALTPATH` file specifies

```
E:\NetBackup\alternate_db\images\mars
```

then move all files and directories (except the `ALTPATH` file) to

```
E:\NetBackup\alternate_db\images\mars
```

- 8 Start the NetBackup Request Daemon, NetBackup Job Manager, and NetBackup Policy Execution manager in the **Daemons** tab.

Backups and restores can now resume for the client.

Moving the image catalog between UNIX hosts

To move the image catalog on UNIX

- 1 Check that no backups are in progress by running:

```
/usr/opensv/netbackup/bin/bpps
```

- 2 Stop `bprd` by running:

```
/usr/opensv/netbackup/bin/admincmd/bprdreq -terminate
```

- 3 Stop `bpdbm` by running:

```
/usr/opensv/netbackup/bin/bpdbm -terminate
```

- 4 Create the directory in the new file system. For example:

```
mkdir /disk3/netbackup/db/images
```

- 5 Move the image catalog to the new location in the other file system.

- 6 Create a symbolic link from `/usr/opensv/netbackup/db/images` to the new location in the other file system.

See [“NetBackup file size considerations on UNIX systems”](#) on page 411.

About image catalog compression

The image catalog contains information about all client backups. It is accessed any time a user lists or restores files. NetBackup lets you compress all portions of the catalog or only older portions of the catalog.

Control image catalog compression by setting the **Compress catalog interval** in the **Global attributes** host property. This interval indicates how old the backup

information must be before it is compressed. Specify the number of days to defer compression information, so users who restore files from recent backups are not affected. By default, **Compress catalog interval** is set to 0 and image compression is not enabled.

Note: Veritas discourages manually compressing or decompressing the catalog backups with the `bpimage -[de]compress` command or any other method. Manually compressing or decompressing a catalog backup while any backup (regular or catalog) is running results in inconsistent image catalog entries. When users list and restore files, the results can be incorrect.

It does not make a difference to NetBackup if the backup session was successful. The operation occurs while NetBackup expires backups and before it runs the `session_notify` script and the backup of the NetBackup catalogs.

The time to perform compression depends on the server speed and the number and size of the files being compressed. Files are compressed serially, and temporary working space is required in the same partition.

When numerous compressed image catalog files must be processed, the backup session is extended until compression is complete. The additional backup time is especially noticeable the first time you perform the compression. To minimize the effect of the initial sessions, consider compressing the files in stages. For example, begin by compressing the records for the backups older than 120 days. Continue to reduce the number of days over a period of time until you reach a comfortable setting.

Compressing the image catalog accomplishes the following objectives:

- Reduces greatly the disk space that is consumed.
- Reduces the media that is required to back up the catalog.

The amount of space that is reclaimed varies with the types of backups you perform. Full backups result in a larger percentage of catalog compression than incremental backups. Normally, more data is duplicated in a catalog file for a full backup. Using catalog compression, a reduction of 80% is possible.

This reduction in disk space and media requirements is achieved at the expense of performance when a user lists or restores files. Since the information is uncompressed at each reference, performance degradation is in direct proportion to the number and size of compressed files that are referenced. If the restore requires numerous catalog files to be uncompressed, increase the **File browse timeout** value that is associated with list requests. (See the **Timeouts** host property for the client.)

Uncompressing the NetBackup catalog

You may find it necessary to temporarily uncompress all records that are associated with an individual client. Uncompress the records if you anticipate large or numerous restore requests, for example.

To uncompress the NetBackup catalog on Windows

- 1 Verify that the partition where the image catalog resides contains enough space to accommodate the uncompressed catalog.
See [“Estimating catalog space requirements”](#) on page 409.
- 2 Stop the NetBackup Request Daemon service, `bprd`.
- 3 Verify that the NetBackup Database Manager, `bpdbm`, is running.
- 4 In the NetBackup web UI, select **Hosts > Host properties**.
- 5 Select the primary server and click **Connect**. Then select the server and click **Edit primary server**.

- 6 Select **Global attributes**.

- 7 Clear the **Compress catalog interval** check box. Then click **Save**.

- 8 Open a command prompt. Change to the following directory:

```
install_path\Veritas\NetBackup\bin\admincmd
```

Run one of the followings commands.

To decompress the records for a specific client, enter:

```
bpimage -decompress -client_name
```

To decompress the records for all clients, enter:

```
bpimage -decompress -allclients
```

- 9 Restart the NetBackup Request Daemon (`bprd`).
- 10 Restore the files from the client.
- 11 Set the **Compress catalog interval** to its previous value.

The records that were uncompressed for this client are compressed after the next backup schedule.

To uncompress the NetBackup catalog on UNIX

- 1 Perform the following steps as root on the primary server to uncompress the NetBackup catalog.

Verify that the partition where the image catalog resides has enough space to uncompress the client's image records.

- 2 Stop the request daemon, `bprd`, by running:

```
/usr/opensv/netbackup/bin/admincmd/bprdrege -terminate
```

- 3 Make sure that `bpdbm` is running:

```
/usr/opensv/netbackup/bin/bpps
```

- 4 In the NetBackup web UI, select **Hosts > Host properties**.

- 5 Select the primary server and click **Connect**. Then select the server and click **Edit primary server**.

- 6 Select **Global attributes**.

- 7 Clear the **Compress catalog interval** check box. Then click **Save**.

- 8 Change your working directory to `/usr/opensv/netbackup/bin` and run the command:

```
admincmd/bpimage -decompress -client name
```

- 9 Restart the request daemon `bprd`. Run the following command:

```
/usr/opensv/netbackup/bin/initbprd
```

- 10 Restore the files from the client.

- 11 Set the **Compress catalog interval** to its previous value.

The records that were uncompresssed for this client are compressed after the next backup schedule.

About the NetBackup database

This chapter includes the following topics:

- [About the NetBackup database installation](#)
- [Post-installation tasks](#)
- [Using the NetBackup Database Administration utility on Windows](#)
- [Using the NetBackup Database Administration utility on UNIX](#)

About the NetBackup database installation

Generally, the implementation of the NetBackup database in the NetBackup catalog is transparent. The NetBackup primary server includes a private, non-shared database server for the NetBackup database (NBDB).

The same installation of the NetBackup database is used for the optionally-licensed product, Bare Metal Restore (BMR) and its associated database (BMRDB). The BMR database is created during the BMR installation process.

By default, the NetBackup database (NBDB) is installed on the primary server. The primary server is also the default location for the Enterprise Media Manager (EMM). Since EMM is the primary user of NBDB, the NetBackup database always resides on the same computer as the Enterprise Media Manager.

See [“About the Enterprise Media Manager \(EMM\)”](#) on page 394.

About NetBackup primary server installed directories and files

The NetBackup Scale-Out Relational Database is installed in the following directories.

Windows

`install_path\Veritas\NetBackupDB`

`install_path\Veritas\NetBackup\bin`

`install_path\Veritas\NetBackupDB\data\instance`

The databases are installed in the following subdirectories:

`install_path\Veritas\NetBackupDB\data\nbdb\`

`install_path\Veritas\NetBackupDB\data\nbazdb\`

`install_path\Veritas\NetBackupDB\data\bmrdb\` (if BMR is installed)

On UNIX

`/usr/opensv/db`

`/usr/opensv/var/global`

`/usr/opensv/db/data/instance/`

The databases are installed in the following subdirectories:

`/usr/opensv/db/data/nbdb/`

`/usr/opensv/db/data/nbazdb/`

`/usr/opensv/db/data/bmrdb/`

About the `bin` directory

The `bin` is located as follows:

`install_path\Veritas\NetBackup\bin`

Warning: Use these utilities and commands in this directory with caution.

Contains the utilities and binaries for running and administering NetBackup services. More information can be found in the *NetBackup Commands Reference Guide*.

For information on using the NetBackup Database Administration utility (`NbDbAdmin.exe` or `dbadm`), see the following topics:

See [“Using the NetBackup Database Administration utility on Windows”](#) on page 428.

See [“Using the NetBackup Database Administration utility on UNIX”](#) on page 433.

About the contents of the NetBackupDB and db directories

The following table describes the contents of the following directories.

On Windows: `install_path\Veritas\NetBackupDB\`

On UNIX: `/usr/openv/db/`

Table 44-1 NetBackupDB and db directory contents

Directory	Description
bin	Contains the utilities and commands for administering the NetBackup database service.
data	The default location of the NetBackup databases (NBDB, NBAZDB, and BMRDB) and certain configuration files.
lib	On UNIX: Contains all the shared libraries for the NetBackup Scale-Out Relational Database. The directory also includes ODBC libraries, used to connect to NBDB and BMRDB.
scripts	Warning: Do not edit the scripts that are located in this directory. Contains the scripts that are used to create the NetBackup database. It also contains the scripts that are used to create the EMM and other schemas.
share	Contains the PostgreSQL document and module files that are required by the NetBackup database server.
staging	Used as a temporary staging area during catalog backup and recovery.
WIN64	(Windows) Contains .dll files for the NetBackup Scale-Out Relational Database.

About the data directory

The following directory is the default location of the NetBackup database, NBDB:

On Windows: `install_path\NetBackupDB\data`

On UNIX: `/usr/openv/db/data`

The `\data\` directory contains the following subdirectories and files:

- `bmrdb`
If BMR is installed, this directory contains the BMR database.
- `nbdb`
The main NetBackup database, including EMM.
- `nbazdb`
The NetBackup Authorization database.
- `vxdbs.conf`

The file that contains the configuration information specific to the installation of the NetBackup database.

See “[vxdbms.conf](#)” on page 420.

- `nbdbinfo.dat`
A backup of the NetBackup DBA password.

vxdbms.conf

On Windows:

```
VXDBMS_NB_SERVER = NB_server_name
VXDBMS_NB_DATABASE = NBDB
VXDBMS_BMR_DATABASE = BMRDB
VXDBMS_AZ_DATABASE = NBAZDB
VXDBMS_NB_STAGING = C:\Program Files\Veritas\NetBackupDB\staging
VXDBMS_NB_PORT = 13785
VXDBMS_NB_DATA = C:\Program Files\Veritas\NetBackupDB\data
VXDBMS_NB_PASSWORD = encrypted_password
AZ_DB_PASSWORD = encrypted_password
VXDBMS_POSTGRESQL_POOLER_ODBC_PORT = 13787
```

On UNIX:

```
VXDBMS_NB_SERVER = NB_server_name
VXDBMS_NB_PORT = 13785
VXDBMS_NB_DATABASE = NBDB
VXDBMS_AZ_DATABASE = NBAZDB
VXDBMS_BMR_DATABASE = BMRDB
VXDBMS_NB_DATA = /usr/opensv/db/data
VXDBMS_NB_STAGING = /usr/opensv/db/staging
VXDBMS_NB_PASSWORD = encrypted_password
AZ_DB_PASSWORD = encrypted_password
VXDBMS_POSTGRESQL_POOLER_ODBC_PORT = 13787
```

The encrypted password that is used to log into the DBA accounts is stored in `vxdbms.conf`. These accounts include NBDB, NBAZDB, and BMRDB and other data accounts.

NetBackup configuration entry

The `VXDBMS_NB_DATA` registry entry (Windows) or the `bp.conf` entry (UNIX) is a required entry and is created upon installation. The entry indicates the path to the directory where the following are located: NetBackup database, authorization database, BMR database, and the `vxdbms.conf` file.

On Windows:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Veritas\NetBackup\CurrentVersion\
Config\VXDBMS_NB_DATA
```

On UNIX: /usr/openv/netbackup/bp.conf

```
VXDBMS_NB_DATA = /usr/openv/db/data
```

NetBackup database server management

This topic describes the commands that are available to manage the NetBackup database.

To start and stop the NetBackup database, use one of the following methods:

- In the **Daemons** tab of the Activity monitor, select the service **NetBackup Scale-Out Relational Database Manager** (vrtsdbsvc_psql).
- (Windows) From the Windows Service Manager, select the service **NetBackup Scale-Out Relational Database Manager** (vrtsdbsvc_psql).

- (Windows) Use the following commands:

```
install_path\Veritas\NetBackup\bin\bpdown -e vrtsdbsvc_psql
```

- `install_path\Veritas\NetBackup\bin\bpup -e vrtsdbsvc_psql`

- (UNIX) Use the following commands:

```
/usr/openv/db/bin/nbdbms_start_server -start
```

Starts the NetBackup Scale-Out Relational Database server if no option is specified.

```
/usr/openv/db/bin/nbdbms_start_server -stop -f
```

Stops the server; `-f` forces a shutdown with active connections.

The **NetBackup Scale-Out Relational Database Manager** daemon is included in the `stop` command or the `start` command, which starts and stops all NetBackup daemons.

Individual databases can be started or stopped, while the NetBackup Scale-Out Relational Database Manager service continues. Use the NetBackup Database Administration utility or the following commands:

- `nbdb_admin [-start | -stop]`

Starts or stops NBDB without shutting down the NetBackup Scale-Out Relational Database server.

To see whether the database is up, enter `nbdb_ping`.

- `nbdb_admin [-start | -stop BMRDB]`

Starts or stops BMRDB without shutting down the NetBackup Scale-Out Relational Database server.

To see whether the BMRDB database is up, enter `nbdb_ping -dbn BMRDB`.

The NetBackup database and clustered environments

The NetBackup database is supported in a clustered environment. Failover is included with the NetBackup server failover solution. The software is installed on all computers in the cluster.

The databases and the configuration files are installed in the following shared locations.

Windows

NetBackup databases:

`shared_drive\VERITAS\NetBackupDB\data`

Configuration files:

`shared_drive\VERITAS\NetBackupDB\data\instance`

UNIX

NetBackup databases:

`shared_drive/db/data`

Configuration files:

`/usr/opensv/var/global`

`shared_drive/db/data/instance`

Post-installation tasks

The tasks that are described in the following topics are optional and can be performed after the initial installation:

- Change the database password.
See [“Changing the NetBackup database password”](#) on page 423.
- Move the NetBackup databases (possibly to tune performance).
See [“Moving a database after installation ”](#) on page 424.
- Recreate NBDB.
See [“Creating the NBDB database manually”](#) on page 426.

Commands and utilities for administering the NetBackup databases

Note: Using the database administration utilities to administer the NetBackup database can potentially break the consistency between the NetBackup catalog and the database. This loss of consistency can lead to loss of data. Only use these utilities and commands with assistance of Veritas Technical Support.

The following utilities are available to administer the databases.

See [“Using the NetBackup Database Administration utility on Windows”](#) on page 428.

See [“Using the NetBackup Database Administration utility on UNIX”](#) on page 433.

Also see the following commands in the *NetBackup Commands Reference Guide*.

`create_nbdb`

`nbdb_backup`

`nbdb_restore`

`nbdb_unload`

Changing the NetBackup database password

The database password is set to a randomly generated password upon installation. This password is used for NBDB and BMRDB and for all DBA and application accounts. You can use this procedure to change it to a known password.

The password is encrypted and stored in the `vxdbsms.conf` file. The permissions for the `vxdbsms.conf` file allow only a Windows administrator or a `root` user to read or write to it.

For requirements when NBAC is enabled, see the *NetBackup Security and Encryption Guide*.

To change the database password

- 1 Log on to the server as a Windows Administrator or as `root`.
- 2 To change the password for the first time after installation, run the following command. The command updates the `vxdbms.conf` file with the new, encrypted string:

On Windows: `install_path\NetBackup\bin\nbdb_admin -dba new_password`

On UNIX: `/usr/opensv/db/bin/nbdb_admin -dba new_password`

The password needs to be an ASCII string. Non-ASCII characters are not allowed in the password string.

- 3 To change a known password to a new password, you can either use the `nbdb_admin` command or the NetBackup Database Administration utility. You must know the current password to log into the NetBackup Database Administration utility.

See [“Using the NetBackup Database Administration utility on Windows”](#) on page 428.

See [“Using the NetBackup Database Administration utility on UNIX”](#) on page 433.

Moving a database after installation

The NetBackup database (NBDB) and the NetBackup authorization database (NBAZDB), are created on the primary server by default. To improve performance, you can use the NetBackup database administration utilities or command-line options to change the location of the databases.

Note the following:

- If BMR is installed and you want to move its database, it must reside on the primary server.
- Due to performance issues, you can only move a database to another disk or volume. The disk or volume must be locally attached.
NetBackup does not support saving the NetBackup database (NBDB, including EMM), NBAZDB, or the configuration files to a remote NFS share. CIFS is supported on some SAN storage and NAS storage.
- Run a catalog backup to back up NBDB and BMRDB both before and after moving the databases.

Moving a NetBackup database on Windows

The following instructions describe how to use the database administration utility to move a database.

You can also use the following command:

```
install_path\Veritas\NetBackup\bin\nbdb_move.exe
```

You can run the `nbdb_move` command at any time because it does not drop the database and recreate it. Therefore all the data is preserved.

To move a NetBackup database on Windows

- 1 Perform a catalog backup.
- 2 Shut down all NetBackup services by typing the following command:

```
install_path\Veritas\NetBackup\bin\bpdown
```
- 3 Start the NetBackup Scale-Out Relational Database Manager service:

```
install_path\Veritas\NetBackup\bin\bpup -e vrtsdbsvc_psql
```
- 4 Start the NetBackup Database Administration utility and enter the database logon password. Click **OK**.
- 5 From the **Database** list, select the database that you want to move.
- 6 Select the **Tools** tab.
- 7 Click **Move**.
- 8 Select **Move data to** and browse to the new location.
- 9 NetBackup does not require that the database directories are world-writable. Make sure that the new database directories (*data_directory*) have appropriate permissions so that the directories are not world-writable.
- 10 Start all services by typing the following command:

```
install_path\Veritas\NetBackup\bin\bpup
```
- 11 Perform a catalog backup.

Moving a NetBackup database on UNIX

To move a NetBackup database on UNIX

- 1 Perform a catalog backup.
- 2 Shut down all NetBackup daemons by typing the following command:

```
/usr/opensv/netbackup/bin/bp.kill_all
```
- 3 Start the NetBackup Scale-Out Relational Database Manager daemon:

```
/usr/opensv/netbackup/bin/nbdbms_start_stop start
```
- 4 Use one of the following methods to move the existing databases:

- Use the **Move Database** option in the NetBackup Database Administration utility (dbadm).

- Enter the following command:

```
/usr/opensv/db/bin/nbdb_move  
-data data_directory
```

You can run the `nbdb_move` command at any time because it does not drop the database and recreate it. Thus, all data is preserved.

```
/usr/opensv/db/bin/nbdb_move -data data_directory
```

Note: NetBackup does not require that the database directories are world-writable. Make sure that the new database directories (`data_directory`) have appropriate permissions so that the directories are not world-writable.

- 5 Start all NetBackup daemons by typing the following command:

```
/usr/opensv/netbackup/bin/bp.start_all
```

- 6 Perform a catalog backup.

Copying the NetBackup databases

A temporary backup of the NBDB, NBAZDB, and BMRDB databases can be made for extra protection before database administration activities such as moving or reorganizing the databases. Also, some customer support situations may require that you create a copy of the NetBackup database.

Use the NetBackup database administration utilities or the `nbdb_backup` command to make this kind of backup.

Creating the NBDB database manually

The NBDB database is created automatically during NetBackup installation. However, it may be necessary during certain catalog recovery situations to create it manually by using the `create_nbdb` command.

Caution: Recreating the database manually is not recommended in most situations.

Note: If the NBDB database already exists, the `create_nbdb` command does not overwrite it. If you want to move the database, move it by using the `nbdb_move` command.

To create the NBDB database manually on Windows

- 1 Shut down all NetBackup services by typing the following command:

```
install_path\Veritas\NetBackup\bin\bpdown
```

- 2 Start the NetBackup Scale-Out Relational Database Manager service with the following command:

```
install_path\Veritas\NetBackup\bin\bpup -e vrtsdbsvc_psql
```

- 3 Run the following command:

```
install_path\Veritas\NetBackup\bin\create_nbdb.exe
```

- 4 Start all NetBackup services by typing the following command:

```
install_path\Veritas\NetBackup\bin\bpup
```

- 5 The new NBDB database is empty and does not contain the EMM data that is loaded during a normal installation.

Make sure that you have the most current support for new devices before the data is repopulated. New devices are added approximately every 2 months.

- 6 Repopulate the EMM data by running the `tpext` utility. `tpext` updates the EMM database with new versions of device mappings and external attribute files.

```
install_path\Veritas\Volmgr\bin\tpext.exe
```

During regular installation, `tpext` is run automatically.

If the `create_nbdb` command is used to create a database manually, the `tpext` utility must also be run. `tpext` loads EMM data into the database.

To create the NBDB database manually on UNIX

- 1 Shut down all NetBackup daemons by typing the following command:

```
/usr/opensv/netbackup/bin/bp.kill_all
```

- 2 Start the NetBackup Scale-Out Relational Database Manager service with the following command:

```
/usr/opensv/netbackup/bin/nbdbms_start_stop start
```

- 3 Run the following command:

```
/usr/opensv/db/bin/create_nbdb
```

- 4 Start all NetBackup daemons by typing the following command:

```
/usr/opensv/netbackup/bin/bp.start_all
```

- 5 The new `NBDB` database is empty and does not contain the `EMM` data that is loaded during a normal installation.

Make sure that you have the most current support for new devices before the data is repopulated. New devices are added approximately every 2 months.

- 6 Repopulate the `EMM` data by running the `tpext` utility. `tpext` updates the `EMM` database with new versions of device mappings and external attribute files.

```
/usr/openv/volmgr/bin/tpext
```

During regular installation, `tpext` is run automatically.

If the `create_nbdb` command is used to create a database manually, the `tpext` utility must also be run. `tpext` loads `EMM` data into the database.

Additional `create_nbdb` options

In addition to using the `create_nbdb` command to create the `NBDB` database, you also can use it to perform the following actions. In each command, *NB_server_name* matches the name in the following file: `postgresql.conf`

- Drop the existing `NBDB` database and recreate it in the default location:

```
create_nbdb -drop
```

On UNIX, the location of the current `NBDB` data directory is retrieved automatically from the `bp.conf` file.

- Drop the existing `NBDB` database and do not recreate it:

```
create_nbdb -drop_only
```

- Drop the existing `NBDB` database and recreate it in the *data* directory:

```
create_nbdb -drop -data data_directory
```

If the `NBDB` database was moved from the default location by using `nbdb_move`, use this command to recreate it in the same location. Specify `current_data_directory`. `BMRDB` must also be recreated. The `BMRDB` database must reside in the same location as the NetBackup database.

Using the NetBackup Database Administration utility on Windows

The NetBackup administrator can use the Database Administration utility to configure the NetBackup databases and to monitor database operations. To use the utility, the administrator must have Administrator user privileges.

The **General** tab contains information about database tablespaces. The tab contains tools to let the administrator reorganize fragmented database objects and validate and rebuild the database.

Table 44-2 General tab options

Option	Description
Refresh	Displays the most current information.
Reorganize All	This option defragments the tablespaces that are fragmented.
Validate	<p>This option performs a database validation on all of the database tablespaces in the selected database.</p> <ul style="list-style-type: none"> Validates the indexes and keys on all of the tables in the database. Scans each table. For each row, a check is made that it exists in the appropriate indexes. The number of rows in the table must match the number of entries in the index. Ensures that every row that is referenced in each index exists in the corresponding table. For foreign key indexes, it also ensures that the corresponding row exists in the primary table. <p>After a validation check runs, the Results screen lists each database object. Each error is listed next to the database object where it was found. The total number of errors are listed at the end of the list of database objects. If no errors were found, that is indicated.</p> <p>If any validation errors are reported, perform the following tasks:</p> <ul style="list-style-type: none"> Shut down NetBackup (all daemons and services). Start only the NetBackup database server (vrtssdbsvc_psql). Click Validate to repeat the validation check or use the <code>nbdb_admin.exe</code> command line utility. <p>If validation errors persist, contact Veritas Technical Support. The administrator may be asked to rebuild the database using the Rebuild option or the <code>nbdb_unload.exe</code> command line utility.</p>
Rebuild	<p>This option unloads and reloads the database. A new database with all of the same options is built in its place.</p> <p>A Database Rebuild may be required if validation errors are reported when you use the Validate option.</p> <p>Note: Before you rebuild the database, it is recommended that you create a copy of the database by performing a backup from the Tools tab.</p> <p>To rebuild the database temporarily suspends NetBackup operations and can take a long time depending on the database size.</p>

About fragmentation

Table fragmentation can impede performance. When rows are not stored contiguously, or if rows are split into more than one page, performance decreases because these rows require additional page accesses.

When an update to a row causes it to grow beyond the originally allocated space, the row is split. The initial row location contains a pointer to another page where the entire row is stored. As more rows are stored on separate pages, more time is required to access the additional pages.

Reorganizing may also reduce the total number of pages that are used to store the table and its indexes. It may reduce the number of levels in an index tree. Note that the reorganization does not result in a reduction of the total size of the database.

The **Rebuild** option on the **General** tab completely rebuilds the database, eliminating any fragmentation, and free space. This option may result in a reduction of the total size of the database.

See [“Estimating catalog space requirements”](#) on page 409.

The **Tools** tab of the NetBackup Database Administration utility contains a variety of tools to administer the selected database:

Password	See “Changing the DBA password using the NetBackup Database Administration utility” on page 430.
Move Database	See “Moving a NetBackup database” on page 431.
Unload	See “Exporting database schema and data” on page 431.
Backup	See “Copying or backing up a database ” on page 431.
Restore	See “Restoring a database from a backup” on page 432.

Changing the DBA password using the NetBackup Database Administration utility

To change a known password to a new password, you can either use the `nbdbb_admin` command or the NetBackup Database Administration utility.

To change the DBA password from a known password to a new password

- 1 Select the **Tools** tab.
- 2 In the **Password** section, click **Change**.
- 3 Enter the new password and confirm the new password. Changing the password changes it for both NBDB and BMRDB, if a BMR database is present.

- 4 Enable **Create a backup file of your new DBA password** to keep track of the password.
- 5 Click **OK**.
 The utility warns you that it is important to remember the password. You cannot recover information within the EMM database if the password is unavailable.
- 6 Restart the database for the password change to take effect.

Moving a NetBackup database

Use the NetBackup Database Administration utility to change the location of a database.

For full instructions on how to move a database, see the following topic.

See [“Moving a database after installation ”](#) on page 424.

Exporting database schema and data

To export database schema and data

- 1 Select the **Tools** tab.
- 2 In the **Unload** section, click **Export**.
- 3 Browse to a destination directory.
- 4 Select one or more of the following options:

Schema	Unload only the database schema. The schema is unloaded as a file that is named <i>database.sql</i> in the named directory. For the NBDB database, the schema is unloaded as a file that is named <i>NBDB.sql</i> in the named directory. For other databases, a similar file is created. For example, for BMRDB the file is <i>BMRDB.sql</i> . For NBAZDB the file is <i>NBAZDB.sql</i> .
Schema and data	Unload both the database schema and the data. The data is unloaded as a set of files in comma-delimited format. One file is created for each database table.

- 5 Click **OK**.

Copying or backing up a database

Use the NetBackup Database Administration utility to back up the database to a specified directory.

It is recommended that you create a backup copy of a database in the following situations:

- | | |
|----------------------------------|--|
| Before you move the database. | See "Moving a NetBackup database" on page 431. |
| Before you rebuild the database. | See "" on page 429. |

Note: Using the NetBackup Database Administration utility to back up and restore the NetBackup database can potentially break the consistency between the NetBackup catalog and the database. This loss of consistency can lead to loss of data. Use the tool to back up and restore the NetBackup catalog only as a precautionary measure.

To copy or back up a database

- 1 Start the NetBackup Database Administration utility and enter the database logon password. Click **OK**.
- 2 Select the **Tools** tab.
- 3 Click **Copy**.
- 4 Browse to a destination directory.

A copy of the database is made to this directory. This directory is also the location of the database that the **Restore** option uses.

Note: This backup is not a catalog backup, performed as part of regular NetBackup operations.

See ["Restoring a database from a backup"](#) on page 432.

- 5 Click **OK**.

Restoring a database from a backup

Use the NetBackup Database Administration utility to restore a database from a backup copy.

The restore overwrites the current database. The database is shut down and restarted after the restore is completed.

A database restore causes NetBackup activity to be suspended, so do not perform a database restore while active backups or other restores run.

Note: Using the Database Administration utility to back up and restore the NetBackup database can potentially break the consistency between the NetBackup catalog and the database. This loss of consistency can lead to loss of data. Use the tool to back up and restore the NetBackup database only as a precautionary measure.

To restore a database from a backup

- 1 Start the NetBackup Database Administration utility and enter the database logon password. Click **OK**.
- 2 Select the **Tools** tab.
- 3 Click **Restore**.
- 4 Browse to the directory that contains the backup database.
- 5 Click **OK**.

Using the NetBackup Database Administration utility on UNIX

The NetBackup Database Administration utility (`dbadm`) is a standalone application that is supported for NBDB and BMRDB. It is installed in the following location:

`/usr/opensv/db/bin`

To use the NetBackup Database Administration utility, you must be an administrator with root user privileges. When you start the NetBackup Database Administration utility, enter the DBA password. The password is set to a randomly generated password upon installation. Use the `nbdb_admin` command to change it to a known password if you have not done so already.

See [“Changing the NetBackup database password”](#) on page 423.

After you log on, the NetBackup Database Administration utility displays the following information about the current database:

Table 44-3 NetBackup Database Administration utility properties

Property	Description
Selected database	The selected database: NBDB or BMRDB
Status	The status of the selected database: UP or DOWN
Consistency	The validation state of the selected database: OK, NOT_OK, or DOWN

The initial screen also displays the following Database Administration main menu:

Table 44-4 Database Administration main menu options

Option	Description
Select/Restart Database and Change Password	This option displays the menu where you can select a database to start or stop, and to change database passwords. See “Select/Restart Database and Change Password menu options” on page 434.
Database Space Management	This option displays the menu where you can perform the following actions: <ul style="list-style-type: none"> ■ Generate a database space utilization report ■ Reorganize fragmented database objects See “Database Space Management menu options” on page 435.
Transaction Log Management	This option is not supported.
Database Validation Check and Rebuild	This option displays the menu where you can validate and rebuild the selected database. See “Database Validation Check and Rebuild menu options” on page 436.
Move Database	This option displays the menu where you can change the location of the database tablespaces. See “Move Database menu options” on page 437.
Unload Database	This option displays the menu where you can unload either the schema or the schema and data from the database. See “Unload Database menu options” on page 438.
Backup and Restore Database	This option displays the menu where you can choose the backup and restore options for the database. See “Backup and Restore Database menu options” on page 438.
Refresh Database Status	This option refreshes the Status and Consistency in the main menu.

Select/Restart Database and Change Password menu options

The Select/Restart Database and Change Password menu contains the following options.

Table 44-5 Select/Restart Database and Change Password options

Option	Description
NBDB	Select NBDB and then view or modify the database using the other <code>dbadm</code> menu options.

Table 44-5 Select/Restart Database and Change Password options
(continued)

Option	Description
BMRDB	Select BMRDB and then view or modify the database using the other <code>dbadm</code> menu options.
Start Selected Database	Starts the selected database.
Stop Selected Database	Stops the selected database.
Change Password	<p>Changes the password for the databases. The password is changed for both NBDB and BMRDB, if applicable. Restart the database for the password change to take effect.</p> <p>To log into the Database Administration utility, you must know the current DBA password.</p> <p>To change the password for the first time after installation, use the <code>nbdb_admin</code> command. The command updates the <code>vxdbms.conf</code> file with the new, encrypted string:</p> <p>See “Changing the NetBackup database password” on page 423.</p> <p>To change a known password to a new password, you can either use the <code>nbdb_admin</code> command or the NetBackup Database Administration utility.</p>

Database Space Management menu options

You can use the Database Space Management option to perform the following functions:

- To report on database space utilization
- To reorganize fragmented database objects

Table 44-6 Database Space and Memory Management options

Option	Description
Report on Database Space	<p>The report contains the tablespaces and the physical pathnames of the databases.</p> <p>For each tablespace, the report displays the name, the amount of free space in KBytes, and the file size in KBytes. The report also displays the amount of free space that remains on each of the file systems being used for the database.</p>

Table 44-6 Database Space and Memory Management options (*continued*)

Option	Description
Database Reorganize	<p>Select this option to reorganize fragmented database tablespaces.</p> <p>These actions are performed from the Database Reorganize menu as follows:</p> <ul style="list-style-type: none"> ■ 1) Defragment All This option automatically determines the tablespaces that are fragmented. ■ 2) Table Level Defragmentation This option generates a fragmentation report for each database table. For each table, the report includes the TABLE_NAME, number of ROWS, number of ROW_SEGMENTS, and SEGS_PER_ROW. In addition, a * displays in the ! column for an individual table if it will be automatically selected for reorganization by the Defragment All option. A row segment is all or part of one row that is contained on one page. A row may have one or more row segments. The ROW_SEGMENTS value indicates total number of row segments for the table. The SEGS_PER_ROW value shows the average number of segments per row, and indicates whether or not a table is fragmented. A SEGS_PER_ROW value of 1 is ideal, and any value more than 1 indicates a high degree of fragmentation. For example, a value of 1.5 means that half of the rows are partitioned. See “About fragmentation” on page 430.

Database Validation Check and Rebuild menu options

The Database Validation Check and Rebuild option lets you validate and rebuild the currently selected database.

Table 44-7 Database Validation Check and Rebuild menu options

Option	Description
Standard Validation	The standard type of validation is not supported. This option performs a full validation.

Table 44-7 Database Validation Check and Rebuild menu options (*continued*)

Option	Description
Full Validation	<p>This option performs a database validation on all of the database tablespaces in the selected database.</p> <ul style="list-style-type: none"> Validates the indexes and keys on all of the tables in the database. Scans each table. For each row, a check is made that it exists in the appropriate indexes. The number of rows in the table must match the number of entries in the index. Ensures that every row that is referenced in each index exists in the corresponding table. For foreign key indexes, it also ensures that the corresponding row exists in the primary table. <p>Note: To perform a full database validation, shut down NetBackup and start only the database service.</p> <p>If any validation errors are reported, perform the following tasks:</p> <ul style="list-style-type: none"> Shut down NetBackup (all daemons and services). Start only the NetBackup database server (vrtsdbsvc_psql). Repeat the validation check using this tool or the <code>nbdb_admin</code> command line utility. <p>If validation errors persist, contact Veritas Technical Support. The administrator may be asked to rebuild the database using the Database Rebuild option or the <code>nbdb_unload.exe</code> command-line utility.</p>
Database Rebuild	<p>This option lets you rebuild the database. A Database Rebuild results in a complete unload and reload of the database. A new database with all of the same options is built in place. A Database Rebuild may be required if Database Validation errors are reported using the Standard or Full Validation options.</p> <p>During a Database Rebuild, all NetBackup operations are suspended.</p> <p>When you select this option, a message appears which recommends that you exit and create a backup using the Backup Database option before you rebuild the database. You then have the choice of whether to continue or not.</p> <p>See “Backup and Restore Database menu options” on page 438.</p>

Move Database menu options

The Move Database menu option lets you change the location of a database. After you select Move Database, you are prompted for the directory name where you want to move the database.

For full instructions on how to move a database, see the following topic.

See [“Moving a database after installation ”](#) on page 424.

Unload Database menu options

The Unload Database menu options let you unload either the schema or the schema and data from the `NBDB` or the `BMRDB` database.

A file is created that can be used to rebuild the database. If the data is also included in the unload, a set of data files in comma-delimited format is created.

The Unload Database menu contains the following options.

Table 44-8 Unload Database menu options

Option	Description
Schema Only	This option lets you unload only the database schema. For the <code>NBDB</code> database, the schema is unloaded as a file that is named <code>NBDB.sql</code> in the named directory. For <code>BMRDB</code> the file is <code>BMRDB.sql</code> .
Data and Schema	This option lets you unload both the database schema and the data. The data is unloaded as a set of files. One file is created for each database table.
Change Directory	This option lets you change the directory location for the files that unload options (1) or (2) create.

Backup and Restore Database menu options

The Backup and Restore Database menu options let you back up the NetBackup database to the specified directory. You can restore from a previously created backup.

It is recommended to create a backup copy of the databases in the following situations:

- Before you move the database.
- Before you rebuild the database.

Note: Using the NetBackup Database Administration utility to back up and restore the NetBackup database can potentially break the consistency between the NetBackup catalog and the database. This loss of consistency can lead to loss of data. Use the tool to back up and restore the NetBackup database only as a precautionary measure.

Table 44-9 Backup and Restore Database menu options

Option	Description
Online Backup	This option lets you make a copy of the databases while the databases are active. Other NetBackup activity is not suspended during this time.
Restore Backup	This option lets you restore from a copy of the databases that was previously made with either options 1 or 2. The currently running databases are overwritten, and the database is shut down and restarted after the restore is completed.
Change Directory	This option lets you change the directory location for the databases that the backup options (1) or (2) create. This directory is the source of the databases for the restore option (3).