

Symantec NetBackup™ Cloud Administrator's Guide

UNIX, Windows, Linux

Release 7.7



Symantec NetBackup™ Cloud Administrator's Guide

Documentation version: 7.7

Legal Notice

Copyright © 2015 Symantec Corporation. All rights reserved.

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

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 Symantec Corporation 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. SYMANTEC CORPORATION 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, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. 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.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.com>

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
 - Error messages and log files
 - Troubleshooting that was performed before contacting Symantec
 - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan customercare_apj@symantec.com

Europe, Middle-East, and Africa semea@symantec.com

North America and Latin America supportsolutions@symantec.com

Contents

Technical Support	3
Chapter 1	About NetBackup Cloud storage 9
	About Amazon S3-compatible cloud providers that NetBackup supports beginning in NetBackup 7.7 9
	About cloud storage features and functionality 10
	About support limitations for NetBackup cloud storage 12
Chapter 2	Configuring cloud storage in NetBackup 14
	Configuring cloud storage in NetBackup 15
	Cloud installation requirements 16
	About the cloud storage providers 17
	About the Amazon cloud storage requirements 18
	About the Amazon GovCloud storage requirements 19
	About AT&T Synaptic cloud storage requirements 20
	About the Cloudfian HyperStore storage requirements 22
	About the Google Nearline cloud storage requirements 23
	About the Hitachi cloud storage requirements 24
	About Rackspace Cloud Files storage requirements 25
	About the Verizon cloud storage requirements 27
	About private clouds from Amazon S3-compatible cloud providers 28
	Scalable Storage properties 29
	Configuring advanced bandwidth throttling settings 31
	Advanced bandwidth throttling settings 32
	About the NetBackup CloudStore Service Container 34
	NetBackup CloudStore Service Container security certificates 35
	NetBackup CloudStore Service Container security modes 36
	NetBackup cloudstore.conf configuration file 36
	Generating a security certificate for a media server 38
	About data encryption for cloud storage 38
	About key management for encryption of NetBackup cloud storage 39
	About cloud storage servers 40

About cloud storage data movers	41
Configuring a storage server for cloud storage	42
Amazon S3 storage server configuration options	47
Amazon GovCloud storage server configuration options	49
AT&T storage server configuration options	52
Cloudian HyperStore storage server configuration options	54
Google Nearline storage server configuration options	57
Hitachi storage server configuration options	58
Rackspace storage server configuration options	61
Verizon storage server configuration options	62
KMS database encryption settings	65
Changing cloud storage server properties	66
NetBackup cloud storage server properties	67
NetBackup storage server cloud connection properties	68
NetBackup cloud storage server bandwidth throttling properties	73
NetBackup cloud storage server encryption properties	76
About cloud storage disk pools	77
Configuring a disk pool for cloud storage	78
Changing cloud disk pool state	86
Saving a record of the KMS key names for NetBackup cloud storage encryption	87
Adding backup media servers to your cloud environment	89
Configuring a storage unit for cloud storage	91
Cloud storage unit properties	92
Configure a favorable client-to-server ratio	94
Control backup traffic to the media servers	95
About NetBackup Accelerator and NetBackup Optimized Synthetic backups	95
Enabling NetBackup Accelerator with cloud storage	95
Enabling optimized synthetic backups with cloud storage	97
Creating a backup policy	99
Changing cloud storage disk pool properties	100
Cloud storage disk pool properties	101
 Chapter 3 Monitoring and Reporting	 104
About monitoring and reporting for cloud backups	104
Viewing cloud storage job details	105
Viewing NetBackup cloud storage disk reports	105
Displaying KMS key information for cloud storage encryption	106

Chapter 4	Operational notes	109
	NetBackup bpstsinfo command operational notes	109
	Unable to configure additional media servers	110
	Cloud configuration may fail if NetBackup Access Control is enabled	110
	Deleting cloud storage server artifacts	111
Chapter 5	Troubleshooting	112
	About unified logging	112
	About using the vxlogview command to view unified logs	113
	Examples of using vxlogview to view unified logs	114
	About legacy logging	115
	Creating NetBackup log file directories	116
	NetBackup cloud storage log files	117
	Enable libcurl logging	119
	NetBackup Administration Console fails to open	120
	Troubleshooting cloud storage configuration issues	120
	NetBackup Scalable Storage host properties unavailable	121
	Connection to the NetBackup CloudStore Service Container fails	121
	Cannot create a cloud storage disk pool	122
	Data transfer to cloud storage server may fail in the SSL mode	122
	Amazon GovCloud cloud storage configuration fails in non-SSL mode	122
	Troubleshooting cloud storage operational issues	123
	Cloud storage backups fail	123
	Stopping and starting the NetBackup CloudStore Service Container	125
	A restart of the nbcssc process reverts all cloudstore.conf settings	126
	NetBackup CloudStore Service Container startup and shutdown troubleshooting	126
Index		127

About NetBackup Cloud storage

This chapter includes the following topics:

- [About Amazon S3-compatible cloud providers that NetBackup supports beginning in NetBackup 7.7](#)
- [About cloud storage features and functionality](#)
- [About support limitations for NetBackup cloud storage](#)

About Amazon S3-compatible cloud providers that NetBackup supports beginning in NetBackup 7.7

Beginning with this release, NetBackup supports the cloud providers that use the Amazon Simple Storage Service (S3) REST API interface. See [Table 1-1](#)

NetBackup supports S3 version 2 authentication API for all Amazon S3-compatible cloud providers. For more details, contact your cloud provider.

Table 1-1 Amazon S3-compatible cloud providers that NetBackup supports in release 7.7

Provider	Topic
Amazon GovCloud	See “About the Amazon GovCloud storage requirements” on page 19.
Cloudian HyperStore	See “About the Cloudian HyperStore storage requirements” on page 22.

Table 1-1 Amazon S3-compatible cloud providers that NetBackup supports in release 7.7 (*continued*)

Provider	Topic
Google Nearline	See “About the Google Nearline cloud storage requirements” on page 23.
Hitachi	See “About the Hitachi cloud storage requirements” on page 24.
Verizon	See “About the Verizon cloud storage requirements” on page 27.

About cloud storage features and functionality

NetBackup Cloud Storage enables you to back up and restore data from cloud Storage as a Service (STaaS) vendors. NetBackup Cloud Storage is integrated with Symantec OpenStorage.

[Table 1-2](#) outlines the features and functionality NetBackup Cloud Storage delivers.

Table 1-2 Features and functionality

Feature	Details
Configuration Wizard	A Cloud Storage Server Configuration Wizard is incorporated to facilitate the cloud storage setup and storage provisioning. Cloud storage provisioning now happens entirely through the NetBackup interface.
Encryption	NetBackup Cloud Storage Encryption encrypts the data inline before it is sent to the cloud. Encryption interfaces with the NetBackup Key Management Service (KMS) to leverage its ability to manage encryption keys. The encryption feature uses an AES 256 cipher feedback (CFB) mode encryption.

Table 1-2 Features and functionality (*continued*)

Feature	Details
Throttling	<p>NetBackup Cloud Storage throttling controls the data transfer rates between your network and the cloud. The throttling values are set on a per NetBackup media server basis.</p> <p>In certain implementations, you want to limit WAN usage for backups and restores to the cloud. You want to implement this limit so you do not constrain other network activity. Throttling provides a mechanism to the NetBackup administrators to limit NetBackup Cloud Storage traffic. By implementing a limit to cloud WAN traffic, it cannot consume more than the allocated bandwidth.</p> <p>NetBackup Cloud Storage Throttling lets you configure and control the following:</p> <ul style="list-style-type: none"> ■ Different bandwidth value for both read and write operations. ■ Maximum number of connections that are supported for each cloud provider at any given time. ■ Network bandwidth as a percent of total bandwidth. ■ Network bandwidth per block of time.
Metering	<p>The NetBackup Cloud Storage metering reports enable you to monitor data transfers within NetBackup Cloud Storage.</p> <p>Cloud-based storage is unlike traditional tape or disk media, which use persistent backup images. Your cloud storage vendor calculates cloud-based storage costs per byte stored and per byte transferred.</p> <p>The NetBackup Cloud Storage software uses several techniques to minimize stored and transferred data. With these techniques, traditional catalog-based information about the amount of protected data no longer equates to the amount of data that is stored or transferred. Metering allows installations to monitor the amount of data that is transferred on a per media server basis across one or more cloud-based storage providers.</p> <p>Metering reports are generated through NetBackup OpsCenter.</p>
Cloud Storage service	<p>The NetBackup CloudStore Service Container (<i>nbcssc</i>) process performs the following functions:</p> <ul style="list-style-type: none"> ■ Controls the configuration parameters that are related to NetBackup Cloud Storage ■ Generates the metering information for the metering plug-in ■ Controls the network bandwidth usage with the help of throttling plug-in <p>On Windows, it is a standard service installed by NetBackup. On UNIX, it runs as a standard daemon.</p>

Table 1-2 Features and functionality (*continued*)

Feature	Details
Storage providers	<p>Symantec currently supports several cloud storage providers. More information is available about each of these vendors.</p> <p>See “About the Amazon cloud storage requirements” on page 18.</p> <p>See “About the Amazon GovCloud storage requirements” on page 19.</p> <p>See “About AT&T Synaptic cloud storage requirements” on page 20.</p> <p>See “About the Cloudian HyperStore storage requirements” on page 22.</p> <p>See “About the Google Nearline cloud storage requirements” on page 23.</p> <p>See “About the Hitachi cloud storage requirements” on page 24.</p> <p>See “About Rackspace Cloud Files storage requirements” on page 25.</p> <p>See “About the Verizon cloud storage requirements” on page 27.</p>
OpsCenter Reporting	<p>Monitoring and reporting of the data that is sent to cloud storage is available through new cloud reports in OpsCenter. The cloud reports include:</p> <ul style="list-style-type: none"> ■ Job Success Rate: Success rate by backup job level across domains, clients, policies, and business level views filtered on cloud-based storage. ■ Data Expiring In Future: Data that expires each day for the next seven days filtered on cloud-based storage. ■ Cloud Metering: Historical view of the data that is written to cloud per cloud provider. ■ Average Data Transfer Rate: Historical view of average data transfer rate to cloud per cloud provider. ■ Cloud Metering Chargeback: Ranking, forecast, and distribution view of the cost that is incurred on cloud-based storage per cloud provider. <p>Note: OpsCenter supports monitoring and reporting of the following cloud providers: Amazon S3, AT&T, and Rackspace</p> <p>Among all Amazon S3-compatible cloud providers that NetBackup supports, OpsCenter supports monitoring and reporting of Amazon S3 only.</p>

About support limitations for NetBackup cloud storage

The following items are some of the limitations of NetBackup cloud storage:

- NetBackup does not support clustered master servers in the environments that use NetBackup cloud storage.
- The cloud vendors do not support optimized duplication.

- The cloud vendors do not support direct to tape (by NDMP).
- The cloud vendors do not support disk volume spanning of backup images.
- If the NetBackup master server is installed on a platform that NetBackup cloud does not support, you may observe issues in cloud storage server configuration. For the operating systems that NetBackup supports for cloud storage, see the NetBackup operating system compatibility list available through the following URL:
<http://www.netbackup.com/compatibility>
- For Hitachi cloud storage, synthetic backups are not successful if you enabled the encryption option. To run the synthetic backups successfully, you need to enable the versioning option for buckets (or namespaces) through the Hitachi cloud portal. For more details on how to enable the versioning option, contact your Hitachi cloud provider.

Configuring cloud storage in NetBackup

This chapter includes the following topics:

- [Configuring cloud storage in NetBackup](#)
- [Cloud installation requirements](#)
- [About the cloud storage providers](#)
- [Scalable Storage properties](#)
- [About the NetBackup CloudStore Service Container](#)
- [Generating a security certificate for a media server](#)
- [About data encryption for cloud storage](#)
- [About key management for encryption of NetBackup cloud storage](#)
- [About cloud storage servers](#)
- [About cloud storage data movers](#)
- [Configuring a storage server for cloud storage](#)
- [Changing cloud storage server properties](#)
- [NetBackup cloud storage server properties](#)
- [About cloud storage disk pools](#)
- [Configuring a disk pool for cloud storage](#)
- [Changing cloud disk pool state](#)

- [Saving a record of the KMS key names for NetBackup cloud storage encryption](#)
- [Adding backup media servers to your cloud environment](#)
- [Configuring a storage unit for cloud storage](#)
- [About NetBackup Accelerator and NetBackup Optimized Synthetic backups](#)
- [Enabling NetBackup Accelerator with cloud storage](#)
- [Enabling optimized synthetic backups with cloud storage](#)
- [Creating a backup policy](#)
- [Changing cloud storage disk pool properties](#)

Configuring cloud storage in NetBackup

This topic describes how to configure cloud storage in NetBackup. [Table 2-1](#) provides an overview of the tasks to configure cloud storage. Follow the steps in the table in sequential order.

The *NetBackup Administrator's Guide, Volume I* describes how to configure a base NetBackup environment. The *NetBackup Administrator's Guide, Volume I* is available through the following URL:

<http://www.symantec.com/docs/DOC5332>

Table 2-1 Overview of the NetBackup cloud configuration process

Step	Task	More information
Step 1	Create NetBackup log file directories on the master server and the media servers	See "NetBackup cloud storage log files" on page 117. See "Creating NetBackup log file directories" on page 116.
Step 2	Review the cloud installation requirements	See "Cloud installation requirements" on page 16.
Step 3	Determine the requirements for provisioning and configuring your cloud storage provider in NetBackup	See "About the cloud storage providers" on page 17.
Step 4	Configure the global cloud storage host properties as necessary	See "Scalable Storage properties" on page 29.
Step 5	Understand the role of the Cloud Storage Service Container	See "About the NetBackup CloudStore Service Container" on page 34.

Table 2-1 Overview of the NetBackup cloud configuration process (*continued*)

Step	Task	More information
Step 6	Provision a security certificate for authentication on the media servers	See “NetBackup CloudStore Service Container security certificates” on page 35. See “Generating a security certificate for a media server” on page 38.
Step 7	Understand key management for encryption	Encryption is optional. See “About data encryption for cloud storage” on page 38. See “About key management for encryption of NetBackup cloud storage” on page 39.
Step 8	Configure the storage server	See “About cloud storage servers” on page 40. See “Configuring a storage server for cloud storage” on page 42.
Step 9	Configure the disk pool	See “About cloud storage disk pools” on page 77. See “Configuring a disk pool for cloud storage” on page 78.
Step 10	Configure additional storage server properties	See “NetBackup cloud storage server properties” on page 67. See “Changing cloud storage server properties” on page 66.
Step 11	Add additional media servers	Adding additional media servers is optional. See “About cloud storage data movers” on page 41. See “Adding backup media servers to your cloud environment” on page 89.
Step 12	Configure a storage unit	See “Configuring a storage unit for cloud storage” on page 91.
Step 13	Configure NetBackup Accelerator and optimized synthetic backups	Accelerator and optimized synthetic backups are optional. See “About NetBackup Accelerator and NetBackup Optimized Synthetic backups” on page 95. See “Enabling NetBackup Accelerator with cloud storage” on page 95. See “Changing cloud storage server properties” on page 66.
Step 14	Configure a backup policy	See “Creating a backup policy” on page 99.

Cloud installation requirements

When you develop a plan to implement a NetBackup Cloud solution, use [Table 2-2](#) to assist with your plan.

Table 2-2 Cloud installation requirements

Requirement	Details
NetBackup media server platform support	<p>For the operating systems that NetBackup supports for cloud storage, see the NetBackup operating system compatibility list available through the following URL:</p> <p>http://www.netbackup.com/compatibility</p> <p>When you install the NetBackup media server software on your host, ensure that you specify the fully-qualified domain name for the NetBackup server name.</p>
Cloud storage provider account	<p>You must have an account created with your preferred cloud storage provider before you configure NetBackup Cloud Storage. Please refer to the list of available NetBackup cloud storage providers.</p> <p>You can create this account in the Cloud Storage Configuration Wizard.</p> <p>See “About the cloud storage providers” on page 17.</p>
NetBackup cloud storage licensing	<p>NetBackup cloud storage is enabled through the NetBackup Data Protection Optimization Option license key.</p> <p>To use NetBackup Accelerator with NetBackup cloud storage, you must install the Data Protection Optimization Option license key. That license key activates the NetBackup Accelerator feature.</p>

About the cloud storage providers

The information that is required to configure cloud storage in NetBackup varies according to each cloud storage provider's requirements. See [Table 2-3](#) for links to the topics that describe the requirements for each provider.

Table 2-3 Cloud storage providers for NetBackup

Cloud storage provider	Topics
Amazon	See “About the Amazon cloud storage requirements” on page 18.
Amazon GovCloud	See “About the Amazon GovCloud storage requirements” on page 19.
AT&T	See “About AT&T Synaptic cloud storage requirements” on page 20.
Cloudian	See “About the Cloudian HyperStore storage requirements” on page 22.

Table 2-3 Cloud storage providers for NetBackup (*continued*)

Cloud storage provider	Topics
Google Nearline	See “About the Google Nearline cloud storage requirements” on page 23.
Hitachi	See “About the Hitachi cloud storage requirements” on page 24.
Rackspace	See “About Rackspace Cloud Files storage requirements” on page 25.
Verizon	See “About the Verizon cloud storage requirements” on page 27.

See [“About Amazon S3-compatible cloud providers that NetBackup supports beginning in NetBackup 7.7”](#) on page 9.

NetBackup also may support private clouds from the vendors that provide a private cloud option.

See [“About private clouds from Amazon S3-compatible cloud providers”](#) on page 28.

See [“About private clouds from AT&T”](#) on page 21.

See [“About private clouds from Rackspace”](#) on page 26.

About the Amazon cloud storage requirements

NetBackup Cloud Storage enables Symantec NetBackup to backup data to and restore data from Amazon Simple Storage Service (S3).

[Table 2-4](#) describes the details and requirements of Amazon cloud storage in NetBackup.

Cloud storage providers other than Amazon also use the Amazon S3 protocol for their storage.

See [“About Amazon S3-compatible cloud providers that NetBackup supports beginning in NetBackup 7.7”](#) on page 9.

Table 2-4 Amazon cloud storage requirements

Requirement	Details
License requirement	You must have a NetBackup Data Protection Optimization Option license key.

Table 2-4 Amazon cloud storage requirements (*continued*)

Requirement	Details
Amazon account requirements	You must obtain an Amazon Simple Storage Service (S3) account and the associated user name and password. You also must obtain an Amazon access ID and secure access token.
Buckets	<p>The following are the requirements for the Amazon storage buckets:</p> <ul style="list-style-type: none"> ■ You can create a maximum of 100 buckets per Amazon account. ■ You can delete empty buckets using the Amazon AWS Management Console. However, you may not be able to reuse the names of the deleted buckets while creating buckets in NetBackup. ■ You can create buckets in any Amazon storage region that NetBackup supports.
Bucket names	<p>Symantec recommends that you use NetBackup to create the buckets that you use with NetBackup. The Amazon S3 interface may allow the characters that NetBackup does not allow. Consequently, by using NetBackup to create the buckets you can limit the potential problems.</p> <p>The following are the NetBackup requirements for bucket names:</p> <ul style="list-style-type: none"> ■ Bucket names must be at least 3 and no more than 63 characters long. ■ Bucket names can contain lowercase letters, numbers, and dashes. <p>Note: The buckets are not available for use in NetBackup in the following scenarios: a. If you have created the buckets in a region that NetBackup does not support. b. The bucket name does not comply with the bucket naming convention.</p>
Number of disk pools	You can create a maximum of 90 disk pools. Attempts to create more than 90 disk pools generate a “failed to create disk volume, invalid request” error message.

NetBackup supports the private clouds from the supported cloud providers.

See “[About private clouds from Amazon S3-compatible cloud providers](#)” on page 28.

More information about Amazon S3 is available from Amazon.

<http://aws.amazon.com/s3/>

See “[About the cloud storage providers](#)” on page 17.

About the Amazon GovCloud storage requirements

NetBackup Cloud Storage enables NetBackup to backup data to and restore data from Amazon GovCloud (US).

Table 2-5 describes the details and requirements of Amazon GovCloud (US) in NetBackup.

Table 2-5 Amazon GovCloud (US) requirements

Requirement	Details
License requirement	You must have a NetBackup Data Protection Optimization Option license key.
Amazon GovCloud (US) account requirements	You must obtain an Amazon GovCloud account and the associated user name and password. You also must obtain an Amazon GovCloud access ID and secure access token.
Buckets	The following are the requirements for the Amazon GovCloud storage buckets: <ul style="list-style-type: none"> You can create a maximum of 100 buckets per Amazon GovCloud account. You can delete empty buckets and then reuse the bucket name, but deleted buckets count toward the 100 bucket limit.
Bucket names	Symantec recommends that you use NetBackup to create the buckets that you use with NetBackup. The Amazon S3 interface may allow the characters that NetBackup does not allow. Consequently, by using NetBackup to create the buckets you can limit the potential problems. <p>The following are the NetBackup requirements for bucket names:</p> <ul style="list-style-type: none"> Bucket names must be at least 3 and no more than 63 characters long. Bucket names can contain lowercase letters, numbers, and dashes (or hyphens).
Number of disk pools	You can create a maximum of 90 disk pools. Attempts to create more than 90 disk pools generate a "failed to create disk volume, invalid request" error message.

About AT&T Synaptic cloud storage requirements

NetBackup Cloud Storage enables Symantec NetBackup to backup data to and restore data from AT&T Synaptic™.

Table 2-6 describes the details and requirements of AT&T Synaptic.

Table 2-6 AT&T Synaptic requirements

Requirement	Details
User account	An AT&T Synaptic user ID and password are required to create the storage server.
Storage requirements	<p>The following are the requirements for AT&T cloud storage:</p> <ul style="list-style-type: none"> ■ You must have a NetBackup Data Protection Optimization Option license key. ■ You must use NetBackup to create the volume for your NetBackup backups. The volume that NetBackup creates contain a required Symantec Partner Key. If you use the AT&T Synaptic interface to create the volume, it does not contain the partner key. Consequently, that volume cannot accept data from NetBackup. ■ The logical storage unit (LSU) name (that is, volume name) must be 50 or fewer characters. You can use the following characters for the volume name: <ul style="list-style-type: none"> ■ Any of the 26 letters of the International Standards Organization (ISO) Latin-script alphabet, both uppercase (capital) letters and lowercase (small) letters. These are the same letters as the English alphabet. ■ Any integer from 0 to 9, inclusive. ■ Any of the following characters: ` # \$ _ - ' , ■ You must have an AT&T Synaptic account user name and password.

NetBackup supports the private clouds from the supported cloud providers.

See “[About private clouds from AT&T](#)” on page 21.

More information about AT&T Synaptic is available from AT&T.

<http://www.business.att.com/enterprise/Family/cloud/storage/>

About private clouds from AT&T

NetBackup supports the private clouds for AT&T cloud storage. When you configure a private cloud in NetBackup, you specify the internal host of the cloud. Two methods exist to specify the internal host, as follows:

- Specify the internal host in the **Cloud Storage Configuration Wizard**
- 1 On the select media server panel of the **Cloud Storage Configuration Wizard**, click **Advanced Settings**.
 - 2 On the **Advanced Server Configuration** dialog box, select **Override storage server** and enter the name of the host to use as the storage server.

With this method, the **Create an account with service provider** link on the wizard media server panel has no value for your configuration process.

Specify the internal host in a configuration file

If you specify the name of the internal host in a configuration file, the **Cloud Storage Configuration Wizard** uses that host as the cloud storage server.

- 1 Open the appropriate configuration file, as follows:
 - UNIX:
`/usr/opensv/java/cloudstorejava.conf`
 - Windows:
`C:\Program Files\Veritas\NetBackup\bin\cloudstorewin.conf`

- 2 In the section of the file for your cloud provider type, change the value of the following parameter to the internal host:

```
DEFAULT_STORAGE_SERVER_NAME
```

Use the fully qualified host name or ensure that your network environment can resolve the host name to an IP address.

- 3 If you want the **Create an account with service provider** link on the wizard panel to open a different Web page, edit the following parameter to use that different URL:

```
CLOUD_PROVIDER_URL
```

Note: To configure a public cloud from your vendor, you must do one of two things: change the configuration file to its original contents or specify the internal host in the **Cloud Storage Configuration Wizard**.

Before you configure a private cloud in NetBackup, it must be set up and available.

See [“Configuring a storage server for cloud storage”](#) on page 42.

About the Clouddian HyperStore storage requirements

NetBackup Cloud Storage enables NetBackup to backup data to and restore data from Clouddian.

[Table 2-7](#) describes the details and requirements of Cloudian in NetBackup. Cloudian HyperStore uses the Amazon S3 protocol for its storage.

Table 2-7 Cloudian requirements

Requirement	Details
License requirement	You must have a NetBackup Data Protection Optimization Option license key.
Cloudian account requirements	You must obtain a Cloudian Cloud Services account and the associated user name and password. You must also obtain a Cloudian Cloud Services access ID and secure access token.
Buckets	For more details on the bucket requirements (for example, the maximum number of buckets that you can create), contact Cloudian cloud provider.
Bucket names	<p>Symantec recommends that you use NetBackup to create the buckets that you use with NetBackup. The Amazon S3 interface may allow the characters that NetBackup does not allow. Consequently, by using NetBackup to create the buckets you can limit the potential problems.</p> <p>The following are the NetBackup requirements for bucket names:</p> <ul style="list-style-type: none"> ■ Bucket names must be at least 3 and no more than 63 characters long. ■ Bucket names can contain lowercase letters, numbers, and dashes (hyphens).
Number of disk pools	You can create a maximum of 90 disk pools. Attempts to create more than 90 disk pools generate a “failed to create disk volume, invalid request” error message.

About the Google Nearline cloud storage requirements

NetBackup Cloud Storage enables NetBackup to backup data to and restore data from Google Nearline.

Note: Among the Standard, Durable Reduced Availability (DRA), and Nearline storage classes by Google cloud, NetBackup supports only Nearline storage class. When you create a Google cloud storage, NetBackup by default uses the Nearline storage class.

[Table 2-8](#) describes the details and requirements of Google Nearline in NetBackup. Google Nearline uses the Amazon S3 protocol for its storage.

Table 2-8 Google Nearline requirements

Requirement	Details
License requirement	You must have a NetBackup Data Protection Optimization Option license key.
Google Nearline account requirements	You must obtain a Google Nearline account and the associated user name and password. You also must obtain a Google Nearline access ID and secure access token.
Buckets	The following are the requirements for the Google Nearline storage buckets: <ul style="list-style-type: none"> ■ You can delete empty buckets and then reuse the bucket name. ■ You can create buckets in any Google Nearline storage region.
Bucket names	Symantec recommends that you use NetBackup to create the buckets that you use with NetBackup. The Amazon S3 interface may allow the characters that NetBackup does not allow. Consequently, by using NetBackup to create the buckets you can limit the potential for problems. The following are the NetBackup requirements for bucket names: <ul style="list-style-type: none"> ■ Bucket names must be at least 3 and no more than 63 characters long. ■ Bucket names can contain lowercase letters, numbers, and dashes. ■ Bucket names cannot begin with goog. ■ Bucket names cannot contain Google or close misspellings of Google. You can refer to the following link: https://cloud.google.com/storage/docs/bucket-naming
Number of disk pools	You can create a maximum of 90 disk pools. Attempts to create more than 90 disk pools generate a “failed to create disk volume, invalid request” error message.

About the Hitachi cloud storage requirements

NetBackup Cloud Storage enables NetBackup to backup data to and restore data from Hitachi Cloud Services.

[Table 2-9](#) describes the details and requirements of Hitachi in NetBackup. Hitachi uses the Amazon S3 protocol for its storage.

Table 2-9 Hitachi requirements

Requirement	Details
License requirement	You must have a NetBackup Data Protection Optimization Option license key.
Hitachi account requirements	You must obtain a Hitachi Cloud Services account and the associated user name and password. You must also obtain a Hitachi Cloud Services access ID and secure access token.
Buckets	For more details on the bucket requirements (for example, the maximum number of buckets that you can create), contact Hitachi cloud provider. Note: Hitachi refers to buckets as namespaces.
Bucket names	Symantec recommends that you use NetBackup to create the buckets that you use with NetBackup. The Amazon S3 interface may allow the characters that NetBackup does not allow. Consequently, by using NetBackup to create the buckets you can limit the potential problems. The following are the NetBackup requirements for bucket names: <ul style="list-style-type: none"> ■ Bucket names must be at least 3 and no more than 63 characters long. ■ Bucket names can contain lowercase letters, numbers, and dashes (hyphens).
Number of disk pools	You can create a maximum of 90 disk pools. Attempts to create more than 90 disk pools generate a “failed to create disk volume, invalid request” error message.

About Rackspace Cloud Files storage requirements

NetBackup Cloud Storage enables Symantec NetBackup to backup data to and restore data from Rackspace Cloud Files™.

[Table 2-10](#) describes the details and requirements of Rackspace CloudFiles.

Table 2-10 Rackspace Cloud Files requirements

Requirement	Details
Rackspace Cloud Files accounts	You must obtain a Rackspace account. The account has a user name and password. You need to follow the Rackspace process to generate an access key. The user name and access key are required when you configure the storage server.

Table 2-10 Rackspace Cloud Files requirements (*continued*)

Requirement	Details
Storage requirements	<p>The following are the requirements for Rackspace CloudFiles:</p> <ul style="list-style-type: none"> ■ You must have a NetBackup Data Protection Optimization Option license key. ■ You must have a Rackspace Cloud Files account user name and password. ■ You must use NetBackup to create the cloud storage volume for your NetBackup backups. The volume that NetBackup creates contains a required Symantec Partner Key. If you use the Cloud Files interface to create the volume, it does not contain the partner key. Consequently, that volume cannot accept data from NetBackup. ■ You can use the following characters in the volume name: <ul style="list-style-type: none"> ■ Any of the 26 letters of the International Standards Organization (ISO) Latin-script alphabet, both uppercase (capital) letters and lowercase (small) letters. These are the same letters as the English alphabet. ■ Any integer from 0 to 9, inclusive. ■ Any of the following characters: ~!@#\$\$%^&* () - _+= \\ \ [] { } ' : ; ? > < . ,

NetBackup supports the private clouds from the supported cloud providers.

See “[About private clouds from Rackspace](#)” on page 26.

More information about Rackspace Cloud Files is available from Rackspace.

<http://www.rackspace.com/cloud/files>

About private clouds from Rackspace

NetBackup supports the private clouds from Rackspace. When you configure a private cloud in NetBackup, you specify the internal host of the cloud. Two methods exist to specify the internal host, as follows:

- | | |
|--|--|
| Specify the internal host in the Cloud Storage Configuration Wizard | <ol style="list-style-type: none"> 1 On the select media server panel of the Cloud Storage Configuration Wizard, click Advanced Settings. 2 On the Advanced Server Configuration dialog box, select Override storage server and enter the name of the host to use as the storage server. |
|--|--|

With this method, the **Create an account with service provider** link on the wizard media server panel has no value for your configuration process.

Specify the internal host in a configuration file If you specify the name of the internal host in a configuration file, the **Cloud Storage Configuration Wizard** uses that host as the cloud storage server.

- 1 Open the appropriate configuration file, as follows:
 - UNIX:
`/usr/opensv/java/cloudstorejava.conf`
 - Windows:
`C:\Program Files\Veritas\NetBackup\bin\cloudstorewin.conf`

- 2 In the section of the file for your cloud provider type, change the value of the following parameter to the internal host:

`DEFAULT_STORAGE_SERVER_NAME`

Use the fully qualified host name or ensure that your network environment can resolve the host name to an IP address.

- 3 If you want the **Create an account with service provider** link on the wizard panel to open a different Web page, edit the following parameter to use that different URL:

`CLOUD_PROVIDER_URL`

Note: To configure a public cloud from your vendor, you must do one of two things: change the configuration file to its original contents or specify the internal host in the **Cloud Storage Configuration Wizard**.

Before you configure a private cloud in NetBackup, it must be set up and available. See [“Configuring a storage server for cloud storage”](#) on page 42.

About the Verizon cloud storage requirements

NetBackup Cloud Storage enables NetBackup to backup data to and restore data from Verizon.

[Table 2-11](#) describes the details and requirements of Verizon in NetBackup. Verizon uses the Amazon S3 protocol for its storage.

Table 2-11 Verizon requirements

Requirement	Details
License requirement	You must have a NetBackup Data Protection Optimization Option license key.

Table 2-11 Verizon requirements (*continued*)

Requirement	Details
Verizon account requirements	You must obtain a Verizon account and the associated user name and password. You also must obtain a Verizon access ID and secure access token.
Buckets	Verizon does not support creating buckets in NetBackup. For more details on creating buckets through Verizon portal, contact Verizon cloud provider.
Bucket names	Verizon does not support creating buckets in NetBackup. While creating buckets through Verizon portal, make sure that you take the following NetBackup requirements into consideration: <ul style="list-style-type: none"> ■ Bucket names must be at least 3 and no more than 63 characters long. ■ Bucket names can contain lowercase letters, numbers, and dashes (or hyphens).
Number of disk pools	You can create a maximum of 90 disk pools. Attempts to create more than 90 disk pools generate a “failed to create disk volume, invalid request” error message.

About private clouds from Amazon S3-compatible cloud providers

NetBackup supports the private clouds from Amazon S3-compatible cloud providers.

Before you configure a private cloud in NetBackup, it must be deployed and available.

Use the Advanced Server Configuration dialog box

On the select media server panel of the **Cloud Storage Configuration Wizard**, click the **Advanced Settings** option. Then, in the **Advanced Server Configuration** dialog box, select the relevant options from the following: **Use SSL**, **Use Proxy Server**, **HTTP Headers**, and so on.

Note: NetBackup supports only Certificate Authority (CA)-signed certificates while it communicates with cloud storage in the SSL mode. Ensure that the cloud server (public or private) has CA-signed certificate. If it does not have the CA-signed certificate, data transfer between NetBackup and cloud provider may fail in the SSL mode.

Note: The FIPS region of Amazon GovCloud cloud provider (that is s3-fips-us-gov-west-1.amazonaws.com) supports only secured mode of communication. Therefore, if you disable the **Use SSL** option while you configure Amazon GovCloud cloud storage with the FIPS region, the configuration fails.

The **Create an account with service provider** link on the wizard panel opens a cloud provider webpage in which you can create an account. If you configure a private cloud, that webpage has no value for your configuration process.

Use the NetBackup `cconfig` command

You can use the NetBackup `cconfig` command to create custom cloud instances for an Amazon S3-compatible cloud provider. You must run the `cconfig` command before you run the `nbdevconfig` and `tpconfig` commands. The following is an example of the `cconfig` command syntax:

```
cconfig -a -in instance_name -pt provider_type -sh service_host_name  
[-se service_endpoint_path] [-http_port port_no] [-https_port port_no]  
[-access_style access_style_type]
```

See the *NetBackup Commands Reference Guide* for a complete description about the commands. The guide is available at the following location:

<http://www.symantec.com/docs/DOC5332>

Scalable Storage properties

The **Scalable Storage Cloud Settings** properties contain information about encryption, metering, bandwidth throttling, and network connections between the NetBackup hosts and your cloud storage provider.

The **Scalable Storage** properties appear only if you install a NetBackup Data Protection Optimization Option license key.

The **Scalable Storage** properties apply to currently selected media servers.

Figure 2-1 Scalable Storage Cloud Settings host properties

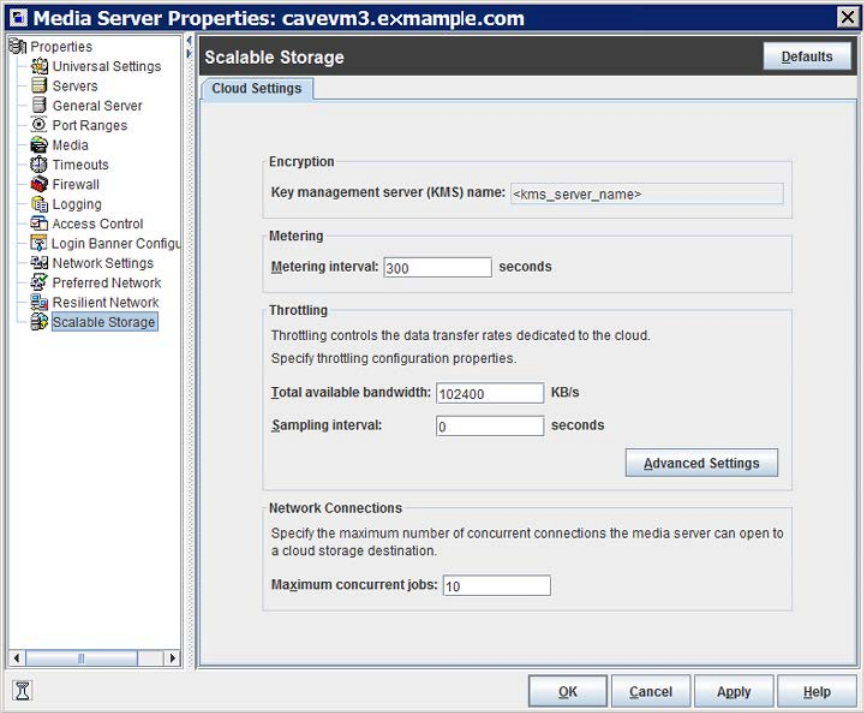


Table 2-12 describes the properties.

Table 2-12 Cloud storage host properties

Property	Description
Key Management Server (KMS) Name	If you configured the NetBackup Key Management Service (KMS), the name of the KMS server.
Metering Interval	Determines how often NetBackup gathers connection information for reporting purposes. NetBackup OpsCenter uses the information that is collected to create reports. The value is set in seconds. The default setting is 300 seconds (5 minutes). If you set this value to zero, metering is disabled.
Total Available Bandwidth	Use this value to specify the speed of your connection to the cloud. The value is specified in kilobytes per second. The default value is 102400 KB/sec.
Sampling interval	The time, in seconds, between measurements of bandwidth usage. The larger this value, the less often NetBackup checks to determine the bandwidth in use.

Table 2-12 Cloud storage host properties (*continued*)

Property	Description
Advanced Settings	<p>Click Advanced Settings to specify additional settings for throttling.</p> <p>See “Configuring advanced bandwidth throttling settings” on page 31.</p> <p>See “Advanced bandwidth throttling settings” on page 32.</p>
Maximum connections	<p>The default maximum number of concurrent jobs that the media server can run for the cloud storage server.</p> <p>This value applies to the media server not to the cloud storage server. If you have more than one media server that can connect to the cloud storage server, each media server can have a different value. Therefore, to determine the total number of connections to the cloud storage server, add the values from each media server.</p> <p>If you configure NetBackup to allow more jobs than the number of connections, NetBackup fails any jobs that start after the number of maximum connections is reached. Jobs include both backup and restore jobs.</p> <p>You can configure job limits per backup policy and per storage unit.</p> <p>Note: NetBackup must account for many factors when it starts jobs: the number of concurrent jobs, the number of connections per media server, the number of media servers, and the job load-balancing logic. Therefore, NetBackup may not fail jobs exactly at the maximum number of connections. NetBackup may fail a job when the connection number is slightly less than the maximum, exactly the maximum, or slightly more than the maximum.</p> <p>In practice, you should not need to set this value higher than 100.</p>

Configuring advanced bandwidth throttling settings

Advanced bandwidth throttling settings let you control various aspects of the connection between the NetBackup hosts and your cloud storage provider.

The total bandwidth and the bandwidth sampling interval are configured on the **Cloud Settings** tab of the **Scalable Storage** host properties screen.

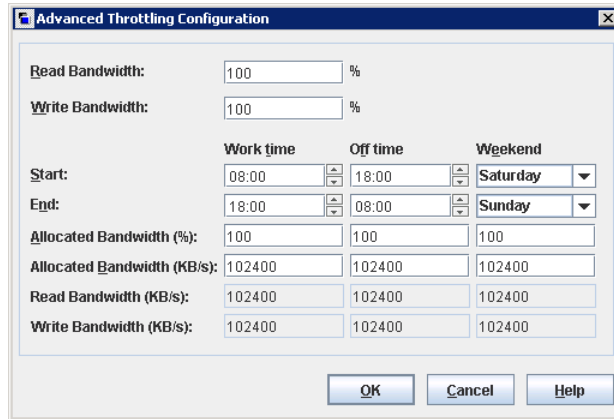
See [“Scalable Storage properties”](#) on page 29.

To configure advanced bandwidth throttling settings

- 1 In the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > Media Servers** in the left pane.
- 2 In the right pane, select the host on which to specify properties.
- 3 Click **Actions > Properties**.
- 4 In the properties dialog box left pane, select **Scalable Storage**.

- In the right pane, click **Advanced Settings**. The **Advanced Throttling Configuration** dialog box appears.

The following is an example of the dialog box:



- Configure the settings and then click **OK**.
See [“Advanced bandwidth throttling settings”](#) on page 32.

Advanced bandwidth throttling settings

The following table describes the advanced bandwidth throttling settings.

Table 2-13 Advanced Throttling Configuration settings

Property	Description
Read Bandwidth	<p>Use this field to specify the percentage of total bandwidth that read operations can use. Specify a value between 0 and 100. If you enter an incorrect value, an error is generated.</p> <p>If there is insufficient bandwidth to transmit the specified amount of data within a few minutes, restore or replication failures may occur due to timeouts.</p> <p>Consider the total load of simultaneous jobs on multiple media servers when you calculate the required bandwidth.</p> <p>Default value: 100</p> <p>Possible values: 0 to 100</p>

Table 2-13 Advanced Throttling Configuration settings (*continued*)

Property	Description
Write Bandwidth	<p>Use this field to specify the percentage of total bandwidth that write operations can use. Specify a value between 0 and 100. If you enter an incorrect value, an error is generated.</p> <p>If there is insufficient bandwidth to transmit the specified amount of data within a few minutes, backup failures may occur due to timeouts.</p> <p>Consider the total load of simultaneous jobs on multiple media servers when you calculate the required bandwidth.</p> <p>Default value: 100</p> <p>Possible values: 0 to 100</p>
Work time	<p>Use this field to specify the time interval that is considered work time for the cloud connection.</p> <p>Specify a start time and end time in 24-hour format. For example, 2:00 P.M. is 14:00.</p> <p>Indicate how much bandwidth the cloud connection can use in the Allocated bandwidth field. This value determines how much of the available bandwidth is used for cloud operations in this time window. The value is expressed as a percentage or in kilobytes per second.</p>
Off time	<p>Use this field to specify the time interval that is considered off time for the cloud connection.</p> <p>Specify a start time and end time in 24-hour format. For example, 2:00 P.M. is 14:00.</p> <p>Indicate how much bandwidth the cloud connection can use in the Allocated bandwidth field. This value determines how much of the available bandwidth is used for cloud operations in this time window. The value is expressed as a percentage or in kilobytes per second.</p>
Weekend	<p>Specify the start and stop time for the weekend.</p> <p>Indicate how much bandwidth the cloud connection can use in the Allocated bandwidth field. This value determines how much of the available bandwidth is used for cloud operations in this time window. The value is expressed as a percentage or in kilobytes per second.</p>

Table 2-13 Advanced Throttling Configuration settings (*continued*)

Property	Description
Read Bandwidth (KB/s)	This field displays how much of the available bandwidth the cloud storage server transmits to a NetBackup media server during each restore job. The value is expressed in kilobytes per second.
Write Bandwidth (KB/s)	This field displays how much of the available bandwidth the NetBackup media server transmits to the cloud storage server during backup jobs. The value is expressed in kilobytes per second.

About the NetBackup CloudStore Service Container

The CloudStore Service Container is a web-based service container that runs on the media server that is configured for cloud storage. This container hosts different services such as the configuration service, the throttling service, and the metering data collector service. NetBackup OpsCenter uses the metering data for monitoring and reporting.

You can configure the CloudStore Service Container behavior by using the **Scalable Storage** host properties in the **NetBackup Administration Console**.

See [“Scalable Storage properties”](#) on page 29.

NetBackup uses several methods of security for the CloudStore Service Container, as follows:

- Security certificates The NetBackup media server on which the CloudStore Service Container runs must be provisioned with a security certificate.
 See [“NetBackup CloudStore Service Container security certificates”](#) on page 35.
 See [“Generating a security certificate for a media server”](#) on page 38.
- Security modes The CloudStore Service Container can run in different security modes.
 See [“NetBackup CloudStore Service Container security modes”](#) on page 36.

The default port number for the `nbcssc` service is 5637.

See [“Stopping and starting the NetBackup CloudStore Service Container”](#) on page 125.

NetBackup CloudStore Service Container security certificates

The NetBackup CloudStore Service Container requires a digital security certificate so that it starts and runs. How the security certificate is provisioned depends on the release level of NetBackup, as follows:

NetBackup 7.7 and later The NetBackup Authentication Service generates certificates for media server authentication, which is the certificate that the CloudStore Service Container uses. You must use a command to install a certificate on a media server that you use for cloud storage. See [“Generating a security certificate for a media server”](#) on page 38.

The security certificates that the NetBackup Authentication Service generates expire after one year. NetBackup automatically replaces existing certificates with new ones as needed.

Note: NetBackup Access Control uses the security certificates for authentication. If you configure Access Control in your environment, certificates are provisioned on all media servers. Therefore, you do not have to provision certificates for your cloud storage media servers.

NetBackup releases earlier than 7.7 The CloudStore Service Container generates a self-signed certificate for authentication. The certificate expires after 365 days. NetBackup automatically replaces existing certificates with new ones as needed.

The CloudStore Service Container in NetBackup releases earlier than 7.7 does not recognize the certificates that a NetBackup 7.7 or later master server generates. If your security policy prohibits self-signed certificates, you must run NetBackup 7.7 or later on the media servers that you use for cloud storage.

Where the media server security certificates reside depend on the release level of NetBackup, as follows:

NetBackup 7.7 and later The certificate name is the host name that you used when you configured the NetBackup media server software on the host. The path for the certificate is as follows, depending on operating system:

- UNIX/Linux: `/usr/opensv/var/vxss/credentials`
- Windows: `install_dir\Veritas\NetBackup\var\VxSS\credentials`

If a certificate does not exist, create one from the NetBackup master server.

NetBackup releases earlier than 7.7

The following are the pathnames to the certificate, depending on operating system:

- UNIX/Linux: `/usr/opensv/lib/ost-plugins/cssc.crt`
- Windows:
`install_path\Veritas\NetBackup\bin\ost-plugins\cssc.crt`

If the certificate becomes corrupt or expires, delete the old certificate and restart the service to regenerate a new certificate.

See [“About the NetBackup CloudStore Service Container”](#) on page 34.

NetBackup CloudStore Service Container security modes

The NetBackup CloudStore Service Container can run in one of two different modes. The security mode determines how the clients communicate with the service, as follows:

Secure mode	In the default secure mode, the client components must authenticate with the CloudStore Service Container. After authentication, communication occurs over a secure HTTPS channel.
Non-secure mode	The CloudStore Service Container uses non-secure communication. Clients communicate with the server over HTTP with no authentication required.

You can use the `CSSC_IS_SECURE` attribute of the `cloudstore.conf` file to set the security mode. The default value is 1, secure communication.

See [“NetBackup cloudstore.conf configuration file”](#) on page 36.

See [“About the NetBackup CloudStore Service Container”](#) on page 34.

NetBackup cloudstore.conf configuration file

[Table 2-14](#) describes the `cloudstore.conf` configuration file parameters. The `cloudstore.conf` file is available on all media servers that are installed on the platforms that NetBackup supports. The `cloudstore.conf` file contains the following parameters. You can modify most of these parameters manually.

Note: You must stop the `nbcssc` service before you modify any of the parameters in the `cloudstore.conf` file. Once you modify the parameters, restart the `nbcssc` service.

The `cloudstore.conf` file resides in the following directories:

- **UNIX or Linux:** `/usr/opensv/lib/ost-plugins`
- **Windows:** `install_path\Veritas\NetBackup\bin\ost-plugins`

Table 2-14 `cloudstore.conf` configuration file parameters and descriptions

Parameter	Description
CSSC_VERSION	Symantec recommends that you do not modify this value. Specifies the version of <code>cloudstore.conf</code> file. The default value is 1.
CSSC_PLUGIN_PATH	Symantec recommends that you do not modify this value. Specifies the path where NetBackup cloud storage plug-ins are installed. The default path is as follows: On Windows: <code>install_path\Veritas\NetBackup\bin\ost-plugins</code> On UNIX: <code>/usr/opensv/lib/ost-plugins</code>
CSSC_PORT	Specifies the port number where <code>nbcssc</code> service is running. The default value is 5637.
CSSC_LOG_DIR	Specifies the directory path where <code>nbcssc</code> generates log files. The default path is as follows: On Windows: <code>install_path\Veritas\NetBackup\logs\nbcssc</code> On UNIX: <code>/usr/opensv/netbackup/logs/nbcssc</code>
CSSC_LOG_FILE	Specifies the file name that the <code>nbcssc</code> service uses to write its logs. The default value is empty, which means that the NetBackup logging mechanism determines the log file name.
CSSC_IS_SECURE	Specifies if the <code>nbcssc</code> service runs in secure (value 1) or non-secure mode (value 0). The default value is 1.
CSSC_CIPHER_LIST	Symantec recommends that you do not modify this value. Specifies the cipher list that NetBackup uses while it communicates with the <code>nbcssc</code> service in the secure (SSL) mode. The default value is <code>HIGH:MEDIUM:!eNULL:!aNULL:!SSLv2:!RC4</code> .
CSSC_LOG_LEVEL	Specifies the log level for <code>nbcssc</code> logging. Value 0 indicates that the logging is disabled and non-zero value indicates that the logging is enabled. The default value is 0.
CSSC_MASTER_PORT	Specifies the port number of NetBackup master server host where the <code>nbcssc</code> service runs. The default value is 5637.

Table 2-14 `cloudstore.conf` configuration file parameters and descriptions
 (continued)

Parameter	Description
<code>CSSC_MASTER_NAME</code>	<p>Specifies the NetBackup master server name. This entry indicates that the <code>nbcssc</code> service runs on this host. It processes all cloud provider-specific requests based on the <code>CloudProvider.xml</code> and <code>CloudInstance.xml</code> files that reside at the following location:</p> <p>On Windows: <code>install_path\Veritas\NetBackup\bin\ost-plugins</code></p> <p>On UNIX: <code>/usr/opensv/lib/ost-plugins</code></p>
<code>CSSC_MASTER_IS_SECURE</code>	<p>Specifies if the <code>nbcssc</code> service is running in secure (value 1) or non-secure mode (value 0) on the NetBackup master server. The default value is 1.</p>

Generating a security certificate for a media server

Under certain conditions, NetBackup media servers require security certificates so that NetBackup can function properly.

See [“About the NetBackup CloudStore Service Container”](#) on page 34.

Use the following procedure to generate a security certificate for a media server.

To generate a certificate for a media server

- 1 Run the following command on the master server.

UNIX/Linux: `/usr/opensv/netbackup/bin/admincmd/bpnbaz -ProvisionCert Media_server_name`

Windows: `install_path\NetBackup\bin\admincmd\bpnbaz -ProvisionCert Media_server_name`

- 2 Restart the services on the media server.

Note: Generating a security certificate is a one-time activity.

About data encryption for cloud storage

You can encrypt your data before you send it to the cloud.

NetBackup uses the Key Management Service (KMS) to manage the keys for the data encryption for cloud disk storage. KMS is a NetBackup master server-based

symmetric key management service. The service runs on the NetBackup master server. An additional license is not required to use the KMS functionality.

See “[About key management for encryption of NetBackup cloud storage](#)” on page 39.

The NetBackup **Cloud Storage Server Configuration Wizard** and the **Disk Pool Configuration Wizard** include the steps that configure key management and encryption.

More information about data-at-rest encryption and security is available.

See the *NetBackup Security and Encryption Guide*:

<http://www.symantec.com/docs/DOC5332>

About key management for encryption of NetBackup cloud storage

NetBackup uses the Key Management Service (KMS) to manage the keys for the data encryption for disk storage. KMS is a NetBackup master server-based symmetric key management service. The service runs on the NetBackup master server. An additional license is not required to use the KMS functionality.

NetBackup uses KMS to manage the encryption keys for cloud storage.

See “[About data encryption for cloud storage](#)” on page 38.

The following table describes the keys that are required for the KMS database. You can enter the pass phrases for these keys when you use the **Cloud Storage Server Configuration Wizard**.

Table 2-15 Encryption keys required for the KMS database

Key	Description
Host Master Key	The Host Master Key protects the key database. The Host Master Key requires a pass phrase and an ID. KMS uses the pass phrase to generate the key.
Key Protection Key	A Key Protection Key protects individual records in the key database. The Key Protection Key requires a pass phrase and an ID. KMS uses the pass phrase to generate the key.

The following table describes the encryption keys that are required for each storage server and volume combination. If you specified encryption when you configured the cloud storage server, you must configure a pass phrases for the key group for

the storage volumes. You enter the pass phrase for these keys when you use the **Disk Pool Configuration Wizard**.

Table 2-16 Encryption keys and key records for each storage server and volume combination

Item	Description
Key group key	<p>A key group key protects the key group. Each storage server and volume combination requires a key group, and each key group key requires a pass phrase. The key group name must use the format for the storage type that is described as follows:</p> <p>For cloud storage, the following is the format:</p> <pre>storage_server_name:volume_name</pre> <p>The following items describe the requirements for the key group name components for cloud storage:</p> <ul style="list-style-type: none"> ■ <i>storage_server_name</i>: You must use the same name that you use for the storage server. The name can be a fully-qualified domain name or a short name, but it must be the same as the storage server. ■ The colon (:) is required after the <i>storage_server_name</i>. ■ <i>volume_name</i>: You must specify the LSU name that the storage vendor exposes to NetBackup. <p>The Disk Pool Configuration Wizard conforms to this format when it creates a key group.</p>
Key record	<p>Each key group that you create requires a key record. A key record stores the actual key that protects the data for the storage server and volume.</p> <p>A name for the key record is optional. If you use a key name, you can use any name. Symantec recommends that you use the same name as the volume name. The Disk Pool Configuration Wizard does not prompt for a key record key; it uses the volume name as the key name.</p>

More information about KMS is available in the *NetBackup Security and Encryption Guide*:

<http://www.symantec.com/docs/DOC5332>

About cloud storage servers

A storage server is an entity that writes data to and reads data from the storage. For cloud storage, it is usually a host on the Internet to which you send the backup

data. Your storage vendor provides the name of the storage server. Use that name when you configure cloud storage in NetBackup.

When you configure a cloud storage server, it inherits the NetBackup Scalable Storage properties.

See [“Scalable Storage properties”](#) on page 29.

After you configure the storage server, you can change the properties of the storage server.

See [“NetBackup cloud storage server properties”](#) on page 67.

Only one storage servers exists in a NetBackup domain for a specific storage vendor.

The NetBackup data movers back up the clients and move the data to the storage server.

See [“About cloud storage data movers”](#) on page 41.

About cloud storage data movers

A data mover is a NetBackup media server that backs up a client and then transfers the data to a storage server. The storage server then writes the data to storage. A data mover also can move data back to primary storage (the client) during restores and from secondary storage to tertiary storage during duplication.

When you configure a cloud storage server, the media server that you specify in the wizard or on the command line becomes a data mover. That media server is used to back up your client computers.

You can add additional media servers. They can help balance the load of the backups that you send to the cloud storage. The media servers that you add are assigned the credentials for the storage server. The credentials allow the data movers to communicate with the storage server.

The data movers host a software plug-in that they use to communicate with the storage implementation.

See [“Adding backup media servers to your cloud environment”](#) on page 89.

You can control which data movers are used for backups and duplications when you configure NetBackup storage units.

See [“Configuring a storage unit for cloud storage”](#) on page 91.

Configuring a storage server for cloud storage

Configure in this context means to configure a host as a storage server that can write to and read from the cloud storage. The NetBackup **Cloud Storage Server Configuration Wizard** communicates with your cloud storage vendor's network and selects the appropriate host for the storage server. The wizard also lets you configure the NetBackup Key Management Service for encryption.

At least one media server must be enabled for cloud storage. To be enabled for cloud storage, a NetBackup media server must meet the following conditions:

- The media server operating system must be supported for cloud storage. For the operating systems that NetBackup supports for cloud storage, see the NetBackup operating system compatibility list available through the following URL:
<http://www.netbackup.com/compatibility>
- The NetBackup CloudStore Service Container (`nbcssc`) must be running. See “[About the NetBackup CloudStore Service Container](#)” on page 34.
- The cloud storage binary files must be present in the `ost-plugins` directory.

NetBackup supports private clouds from the supported cloud providers.

See “[About private clouds from AT&T](#)” on page 21.

See “[About private clouds from Amazon S3-compatible cloud providers](#)” on page 28.

See “[About cloud storage servers](#)” on page 40.

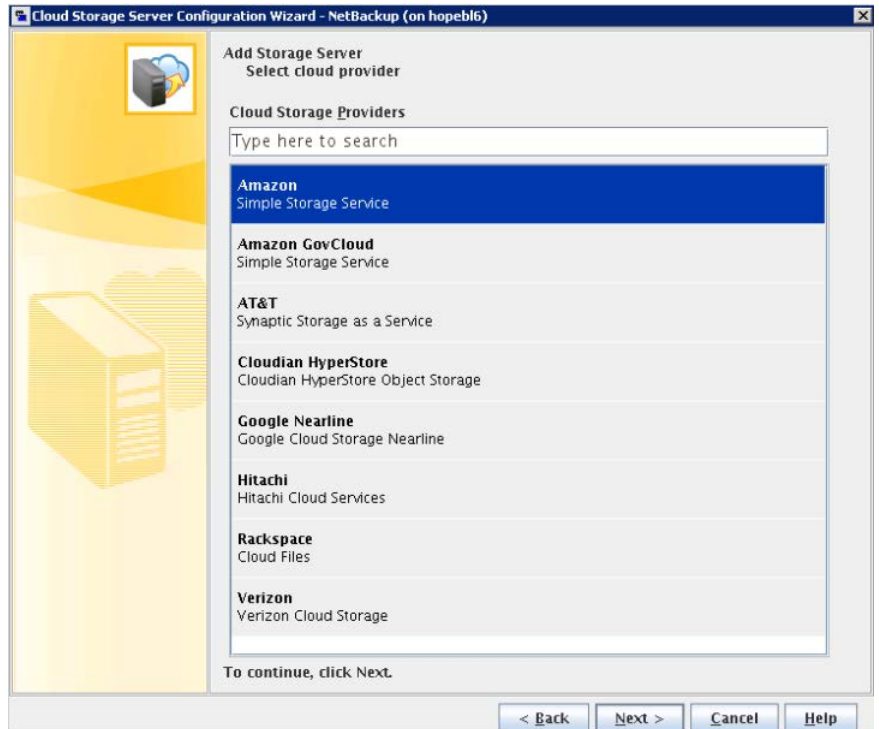
To configure a cloud storage server by using the wizard

- 1 In the **NetBackup Administration Console** connected to the NetBackup master server, select either **NetBackup Management** or **Media and Device Management**.
- 2 In the right pane, click **Configure Cloud Storage Servers**.

3 Click **Next** on the welcome panel of the wizard.

The **Select cloud provider** panel appears.

The following is an example of the wizard panel:



On the **Select cloud provider** panel, either select the cloud provider or in the search box type the cloud provider name that you want to select. If the cloud provider that you have entered exists in the list, the wizard selects it.

Click **Next**; a wizard panel for the selected cloud provider appears.

- 4 On the wizard panel for your cloud provider, select or enter the appropriate information. The information that is required depends on the cloud vendor.

Descriptions of the information that is required for each provider is provided in other topics. Those topics also include examples of the wizard panels.

Note: The provider information topics may include notes, caveats, or warnings. Ensure that you review the topics before you complete the fields in the wizard panel.

See [“Amazon S3 storage server configuration options”](#) on page 47.

See [“Amazon GovCloud storage server configuration options”](#) on page 49.

See [“AT&T storage server configuration options”](#) on page 52.

See [“Cloudian HyperStore storage server configuration options”](#) on page 54.

See [“Google Nearline storage server configuration options”](#) on page 57.

See [“Hitachi storage server configuration options”](#) on page 58.

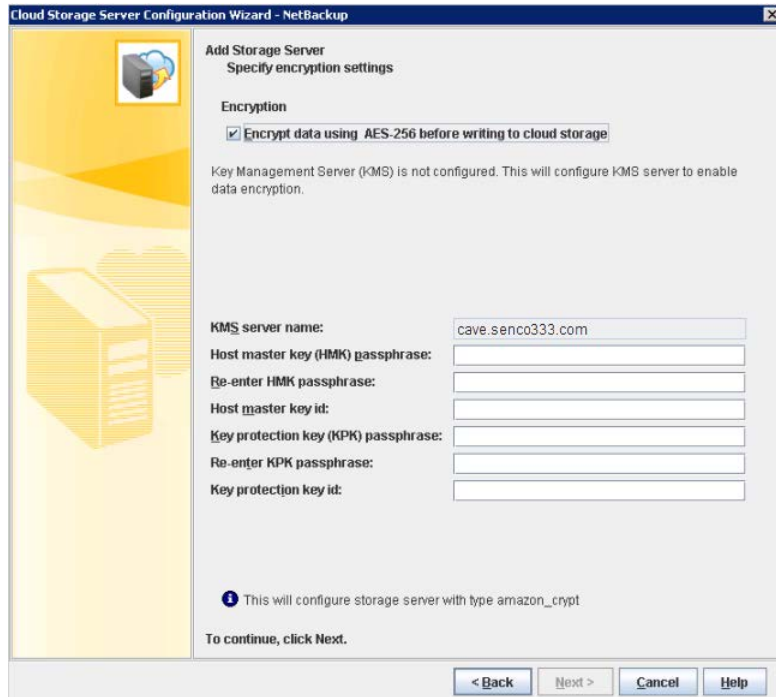
See [“Rackspace storage server configuration options”](#) on page 61.

See [“Verizon storage server configuration options”](#) on page 62.

After you specify the configuration options for your cloud provider, click **Next**; the **Specify encryption settings** panel appears.

- To encrypt your backups, select **Encrypt data using AES-256 before writing to cloud storage** on the **Specify Encryption Settings** panel. Then, enter the information to protect the KMS database.

The following is an example of the panel:



See [“KMS database encryption settings”](#) on page 65.

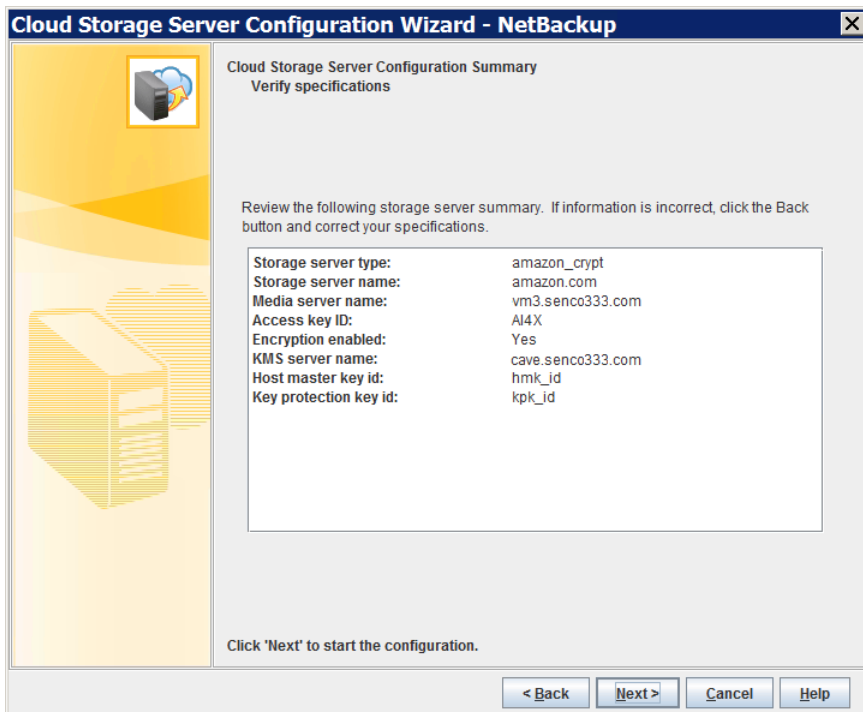
After you configure the storage server and disk pool, Symantec recommends that you save a record of the key names.

See [“Saving a record of the KMS key names for NetBackup cloud storage encryption”](#) on page 87.

Click **Next**; the **Cloud Storage Server Configuration Summary** panel appears.

- 6 On the **Cloud Storage Server Configuration Summary** panel, verify the selections.

The following is an example of the panel:



If not OK, click **Back** until you reach the panel on which you need to make corrections.

If OK, click **Next**. The wizard creates the storage server, and the **Storage Server Creation Confirmation** panel appears.

- 7 On the **Storage Server Creation Confirmation** panel, do one of the following:
 - To continue to the **Disk Pool Configuration Wizard**, click **Next**. See "Configuring a disk pool for cloud storage" on page 78.
 - To exit from the wizard, click **Finish**. If you exist, you can still create a disk pool. See "Configuring a disk pool for cloud storage" on page 78.

Amazon S3 storage server configuration options

shows the **Cloud Storage Configuration Wizard** panel for Amazon S3 cloud storage.

Figure 2-2 Cloud Storage Server Configuration Wizard panel for Amazon

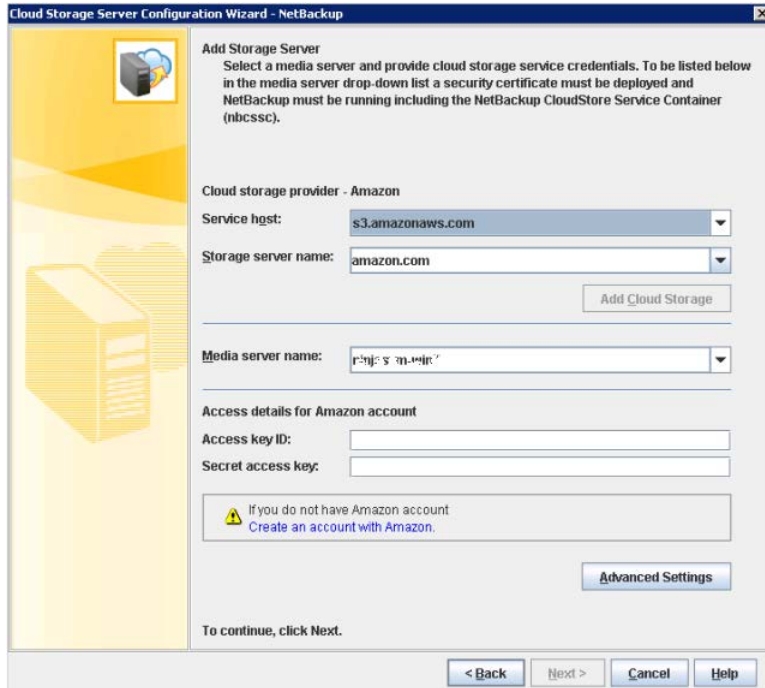


Table 2-17 describes the storage server configuration options for Amazon S3.

Table 2-17 Amazon S3 storage server configuration options

Field name	Required content
Service host	Displays the service host from the drop-down list. The service host is the host name of the cloud service end point of Amazon S3.

Table 2-17 Amazon S3 storage server configuration options (*continued*)

Field name	Required content
Storage server name	<p>Displays the default Amazon storage server, which is amazon.com. You can select a storage server other than the default one.</p> <p>The drop-down list displays only those names that are available for use.</p> <p>You can type a different storage server name in the drop-down list, which can be a logical name for the cloud storage. You can create multiple storage servers with the different names that refer to the same physical service host for Amazon. If there are no names available in the list, you can create a new storage server name by typing the name in the drop-down list.</p> <p>Note: Symantec recommends that a storage server name that you add while configuring an Amazon S3-compatible cloud provider should be a logical name and should not match a physical host name. For example: While you add an Amazon GovCloud storage server, avoid using names like 'amazon.gov.com' or 'amazon123.com'. These servers may be physical hosts, which can cause failures during cloud storage configuration. Instead, use storage server names like 'amazongov1' or 'amazonserver1' and so on.</p> <p>Note: The Add Cloud Storage option is disabled, because Amazon S3 does not support private cloud deployments.</p>
Media server name	<p>Select NetBackup media server from the drop-down list. The drop-down list displays only NetBackup 7.7 and later media servers.</p> <p>Only those media servers that are enabled for cloud storage appear in the list, as follows:</p> <ul style="list-style-type: none"> ■ The media server operating system must be supported for cloud storage. For the operating systems that NetBackup supports for cloud storage, see the NetBackup operating system compatibility list available through the following URL: http://www.netbackup.com/compatibility ■ The NetBackup Cloud Storage Service Container (<code>nbcssc</code>) must be running. ■ The cloud storage binary files must be present in the <code>ost-plugins</code> directory. <p>The host that you select queries the storage vendor's network for its capabilities and for the available storage. The media server also becomes a data mover for your backups and restores.</p> <p>See "About cloud storage data movers" on page 41.</p>
Access key ID	<p>Enter your Amazon S3 Access key ID.</p> <p>If you do not have an account, click Create an account with the service provider link.</p>
Secret access key	<p>Enter your Amazon S3 Secret access key.</p>
Advanced Settings	<p>To change SSL, proxy, or HTTP header settings for Amazon S3, click Advanced Settings.</p>

Amazon GovCloud storage server configuration options

Figure 2-3 shows the **Cloud Storage Configuration Wizard** for Amazon GovCloud cloud storage.

Figure 2-3 Cloud Storage Server Configuration Wizard panel for Amazon GovCloud

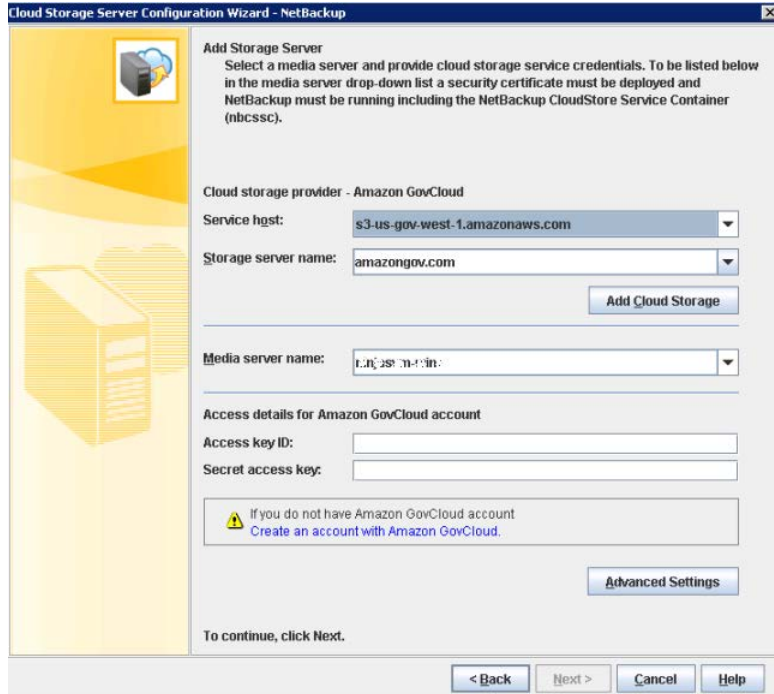


Table 2-18 describes the storage server configuration options for Amazon GovCloud.

Table 2-18 Amazon GovCloud storage server configuration options

Field name	Required content
Service host	Select the host name of one of the cloud service service host endpoints of Amazon GovCloud, as follows: <ul style="list-style-type: none"> ■ s3-us-gov-west-1.amazonaws.com ■ s3-fips-us-gov-west-1.amazonaws.com (FIPS region)

Table 2-18 Amazon GovCloud storage server configuration options (*continued*)

Field name	Required content
Storage server name	<p>Displays the default Amazon GovCloud storage server, which is amazongov.com. You can select a storage server other than the default one.</p> <p>The drop-down list displays only those names that are available for use.</p> <p>You can type a different storage server name in the drop-down list, which can be a logical name for the cloud storage. You can create multiple cloud storage servers with the different names that refer to the same physical service host for Amazon. If there are no names available in the list, you can create a new storage server name by typing the name in the drop-down list.</p> <p>Note: Symantec recommends that a storage server name that you add while configuring an Amazon S3-compatible cloud provider should be a logical name and should not match a physical host name. For example: While you add an Amazon GovCloud storage server, avoid using names like 'amazongov.com' or 'amazon123.com'. These servers may be physical hosts, which can cause failures during cloud storage configuration. Instead, use storage server names like 'amazongov1' or 'amazonserver1' and so on.</p> <p>Note: To create a storage server with a name that is different than the default one, you can also use the command-line interface. Use the 'add storage server' option of the <code>csconfig</code> command before running <code>nbdevconfig</code> and <code>tpconfig</code> commands.</p> <p>See the <i>NetBackup Commands Reference Guide</i> for a complete description about these commands. The guide is available through the following URL:</p> <p>http://www.symantec.com/docs/DOC5332</p>

Table 2-18 Amazon GovCloud storage server configuration options (*continued*)

Field name	Required content
Add Cloud Storage	<p>The Add Cloud Storage option lets you add customized cloud deployment details for NetBackup to communicate with the cloud storage. The customized cloud deployment refers to the cloud instances that are not already listed in the Service Host drop-down list.</p> <p>Click the Add Cloud Storage option to open the Add Cloud Storage dialog box. Use the dialog box to configure the general settings and region settings of Amazon GovCloud.</p> <p>Once the cloud storage is added, you cannot modify or delete it using the NetBackup Administration Console. However, you can modify or delete a storage server by using the <code>csconfig</code> command.</p> <p>Note: You can use the NetBackup <code>csconfig -a</code> command to create custom cloud instances for an Amazon S3-compatible cloud provider. You must run the <code>csconfig</code> command before you run the <code>nbdevconfig</code> and <code>tpconfig</code> commands.</p> <p>See the <i>NetBackup Commands Reference Guide</i> for a complete description about these commands. The guide is available through the following URL:</p> <p>http://www.symantec.com/docs/DOC5332</p>
Media server name	Select NetBackup media server from the drop-down list. The drop-down list displays only NetBackup 7.7 and later media servers.
Access key ID	Enter your Amazon GovCloud access key ID. If you do not have an account, click Create an account with the service provider link.
Secret access key	Enter your Amazon GovCloud secret access key.
Advanced Settings	<p>To change SSL, proxy, or HTTP header settings for Amazon GovCloud, click Advanced Settings.</p> <p>Note: The FIPS region of Amazon GovCloud cloud provider (that is <code>s3-fips-us-gov-west-1.amazonaws.com</code>) supports only secured mode of communication. Therefore, if you disable the Use SSL option while you configure Amazon GovCloud cloud storage with the FIPS region, the configuration fails.</p> <p>See “About private clouds from Amazon S3-compatible cloud providers” on page 28.</p>

AT&T storage server configuration options

Figure 2-4 shows the **Cloud Storage Server Configuration Wizard** panel for the AT&T cloud storage.

Figure 2-4 Cloud Storage Server Configuration Wizard panel for AT&T

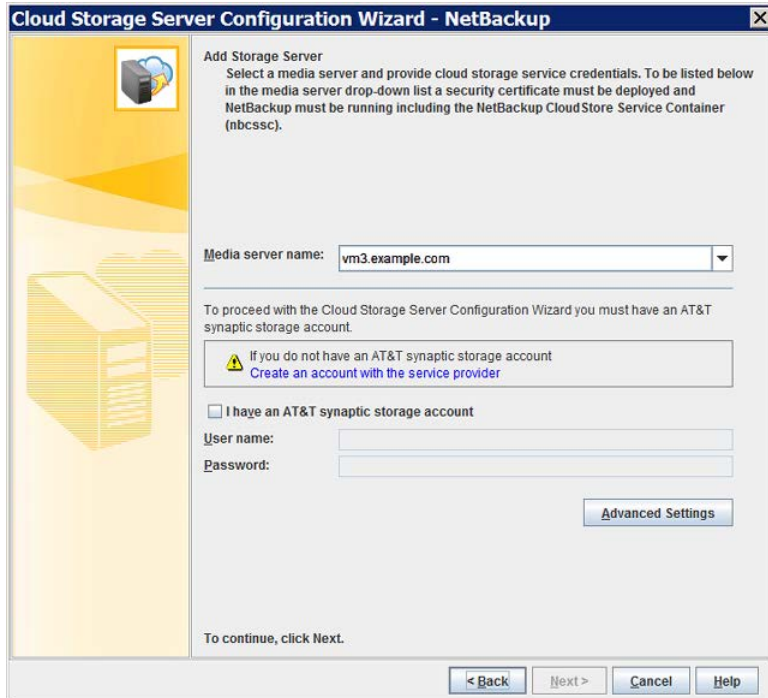


Table 2-19 describes the configuration options for AT&T.

Table 2-19 AT&T Storage server configuration options

Field name	Required content
<p>Media Server Name</p>	<p>Select a NetBackup media server. The host that you select queries the storage vendor’s network for its capabilities and for the available storage. The media server also becomes a data mover for your backups and restores.</p> <p>Only those media servers that are enabled for cloud storage appear in the list, as follows:</p> <ul style="list-style-type: none"> ■ The media server operating system must be supported for cloud storage. For the operating systems that NetBackup supports for cloud storage, see the NetBackup operating system compatibility list available through the following URL: http://www.netbackup.com/compatibility ■ The NetBackup Cloud Storage Service Container (<code>nbcssc</code>) must be running. The NetBackup Cloud Storage Service Container requires an authentication certificate to run. See “About the NetBackup CloudStore Service Container” on page 34. ■ The cloud storage binary files must be present in the <code>ost-plugins</code> directory. <p>The NetBackup master server always has a certificate. If it meets the other two criteria, it appears in the Media Server Name drop-down list.</p> <p>After you configure the storage server, you cannot change the media server that you specify here. This behavior is the result of the OpenStorage plugin design. Attempts to change the media server generate an authorization error.</p>
<p>Create an account with the service provider</p>	<p>If you do not have an account with AT&T, click Create an account with the service provider link. A web browser opens in which you can create an account with AT&T.</p>
<p>I have an AT&T Synaptic storage account</p>	<p>Select I have an AT&T Synaptic storage account to enter the required account information.</p>
<p>User Name</p>	<p>Enter your AT&T user name.</p> <p>If you do not have an account, click Create an account with the service provider link.</p>
<p>Password</p>	<p>Enter the password for the User Name account.</p>

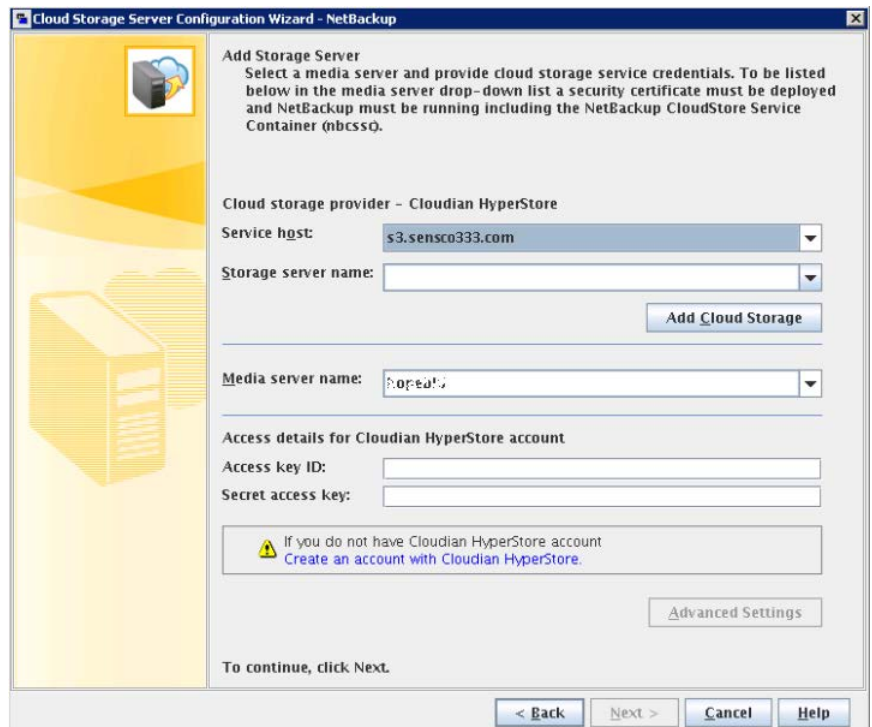
Table 2-19 AT&T Storage server configuration options (*continued*)

Field name	Required content
Advanced	To change the default storage server for your cloud vendor or specify the maximum number of network connections, click Advanced . See “About private clouds from AT&T” on page 21.

Cloudian HyperStore storage server configuration options

[Figure 2-5](#) shows the **Cloud Storage Server Configuration Wizard** panel for the Cloudian HyperStore cloud storage.

Figure 2-5 Cloud Storage Server Configuration Wizard panel for Cloudian HyperStore



[Table 2-20](#) describes the storage server configuration options for Cloudian.

Table 2-20 Cloudian storage server configuration options

Field name	Required content
Service host	<p>Displays the host name of the cloud service end point of Cloudian. Initially, the drop-down list does not contain any service hosts. You need to add a service host by clicking the Add Cloud Storage option.</p> <p>For details on the Cloudian HyperStore cloud storage, refer to the Cloudian documentation.</p>
Storage server name	<p>Displays the default Cloudian storage server. Initially, the drop-down list does not contain any storage server names.</p> <p>Type a storage server name in the drop-down list, which can be a logical name for the Cloudian cloud storage. You can create multiple storage servers with the different names that refer to the same physical service host for Cloudian.</p> <p>The drop-down list displays only those storage server names that are available for use.</p> <p>Note: Symantec recommends that a storage server name that you add while configuring an Amazon S3-compatible cloud provider should be a logical name and should not match a physical host name. For example: While you add an Amazon GovCloud storage server, avoid using names like 'amazongov.com' or 'amazon123.com'. These servers may be physical hosts, which can cause failures during cloud storage configuration. Instead, use storage server names like 'amazongov1' or 'amazonserver1' and so on.</p>

Table 2-20 Cloudian storage server configuration options (*continued*)

Field name	Required content
<p>Add Cloud Storage</p>	<p>The Add Cloud Storage option lets you add customized cloud deployment details for NetBackup to communicate with the cloud storage. The customized cloud deployment refers to the cloud instances that are not already listed in the Service Host drop-down list.</p> <p>Click the Add Cloud Storage option to open the Add Cloud Storage dialog box. Use the dialog box to configure the general settings and region settings of Cloudian.</p> <p>Once the cloud storage is added, you cannot modify or delete it using the NetBackup Administration Console. However, you can modify or delete a storage server by using the <code>csconfig</code> command.</p> <p>Note: You can use the NetBackup <code>csconfig -a</code> command to create custom cloud instances for an Amazon S3-compatible cloud provider. You must run the <code>csconfig</code> command before you run the <code>nbdevconfig</code> and <code>tpconfig</code> commands.</p> <p>See the <i>NetBackup Commands Reference Guide</i> for a complete description about these commands. The guide is available through the following URL:</p> <p>http://www.symantec.com/docs/DOC5332</p>
<p>Media server name</p>	<p>Select NetBackup media server from the drop-down list. The drop-down list displays only NetBackup 7.7 and later media servers.</p>
<p>Access key ID</p>	<p>Enter your Cloudian access key ID.</p> <p>If you do not have an account, click Create an account with the service provider link.</p> <p>In the case of private cloud deployments, the link leads you to the product help or contact page of your cloud provider. To create an account, you need to access Cloud Storage administration console of your private cloud storage.</p>
<p>Secret access key</p>	<p>Enter your Cloudian secret access key.</p>
<p>Advanced Settings</p>	<p>To change SSL, proxy, or HTTP header settings for Cloudian, click Advanced Settings.</p>

Google Nearline storage server configuration options

Figure 2-6 shows the **Cloud Storage Server Configuration Wizard** panel for the Google Nearline cloud storage.

Figure 2-6 Cloud Storage Server Configuration Wizard panel for Google Nearline

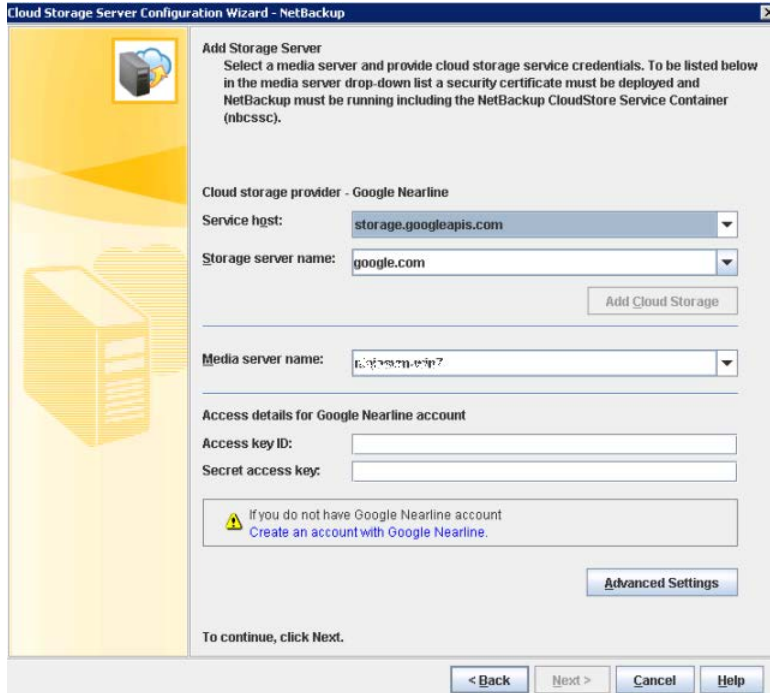


Table 2-21 describes the storage server configuration options for Google Nearline.

Table 2-21 Google Nearline storage server configuration options

Field name	Required content
Service host	Select the host name of the cloud service end point of Google Nearline.

Table 2-21 Google Nearline storage server configuration options (*continued*)

Field name	Required content
Storage server name	<p>Displays the default storage server, which is Google Nearline. You can select a storage server other than the default one.</p> <p>The drop-down list displays only those names that are available for use.</p> <p>You can type a different storage server name in the drop-down list, which can be a logical name for the cloud storage. You can create multiple storage servers with the different names that refer to the same physical service host for Amazon. If there are no names available in the list, you can create a new storage server name by typing the name in the drop-down list.</p> <p>Note: Symantec recommends that a storage server name that you add while configuring an Amazon S3-compatible cloud provider should be a logical name and should not match a physical host name. For example: While you add an Amazon GovCloud storage server, avoid using names like 'amazongov.com' or 'amazon123.com'. These servers may be physical hosts, which can cause failures during cloud storage configuration. Instead, use storage server names like 'amazongov1' or 'amazonserver1' and so on.</p> <p>The Add Cloud Storage option is disabled, because Google Nearline does not support private cloud deployments.</p>
Media server name	<p>Select NetBackup media server from the drop-down list. The drop-down list displays only NetBackup 7.7 and later media servers.</p>
Access key ID	<p>Enter your Google Nearline Access key ID.</p> <p>If you do not have an account, click Create an account with the service provider link.</p>
Secret access key	<p>Enter your Google Nearline secret access key</p>
Advanced Settings	<p>To change SSL, proxy, or HTTP header settings for Google Nearline, click Advanced Settings.</p>

Hitachi storage server configuration options

Figure 2-7 shows the **Cloud Storage Server Configuration Wizard** panel for the Hitachi cloud storage.

Figure 2-7 Cloud Storage Server Configuration Wizard panel for Hitachi

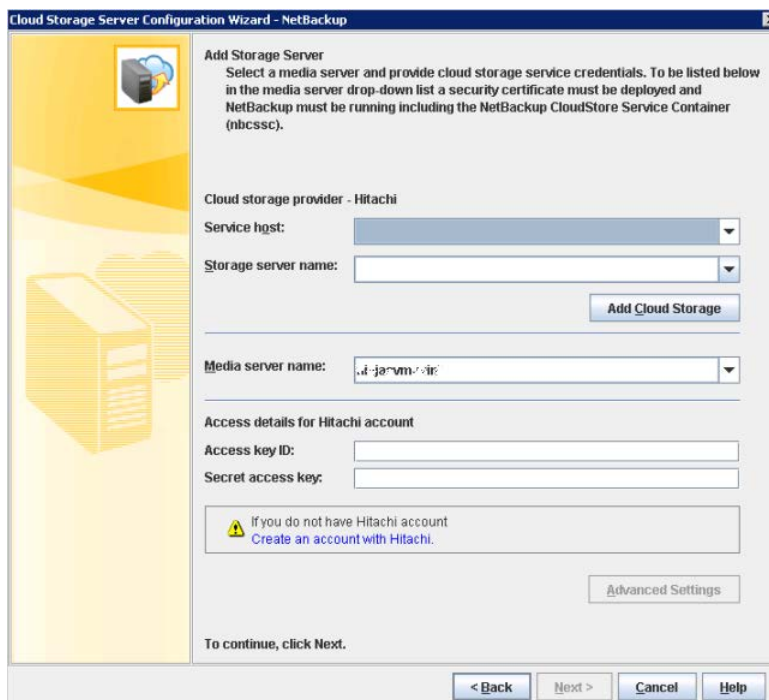


Table 2-22 describes the storage server configuration options for Hitachi.

Table 2-22 Hitachi storage server configuration options

Field name	Required content
Service host	<p>Displays the host name of the cloud service end point of Hitachi. Initially, the drop-down list does not contain any service hosts. You need to create a service host by clicking the Add Cloud Storage option.</p> <p>For details on the Hitachi public cloud, refer to the Hitachi documentation.</p>

Table 2-22 Hitachi storage server configuration options (*continued*)

Field name	Required content
Storage server name	<p>Displays the default Hitachi storage server. Initially, the drop-down list does not contain any storage server names.</p> <p>Type a storage server name in the drop-down list, which can be a logical name for the Hitachi cloud storage. You can create multiple storage servers with the different names that refer to the same physical service host for Hitachi.</p> <p>The drop-down list displays only those storage server names that are available for use.</p> <p>Note: Symantec recommends that a storage server name that you add while configuring an Amazon S3-compatible cloud provider should be a logical name and should not match a physical host name. For example: While you add an Amazon GovCloud storage server, avoid using names like 'amazongov.com' or 'amazon123.com'. These servers may be physical hosts, which can cause failures during cloud storage configuration. Instead, use storage server names like 'amazongov1' or 'amazonserver1' and so on.</p>
Add Cloud Storage	<p>The Add Cloud Storage option lets you add customized cloud deployment details for NetBackup to communicate with the cloud storage. The customized cloud deployment refers to the cloud instances that are not already listed in the Service Host drop-down list.</p> <p>Click the Add Cloud Storage option to open the Add Cloud Storage dialog box. Use the dialog box to configure the general settings and region settings of Hitachi.</p> <p>Once the cloud storage is added, you cannot modify or delete it using the NetBackup Administration Console. However, you can modify or delete a storage server by using the <code>cscnfig</code> command.</p> <p>Note: You can use the NetBackup <code>cscnfig -a</code> command to create custom cloud instances for an Amazon S3-compatible cloud provider. You must run the <code>cscnfig</code> command before you run the <code>nbdevcnfig</code> and <code>tpcnfig</code> commands.</p> <p>See the <i>NetBackup Commands Reference Guide</i> for a complete description about these commands. The guide is available through the following URL:</p> <p>http://www.symantec.com/docs/DOC5332</p>
Media server name	<p>Select NetBackup media server from the drop-down list. The drop-down list displays only NetBackup 7.7 and later media servers.</p>

Table 2-22 Hitachi storage server configuration options (*continued*)

Field name	Required content
Access key ID	Enter your Hitachi access key ID. If you do not have an account, click Create an account with the service provider link.
Secret access key	Enter your Hitachi secret access key.
Advanced Settings	To change SSL, proxy, or HTTP header settings for Hitachi, click Advanced Settings .

Rackspace storage server configuration options

Figure 2-8 shows the **Cloud Storage Server Configuration Wizard** panel for the Rackspace cloud storage.

Figure 2-8 Cloud Storage Server Configuration Wizard panel for Rackspace

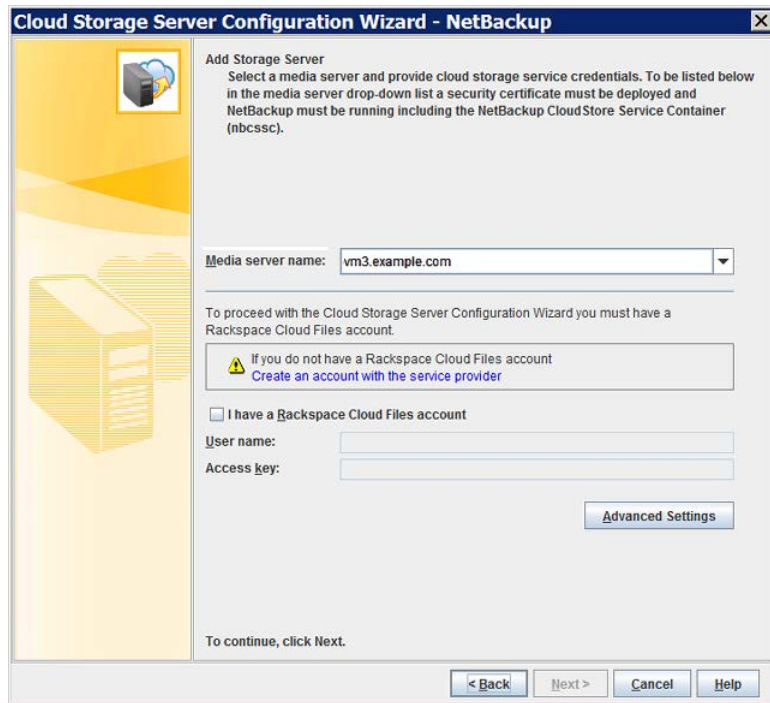


Table 2-23 describes the configuration options for AT&T.

Table 2-23 Rackspace storage server configuration options

Field name	Required content
Media Server Name	<p>Select a NetBackup media server. The host that you select queries the storage vendor's network for its capabilities and for the available storage. The media server also becomes a data mover for your backups and restores.</p> <p>Only those media servers that are enabled for cloud storage appear in the list, as follows:</p> <ul style="list-style-type: none"> ■ The media server operating system must be supported for cloud storage. For the operating systems that NetBackup supports for cloud storage, see the NetBackup operating system compatibility list available through the following URL: http://www.netbackup.com/compatibility ■ The NetBackup Cloud Storage Service Container (<i>nbcssc</i>) must be running. The NetBackup Cloud Storage Service Container requires an authentication certificate to run. See “About the NetBackup CloudStore Service Container” on page 34. ■ The cloud storage binary files must be present in the <code>ost-plugins</code> directory. <p>The NetBackup master server always has a certificate. If it meets the other two criteria, it appears in the Media Server Name drop-down list.</p> <p>After you configure the storage server, you cannot change the media server that you specify here. This behavior is the result of the OpenStorage plugin design. Attempts to change the media server generate an authorization error.</p>
Create an account with the service provider	<p>If you do not have an account with Rackspace, click Create an account with the service provider link. A web browser opens in which you can create an account with Rackspace.</p>
I have a Rackspace Cloud Files account	<p>Select I have a Rackspace Cloud Files account to enter the required account information.</p>
User Name	<p>Enter your Rackspace Cloud Files account user name.</p> <p>If you do not have an account, click Create an account with the service provider link.</p>
Access Key	<p>Enter your Rackspace Cloud Files account access key.</p>
Advanced Settings	<p>To change the default storage server for your cloud vendor or specify the maximum number of network connections, click Advanced Settings.</p> <p>See “About private clouds from Rackspace” on page 26.</p>

Verizon storage server configuration options

[Figure 2-9](#) shows the **Cloud Storage Configuration Wizard** panel for the Verizon cloud storage.

Figure 2-9 Cloud Storage Server Configuration Wizard panel for Verizon

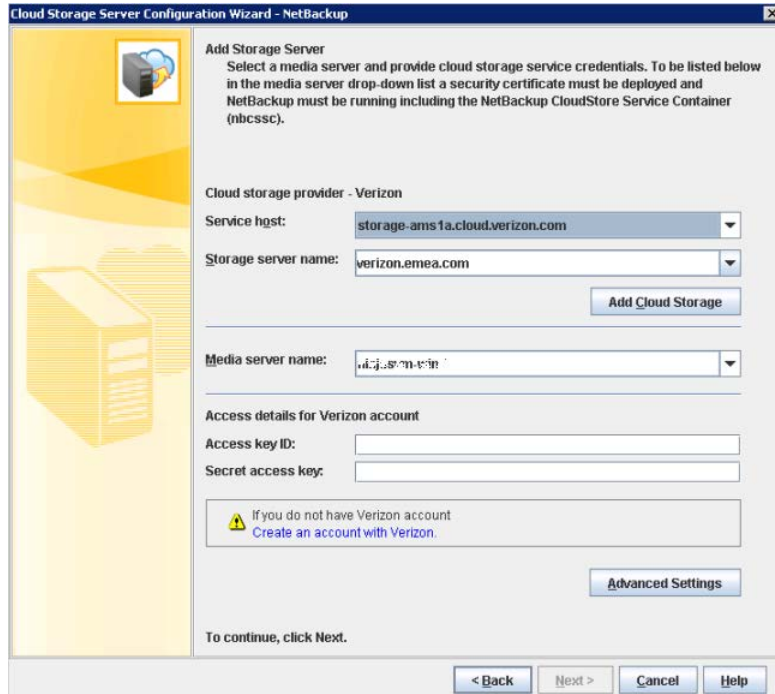


Table 2-24 describes the storage server configuration options for Verizon.

Table 2-24 Verizon storage server configuration options

Field name	Required content
Service host	Select the host name of the cloud service end point of Verizon. Select one of the following service hosts: storage-ams1a.cloud.verizon.com, storage-iad3a.cloud.verizon.com, storage-ushaa.cloud.verizon.com

Table 2-24 Verizon storage server configuration options (*continued*)

Field name	Required content
Storage server name	<p>Displays the default Verizon storage server. You can select a storage server other than the default one.</p> <p>The drop-down list displays only those names that are available for use.</p> <p>You can type a different storage server name in the drop-down list, which can be a logical name for the cloud storage. You can create multiple storage servers with the different names that refer to the same physical service host for Amazon. If there are no names available in the list, you can create a new storage server name by typing the name in the drop-down list.</p> <p>Note: Symantec recommends that a storage server name that you add while configuring an Amazon S3-compatible cloud provider should be a logical name and should not match a physical host name. For example: While you add an Amazon GovCloud storage server, avoid using names like 'amazongov.com' or 'amazon123.com'. These servers may be physical hosts, which can cause failures during cloud storage configuration. Instead, use storage server names like 'amazongov1' or 'amazonserver1' and so on.</p>
Add Cloud Storage	<p>The Add Cloud Storage option lets you add customized cloud deployment details for NetBackup to communicate with the cloud storage. The customized cloud deployment refers to the cloud instances that are not already listed in the Service Host drop-down list.</p> <p>Click the Add Cloud Storage option to open the Add Cloud Storage dialog box. Use the dialog box to configure the general settings and region settings of Verizon.</p> <p>Once the cloud storage is added, you cannot modify or delete it using the NetBackup Administration Console. However, you can modify or delete a storage server by using the <code>csconfig</code> command.</p> <p>Note: You can use the NetBackup <code>csconfig -a</code> command to create custom cloud instances for an Amazon S3-compatible cloud provider. You must run the <code>csconfig</code> command before you run the <code>nbdevconfig</code> and <code>tpconfig</code> commands.</p> <p>See the NetBackup Commands Reference Guide for a complete description about these commands. The guide is available through the following URL:</p> <p>http://www.symantec.com/docs/DOC5332</p>

Table 2-24 Verizon storage server configuration options (*continued*)

Field name	Required content
Media server name	Select NetBackup media server from the drop-down list. The drop-down list displays only NetBackup 7.7 and later media servers.
Access key ID	Enter your Verizon Access key ID. If you do not have an account, click Create an account with the service provider link.
Secret access key	Enter your Verizon secret access key.
Advanced Settings	To change SSL, proxy, or HTTP header settings for Verizon, click Advanced Settings .

KMS database encryption settings

[Table 2-25](#) describes the settings to configure the NetBackup Key Management Service database and the encryption keys for your cloud storage. This information protects the database that contains the keys that NetBackup uses to encrypt the data. Key groups and key records also are required for encryption. The **Cloud Storage Server Configuration Wizard** and the **Disk Pool Configuration Wizard** configures the encryption for you.

Table 2-25 Required information for the encryption database

Field Name	Required information
KMS Server Name	This field displays the name of your NetBackup master server. You can only configure KMS on your master server. This field cannot be changed. If KMS is not configured, this field displays <code><kms_server_name></code> .
Host Master Key (HMK) Passphrase	Enter the key that protects the database. In KMS terminology, the key is called a <i>passphrase</i> .
Re-enter HMK Passphrase	Re-enter the host master key.
Host Master Key ID	The ID is a label that you assign to the master key. The ID lets you identify the particular host master key. You are limited to 255 characters in this field. To decipher the contents of a keystore file, you must identify the correct Key Protection Key and Host Master Key. These IDs are stored unencrypted in the keystore file header. You can select the correct ones even if you only have access to the keystore file. To perform a disaster recovery you must remember the correct IDs and the pass phrases that are associated with the files.

Table 2-25 Required information for the encryption database (*continued*)

Field Name	Required information
Key Protection Key (KPK) Passphrase	Enter the password that protects the individual records within the KMS database. In KMS terminology, the key is called a <i>passphrase</i> .
Re-enter KPK Passphrase	Re-enter the key protection password.
Key Protection Key ID	The ID is a label that you assign to the key. The ID lets you identify the particular key protection key. You are limited to 255 characters in this field. To decipher the contents of a keystore file, you must identify the correct Key Protection Key and Host Master Key. These IDs are stored unencrypted in the keystore file header. You can select the correct ones even if you only have access to the keystore file. To perform a disaster recovery you must remember the correct IDs and the pass phrases that are associated with the files.

After you configure the storage server and disk pool, Symantec recommends that you save a record of the key names.

See [“Saving a record of the KMS key names for NetBackup cloud storage encryption”](#) on page 87.

Changing cloud storage server properties

The Change Storage Server dialog box lists all storage server properties. You can change these properties, if required.

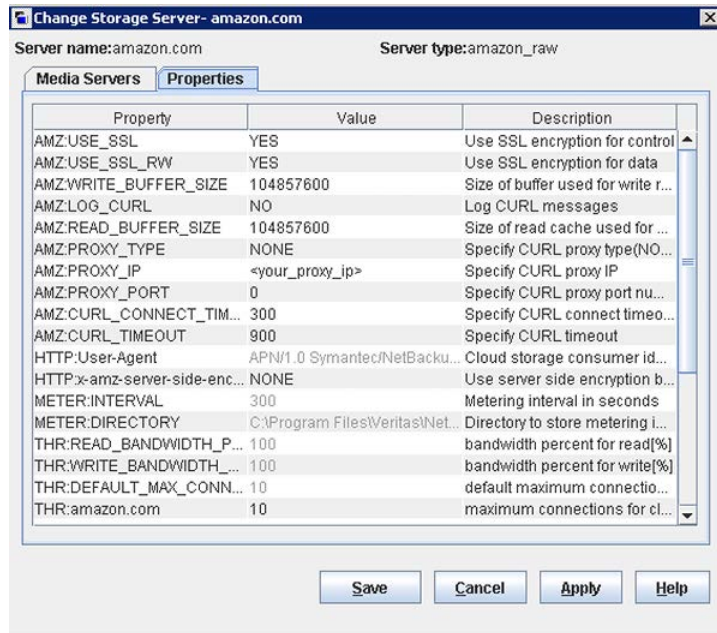
See [“Configuring cloud storage in NetBackup”](#) on page 15.

To change storage server properties

- 1 In the **NetBackup Administration Console**, expand **Media and Device Management > Credentials > Storage Server**.
- 2 Select the storage server.
- 3 On the **Edit** menu, select **Change**.

- 4 In the **Change Storage Server** dialog box, select the **Properties** tab.

The following is an example of the **Properties** for Amazon S3 storage server of type `amazon_raw`:



- 5 To change a property, select its value in the **Value** column and then change it.
 See [“NetBackup cloud storage server properties”](#) on page 67.
 See [“NetBackup storage server cloud connection properties”](#) on page 68.
 See [“NetBackup cloud storage server encryption properties”](#) on page 76.
- 6 Repeat step 5 until you have finishing changing properties.
- 7 Click **OK**.
- 8 Restart the NetBackup Remote Manager and Monitor Service (`nbrmms`) by using the **NetBackup Administration Console Activity Monitor**.

NetBackup cloud storage server properties

The **Properties** tab of the **Change Storage Server** dialog box lets you change some of the properties that affect the NetBackup interaction with the cloud storage.

Not all properties apply to all storage vendors.

[Table 2-26](#) describes the prefixes for the various properties.

Table 2-26 Prefix definitions

Prefix	Prefix meaning
AMZ	Amazon
AMZGOV	Amazon GovCloud
CLD	Cloudian Hyperstore
GOOG	Google Nearline
HT	Hitachi
VER	Verizon
ATT	AT&T
CRYPT	Encryption
METER	Metering
RACKS	Rackspace
THR	Throttling
HTTP	HTTP headers Note: This field is applicable only for Amazon S3-compatible cloud providers.

See [“Changing cloud storage server properties”](#) on page 66.

See [“NetBackup cloud storage server bandwidth throttling properties”](#) on page 73.

See [“NetBackup cloud storage server encryption properties”](#) on page 76.

See [“NetBackup storage server cloud connection properties”](#) on page 68.

NetBackup storage server cloud connection properties

All or most of the cloud storage servers use the storage server properties in [Table 2-27](#). The following are the prefixes for the currently supported cloud vendors:

- Amazon: AMZ
- AT&T: ATT
- Amazon GovCloud: AMZGOV

- Cloudian: CLD
- Google Nearline: GOOG
- Hitachi: HT
- Rackspace: RACKS
- Verizon: VER

Table 2-27 Storage server cloud connection properties

Property	Description
METER: DIRECTORY	<p>This read-only field displays the directory in which to store data stream metering information.</p> <p>Default value: /usr/opensv/lib/ost-plugins/meter (UNIX) or <i>install_path</i>\VERITAS\NetBackup\bin\ost-plugins\ (Windows)</p>
METER: INTERVAL	<p>The interval at which NetBackup gathers connection information for reporting purposes.</p> <p>NetBackup OpsCenter uses the information that is collected to create reports. The value is set in seconds. The default setting is 300 seconds (5 minutes). If you set this value to zero, metering is disabled</p> <p>To change this property, use the Cloud Settings tab of the Scalable Storage host properties.</p> <p>See “Scalable Storage properties” on page 29.</p> <p>Default value: 300</p> <p>Possible values: 1 to 10000</p>
PREFIX: CURL_CONNECT_TIMEOUT	<p>The amount of time that is allocated for the media server to connect to the cloud storage server. This value is specified in seconds. The default is 300 seconds or five minutes.</p> <p>This only limits the connection time, not the session time. If the media server cannot connect to the cloud storage server in the specified time, the job fails.</p> <p>This value cannot be disabled. If an invalid number is entered, the <code>CURL_CONNECT_TIMEOUT</code> returns to the default value of 300.</p> <p>Default value: 300</p> <p>Possible values: 1 to 10000</p>

Table 2-27 Storage server cloud connection properties (*continued*)

Property	Description
<i>PREFIX:CURL_TIMEOUT</i>	<p>The maximum time in seconds to allow for the completion of a data operation. This value is specified in seconds. If the operation does not complete in the specified time, the operation fails. The default is 900 seconds (15 minutes). To disable this timeout, set the value to 0 (zero).</p> <p>Default value: 900</p> <p>Possible values: 1 to 10000</p>
<i>PREFIX:LOG_CURL</i>	<p>Determines if cURL activity is logged. The default is NO which means log activity is disabled.</p> <p>Default value: NO</p> <p>Possible values: NO (disabled) and YES (enabled)</p>
<i>PREFIX:PROXY_IP</i>	<p>The TCP/IP address of the proxy server. If you do not use a proxy server, leave this field blank.</p> <p>Default value: No default</p> <p>Possible values: Valid TCP/IP address</p>
<i>PREFIX:PROXY_PORT</i>	<p>The port number that is used to connect to the proxy server. The default is 70000 which indicates you do not use a proxy server.</p> <p>Default value: 70000</p> <p>Possible values: Valid port number</p>
<i>PREFIX:PROXY_TYPE</i>	<p>Used to define the proxy server type. If a firewall prevents access to your cloud vendor, use this value to define your proxy server type. If you do not use a proxy server, leave this field blank.</p> <p>Default value: NONE</p> <p>Possible values: NONE, HTTP, SOCKS, SOCKS4, SOCKS5, SOCKS4A</p>

Table 2-27 Storage server cloud connection properties (*continued*)

Property	Description
<i>PREFIX:READ_BUFFER_SIZE</i>	<p>The size of the buffer to use for read operations. <i>READ_BUFFER_SIZE</i> is specified in bytes.</p> <p>To enable the use of the buffer, set this value to a non-zero number. Symantec recommends that this value be a multiple of 256.</p> <p>The <i>READ_BUFFER_SIZE</i> determines the size of the data packets that the storage server transmits during each restore job. An increase in the value may increase performance when a large amount of contiguous data is accessed. If insufficient bandwidth exists to transmit the specified amount of data within a few minutes, restore failures may occur due to timeouts. When you calculate the required bandwidth, consider the total load of simultaneous backup jobs and restore jobs on multiple media servers.</p> <p>Default value for Amazon S3-compatible cloud providers: 104875600 (100 MB)</p> <p>Default value for cloud providers other than Amazon S3-compatible providers: 0</p> <p>Possible values for Amazon S3-compatible cloud providers: 1048756 (1 MB) to 1073741824 (1 GB)</p> <p>Possible values for cloud providers other than Amazon S3-compatible providers: 524288 (512 KB) to 1073741824 (1 GB)</p>
<i>PREFIX:USE_SSL</i>	<p>Determines if Secure Sockets Layer encryption is used for the control APIs. The default value is <i>YES</i>, meaning SSL is enabled.</p> <p>Default value: <i>YES</i></p> <p>Possible values: <i>YES</i> or <i>NO</i></p>
<i>PREFIX:USE_SSL_RW</i>	<p>Determines if Secure Sockets Layer encryption is used for read and write operations. The default value is <i>YES</i>, meaning SSL is enabled.</p> <p>Default value: <i>YES</i></p> <p>Possible values: <i>YES</i> or <i>NO</i></p>
<i>PREFIX: WRITE_BUFFER_NUM</i>	<p>This parameter is not applicable for Amazon S3-compatible cloud providers.</p> <p>This read-only field displays the total number of write buffers that are used by the plug-in. The <i>WRITE_BUFFER_SIZE</i> value defines the size of the buffer. The value is set to 1 and cannot be changed.</p> <p>Default value: 1</p> <p>Possible values: 1</p>

Table 2-27 Storage server cloud connection properties (*continued*)

Property	Description
<p><code>PREFIX:WRITE_BUFFER_SIZE</code></p>	<p>The size of the buffer to use for write operations. <code>WRITE_BUFFER_SIZE</code> is specified in bytes.</p> <p>To disable the use of the buffer, set this value to 0 (zero).</p> <p>The <code>WRITE_BUFFER_SIZE</code> value determines the size of the data packs transmitted from the data mover to the storage server during a backup. An increase in the value may increase performance when a large amount of contiguous data is accessed. If insufficient bandwidth exists to transmit the specified amount of data within a few minutes, backup failures may occur due to timeouts. When you calculate the required bandwidth, consider the total load of simultaneous backup jobs and restore jobs on multiple media servers.</p> <p>Default value for Amazon S3-compatible cloud providers: 104875600 (100 MB)</p> <p>Default value for cloud providers other than Amazon S3-compatible cloud providers: 10485760 (10 MB)</p> <p>Possible values for all cloud providers: 1048576 (1 MB) to 1073741824 (1 GB)</p>
<p><code>HTTP:User-Agent</code></p>	<p>This is applicable only for Amazon S3-compatible cloud providers.</p> <p>See “About Amazon S3-compatible cloud providers that NetBackup supports beginning in NetBackup 7.7” on page 9.</p> <p>You cannot edit this property.</p>
<p><code>HTTP:x-amz-server-side-encryption</code></p>	<p>This is applicable only for the following cloud providers: Amazon S3 and Amazon GovCloud</p> <p>Use this property to enable the server-side encryption of the data that you need to transfer to the cloud storage.</p> <p>AES-256 is a server-side encryption standard.</p> <p>Set this property to NONE to disable the server-side encryption for the cloud provider.</p> <p>Note: You should not enable this property, if you have already enabled the media server-side encryption option while configuring cloud storage server using the NetBackup Administration Console.</p>

See [“Changing cloud storage server properties”](#) on page 66.

See [“NetBackup cloud storage server properties”](#) on page 67.

NetBackup cloud storage server bandwidth throttling properties

The following storage server properties apply to bandwidth throttling. The `THR` prefix specifies a throttling property. Use the correct cloud provider URL for the desired cloud vendor.

To change these properties, use the **Scalable Storage** host properties **Cloud Settings** tab.

See [“Scalable Storage properties”](#) on page 29.

Table 2-28 Cloud storage server bandwidth throttling properties

Property	Description
<code>THR:storage_server</code>	<p>Shows maximum number of concurrent jobs that can be run for a specific cloud storage server.</p> <p>Default value: Not applicable</p> <p>Possible values: See Description</p>
<code>THR:AVAIL_BANDWIDTH</code>	<p>This read-only field displays the total available bandwidth value for the cloud feature. The value is displayed in bytes per second. You must specify a number greater than zero. If you enter zero, an error is generated.</p> <p>Default value: 104857600</p> <p>Possible values: Any positive integer</p>

Table 2-28 Cloud storage server bandwidth throttling properties (*continued*)

Property	Description
<p>THR:DEFAULT_MAX_CONNECTIONS</p>	<p>The default maximum number of concurrent jobs that the media server can run for the cloud storage server.</p> <p>If THR:<i>storage_server</i> is set, NetBackup uses THR:<i>storage_server</i> instead of THR:DEFAULT_MAX_CONNECTIONS.</p> <p>This is a read-only field.</p> <p>This value applies to the media server not to the cloud storage server. If you have more than one media server that can connect to the cloud storage server, each media server can have a different value. Therefore, to determine the total number of jobs that can run on the cloud storage server, add the values from each media server.</p> <p>If NetBackup is configured to allow more jobs than THR:DEFAULT_MAX_CONNECTIONS, NetBackup fails any jobs that start after the number of maximum jobs is reached. Jobs include both backup and restore jobs.</p> <p>You can configure job limits per backup policy and per storage unit.</p> <p>See the <i>NetBackup Administrator's Guide, Volume I</i>: http://www.symantec.com/docs/DOC5332</p> <p>Note: NetBackup must account for many factors when it starts jobs: the number of concurrent jobs, the number of THR:DEFAULT_MAX_CONNECTIONS per media server, the number of media servers, and the job load-balancing logic. Therefore, NetBackup may not fail jobs exactly at the maximum number of connections. NetBackup may fail a job when the connection number is slightly less than the maximum, exactly the maximum, or slightly more than the maximum.</p> <p>In practice, you should not need to set this value higher than 100.</p> <p>Default value: 10</p> <p>Possible values: 1 to 2147483647</p>
<p>THR:OFF_TIME_BANDWIDTH_PERCENT</p>	<p>This read-only field displays the bandwidth percent that is used during off time.</p> <p>Default value: 100</p> <p>Possible values: 0 to 100</p>

Table 2-28 Cloud storage server bandwidth throttling properties (*continued*)

Property	Description
THR:OFF_TIME_END	<p>This read-only field displays the end of off time. Specify the time in 24-hour format. For example, 8:00 A.M. is 8 and 6:30 P.M. is 1830.</p> <p>Default value: 8</p> <p>Possible values: 0 to 2359</p>
THR:OFF_TIME_START	<p>This read-only field displays the start of off time. Specify the time in 24-hour format. For example, 8:00 A.M. is 8 and 6:30 P.M. is 1830.</p> <p>Default value: 18</p> <p>Possible values: 0 to 2359</p>
THR:READ_BANDWIDTH_PERCENT	<p>This read-only field displays the read bandwidth percentage the cloud feature uses. Specify a value between 0 and 100. If you enter an incorrect value, an error is generated.</p> <p>Default value: 100</p> <p>Possible values: 0 to 100</p>
THR:SAMPLE_INTERVAL	<p>This read-only field displays the rate at which backup streams sample their utilization and adjust their bandwidth use. The value is specified in seconds. When this value is set to zero, throttling is disabled.</p> <p>Default value: 0</p> <p>Possible values: 1 to 2147483647</p>
THR:WEEKEND_BANDWIDTH_PERCENT	<p>This read-only field displays the bandwidth percent that is used during the weekend.</p> <p>Default value: 100</p> <p>Possible values: 0 to 100</p>
THR:WEEKEND_END	<p>This read-only field displays the end of the weekend. The day value is specified with numbers, 1 for Monday, 2 for Tuesday, and so on.</p> <p>Default value: 7</p> <p>Possible values: 1 to 7</p>
THR:WEEKEND_START	<p>This read-only field displays the start of the weekend. The day value is specified with numbers, 1 for Monday, 2 for Tuesday, and so on.</p> <p>Default value: 6</p> <p>Possible values: 1 to 7</p>

Table 2-28 Cloud storage server bandwidth throttling properties (*continued*)

Property	Description
THR:WORK_TIME_BANDWIDTH_PERCENT	This read-only field displays the bandwidth percent that is used during the work time. Default value: 100 Possible values: 0 to 100
THR:WORK_TIME_END	This read-only field displays the end of work time. Specify the time in 24-hour format. For example, 8:00 A.M. is 8 and 6:30 P.M. is 1830. Default value: 18 Possible values: 0 to 2359
THR:WORK_TIME_START	This read-only field displays the start of work time. Specify the time in 24-hour format. For example, 8:00 A.M. is 8 and 6:30 P.M. is 1830. Default value: 8 Possible values: 0 to 2359
THR:WRITE_BANDWIDTH_PERCENT	This read-only field displays the write bandwidth percentage the cloud feature uses. Specify a value between 0 and 100. If you enter an incorrect value, an error is generated. Default value: 100 Possible values: 0 to 100

See [“Changing cloud storage server properties”](#) on page 66.

See [“NetBackup cloud storage server properties”](#) on page 67.

NetBackup cloud storage server encryption properties

The following encryption-specific storage server properties are used by all or most of the storage vendors. The `CRYPT` prefix specifies an encryption property. These values are for display purposes only and cannot be changed.

Table 2-29 Encryption cloud storage server properties

Property	Description
CRYPT:KMS_SERVER	This read-only field displays NetBackup server that hosts the KMS service. When you set the storage server properties, enter the name of the KMS server host. By default, this field contains the NetBackup master server name. You cannot change this value. Default value: The NetBackup master server name Possible values: N/A
CRYPT:KMS_VERSION	This read-only field displays the NetBackup Key Management Service version. You cannot change this value. Default value: 16 Possible values: N/A
CRYPT:LOG_VERBOSE	This read-only field displays if logs are enabled for encryption activities. The value is either YES for logging or NO for no logging. Default value: NO Possible values: YES and NO
CRYPT:VERSION	This read-only field displays the encryption version. You cannot change this value. Default value: 13107 Possible values: N/A

See [“Changing cloud storage server properties”](#) on page 66.

About cloud storage disk pools

A disk pool represents disk volumes on the underlying disk storage. A disk pool is the storage destination of a NetBackup storage unit. For cloud storage, you must specify only one volume for a disk pool.

Disk pool and disk volume names must be unique within your cloud storage provider's environment.

See [“Configuring a disk pool for cloud storage”](#) on page 78.

If a cloud storage disk pool is a storage destination in a storage lifecycle policy, NetBackup capacity management applies.

See the *NetBackup Administrator's Guide, Volume I*:

<http://www.symantec.com/docs/DOC5332>

Configuring a disk pool for cloud storage

Use the NetBackup **Disk Pool Configuration Wizard** to create a disk pool for cloud storage. If you create encrypted storage, you must enter a pass phrase for each selected volume that uses encryption. The pass phrase creates the encryption key for that volume.

To configure a cloud storage disk pool by using the wizard

- 1 If the **Disk Pool Configuration Wizard** was launched from the **Storage Server Configuration Wizard**, go to step 5.

Otherwise, in the **NetBackup Administration Console**, select either **NetBackup Management** or **Media and Device Management**.

- 2 From the list of wizards in the right pane, click **Configure Disk Pool**.

- 3 On the **Welcome** panel, the types of disk pools that you can configure depend on the types of storage servers that exist in your environment.

The following is an example of the wizard panel:

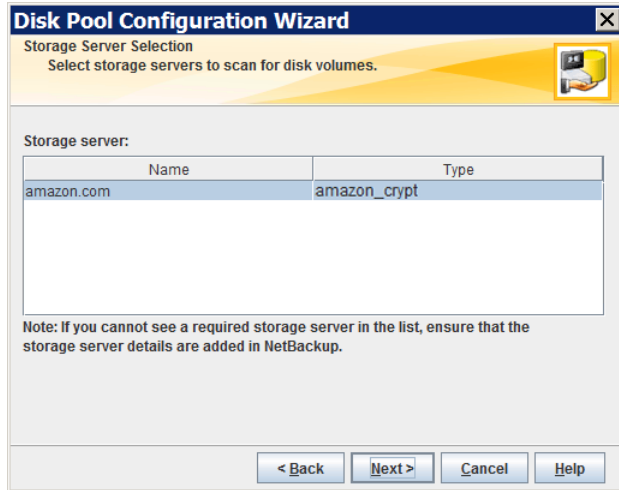


Read the information on the welcome panel of the wizard. Then, select the appropriate storage server type and click **Next**.

The **Storage Server Selection** panel appears.

- 4 On the **Storage Server Selection** panel, the storage servers that you configured for the selected storage server type appear.

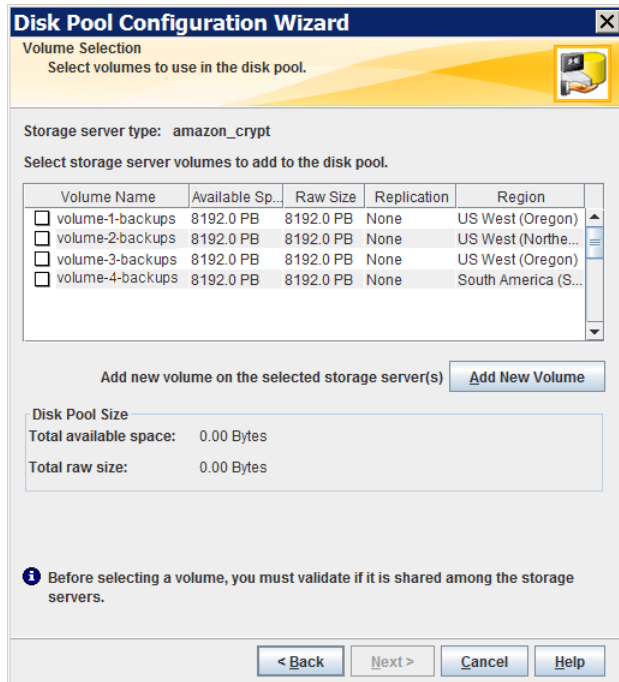
The following is an example of the wizard panel:



Select the storage server for this disk pool.

After you select the cloud storage server, click **Next**. The **Volume Selection** wizard panel appears.

- 5 On the **Volume Selection** panel, the wizard displays the volumes that have been created already under your account within the vendor's cloud storage. The following is an example of the wizard panel:



To add a volume, click **Add New Volume**. A dialog box appears that contains the information that is required for a volume for your cloud vendor. In that dialog box, enter the required information. Information is available about the requirements for the volume names.

See [“About the cloud storage providers”](#) on page 17.

To select a volume, click the check box for the volume. You can select one volume only.

After you select the volume for the disk pool, click **Next**. The behavior of the wizard depends on whether you configured encryption for the storage server, as follows:

No encryption If you select a volume on a storage destination that does not require encryption, the **Disk Pool Properties** panel appears.

Go to step 7.

Encryption

If you select a volume on a storage destination that requires encryption, a dialog box appears in which you must enter an encryption pass phrase. The pass phrase is for the *key group key* for this storage volume and storage server combination.

The volume requires encryption if you selected **Encrypt data using AES-256 before writing to cloud storage** when you configured the storage server.

Continue to the next step, step 6.

- 6 For encrypted storage, enter a pass phrase for the key group key in the **Settings** dialog box, then click **OK**.

See [“About key management for encryption of NetBackup cloud storage”](#) on page 39.

Click **Next**. The **Additional Disk Pool Information** wizard panel appears.

- 7 The **Additional Disk Pool Information** panel is the panel on which you enter or select the properties for this disk pool.

The following is an example of the wizard panel:

Disk Pool Configuration Wizard

Additional Disk Pool Information
 Provide additional disk pool information.

Storage server type: amazon_crypt

Disk Pool Size
 Total available space: 8192.00 PB
 Total raw size: 8192.00 PB

Disk Pool name:

Comments:

High water mark: 98 %

Low water mark: 80 %

Maximum I/O Streams
 ⓘ Concurrent read and write jobs affect disk performance.
 Limit I/O streams to prevent disk overload.
 Limit I/O streams: 1 per volume

< Back Next > Cancel Help

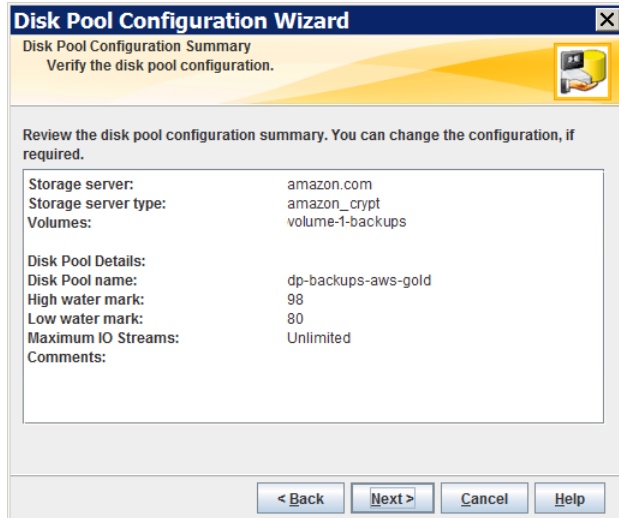
Enter or select the values for the properties for this disk pool.

See [“Cloud storage disk pool properties”](#) on page 101.

Click **Next**. The **Summary** panel appears.

8 On the **Summary** panel, verify the selections.

The following is an example of the wizard panel:



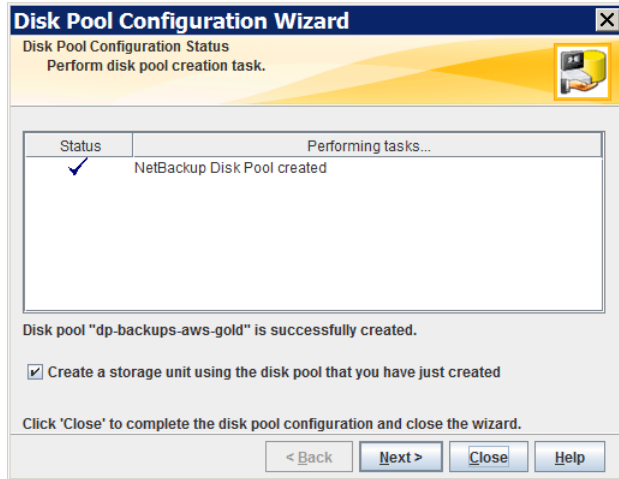
If the summary shows your selections accurately, click **Next**.

Symantec recommends that you save the KMS key group name and the KMS key name. They are required to recover the keys.

See [“Saving a record of the KMS key names for NetBackup cloud storage encryption”](#) on page 87.

- 9 After NetBackup creates the disk pool, a wizard panel describes the successful action.

The following is an example of the wizard panel:

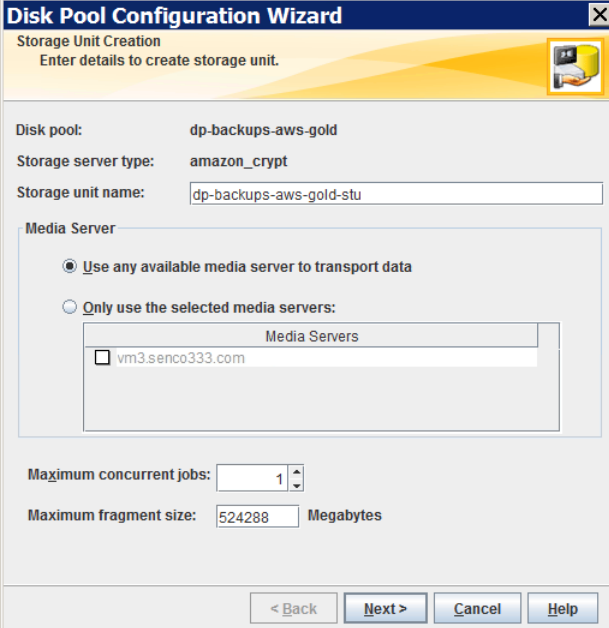


After NetBackup creates the disk pool, you can do the following:

- Configure a storage unit Ensure that **Create a storage unit using the disk pool that you have just created** is selected and then click **Next**. The **Storage Unit Creation** wizard panel appears. Continue to the next step.
- Exit Click **Close**.
 You can configure one or more storage units later.
 See [“Configuring a storage unit for cloud storage”](#) on page 91.

- 10 On **Storage Unit Creation** wizard panel, enter the appropriate information for the storage unit.

The following is an example of the wizard panel:



The screenshot shows the "Disk Pool Configuration Wizard" window, specifically the "Storage Unit Creation" step. The window title is "Disk Pool Configuration Wizard" and the subtitle is "Storage Unit Creation". Below the subtitle, it says "Enter details to create storage unit." The form contains the following fields and options:

- Disk pool:** dp-backups-aws-gold
- Storage server type:** amazon_crypt
- Storage unit name:** dp-backups-aws-gold-stu
- Media Server:**
 - Use any available media server to transport data
 - Only use the selected media servers:
 - Media Servers list: vm3.senco333.com (unchecked)
- Maximum concurrent jobs:** 1
- Maximum fragment size:** 524288 Megabytes

At the bottom of the window, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

See [“Cloud storage unit properties”](#) on page 92.

After you enter or select the information for the storage unit, click **Next** to create the storage unit.

You can use storage unit properties to control your backup traffic.

See [“Configure a favorable client-to-server ratio”](#) on page 94.

See [“Control backup traffic to the media servers”](#) on page 95.

- 11 After NetBackup configures the storage unit, the **Finished** panel appears. Click **Finish** to exit from the wizard.

Changing cloud disk pool state

You can change the state of a NetBackup disk pool. Pool states are UP or DOWN.

To change the state to DOWN, the disk pool must not be busy. If backup jobs are assigned to the disk pool, the state change fails. Cancel the backup jobs or wait until the jobs complete.

To change cloud disk pool state

- 1 In the **NetBackup Administration Console**, in the left pane, select **Media and Device Management > Device Monitor**.
- 2 Select the **Disk Pools** tab.
- 3 Select the disk pool.
- 4 Select either **Actions > Up** or **Actions > Down**.

Saving a record of the KMS key names for NetBackup cloud storage encryption

Symantec recommends that you save a record of the encryption key names and tags. The key tag is necessary if you need to recover or recreate the keys.

See [“About data encryption for cloud storage”](#) on page 38.

To save a record of the key names

- 1 To determine the key group names, use the following command on the master server:

UNIX: `/usr/opensv/netbackup/bin/admincmd/nbkmsutil -listkgs`

Windows: `install_path\Program`

`Files\Veritas\NetBackup\bin\admincmd\nbkmsutil.exe -listkgs`

The following is example output:

```
Key Group Name       : CloudVendor.com:symc_backups_gold
Supported Cypher     : AES_256
Number of Keys       : 1
Has Active Key       : Yes
Creation Time        : Tues Oct 01 01:00:00 2013
Last Modification Time: Tues Oct 01 01:00:00 2013
Description          : CloudVendor.com:symc_backups_gold
```


- 2 For each key group, write all of the keys that belong to the group to a file. Run the command on the master server. The following is the command syntax:

UNIX: `/usr/opensv/netbackup/bin/admincmd/nbkmsutil -listkeys -kgname key_group_name > filename.txt`

Windows: `install_path\Program`

`Files\Veritas\NetBackup\bin\admincmd\nbkmsutil.exe -listkeys -kgname key_group_name > filename.txt`

The following is example output:

```
nbkmsutil.exe -listkeys -kgname CloudVendor.com:symc_backups_gold
> encrypt_keys_CloudVendor.com_symc_backups_gold.txt
```

```
Key Group Name       : CloudVendor.com:symc_backups_gold
Supported Cypher     : AES_256
Number of Keys       : 1
Has Active Key       : Yes
Creation Time        : Tues Jan 01 01:00:00 2013
Last Modification Time: Tues Jan 01 01:00:00 2013
Description          : Key group to protect cloud volume
FIPS Approved Key    : Yes
```

```
Key Tag              : 532cf41cc8b3513a13c1c26b5128731e
                    : 5ca0b9b01e0689cc38ac2b7596bbae3c
```

```
Key Name             : Encrypt_Key_April
Current State        : Active
Creation Time        : Tues Jan 01 01:02:00 2013
Last Modification Time: Tues Jan 01 01:02:00 2013
Description          : -
```

```
Number of Keys: 1
```

- 3 Include in the file the pass phrase that you used to create the key record.
- 4 Store the file in a secure location.

Adding backup media servers to your cloud environment

You can add additional media servers to your cloud environment. Additional media servers can help improve backup performance. Such servers are known as *data movers*.

See “[About cloud storage data movers](#)” on page 41.

A NetBackup media server must meet the following conditions so that you can add it as a data mover:

- The media server operating system must be supported for cloud storage. For the operating systems that NetBackup supports for cloud storage, see the NetBackup operating system compatibility list available through the following URL:
<http://www.netbackup.com/compatibility>
- The NetBackup CloudStore Service Container (`nbcssc`) must be running. See “[About the NetBackup CloudStore Service Container](#)” on page 34.
- The cloud storage binary files must be present in the `ost-plugins` directory.
- For Amazon S3-compatible cloud providers, only NetBackup 7.7 and later media servers can be data movers.

Adding backup media servers to your cloud environment

- 1 In the NetBackup Administration Console, expand **Media and Device Management > Credentials > Storage Servers**.
- 2 Select the cloud storage server.
- 3 From the **Edit** menu, select **Change**.
- 4 In the **Change Storage Server** dialog box, select the **Media Servers** tab.
- 5 Select the media server or servers that you want to enable for cloud backup. The media servers that you select are configured as cloud servers.

Note: For Amazon S3-compatible cloud providers, only NetBackup 7.7 and later media servers are available for selection.

- 6 Click **OK**.
- 7 For AT&T and Rackspace cloud providers only, do the following:
 - a Copy the appropriate configuration file from the media server that you specified when you configured the storage server. The file name depends on your storage vendor. The following is the format:

```
libstspiVendorName.conf
```

The file resides in the following directory, depending on operating system:

- UNIX and Linux: `/usr/opensv/lib/ost-plugins/`
- Windows: `install_path\VERITAS\NetBackup\bin\ost-plugins\`

- b Save the file to the appropriate directory on the media server or servers that you added, as follows:
 - UNIX and Linux: `/usr/opensv/lib/ost-plugins/`
 - Windows: `install_path\VERITAS\NetBackup\bin\ost-plugins\`

Caution: If you do not copy the `libstspiVendorName.conf` to the new media server, any backups that attempt to use the media server fail. The backups fail with a NetBackup Status Code 83 (media open error).

- 8 Modify disk pools, storage units, and policies as desired.

Configuring a storage unit for cloud storage

Create one or more storage units that reference the disk pool.

The **Disk Pool Configuration Wizard** lets you create a storage unit; therefore, you may have created a storage unit when you created a disk pool. To determine if storage units exist for the disk pool, see the **NetBackup Management > Storage > Storage Units** window of the Administration Console.

A storage unit inherits the properties of the disk pool. If the storage unit inherits replication properties, the properties signal to a NetBackup storage lifecycle policy the intended purpose of the storage unit and the disk pool. Auto Image Replication requires storage lifecycle policies.

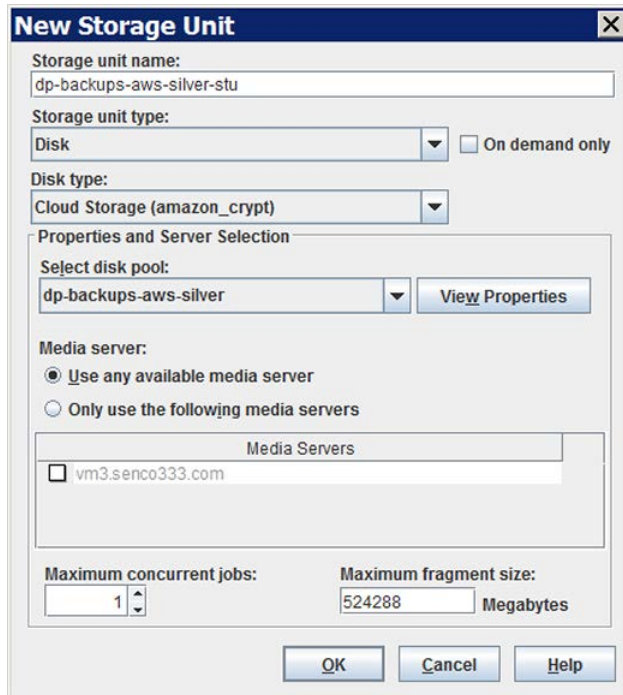
You can use storage unit properties to control your backup traffic.

See [“Configure a favorable client-to-server ratio”](#) on page 94.

See [“Control backup traffic to the media servers”](#) on page 95.

To configure a storage unit from the Actions menu

- 1 In the **NetBackup Administration Console**, expand **NetBackup Management > Storage > Storage Units**.
- 2 On the **Actions** menu, select **New > Storage Unit**.



- 3 Complete the fields in the **New Storage Unit** dialog box.
 See [“Cloud storage unit properties”](#) on page 92.

Cloud storage unit properties

The following are the configuration options for a cloud disk pool storage unit.

Table 2-30 Cloud storage unit properties

Property	Description
Storage unit name	A unique name for the new storage unit. The name can describe the type of storage. The storage unit name is the name used to specify a storage unit for policies and schedules. The storage unit name cannot be changed after creation.

Table 2-30 Cloud storage unit properties (*continued*)

Property	Description
Storage unit type	Select Disk as the storage unit type.
Disk type	Select Cloud Storage (type) for the disk type. <i>type</i> represents the disk pool type, based on storage vendor, encryption, and so on.
Disk pool	<p>Select the disk pool that contains the storage for this storage unit.</p> <p>All disk pools of the specified Disk type appear in the Disk pool list. If no disk pools are configured, no disk pools appear in the list.</p>
Media server	<p>The Media server setting specifies the NetBackup media servers that can backup clients and move the data to the cloud storage server. The media servers can also move the data for restore or duplication operations.</p> <p>Specify the media server or servers as follows:</p> <ul style="list-style-type: none"> ■ To allow any server in the media server list to deduplicate data, select Use any available media server. ■ To use specific media servers to deduplicate the data, select Only use the following media servers. Then, select the media servers to allow. <p>NetBackup selects the media server to use when the policy runs.</p>
Maximum concurrent jobs	<p>The Maximum concurrent jobs setting specifies the maximum number of jobs that NetBackup can send to a disk storage unit at one time. (Default: one job. The job count can range from 0 to 256.) This setting corresponds to the Maximum concurrent write drives setting for a Media Manager storage unit.</p> <p>NetBackup queues jobs until the storage unit is available. If three backup jobs are scheduled and Maximum concurrent jobs is set to two, NetBackup starts the first two jobs and queues the third job. If a job contains multiple copies, each copy applies toward the Maximum concurrent jobs count.</p> <p>Maximum concurrent jobs controls the traffic for backup and duplication jobs but not restore jobs. The count applies to all servers in the storage unit, not per server. If you select multiple media servers in the storage unit and 1 for Maximum concurrent jobs, only one job runs at a time.</p> <p>The number to enter depends on the available disk space and the server's ability to run multiple backup processes.</p> <p>Warning: A Maximum concurrent jobs setting of 0 disables the storage unit.</p>

Table 2-30 Cloud storage unit properties (*continued*)

Property	Description
Maximum fragment size	<p>For normal backups, NetBackup breaks each backup image into fragments so it does not exceed the maximum file size that the file system allows. You can enter a value from 20 MBs to 51200 MBs.</p> <p>For a FlashBackup policy, Symantec recommends that you use the default, maximum fragment size to ensure optimal duplication performance.</p>

Configure a favorable client-to-server ratio

You can use storage unit settings to configure a favorable client-to-server ratio. You can use one disk pool and configure multiple storage units to separate your backup traffic. Because all storage units use the same disk pool, you do not have to partition the storage.

For example, assume that you have 100 important clients, 500 regular clients, and four media servers. You can use two media servers to back up your most important clients and two media servers to back up your regular clients.

The following example describes how to configure a favorable client-to-server ratio:

- Configure the media servers for NetBackup deduplication and configure the storage.
- Configure a disk pool.
- Configure a storage unit for your most important clients (such as STU-GOLD). Select the disk pool. Select **Only use the following media servers**. Select two media servers to use for your important backups.
- Create a backup policy for the 100 important clients and select the STU-GOLD storage unit. The media servers that are specified in the storage unit move the client data to the deduplication storage server.
- Configure another storage unit (such as STU-SILVER). Select the same disk pool. Select **Only use the following media servers**. Select the other two media servers.
- Configure a backup policy for the 500 regular clients and select the STU-SILVER storage unit. The media servers that are specified in the storage unit move the client data to the deduplication storage server.

Backup traffic is routed to the wanted data movers by the storage unit settings.

Note: NetBackup uses storage units for media server selection for write activity (backups and duplications) only. For restores, NetBackup chooses among all media servers that can access the disk pool.

Control backup traffic to the media servers

On disk pool storage units, you can use the **Maximum concurrent jobs** settings to control the backup traffic to the media servers. Effectively, this setting directs higher loads to specific media servers when you use multiple storage units for the same disk pool. A higher number of concurrent jobs means that the disk can be busier than if the number is lower.

For example, two storage units use the same set of media servers. One of the storage units (STU-GOLD) has a higher **Maximum concurrent jobs** setting than the other (STU-SILVER). More client backups occur for the storage unit with the higher **Maximum concurrent jobs** setting.

About NetBackup Accelerator and NetBackup Optimized Synthetic backups

NetBackup Cloud Storage supports NetBackup Accelerator and NetBackup Optimized Synthetics. Encryption, metering, and throttling are functional and supported when you enable NetBackup Accelerator or NetBackup Optimized Synthetic backups. You enable both NetBackup Accelerator and NetBackup Optimized Synthetic backups in the same way as non-Cloud backups. More information about NetBackup Accelerator and NetBackup Optimized Synthetic backups is available.

- *Symantec NetBackup Deduplication Guide*
- *Symantec NetBackup Administrator's Guide, Volume I*

These guides are available through the following URL:

<http://www.symantec.com/docs/DOC5332>

Enabling NetBackup Accelerator with cloud storage

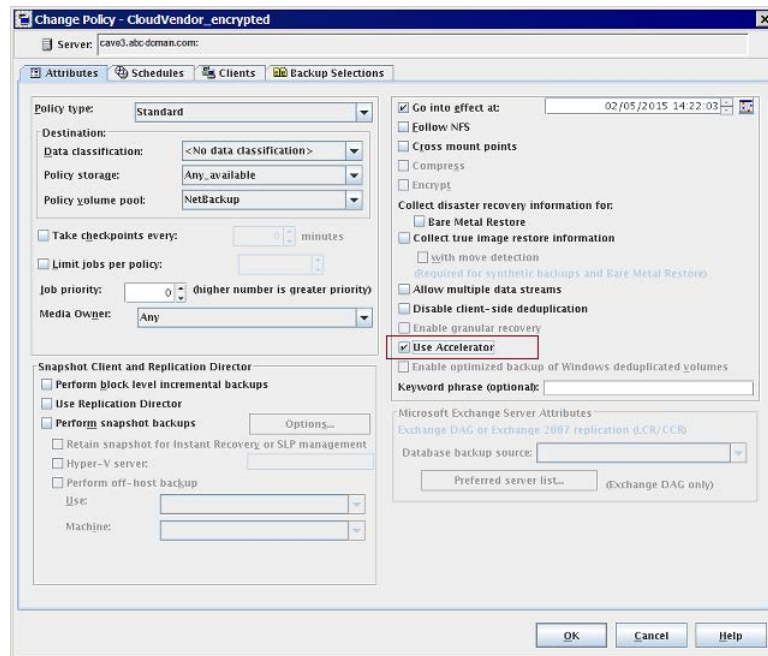
Use the following procedure to enable NetBackup Accelerator for use with NetBackup cloud storage.

Enabling Accelerator for use with NetBackup cloud storage

- 1 In the NetBackup Administration Console, select **NetBackup Management > Policies > *policy_name***. Select **Edit > Change**, and select the **Attributes** tab.
- 2 Select **Use accelerator**.
- 3 Confirm the **Policy storage** option is a valid Cloud storage unit.

The storage unit that is specified under **Policy storage** must be one of the supported Cloud vendors. You can't set **Policy storage** to **Any Available**.

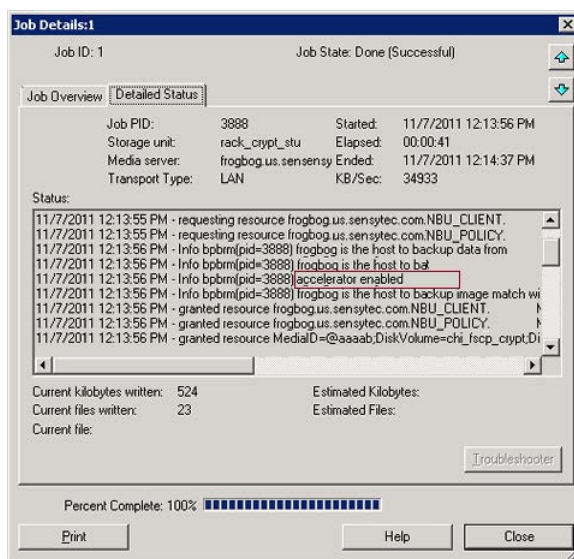
Figure 2-10 Enable Accelerator



Determining if NetBackup Accelerator was used during a backup operation

- 1 In the NetBackup Administration Console, select **Activity Monitor**. Double click the backup that you want to check.
- 2 Click the **Detailed Status** tab.
- 3 Review the status for **accelerator enabled**. This text indicates the backup used NetBackup Accelerator.

Figure 2-11 Confirm Accelerator used during backup



Enabling optimized synthetic backups with cloud storage

Optimized Synthetic backups require three backup schedules. You must have a **Full backup**, an **Incremental backup**, and a **Full Backup with Synthetic backup enabled**. You can use either a Differential incremental or a Cumulative incremental for the incremental backup. You must then perform a full backup, then at least one incremental backup, and finally a full backup with synthetic enabled. The final backup is the optimized synthetic backup.

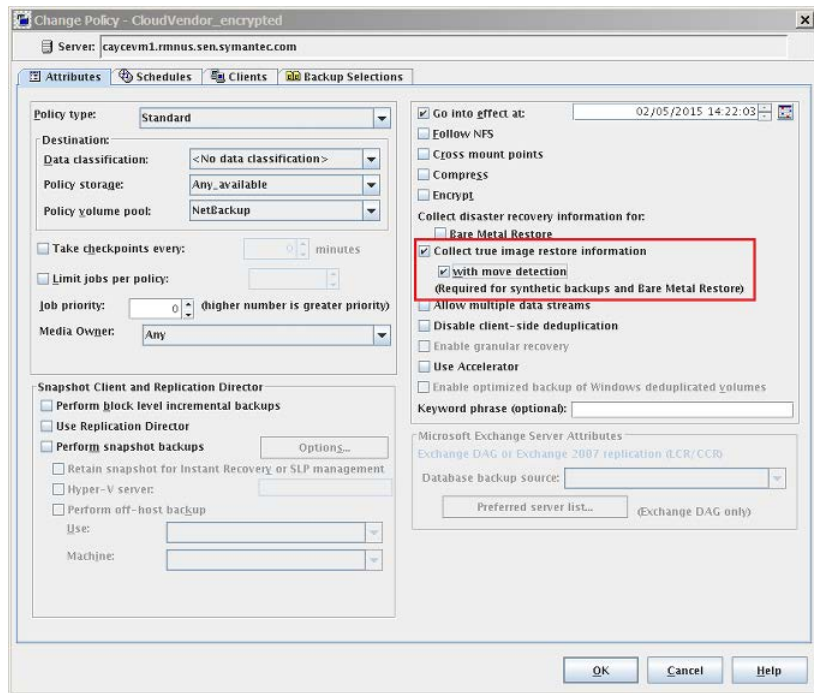
Note: In the case of Hitachi cloud configuration, the True Image Restore (TIR) or synthetic backups do not work, if you have enabled the encryption option. To successfully run the TIR or synthetic backups, you need to enable the versioning option for buckets (or namespaces) through the Hitachi cloud portal. For more details on how to enable the versioning option, contact Hitachi cloud provider.

Enabling Optimized Synthetic backups for use with NetBackup Cloud Storage

- 1 In the NetBackup Administration Console, select **NetBackup Management > Policies > *policy_name***. Select **Edit > Change**, and select the **Attributes** tab.
- 2 Select **Collect true image restore information** and **with move detection**.
- 3 Confirm the **Policy storage** option is a valid Cloud storage unit.

The storage unit that is specified under **Policy storage** must be one of the supported Cloud vendors. You can't set **Policy storage** to **Any Available**.

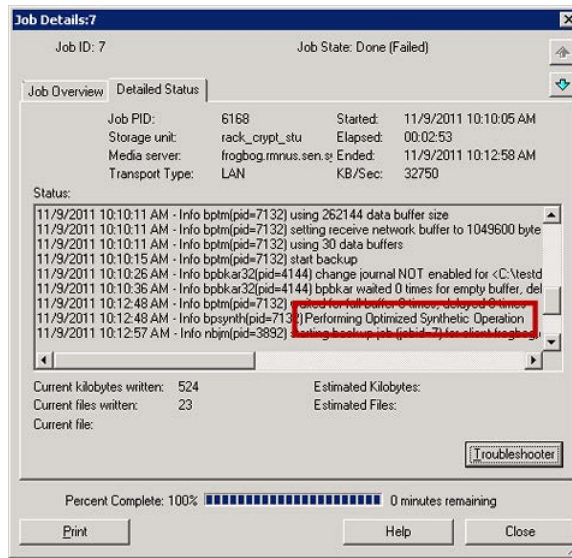
Figure 2-12 Enable Optimized Synthetic backups



Determining if a backup was an Optimized Synthetic backup

- 1 In the NetBackup Administration Console, select **Activity Monitor**. Double click the backup that you want to check.
- 2 Click the **Detailed Status** tab.
- 3 Review the status for **Performing Optimized Synthetic Operation**. This text indicates the backup was an Optimized Synthetic backup.

Figure 2-13 Confirm backup was Optimized Synthetic



Creating a backup policy

The easiest method to set up a backup policy is to use the **Policy Configuration Wizard**. This wizard guides you through the setup process by automatically choosing the best values for most configurations.

Not all policy configuration options are presented through the wizard. For example, calendar-based scheduling and the **Data Classification** setting. After the policy is created, modify the policy in the **Policies** utility to configure the options that are not part of the wizard.

Note: Do not use the Policy Configuration Wizard to configure policies for Replication Director.

Using the Policy Configuration Wizard to create a backup policy

Use the following procedure to create a backup policy with the Policy Configuration Wizard.

To create a backup policy with the Policy Configuration Wizard

- 1 In the **NetBackup Administration Console**, in the left pane, click **NetBackup Management**.
- 2 In the right pane, click **Create a Policy** to begin the **Policy Configuration Wizard**.
- 3 Select **File systems, databases, applications**.
- 4 Click **Next** to start the wizard and follow the prompts.

Click **Help** on any wizard panel for assistance while running the wizard.

Creating a backup policy without using the Policy Configuration Wizard

Use the following procedure to create a backup policy in the **NetBackup Administration Console** without using the Policy Configuration Wizard.

To create a policy without the Policy Configuration Wizard

- 1 In the **NetBackup Administration Console**, in the left pane, expand **NetBackup Management > Policies**.
- 2 On the **Actions** menu, click **New > Policy**.
- 3 Type a unique name for the new policy in the **Add a New Policy** dialog box.
- 4 If necessary, clear the **Use Policy Configuration Wizard** check box.
- 5 Click **OK**.
- 6 Configure the attributes, the schedules, the clients, and the backup selections for the new policy.

Changing cloud storage disk pool properties

You can change some of the properties of a disk pool.

To change disk pool properties

- 1 In the **NetBackup Administration Console**, expand **Media and Device Management > Devices > Disk Pools**.
- 2 Select the disk pool that you want to change in the details pane.

- 3 On the **Edit** menu, select **Change**.

Change Disk Pool

Name: dp-backups-aws-silver

Storage servers: (amazon_crypt) amazon.com

Volume Name	Available Space	Raw Size	Replication
volume-3-backups	8192.0 PB	8192.0 PB	None

Total raw size: 8192.00 PB
 Total available space: 8192.00 PB
 Targeted replication: ---

Comments:

Disk Volume Settings
 High water mark: 98 %
 Low water mark: 80 %

Maximum I/O Streams
 Concurrent read and write jobs affect disk performance.
 Limit I/O streams to prevent disk overload.
 Limit I/O streams: 2 per volume

OK Cancel Help

- 4 Change the properties as necessary.
 See [“Cloud storage disk pool properties”](#) on page 101.
- 5 Click **OK**.

Cloud storage disk pool properties

The properties of an disk pool may vary depending on the purpose the disk pool. The following table describes the possible properties:

Table 2-31 Cloud storage disk pool properties

Property	Description
Name	The disk pool name.
Storage server	The storage server name.
Disk volumes	The disk volume that comprises the disk pool.
Total size	The total amount of space available in the disk pool.
Total raw size	The total raw, unformatted size of the storage in the disk pool. The storage host may or may not expose the raw size of the storage.
Comment	A comment that is associated with the disk pool.
High water mark	<p>The High water mark setting is a threshold that triggers the following actions:</p> <ul style="list-style-type: none"> ■ When an individual volume in the disk pool reaches the High water mark, NetBackup considers the volume full. NetBackup chooses a different volume in the disk pool to write backup images to. ■ When all volumes in the disk pool reach the High water mark, the disk pool is considered full. NetBackup fails any backup jobs that are assigned to a storage unit in which the disk pool is full. NetBackup also does not assign new jobs to a storage unit in which the disk pool is full. ■ NetBackup begins image cleanup when a volume reaches the High water mark; image cleanup expires the images that are no longer valid. For a disk pool that is full, NetBackup again assigns jobs to the storage unit when image cleanup reduces any disk volume's capacity to less than the High water mark. <p>The default is 98%.</p>
Low water mark	<p>The Low water mark is a threshold at which NetBackup stops image cleanup.</p> <p>The Low water mark setting cannot be greater than or equal to the High water mark setting.</p> <p>The default is 80%.</p>

Table 2-31 Cloud storage disk pool properties (*continued*)

Property	Description
Limit I/O streams	<p>Select to limit the number of read and write streams (that is, jobs) for each volume in the disk pool. A job may read backup images or write backup images. By default, there is no limit.</p> <p>When the limit is reached, NetBackup chooses another volume for write operations, if available. If not available, NetBackup queues jobs until a volume is available.</p> <p>Too many streams may degrade performance because of disk thrashing. Disk thrashing is excessive swapping of data between RAM and a hard disk drive. Fewer streams can improve throughput, which may increase the number of jobs that complete in a specific time period.</p> <p>A starting point is to divide the Maximum concurrent jobs of all of the storage units by the number of volumes in the disk pool.</p>
per volume	<p>Select or enter the number of read and write streams to allow per volume.</p> <p>Many factors affect the optimal number of streams. Factors include but are not limited to disk speed, CPU speed, and the amount of memory.</p> <p>For the disk pools that are configured for Snapshot and that have a Replication source property:</p> <ul style="list-style-type: none"> ■ Always use increments of 2 when you change this setting. A single replication job uses two I/O streams. ■ If more replication jobs exist than streams are available, NetBackup queues the jobs until streams are available. ■ Batching can cause many replications to occur within a single NetBackup job. Another setting affects snapshot replication job batching.

Monitoring and Reporting

This chapter includes the following topics:

- [About monitoring and reporting for cloud backups](#)
- [Viewing cloud storage job details](#)
- [Viewing NetBackup cloud storage disk reports](#)
- [Displaying KMS key information for cloud storage encryption](#)

About monitoring and reporting for cloud backups

Symantec provides several methods to monitor and report NetBackup cloud storage and cloud storage activity, as follows:

NetBackup OpsCenter The NetBackup OpsCenter provides the most detailed reports of NetBackup cloud storage activity. See the *NetBackup OpsCenter Administrator's Guide* for details on cloud monitoring and reporting:

<http://www.symantec.com/docs/DOC5332>

If OpsCenter cannot connect to the CloudStore Service Container, it cannot obtain the necessary data for reporting. Therefore, ensure that the CloudStore Service Container is active on the NetBackup media servers that you use for cloud storage.

See "[Connection to the NetBackup CloudStore Service Container fails](#)" on page 121.

The NetBackup Administration Console **Disk Pools** window

The **Disk Pools** window displays the values that were stored when NetBackup polled the disk pools. NetBackup polls the disk pools every five minutes.

To display the window, in the **NetBackup Administration Console**, in the left pane, select **Media and Device Management > Devices > Disk Pools**.

Note: The information that is displayed for **Used Capacity** and **Available Space** is inaccurate in the **NetBackup Administration Console**. Even if there is data in the disk pool, the value that is displayed for **Used Capacity** is zero. The value for **Available Space** displays the maximum amount. You must review the information on the provider website for accurate use information.

NetBackup disk reports See "[Viewing NetBackup cloud storage disk reports](#)" on page 105.

Viewing cloud storage job details

Use the NetBackup Activity Monitor to view job details.

To view cloud storage job details

- 1 In the **NetBackup Administration Console**, click **Activity Monitor**.
- 2 Click the **Jobs** tab.
- 3 To view the details for a specific job, double-click on the job that is displayed in the **Jobs** tab pane.
- 4 In the **Job Details** dialog box, click the **Detailed Status** tab.

Viewing NetBackup cloud storage disk reports

The NetBackup disk reports include information about the disk pools, disk storage units, disk logs, and images that are stored on disk media.

[Table 3-1](#) describes the disk reports available.

Table 3-1 Disk reports

Report	Description
Images on Disk	<p>The Images on Disk report generates the image list present on the disk storage units that are connected to the media server. The report is a subset of the Images on Media report; it shows only disk-specific columns.</p> <p>The report provides a summary of the storage unit contents. If a disk becomes bad or if a media server crashes, this report can let you know what data is lost.</p>
Disk Logs	<p>The Disk Logs report displays the media errors or the informational messages that are recorded in the NetBackup error catalog. The report is a subset of the Media Logs report; it shows only disk-specific columns.</p>
Disk Storage Unit Status	<p>The Disk Storage Unit Status report displays the state of disk storage units in the current NetBackup configuration.</p> <p>Multiple storage units can point to the same disk pool. When the report query is by storage unit, the report counts the capacity of disk pool storage multiple times.</p>
Disk Pool Status	<p>The Disk Pool Status report displays the state of disk pool storage units. This report displays only when a Data Protection Optimization Option license is installed.</p>

See [“About monitoring and reporting for cloud backups”](#) on page 104.

To view disk reports

- 1 In the **NetBackup Administration Console**, in the left pane, expand **NetBackup Management > Reports > Disk Reports**.
- 2 Select the name of a disk report.
- 3 In the right pane, select the report settings.
- 4 Click **Run Report**.

Displaying KMS key information for cloud storage encryption

You can use the `nbkmsutil` command to list the following information about the key groups and the key records:

Key groups See [To display KMS key group information](#).

Keys See [To display KMS key information](#).

Note: Symantec recommends that you keep a record key information. The key tag that is listed in the output is necessary if you need to recover keys.

To display KMS key group information

- ◆ To list all of the key groups, use the `nbkmsutil` with the `-listkgs` option. The following is the command format:

UNIX: `/usr/opensv/netbackup/bin/admincmd/nbkmsutil -listkgs`

Windows: `install_path\Veritas\NetBackup\bin\admincmd\nbkmsutil -listkgs`

The following is example output on UNIX hosted storage. On Windows, the volume name is not used.

```
nbkmsutil -listkgs
```

```
Key Group Name      : CloudStorageVendor.com:symc_volume_for_backups
Supported Cypher    : AES_256
Number of Keys      : 1
Has Active Key      : Yes
Creation Time       : Tues Jan 01 01:00:00 2013
Last Modification Time: Tues Jan 01 01:00:00 2013
Description         : -
```

To display KMS key information

- ◆ To list all of the keys that belong to a key group name, use the `nbkmsutil` with the `-listkgs` and `-kgname` options. The following is the command format:

UNIX: `/usr/openv/netbackup/bin/admincmd/nbkmsutil -listkeys -kgname AdvDiskServer1.example.com:AdvDisk_Volume`

Windows: `install_path\Veritas\NetBackup\bin\admincmd\nbkmsutil -listkeys -kgname AdvDiskServer1.example.com:`

The following is example output on UNIX hosted storage. On Windows, the volume name is not used.

```
nbkmsutil -listkeys -kgname CloudStorageVendor.com:symc_volume_for_backup
```

```
Key Group Name      : CloudStorageVendor.com:symc_volume_for_backups
Supported Cypher    : AES_256
Number of Keys      : 1
Has Active Key      : Yes
Creation Time       : Tues Jan 01 01:00:00 2013
Last Modification Time: Tues Jan 01 01:00:00 2013
Description         : -
```

```
Key Tag            : 532cf41cc8b3513a13c1c26b5128731e5ca0b9b01e0689cc38ac2b7596bbae3c
Key Name           : Encrypt_Key_April
Current State      : Active
Creation Time      : Tues Jan 01 01:02:00 2013
Last Modification Time: Tues Jan 01 01:02:00 2013
Description        : -
```

Operational notes

This chapter includes the following topics:

- [NetBackup bpstsinfo command operational notes](#)
- [Unable to configure additional media servers](#)
- [Cloud configuration may fail if NetBackup Access Control is enabled](#)
- [Deleting cloud storage server artifacts](#)

NetBackup bpstsinfo command operational notes

The following table describes operational notes for the `bpstsinfo` command with NetBackup cloud storage.

Table 4-1 `bpstsinfo` command operational notes

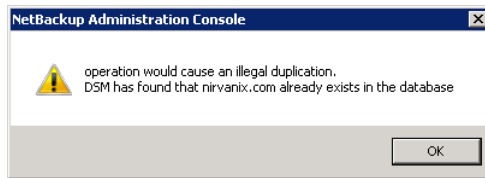
Note	Description
Use either the <code>-stype</code> option or the <code>-storageserverprefix</code>	Use either the <code>-stype</code> option or the <code>-storageserverprefix</code> option to constrain the <code>bpstsinfo</code> command to list storage server information. If you do not, the command searches all providers, which may be time consuming and may result in a timeout.
Specify the correct <code>-stype</code>	The plug-in that requests the information affects the information that is returned. Therefore, use the correct <code>-stype</code> with the <code>bpstsinfo</code> command. To determine the <code>-stype</code> , use the following command: <pre>nbdevquery -liststs -storage_server fq_host_name</pre> <p>If the storage is encrypted, the <code>-stype</code> includes an <code>_crypt</code> suffix.</p>

Table 4-1 `bpstsinfo` command operational notes (continued)

Note	Description
Encrypted and non-encrypted storage units are displayed in <code>bpstsinfo</code> command output	<p>When you use the <code>bpstsinfo</code> command to display the encrypted logical storage unit (LSU) information, the output shows both encrypted and non-encrypted LSUs if both types exist. That output is the expected result. The <code>bpstsinfo</code> command operates on the level of the storage plug-in, which is not aware of any higher-level detail, such as encryption.</p> <p>The following is an example of a command that specifies encrypted storage:</p> <pre>bpstsinfo -lsuinfo -storage_server amazon.com -stype amazon_crypt</pre>

Unable to configure additional media servers

If you attempt to run the **Cloud Storage Server Configuration Wizard** on a second media server that uses the same master server as the first media server, the operation fails. An `illegal duplication` error similar to the following appears:



Your only options in the wizard are to click **Cancel** or **Back**. If you click **Back**, there are no configuration changes that allow the wizard to continue.

You must use the correct procedure if you want multiple media servers in your cloud environment. More information is available in a different topic.

See [“Adding backup media servers to your cloud environment”](#) on page 90.

Cloud configuration may fail if NetBackup Access Control is enabled

If you attempt to configure a cloud storage server in an environment that uses NetBackup Access Control, you may receive an error message similar to the following:

```
Error creating Key Group and Keys cannot connect on socket
```

NetBackup generates this error message because the user does not have sufficient rights within NetBackup Access Control. The user account that configures the cloud storage server must be a member of the NBU_KMS Admin Group.

See the *NetBackup Security and Encryption Guide* for more information about NetBackup Access Control and account setup:

<http://www.symantec.com/docs/DOC5332>

Deleting cloud storage server artifacts

If you incorrectly remove a storage server, configuration files are left orphaned on the computer. Attempts to create a new storage server fail with an error message that indicates a logon failure. Use the following procedure to correctly delete a storage server:

Deleting a storage server

- 1 Expire all images on the storage server.
- 2 Delete the storage unit.
- 3 Delete the disk pool.
- 4 Delete the storage server.
- 5 Delete all of the `.conf` and `.pref` files from `lib/ost-plugins` or `bin/ost-plugins` directory.

Troubleshooting

This chapter includes the following topics:

- [About unified logging](#)
- [About legacy logging](#)
- [NetBackup cloud storage log files](#)
- [Enable libcurl logging](#)
- [NetBackup Administration Console fails to open](#)
- [Troubleshooting cloud storage configuration issues](#)
- [Troubleshooting cloud storage operational issues](#)

About unified logging

Unified logging and legacy logging are the two forms of debug logging used in NetBackup. Unified logging creates log file names and messages in a standardized format. All NetBackup processes use either unified logging or legacy logging.

Unlike the files that are written in legacy logging, unified logging files cannot be easily viewed with a text editor. The unified logging files are in binary format, and some of the information is contained in an associated resource file. Only the `vxlogview` command can assemble and display the log information correctly.

See [“About legacy logging”](#) on page 115.

Server processes and client processes use unified logging.

Unlike legacy logging, unified logging does not require that you create logging subdirectories. Log files for originator IDs are written to a subdirectory with the name specified in the log configuration file. All unified logs are written to subdirectories in the following directory:

Windows `install_path\NetBackup\logs`

UNIX `/usr/opensv/logs`

You can access logging controls in the **NetBackup Administration Console**. In the left pane, expand **NetBackup Management > Host Properties > Master Servers** or **Media Servers**. Double-click the server you want to change. In the left pane of the dialog box, click **Logging**.

You can also manage unified logging by using the following commands:

<code>vxlogcfg</code>	Modifies the unified logging configuration settings. for more information about the <code>vxlogcfg</code> command.
<code>vxlogmgr</code>	Manages the log files that the products that support unified logging generate. for more information about the <code>vxlogmgr</code> command.
<code>vxlogview</code>	Displays the logs that unified logging generates. See “Examples of using vxlogview to view unified logs” on page 114. for more information about the <code>vxlogview</code> command.

See the *NetBackup Commands Reference Guide* for a complete description about these commands. The guide is available through the following URL:

<http://www.symantec.com/docs/DOC5332>

These commands are located in the following directory:

Windows `install_path\NetBackup\bin`

UNIX `/usr/opensv/netbackup/bin`

About using the vxlogview command to view unified logs

Use the `vxlogview` command to view the logs that unified logging creates. These logs are stored in the following directory.

UNIX `/usr/opensv/logs`

Windows `install_path\NetBackup\logs`

Unlike the files that are written in legacy logging, unified logging files cannot be easily viewed with a text editor. The unified logging files are in binary format, and

some of the information is contained in an associated resource file. Only the `vxlogview` command can assemble and display the log information correctly.

You can use `vxlogview` to view NetBackup log files as well as PBX log files.

To view PBX logs using the `vxlogview` command, do the following:

- Ensure that you are an authorized user. For UNIX and Linux, you must have root privileges. For Windows, you must have administrator privileges.
- To specify the PBX product ID, enter `-p 50936` as a parameter on the `vxlogview` command line.

`vxlogview` searches all the files, which can be a slow process. Refer to the following topic for an example of how to display results faster by restricting the search to the files of a specific process.

Examples of using vxlogview to view unified logs

The following examples demonstrate how to use the `vxlogview` command to view unified logs.

Table 5-1 Example uses of the `vxlogview` command

Item	Example
Display all the attributes of the log messages	<code>vxlogview -p 51216 -d all</code>
Display specific attributes of the log messages	Display the log messages for NetBackup (51216) that show only the date, time, message type, and message text: <code>vxlogview --prodid 51216 --display D,T,m,x</code>
Display the latest log messages	Display the log messages for originator 116 (<code>nbpem</code>) that were issued during the last 20 minutes. Note that you can specify <code>-o nbpem</code> instead of <code>-o 116</code> : <code># vxlogview -o 116 -t 00:20:00</code>
Display the log messages from a specific time period	Display the log messages for <code>nbpem</code> that were issued during the specified time period: <code># vxlogview -o nbpem -b "05/03/05 06:51:48 AM" -e "05/03/05 06:52:48 AM"</code>

Table 5-1 Example uses of the vxlogview command (*continued*)

Item	Example
Display results faster	<p>You can use the <code>-i</code> option to specify an originator for a process:</p> <pre># vxlogview -i nbpem</pre> <p>The <code>vxlogview -i</code> option searches only the log files that the specified process (<code>nbpem</code>) creates. By limiting the log files that it has to search, <code>vxlogview</code> returns a result faster. By comparison, the <code>vxlogview -o</code> option searches all unified log files for the messages that the specified process has logged.</p> <p>Note: If you use the <code>-i</code> option with a process that is not a service, <code>vxlogview</code> returns the message "No log files found." A process that is not a service has no originator ID in the file name. In this case, use the <code>-o</code> option instead of the <code>-i</code> option.</p> <p>The <code>-i</code> option displays entries for all OIDs that are part of that process including libraries (137, 156, 309, etc.).</p>
Search for a job ID	<p>You can search the logs for a particular job ID:</p> <pre># vxlogview -i nbpem grep "jobid=job_ID"</pre> <p>The <code>jobid=</code> search key should contain no spaces and must be lowercase.</p> <p>When searching for a job ID, you can use any <code>vxlogview</code> command option. This example uses the <code>-i</code> option with the name of the process (<code>nbpem</code>). The command returns only the log entries that contain the job ID. It misses related entries for the job that do not explicitly contain the <code>jobid=job_ID</code>.</p>

See the *NetBackup Commands Reference Guide* for a complete description of the `vxlogview` command. The guide is available through the following URL:

<http://www.symantec.com/docs/DOC5332>

About legacy logging

Legacy logging and unified logging are the two forms of debug logging used in NetBackup. All NetBackup processes use either unified logging or legacy logging.

See “[About unified logging](#)” on page 112.

In legacy debug logging, each process creates log files of debug activity in its own logging directory. Each log file grows to a certain size before the NetBackup process

closes it and creates a new log file.

The NetBackup legacy debug log directories are located in the following directories:

Windows	<code>install_path\NetBackup\logs</code> <code>install_path\Volmgr\debug</code>
UNIX	<code>/usr/opensv/netbackup/logs</code> <code>/usr/opensv/volmgr/debug</code>

These top-level directories can contain a directory for each NetBackup process that uses legacy logging. By default, NetBackup creates only a subset of all of the possible log directories (the `bpbrm`, `bpcd`, `bpdm`, and `bptm` directories). To enable logging for all NetBackup processes that use legacy logging, you must create the log file directories that do not exist already.

You can use the following batch files to create all of the debug log directories at once:

- Windows: `install_path\NetBackup\Logs\mklogdir.bat`
- UNIX: `usr/opensv/netbackup/logs/mklogdir`

See the *NetBackup Commands Reference Guide* for a complete description about the `mklogdir` command. The guide is available at the following location:

<http://www.symantec.com/docs/DOC5332>

After the directories are created, NetBackup creates log files in the directory that is associated with each process. A debug log file is created when the process begins.

To enable debug logging for the NetBackup Status Collection Daemon (`vmgcd`), create the following directory before you start `nbemm`.

Windows	<code>install_path\Volmgr\debug\vmgcd\</code>
UNIX	<code>/usr/opensv/volmgr/debug/vmgcd</code>

As an alternative, you can restart `vmgcd` after creating the directory.

Creating NetBackup log file directories

Before you configure your NetBackup feature, create the directories into which the NetBackup commands write log files. Create the directories on the master server

and on each media server that you use for your feature. The log files reside in the following directories:

- UNIX: `/usr/opensv/netbackup/logs/`
- Windows: `install_path\NetBackup\logs\`

More information about NetBackup logging is available in the *NetBackup Troubleshooting Guide*, available through the following URL:

<http://www.symantec.com/docs/DOC5332>

To create log directories for NetBackup commands

- ◆ Depending on the operating system, run one of the following scripts:

UNIX: `/usr/opensv/netbackup/logs/mklogdir`

Windows: `install_path\NetBackup\logs\mklogdir.bat`

To create the `tpconfig` command log directory

- ◆ Depending on the operating system, create the `debug` directory and the `tpcommand` directory (by default, the `debug` directory and the `tpcommand` directory do not exist). The pathnames of the directories are as follows:

UNIX: `/usr/opensv/volmgr/debug/tpcommand`

Windows: `install_path\Veritas\Volmgr\debug\tpcommand`

NetBackup cloud storage log files

NetBackup cloud storage exists within the Symantec OpenStorage framework. Therefore, the log files for cloud activity are the same as for OpenStorage with several additions.

Some NetBackup commands or processes write messages to their own log files. For those commands and processes, the log directories must exist so that the utility can write log messages.

See “[Creating NetBackup log file directories](#)” on page 116.

Other processes use Veritas unified log (VxUL) files. Each process has a corresponding VxUL originator ID. VxUL uses a standardized name and file format for log files. To view VxUL log files, you must use the NetBackup `vxlogview` command.

More information about how to view and manage VxUL log files is available. See the *NetBackup Logging Reference Guide*:

<http://www.symantec.com/docs/DOC5332>

The following are the component identifiers for log messages:

- An `sts_` prefix relates to the interaction with the plug-in that writes to and reads from the storage.
- A cloud storage server prefix relates to interaction with that cloud vendor's storage network.
- An `encrypt` prefix relates to interaction with the encryption plug-in.
- A `KMSCLIB` prefix relates to interaction with the NetBackup Key Management Service.

Most interaction occurs on the NetBackup media servers. Therefore, the log files on the media servers that you use for disk operations are of most interest.

Warning: The higher the log level, the greater the affect on NetBackup performance. Use a log level of 5 (the highest) only when directed to do so by a Symantec representative. A log level of 5 is for troubleshooting only.

Specify the NetBackup log levels in the **Logging** host properties on the NetBackup master server. The log levels for some processes specific to certain options are set in configuration files as described in [Table 5-2](#).

[Table 5-2](#) describes the logs.

Table 5-2 NetBackup logs

Activity	OID	Processes
Backups and restores	N/A	<p>Messages appear in the log files for the following processes:</p> <ul style="list-style-type: none"> ■ The <code>bpbrm</code> backup and restore manager. ■ The <code>bpdbm</code> database manager. ■ The <code>bpdm</code> disk manager. ■ The <code>bptm</code> tape manager for I/O operations. <p>The log files reside in the following directories:</p> <ul style="list-style-type: none"> ■ UNIX: <code>/usr/opensv/netbackup/logs/</code> ■ Windows: <code>install_path\NetBackup\logs\</code>
Backups and restores	117	The <code>nbjm</code> Job Manager.

Table 5-2 NetBackup logs (*continued*)

Activity	OID	Processes
Image cleanup, verification, import, and duplication	N/A	The <code>bpdbm</code> database manager log files. The log files reside in the following directories: <ul style="list-style-type: none"> ■ UNIX: <code>/usr/opensv/netbackup/logs/bpdbm</code> ■ Windows: <code>install_path\NetBackup\logs\bpdbm</code>
Cloud connection operations	N/A	The <code>bpstsinfo</code> utility writes information about connections to the cloud storage server in its log files.
Cloud account configuration	222	The Remote Manager and Monitor Service is the process that creates the cloud storage accounts. RMMS runs on media servers.
Cloud Storage Service Container	N/A	The NetBackup Cloud Storage Service Container (<code>nbcssc</code>) writes log files to the following directories: <ul style="list-style-type: none"> ■ For Windows: <code>install_path\Veritas\NetBackup\logs\nbcssc</code> ■ For UNIX/Linux: <code>/usr/opensv/netbackup/logs/nbcssc</code>
Credentials configuration	N/A	The <code>tpconfig</code> utility. The <code>tpconfig</code> command writes log files to the <code>tpcommand</code> directory.
Device configuration	111	The <code>nbemm</code> process.
Device configuration	178	The Disk Service Manager process that runs in the Enterprise Media Manager (EMM) process.
Device configuration	202	The Storage Server Interface process that runs in the Remote Manager and Monitor Service. RMMS runs on media servers.
Device configuration	230	The Remote Disk Service Manager interface (RDSM) that runs in the Remote Manager and Monitor Service. RMMS runs on media servers.

Enable libcurl logging

Set the storage server property `CLOUD_PREFIX:LOG_CURL` to `YES` to enable cURL logging. The `CLOUD_PREFIX` value is the prefix value of each storage provider. The possible values are:

- AMZ for Amazon
- ATT for AT&T
- AMZGOV for Amazon GovCloud

- CLD for Clouidian HyperStore
- GOOG for Google Nearline
- HT for Hitachi
- RACKS for Rackspace
- VER Verizon

To example, to enable `LOG_CURL` for AT&T set `ATT:LOG_CURL` to `YES`.

See [“Changing cloud storage server properties”](#) on page 66.

NetBackup Administration Console fails to open

If you change the default port of the NetBackup CloudStore Service Container, the **NetBackup Administration Console** may not open. You must change the value in two places.

The CloudStore Service Container configuration file

The CloudStore Service Container configuration file resides in the following directories:

- UNIX: `/usr/opensv/java/cloudstorejava.conf`
- Windows:
`install_path\Veritas\NetBackup\bin\cloudstorewin.conf`

The following is an example that shows the default value:

```
[NBCSSC]
NBCSSC_PORT=5637
```

The operating system's `services` file

The `services` file is in the following locations:

- Windows:
`C:\WINDOWS\system32\drivers\etc\services`
- Linux: `/etc/services`

If you change the value in the CloudStore Service Container configuration file also change the value in the `services` file.

By default, the NetBackup CloudStore Server Container port is 5637.

See [“Connection to the NetBackup CloudStore Service Container fails”](#) on page 121.

Troubleshooting cloud storage configuration issues

The following sections may help you troubleshoot configuration issues.

- See [“NetBackup Scalable Storage host properties unavailable”](#) on page 121.
- See [“Connection to the NetBackup CloudStore Service Container fails”](#) on page 121.
- See [“Cannot create a cloud storage disk pool”](#) on page 122.
- See [“NetBackup Administration Console fails to open”](#) on page 120.
- See [“Data transfer to cloud storage server may fail in the SSL mode”](#) on page 122.
- See [“Amazon GovCloud cloud storage configuration fails in non-SSL mode”](#) on page 122.

NetBackup Scalable Storage host properties unavailable

If the NetBackup CloudStore Service Container is not active, the **Scalable Storage** host properties are unavailable. Either of the following two symptoms may occur:

- The **Scalable Storage** properties for a media server are unavailable
- A pop-up box may appear that displays an **“Unable to fetch Scalable Storage settings”** message.

You should determine why the NetBackup CloudStore Service Container is inactive, resolve the problem, and then start the Service Container.

See [“NetBackup CloudStore Service Container startup and shutdown troubleshooting”](#) on page 126.

See [“Stopping and starting the NetBackup CloudStore Service Container”](#) on page 125.

Connection to the NetBackup CloudStore Service Container fails

The NetBackup cloud storage `csconfig` configuration command makes three attempts to connect to the NetBackup CloudStore Service Container with a 60-second timeout for each connection attempt. The NetBackup OpsCenter also connects to the CloudStore Service Container to obtain data for reporting.

If they cannot establish a connection, verify the following information:

- That the NetBackup CloudStore Service Container is active.
 See [“NetBackup CloudStore Service Container startup and shutdown troubleshooting”](#) on page 126.
- Your firewall settings are appropriate.

See [“Stopping and starting the NetBackup CloudStore Service Container”](#) on page 125.

Cannot create a cloud storage disk pool

The following table describes potential solutions if you cannot create a disk pool in NetBackup.

Table 5-3 Cannot create disk pool solutions

Error	Description
<p>The wizard is not able to obtain Storage Server information. Cannot connect on socket. (25)</p>	<p>The error message appears in the Disk Configuration Wizard.</p> <p>The Disk Configuration Wizard query to the cloud vendor host timed-out. The network may be slow or a large number of objects (for example, buckets on Amazon S3) may exist.</p> <p>To resolve the issue, use the NetBackup <code>nbdevconfig</code> command to configure the disk pool. Unlike the wizard, the <code>nbdevconfig</code> command does not monitor the command response times.</p> <p>See the <i>NetBackup Commands Reference Guide</i> for a complete description of the commands. The guide is available at the following location: http://www.symantec.com/docs/DOC5332</p>

Data transfer to cloud storage server may fail in the SSL mode

NetBackup supports only Certificate Authority (CA)-signed certificates while it communicates with cloud storage in the SSL mode. Ensure that the cloud server (public or private) has CA-signed certificate. If it does not have the CA-signed certificate, data transfer between NetBackup and cloud provider may fail in the SSL mode.

Amazon GovCloud cloud storage configuration fails in non-SSL mode

The FIPS region of Amazon GovCloud cloud provider (that is `s3-fips-us-gov-west-1.amazonaws.com`) supports only secured mode of communication. Therefore, if you disable the **Use SSL** option while you configure Amazon GovCloud cloud storage with the FIPS region, the configuration fails.

To enable the SSL mode again, run the `csconfig` command with `-us` parameter to set the value of SSL to '2'.

See the *NetBackup Commands Reference Guide* for a complete description about the commands. The guide is available at the following location:

<http://www.symantec.com/docs/DOC5332>

Troubleshooting cloud storage operational issues

The following sections may help you troubleshoot operational issues.

See [“NetBackup Scalable Storage host properties unavailable”](#) on page 121.

See [“Cloud storage backups fail”](#) on page 123.

See [“A restart of the nbcssc process reverts all cloudstore.conf settings”](#) on page 126.

See [“NetBackup CloudStore Service Container startup and shutdown troubleshooting”](#) on page 126.

See [“NetBackup Administration Console fails to open”](#) on page 120.

Cloud storage backups fail

See the following topics:

- [Accelerator backups fail](#)
- [Backups fail after the WRITE_BUFFER_SIZE is increased](#)
- [The storage volume was created by the cloud vendor interface](#)
- [AIX media server backs up large files](#)
- [The NetBackup CloudStore Service Container is not active](#)

Accelerator backups fail

A message similar to the following is in the job details:

```
Critical bptm(pid=28291) accelerator verification failed: backupid=
  host_name_1373526632, offset=3584, length=141976576, error=
  2060022, error message: software error
Critical bptm(pid=28291) image write failed: error 2060022: software
  error
Error bptm(pid=28291) cannot write image to disk, Invalid argument end
  writing; write time: 0:02:31
Info bptm(pid=28291) EXITING with status 84
Info bpbkar(pid=6044) done. status: 84: media write error media write
  error(84)
```

This error may occur in the environments that have more than one cloud storage server. It indicates that NetBackup Accelerator backups of a client to one cloud storage server were later directed to a different cloud storage server.

For Accelerator backups to cloud storage, ensure the following:

- Always back up each client to the same storage server. Do so even if the other storage server represents storage from the same cloud storage vendor.
- Always use the same backup policy to back up a client, and do not change the storage destination of that policy.

Backups fail after the `WRITE_BUFFER_SIZE` is increased

If the cloud storage server `WRITE_BUFFER_SIZE` property exceeds the total swap space of the computer, backups can fail with a status 84.

Adjust the `WRITE_BUFFER_SIZE` size to a value lower than the computer's total swap space to resolve this issue.

The storage volume was created by the cloud vendor interface

A message similar to the following is in the job details:

```
Info bptm(pid=xxx) start backup
Critical bptm(pid=xxxx) image open failed: error 2060029: authorization
failure
Error bpbrm(pid=xxxx) from client gabby: ERR - Cannot write to STDOUT. E
rrno = 32: Broken pipe
Info bptm(pid=xxxx) EXITING with status 84
```

A message similar to the following appears in the `bptm` log file:

```
Container container_name is not Symantec container or tag data error,
fail to create image. Please make sure that the LSU is created by
means of NBU.
```

This error indicates that the volume was created by using the cloud storage vendor's interface.

You must use the **NetBackup Disk Pool Configuration Wizard** to create the volume on the cloud storage. The wizard applies a required partner ID to the volume. If you use the vendor interface to create the container, the partner ID is not applied.

To resolve the problem, use the cloud storage vendor's interface to delete the container. In NetBackup, delete the disk pool and then recreate it by using the **Disk Pool Configuration Wizard**.

See [“Viewing cloud storage job details”](#) on page 105.

See [“NetBackup cloud storage log files”](#) on page 117.

AIX media server backs up large files

When an AIX media server backs up large files, you may encounter memory issues. These memory issues can result in failed backups. The backups fail with a NetBackup status code 84 (media write error) or a NetBackup status code 87 (media

close error). Change the AIX `ulimit` size to unlimited to resolve this issue. Be sure to stop and restart the NetBackup services or daemons after you change the `ulimit` value.

The following are examples:

```
ulimit -m unlimited
```

```
ulimit -d unlimited
```

```
ulimit -s unlimited
```

The NetBackup CloudStore Service Container is not active

If the NetBackup CloudStore Service Container is not active, backups cannot be sent to the cloud storage.

NetBackup does not validate that the CloudStore Service Container is active when you use NetBackup commands to configure NetBackup cloud storage. Therefore, any backups that initiate in such a scenario fail.

See [“NetBackup CloudStore Service Container startup and shutdown troubleshooting”](#) on page 126.

Stopping and starting the NetBackup CloudStore Service Container

Use the **NetBackup Administration Console** to stop and start the NetBackup CloudStore Service Container (`nbcssc`) service.

See [“About the NetBackup CloudStore Service Container”](#) on page 34.

See [“NetBackup CloudStore Service Container startup and shutdown troubleshooting”](#) on page 126.

To start or stop the CloudStore Service Container

- 1 In the **NetBackup Administration Console**, expand **NetBackup Administration > Activity Monitor**.
- 2 Click the **Daemons** tab (UNIX) or the **Services** tab (Windows).
- 3 In the **Details** pane, select `nbcssc` (UNIX and Linux) or **NetBackup CloudStore Service Container** (Windows).
- 4 On the **Actions** menu, select **Stop Selected** or **Start Selected** (Windows) or **Stop Daemon** or **Start Daemon** (UNIX).

A restart of the nbcssc process reverts all cloudstore.conf settings

Missing entries and comments are not allowed in the `cloudstore.conf` file. If you remove or comment out values in the `cloudstore.conf` file, a restart of the `nbcssc` process returns all settings to their default values.

NetBackup CloudStore Service Container startup and shutdown troubleshooting

See the following topics:

- [Security certificate not provisioned](#)
- [Security mode changed while service is active](#)

Security certificate not provisioned

The NetBackup media servers that you use for cloud storage must have a security certificate provisioned. If not, the CloudStore Service Container cannot start. Verify that the certificate exists.

See [“NetBackup CloudStore Service Container security certificates”](#) on page 35.

NetBackup 7.7 and later If a certificate does not exist, create one from the NetBackup master server.

See [“Generating a security certificate for a media server”](#) on page 38.

NetBackup releases earlier than 7.7 If the certificate becomes corrupt or expires, delete the old certificate and restart the services to regenerate a new certificate.

Security mode changed while service is active

Do not change the security mode of the NetBackup CloudStore Service Container while the service is active. If the security mode is changed while the service is active, you may encounter service startup or service shutdown problems. Be sure to stop the service in the same mode it was started.

See [“NetBackup CloudStore Service Container security modes”](#) on page 36.

See [“Stopping and starting the NetBackup CloudStore Service Container”](#) on page 125.

Index

A

- Amazon GovCloud (US)
 - requirements 19
- Amazon S3-compatible cloud providers
 - NetBackup support 9
- Amazon Simple Storage Service (S3)
 - requirements 18

B

- backups fail
 - Accelerator backups fail 123
 - after the WRITE_BUFFER_SIZE is increased 124
 - AIX media server backs up large files 124
 - storage volume was created by the cloud vendor interface 124
 - The NetBackup CloudStore Service Container is not active 125
- bandwidth
 - throttling 73
- bpstsinfo command
 - operational notes 109

C

- cloud
 - storage unit properties 92
- cloud disk pool
 - changing properties 100
- Cloud Settings tab 29
- cloud storage
 - configuring 15
 - cloud storage Amazon GovCloud 19
 - cloud storage Cloudian HyperStore 22
 - cloud storage Google Nearline 23
- cloud storage provider
 - Amazon 18
 - Hitachi 24
- cloud storage server
 - about 41
 - bandwidth properties 73

- cloud storage server *(continued)*
 - changing properties 66
 - connection properties 68
 - encryption properties 76
 - properties 67
- cloud storage Verizon 27
- Cloudian HyperStore
 - requirements 22
- CloudStore Service Container
 - about 34
 - security certificate for 35
 - security mode changed while service is active 126
 - security modes 36
 - startup and shutdown troubleshooting 126
- cloudstore.conf configuration file 36
- Configuration
 - Accelerator 96
- configuration
 - disk pool configuration wizard 78
 - optimized synthetic backups for cloud storage 97
- configuring a deduplication storage unit 91
- configuring cloud storage 15

D

- Deduplication storage unit
 - Only use the following media servers 93
 - Use any available media server 93
- disk pool
 - changing the state 86
- Disk type 93

E

- encryption
 - properties 76
 - see also 39

F

- Features and functionality 10

FlashBackup policy
 Maximum fragment size (storage unit setting) 94

G

Google Nearline
 requirements 23

H

Hitachi Cloud Services
 requirements 24

J

job ID search in unified logs 115

L

legacy logging 115
 directories 116
 locations 116
 logging
 see legacy logging 115

M

Maximum concurrent jobs 93
 Maximum fragment size 94
 Media Server Deduplication Pool
 changing the state 86
 mklogdir.bat 116
 Monitoring 104

N

NetBackup Accelerator
 about 95
 NetBackup CloudStore Service Container. *See*
 CloudStore Service Container
 NetBackup Scalable Storage 31–32
 NetBackup Scalable Storage host properties
 unavailable 121

O

Optimized Synthetic backups
 about 95

P

policies
 changing properties 100
 creating 99

Preferences

common 69
 encryption 77
 throttling 76
 private clouds
 Amazon S3-compatible cloud providers 28
 AT&T 21
 Rackspace 26
 properties
 bandwidth 73
 cloud storage server 67
 connection 68
 encryption 76

R

read buffer size
 about 71
 Replication Director
 Policy Configuration Wizard, unsupported 99
 Reporting 104
 requirements 16

S

Scalable Storage host properties 29, 31–32
 Scalable Storage host properties unavailable 121
 Scalable Storage, NetBackup 31–32
 security certificates
 for cloud storage 35
 generating 38
 server
 NetBackup debug logs 116
 Status Collection Daemon 116
 storage provider
 AT&T 20
 Rackspace 25
 storage server. *See* cloud storage server
 changing properties for cloud 66
 storage unit
 configuring for deduplication 91
 properties for cloud 92
 Storage unit name 92
 Storage unit type 93

U

unified logging 112
 format of files 114
 location 112

V

Verizon

 requirements 27

vmscd 116

vmscd directory 116

vxlogview command 113

 with job ID option 115

W

wizards

 Policy Configuration 99

write buffer size

 about 72