Veritas NetBackup™ Cloud Administrator's Guide

UNIX, Windows, Linux

Release 8.1

VERITAS™

Veritas NetBackup™ Cloud Administrator's Guide

Legal Notice

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

The latest documentation is available on the Veritas website:

https://sort.veritas.com/documents

Documentation feedback

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

NB.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 1

About NetBackup cloud storage

This chapter includes the following topics:

Providing feedback on Beta documentation

To provide feedback on this beta documentation, please send us email at the following address:

DL-VTAS-ENG-NBU-Early-Release@veritas.com

New cloud features in NetBackup 8.1

- Support for Amazon Virtual Private Cloud.See “Amazon virtual private cloud support with NetBackup ” on page 36.
- Support is added for the following cloud vendors:
  - CMCC Cloud Storage v5.x(S3).See “Amazon S3 cloud storage vendors certified for NetBackup” on page 18.
  - Openstack Swift Identity v3 Authentication version. See “About OpenStack Swift cloud storage API type” on page 59.

  - IBM Softlayer. See "About OpenStack Swift cloud storage API type" on page 59.
  - FUJITSU Cloud Service K5. See "About OpenStack Swift cloud storage API type" on page 59.
  - Microsoft Azure Government. See "About Microsoft Azure cloud storage API type" on page 52.
- For proxy server type HTTP:
  - Authentication type BASIC and NTLM are supported.
    You need username and password for authentication type BASIC and NTLM.
  - Proxy tunneling is made configurable.
- NetBackup CloudCatalyst harnesses Media Server Deduplication Pool (MSDP) technology to upload deduplicated data to the cloud. By deduplicating the data, customers realize a cost savings both when sending, and then when storing, the data in the cloud.

  CloudCatalyst is offered on the following hosts:
  - A Veritas NetBackup CloudCatalyst appliance.
  - A NetBackup 8.1 media server that is configured as a CloudCatalyst storage server. The media server must be Red Hat Enterprise Linux, 7.3 or later.

  CloudCatalyst configuration is described in the *NetBackup Deduplication Guide*.
- The object size for Amazon (S3) and Amazon GovCloud storage servers has changed. This change affects the valid range for the read and write buffer size for these cloud storage servers.
  You must update the read and write buffer size values for pre-NetBackup 8.1 servers using the NetBackup Administration Console on the master server. Update these settings for each cloud storage server that is associated with a media server.See "About object size for cloud storage" on page 100.
  For procedures on how to update the read or write buffer size, see the *NetBackup Upgrade Guide*.

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 Veritas OpenStorage.

Table 1-1 outlines the features and functionality NetBackup Cloud Storage delivers.

Table 1-1 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.
Compression	NetBackup Cloud Storage Compression compresses the data inline before it is sent to the cloud. The compression feature uses a third-party library called LZO Pro (with compression level 3).
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.
Throttling	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. 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. NetBackup Cloud Storage Throttling lets you configure and control the following: ■ Different bandwidth value for both read and write operations. ■ The 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.

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

Feature	Details
Metering	The NetBackup Cloud Storage metering reports enable you to monitor data transfers within NetBackup Cloud Storage. 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. 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. Metering reports are generated through NetBackup OpsCenter.
Cloud Storage service	The NetBackup CloudStore Service Container (`nbcssc`) process performs the following functions: ■ 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 the throttling plug-in On Windows, it is a standard service installed by NetBackup. On UNIX, it runs as a standard daemon. The NetBackup CloudStore Service Container (nbcssc) uses certificate-based authentication. The authentication method used in previous releases (legacy authentication) is disabled by default. Veritas recommends that you upgrade media servers configured as a cloud storage server to NetBackup 8.1 or later. If you cannot upgrade these servers, use the **Enable insecure communication with 8.0 and earlier hosts** option on the NetBackup master server. The option is available in the **NetBackup Administration Console** on the **Security Management > Global Security Settings > Secure Communication** tab.
Storage providers	Veritas currently supports several cloud storage providers. More information is available about each of these vendors. See “About the cloud storage vendors for NetBackup” on page 15.

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

Feature	Details
OpsCenter Reporting	Monitoring and reporting of the data that is sent to cloud storage is available through new cloud reports in OpsCenter. The cloud reports include: ■ **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 7 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. **Note:** OpsCenter supports monitoring and reporting of the following cloud providers: Amazon S3, AT&T, and Rackspace Among all Amazon S3-compatible cloud providers that NetBackup supports, OpsCenter supports monitoring and reporting of Amazon S3 only. **Note:** Where Amazon is the cloud service provider, OpsCenter cannot report on the data that MSDP cloud storage servers upload to the cloud.

About the catalog backup of cloud configuration files

The following cloud configuration files are backed up during the NetBackup catalog backup process:

- All `.txt` files in the `meter` directory, which contain intermediate metering data
- `CloudInstance.xml`
- `CloudProvider.xml`
- `cloudstore.conf`
- `libstspiencrypt.conf`
- `libstspimetering.conf`
- `libstspithrottling.conf`
- `libstspi`*`cloud_provider_name`*`.conf`
  All `.conf` files that are specific to the cloud providers that NetBackup supports

- libstspi*cloud_provider_name*.pref
  All .pref files that are specific to the cloud providers that NetBackup supports

The cloud configuration files that are backed up during the catalog backup process reside at the following location:

Windows	*install_path*\NetBackup\db\cloud
UNIX	usr/openv/netbackup/db/cloud

Note: The cacert.pem file is not backed up during the NetBackup catalog backup process.

This cacert.pem file is a cloud provider-specific file. This file is installed as part of the NetBackup installation. This file includes the certificates of NetBackup supported Certificate Authorities (CA).

About support limitations for NetBackup cloud storage

The following items are some of the limitations of 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.
- Cloud storage servers cannot use the same volume (bucket or container) to store data. You should create a separate volume (bucket or container) for each cloud storage server.

- NetBackup 7.7.1 and later versions support configuring cloud storage using the Frankfurt region.
- In the NetBackup Cloud Storage Configuration wizard, the following items are displayed only in the English language:
  - All the cloud provider names.
  - Description of the cloud providers.
  - In case of AmazonGov, the following fields: **Certificate File Name**, **Private Key File Name, Private Key Passphrase**, **Agency**, **Mission Name**, and **Role**.
  - In case of Openstack Swift, the following fields: **Tenant Type**, **Tenant Value**, **User Type**, **User Domain Type**, **User Domain Value**, **Project Domain Type**, and **Project Domain Value**.
- NetBackup now supports IPv6. The support is available only with all the cloud vendors and proxy server types that support IPv6.

Chapter 2

About the cloud storage

This chapter includes the following topics:

About the cloud storage vendors for NetBackup

NetBackup supports cloud storage based on the storage API type. All of the cloud vendors that NetBackup supports for cloud storage use one of the supported types. For more information about the storage API types and cloud vendors, see the following:

Cloud storage API types	Table 2-1 provides links to the topics that describe the requirements for each storage API type and for the cloud providers who use that storage API type.
Supported cloud vendors	Table 2-2 identifies the cloud vendors who are certified for NetBackup cloud storage and their storage API type. For configuration help, see the information about their storage API type.

http://www.netbackup.com/compatibility

Table 2-1 identifies the cloud storage APIs that are certified for NetBackup cloud storage.

Table 2-1 Supported cloud storage API types for NetBackup

API type	More information
Amazon S3	See "About the Amazon S3 cloud storage API type" on page 17.
EMC Atmos	See "About EMC Atmos cloud storage API type" on page 45.
Microsoft Azure	See "About Microsoft Azure cloud storage API type" on page 52.
OpenStack Swift	See "About OpenStack Swift cloud storage API type" on page 59.

Table 2-2 identifies the cloud vendors who are certified for NetBackup cloud storage. For configuration help, see the information about their storage API type.

Table 2-2 Alphabetical list of supported cloud vendors

Cloud vendor	Storage API type topic to consult for information
Amazon (S3)	See "About the Amazon S3 cloud storage API type" on page 17.
Amazon GovCloud (S3)	See "About the Amazon S3 cloud storage API type" on page 17.
AT&T (Atmos)	See "About EMC Atmos cloud storage API type" on page 45.
China Mobile Cloud Connector (S3)	See "About the Amazon S3 cloud storage API type" on page 17.
CMCC Cloud Storage v5.x(S3)	See "About the Amazon S3 cloud storage API type" on page 17.
Chunghwa Telecom hicloud S3 (S3)	See "About the Amazon S3 cloud storage API type" on page 17.
Cloudian HyperStore (S3)	See "About the Amazon S3 cloud storage API type" on page 17.
EMC ATMOS Private Cloud	See "About the Amazon S3 cloud storage API type" on page 17.
FUJITSU Cloud Service K5	See "About OpenStack Swift cloud storage API type" on page 59.
Google Nearline (S3)	See "About the Amazon S3 cloud storage API type" on page 17.
HGST Storage (S3)	See "About the Amazon S3 cloud storage API type" on page 17.
Hitachi Cloud Service (HCS) (S3)	See "About the Amazon S3 cloud storage API type" on page 17.

Table 2-2 Alphabetical list of supported cloud vendors *(continued)*

Cloud vendor	Storage API type topic to consult for information
Hitachi Content Platform (HCP) (S3)	See "About the Amazon S3 cloud storage API type" on page 17.
IBM Softlayer	See "About OpenStack Swift cloud storage API type" on page 59.
Microsoft Azure	See "About Microsoft Azure cloud storage API type" on page 52.
Microsoft Azure Government	See "About Microsoft Azure cloud storage API type" on page 52.
NetApp AltaVault	See "About the Amazon S3 cloud storage API type" on page 17.
Oracle (Swift)	See "About OpenStack Swift cloud storage API type" on page 59.
Rackspace	See "About Rackspace Cloud Files storage requirements" on page 68.
StorReduce (S3)	See "About the Amazon S3 cloud storage API type" on page 17.
SwiftStack (S3)	See "About the Amazon S3 cloud storage API type" on page 17.
SwiftStack (Swift)	See "About OpenStack Swift cloud storage API type" on page 59.
StorageGRID Webscale Object Storage	See "About the Amazon S3 cloud storage API type" on page 17.
Telefonica (S3)	See "About the Amazon S3 cloud storage API type" on page 17.
Verizon (S3)	See "About the Amazon S3 cloud storage API type" on page 17.

Note: Veritas may certify vendors between NetBackup releases. If your cloud storage vendor is not listed in this table, see the following webpage for the most up-to-date list of supported cloud vendors:

http://www.veritas.com/docs/000115793

About the Amazon S3 cloud storage API type

NetBackup supports cloud storage from the vendors that use the Amazon S3 storage API for their storage. Information about the requirements and configuration options for the Amazon S3 storage API vendors is provided as follows:

Table 2-3 Amazon S3 storage API type information and topics

Information	Topic
Certified vendors	See "Amazon S3 cloud storage vendors certified for NetBackup" on page 18.
Requirements	See "Amazon S3 storage type requirements" on page 22.
Storage server configuration options	See "Amazon S3 cloud storage provider options" on page 23.
Service host and endpoint configuration options	See "Amazon S3 cloud storage options" on page 28.
SSL, proxy, and HTTP header options	See "Amazon S3 advanced server configuration options" on page 30.
Credential broker options	See "Amazon S3 credentials broker details" on page 33.
Storage classes	See "About Amazon S3 storage classes" on page 36.

Some vendors may support private clouds that use the Amazon S3 storage type API.

See "About private clouds from Amazon S3-compatible cloud providers" on page 35.

Amazon S3 cloud storage vendors certified for NetBackup

Table 2-4 identifies the Amazon S3 compliant cloud vendors who are certified for NetBackup as of the NetBackup 8.1 release. Cloud vendors achieve certification by participating in the Veritas Technology Partner Program (VTPP).

Table 2-4 Amazon S3 compliant cloud vendors that NetBackup supports

Cloud vendor	Notes
Amazon	NetBackup supports Amazon Web Services (AWS) Signature Version 2 and Signature Version 4. The following storage classes are supported: ■ STANDARD ■ STANDARD_IA ■ GLACIER NetBackup also supports custom HTTP headers.

Table 2-4 Amazon S3 compliant cloud vendors that NetBackup supports *(continued)*

Cloud vendor	Notes
Amazon GovCloud	By default, you enter credentials for the vendor host. To use a credentials broker rather than enter credentials, select **Use Credentials Broker** in the **Cloud Storage Server Configuration Wizard**. You then enter the broker details on a separate wizard panel.
China Mobile Cloud Connector (CMCC)	You can add the service host endpoint before you configure the NetBackup storage server. To do so, use the NetBackup **Cloud Storage** host properties. See "Cloud Storage properties" on page 83. If you do not add it in the **Cloud Storage** host properties, you must add it when you configure the storage server.
CMCC Cloud Storage v5.x(S3)	You can add the service host endpoint before you configure the NetBackup storage server. To do so, use the NetBackup **Cloud Storage** host properties. See "Cloud Storage properties" on page 83. If you do not add it in the **Cloud Storage** host properties, you must add it when you configure the storage server.
Cloudian HyperStore	For more details on the bucket requirements (for example, the maximum number of buckets that you can create), contact Cloudian cloud provider. You can add the service host endpoint before you configure the NetBackup storage server. To do so, use the NetBackup **Cloud Storage** host properties. See "Cloud Storage properties" on page 83. If you do not add it in the **Cloud Storage** host properties, you must add it when you configure the storage server.
EMC ATMOS Private Cloud	You can add the service host endpoint before you configure the NetBackup storage server. To do so, use the NetBackup **Cloud Storage** host properties. See "Cloud Storage properties" on page 83. If you do not add it in the **Cloud Storage** host properties, you must add it when you configure the storage server.

Table 2-4 Amazon S3 compliant cloud vendors that NetBackup supports *(continued)*

Cloud vendor	Notes
Google Nearline	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 You can delete empty buckets and then reuse the bucket name. You can create buckets in any Google Nearline storage region.
HGST Storage (S3)	You can add the service host endpoint before you configure the NetBackup storage server. To do so, use the NetBackup **Cloud Storage** host properties. See "Cloud Storage properties" on page 83. If you do not add it in the **Cloud Storage** host properties, you must add it when you configure the storage server.
hicloud S3	You can add the service host endpoint before you configure the NetBackup storage server. To do so, use the NetBackup **Cloud Storage** host properties. See "Cloud Storage properties" on page 83. If you do not add it in the **Cloud Storage** host properties, you must add it when you configure the storage server.
Hitachi Cloud Service (HCS)	You can add the service host endpoint before you configure the NetBackup storage server. To do so, use the NetBackup **Cloud Storage** host properties. See "Cloud Storage properties" on page 83. If you do not add it in the **Cloud Storage** host properties, you must add it when you configure the storage server.
Hitachi Content Platform (HCP)	You can add the service host endpoint before you configure the NetBackup storage server. To do so, use the NetBackup **Cloud Storage** host properties. See "Cloud Storage properties" on page 83. If you do not add it in the **Cloud Storage** host properties, you must add it when you configure the storage server.

Table 2-4 Amazon S3 compliant cloud vendors that NetBackup supports *(continued)*

Cloud vendor	Notes
NetApp AltaVault	You can add the service host endpoint before you configure the NetBackup storage server. To do so, use the NetBackup **Cloud Storage** host properties. See "Cloud Storage properties" on page 83. If you do not add it in the **Cloud Storage** host properties, you must add it when you configure the storage server.
SwiftStack	You can add the service host endpoint before you configure the NetBackup storage server. To do so, use the NetBackup **Cloud Storage** host properties. See "Cloud Storage properties" on page 83. If you do not add it in the **Cloud Storage** host properties, you must add it when you configure the storage server.
StorReduce	You can add the service host endpoint before you configure the NetBackup storage server. To do so, use the NetBackup **Cloud Storage** host properties. See "Cloud Storage properties" on page 83. If you do not add it in the **Cloud Storage** host properties, you must add it when you configure the storage server.
StorageGRID Webscale Object Storage	You can add the service host endpoint before you configure the NetBackup storage server. To do so, use the NetBackup **Cloud Storage** host properties. See "Cloud Storage properties" on page 83. If you do not add it in the **Cloud Storage** host properties, you must add it when you configure the storage server.
Telefonica	You can add the service host endpoint before you configure the NetBackup storage server. To do so, use the NetBackup **Cloud Storage** host properties. See "Cloud Storage properties" on page 83. If you do not add it in the **Cloud Storage** host properties, you must add it when you configure the storage server.

Table 2-4 Amazon S3 compliant cloud vendors that NetBackup supports *(continued)*

Cloud vendor	Notes
Verizon	You can add the service host endpoint before you configure the NetBackup storage server. To do so, use the NetBackup **Cloud Storage** host properties. See "Cloud Storage properties" on page 83. If you do not add it in the **Cloud Storage** host properties, you must add it when you configure the storage server.

Note: Veritas may certify vendors between NetBackup releases. If your cloud storage vendor is not listed in this table, see the following webpage for the most up-to-date list of supported cloud vendors:

http://www.veritas.com/docs/000115793

Amazon S3 storage type requirements

The following tables describes the details and requirements of Amazon S3 type cloud storage in NetBackup:

Table 2-5 Amazon cloud storage requirements

Requirement	Details
License requirement	You must have a NetBackup license that allows for cloud storage.
Vendor account requirements	You must obtain an account that allows you to create, write to, and read from the storage that your vendor provides.
Buckets	The following are the requirements for the Amazon storage buckets: ■ 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.

Table 2-5 Amazon cloud storage requirements *(continued)*

Requirement	Details
Bucket names	Veritas 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 in the US Standard region. ■ The bucket name must be between 3 and 255 characters. ■ Any of the 26 lowercase (small) letters of the International Standards Organization (ISO) Latin-script alphabet. These are the same lowercase (small) letters as the English alphabet. ■ Any integer from 0 to 9, inclusive. ■ The following character (you cannot use this as the first character in the bucket name): Period (.), underscore (_), and dash (-). Dash - *Exception*: You cannot use a period (.) if you use SSL for communication. By default, NetBackup uses SSL for communication. See "NetBackup cloud storage server connection properties" on page 117. **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.
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.

Amazon S3 cloud storage provider options

Figure 2-1 shows the **Cloud Storage Configuration Wizard** panel for Amazon S3 cloud storage.

Figure 2-1 Cloud Storage Server Configuration Wizard panel for Amazon

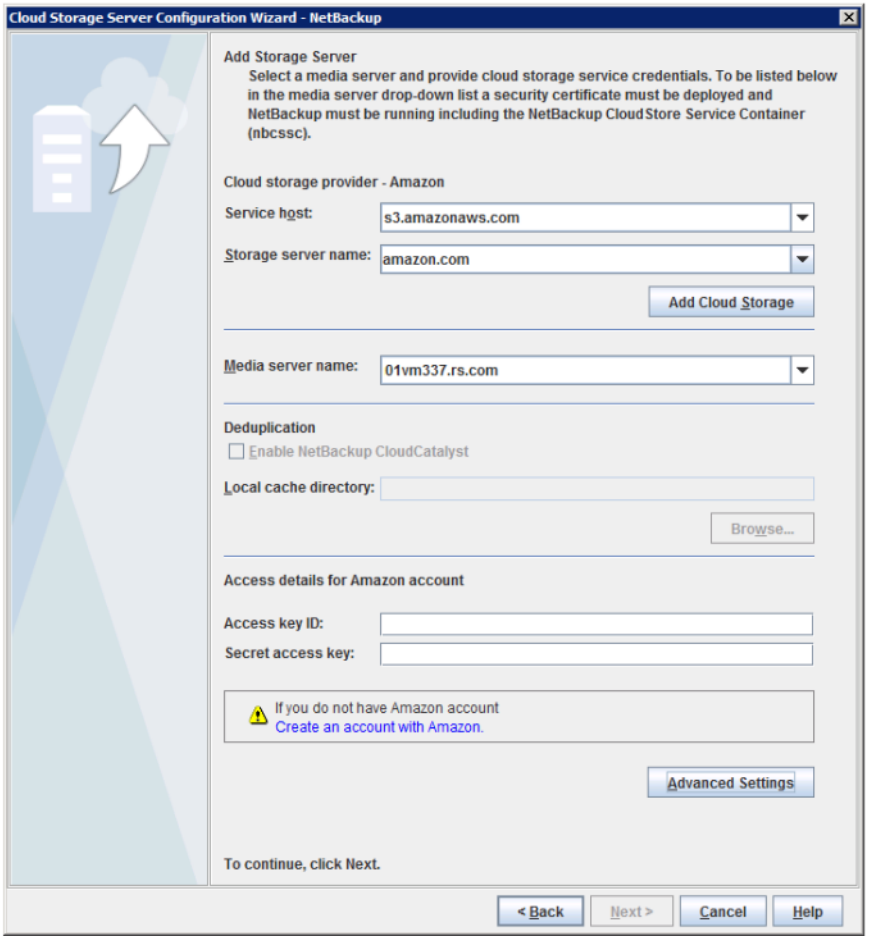


Table 2-6 describes the storage server configuration options for Amazon S3.

Table 2-6 Amazon S3 cloud storage provider configuration options

Field name	Required content
Service host	Select the name of the cloud service end point for your vendor from the drop-down list. If the cloud service end point for your vendor does not appear in the drop-down list, you must add a cloud storage instance. See the **Add Cloud Storage** description in this table.

Table 2-6 Amazon S3 cloud storage provider configuration options *(continued)*

Field name	Required content
Storage server name	Displays the default storage server for your vendor. The drop-down list displays only those names that are available for use. If more than one storage server is available, you can select a storage server other than the default one. 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 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. **Note:** Veritas 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. **Note:** The **Add Cloud Storage** option is disabled for public clouds. You must use existing cloud storage.
Add Cloud Storage	To configure cloud deployment details, click **Add Cloud Storage**. The customized cloud deployment refers to the cloud instances that are not already listed in the **Service Host** drop-down list. After you configure cloud deployment details, the service host appears in the **Service Host** drop-down list. See "Amazon S3 cloud storage options" on page 28. 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 `csconfig` command. **Note:** You can use the NetBackup `csconfig -a` command to create custom cloud instances for an Amazon S3-compatible cloud provider. You must run the `csconfig` command before you run the `nbdevconfig` and `tpconfig` commands. See the *NetBackup Commands Reference Guide* for a complete description about these commands. The guide is available through the following URL: http://www.veritas.com/docs/DOC5332

Table 2-6 Amazon S3 cloud storage provider configuration options *(continued)*

Field name	Required content
Media server name	Select a NetBackup media server from the drop-down list. The drop-down list displays only NetBackup 8.1 and later media servers. In addition, only the media servers that conform to the requirements for cloud storage appear in the drop-down list. The requirements are described in the following topic: See "About the NetBackup media servers for cloud storage" on page 102. 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. To support cloud storage, a media server must conform to the following items: ■ The 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 (`nbcssc`) must be running. See "About the NetBackup CloudStore Service Container" on page 88. ■ For Amazon S3-compatible cloud providers, the media server must run a NetBackup 8.1 or later release. ■ The NetBackup media servers that you use for cloud storage must be the same NetBackup version as the master server.
Enter Credentials	*Applies to: Amazon GovCloud only.* This option is the default selection. Select this option to configure cloud storage server credentials on this wizard panel by entering the access key ID and secret access key.
Use Credentials Broker	*Applies to: Amazon GovCloud only.* Select this option to configure cloud storage server using credentials broker. If you select this option, you then use the **Credentials Broker Details** wizard panel that appears next to configure the credentials broker information.

Table 2-6 Amazon S3 cloud storage provider configuration options *(continued)*

Field name	Required content
Deduplication	Enabling this option creates a CloudCatalyst storage server that can be used to upload deduplicated data to the cloud. This option is grayed out if any of the following cases are true: ■ The selected media server does not have NetBackup 8.1 or later installed. ■ CloudCatalyst does not support the media server operating system. ■ CloudCatalyst does not support the cloud vendor. See the NetBackup compatibility lists for support information: http://www.netbackup.com/compatibility For information about CloudCatalyst, see the *NetBackup Deduplication Guide*: http://www.veritas.com/docs/DOC5332
Local cache directory	Enter the mount path to be used as the storage path on the CloudCatalyst storage server. For example: `/space/mnt/esfs` The deduplicated data is written to this local cache directory before it is uploaded to the cloud. The larger the cache, the more likely that NetBackup can service requests locally, avoiding cloud access to read and write. Notes: ■ This path should be to a file system which is dedicated for CloudCatalyst cache use. Inaccurate cache eviction occurs if the path shares any storage with other data or applications. ■ NetBackup manages the files in the local cache directory. Users should not manually delete files in this directory.
Access key ID	*Does not apply for Amazon GovCloud if you select* **Use Credentials Broker**. Enter the access key ID for your vendor account. If you do not have an account, click **Create an account with the service provider** link.
Secret access key	*Does not apply for Amazon GovCloud if you select* **Use Credentials Broker**. Enter the secret access key for your vendor account. It must be 100 or fewer characters.

Table 2-6 Amazon S3 cloud storage provider configuration options *(continued)*

Field name	Required content
Advanced Settings	To change SSL, proxy, or HTTP header (server-side encryption or storage class) settings for your cloud storage hosts, click **Advanced Settings**. See "Amazon S3 advanced server configuration options" on page 30.

Amazon S3 cloud storage options

The **Add Cloud Storage** dialog box appears when you click **Add Cloud Storage** on the wizard panel for Amazon S3 providers. It contains the following tabs:

General Settings tab — See Table 2-7 on page 28.

Region Settings tab — See Table 2-8 on page 30.

Note: If your cloud storage deployment is not configured for multiple regions, you do not need to configure any regions.

Note: To add a cloud storage server in Amazon virtual private cloud (VPC) environment, enure that you have reviewed the considerations.

See "Amazon virtual private cloud support with NetBackup " on page 36.

Table 2-7 General Settings tab options

Option	Description
Provider type	The cloud storage provider. The following describes the state of this field: ■ Active if you add cloud storage from the **Cloud Storage** host properties. Select the required provider from the list. ■ Inactive if you add cloud storage from the **Cloud Storage Server Configuration Wizard** or change settings from the **Cloud Storage** host properties. It shows the host that you selected in the wizard or **Cloud Storage** host properties.

Table 2-7 General Settings tab options *(continued)*

Option	Description
Service host	Enter the cloud service provider host name. If you want to add a public cloud instance, you need to get the service host details from the cloud storage provider. Type the service host details in the text box. If you want to add a cloud storage instance for a private cloud deployment, enter a service host name like 'service.my-cloud.com', in case you can access your cloud provider using the following URL: 'service.my-cloud.com/services/objectstore' **Note:** Do not prefix the service host name with 'http' or 'https'. **Note:** For VPC in default (**US East (N. Virginia)**) AWS region, use **external-1.amazonaws.com** as the service host.
Service endpoint	Enter the cloud service provider endpoint. Service endpoint - Enter the cloud service provider endpoint. For example, '/services/objectstorage' in case your cloud provider service can be accessed using the 'service.my-cloud.com/services/objectstore' URL. You can leave it blank, if the cloud provider service can be accessed directly from the 'service.my-cloud.com' URL.
HTTP port	Enter the HTTP port with which you can access the cloud provider service in a non-secure mode.
HTTPS port	Enter the HTTPS port with which you can access the cloud provider service in a secure mode.
Storage server name	Enter a logical name for the cloud storage that you want to configure and access using NetBackup. **Note:** You can configure multiple storage servers that are associated with the same public or private cloud storage instance.
Endpoint access style	Select the endpoint access style for the cloud service provider. **Path Style** is the default endpoint access style. If your cloud service provider additionally supports virtual hosting of URLs, select **Virtual Hosted Style**.

Note: If your cloud storage deployment is not configured for multiple regions, you do not need to configure any regions.

Table 2-8 Region Settings tab

Option	Description
Region name	Enter a logical name to identify a specific region where the cloud storage is deployed. For example: East zone.
Location constraint	Enter the location identifier that the cloud provider service uses for any data transfer operations in the associated region. For a public cloud storage, you need to get the location constraint details from the cloud provider. **Note:** For VPC in default (**US East (N. Virginia)**) AWS region, use **US-east-1** as the location identifier.
Service host	Enter the service host name for the region. The Service endpoint, HTTP port, and HTTPS port information that you have entered in the **General Settings** tab are used while accessing information from any region.
Add	Click **Add** to add the region.

Amazon S3 advanced server configuration options

The following tables describes the SSL, HTTP header configuration, and proxy server options that are specific to all Amazon S3-compatible cloud providers. These options appear on the **Advanced Server Configuration** dialog box.

Table 2-9 General Settings tab options

Option	Description
Use SSL	Select **Use SSL** if you want to use the SSL (Secure Sockets Layer) protocol for user authentication or data transfer between NetBackup and cloud storage provider. ■ **Authentication only**. Select this option, if you want to use SSL only at the time of authenticating users while they access the cloud storage. ■ **Data Transfer**. Select this option, if you want to use SSL to authenticate users and transfer the data from NetBackup to the cloud storage. **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 fails 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.

Table 2-9 General Settings tab options *(continued)*

Option	Description
HTTP Headers	Specify appropriate value for the selected HTTP header. Click the **Value** column to see the drop-down list and select the value. ■ **x-amz-server-side-encryption**. Select **AE256** from the **Value** drop-down list, if you want to protect data in Amazon S3 cloud storage. **AE256** stands for 256-bit Advanced Encryption Standard. By setting the header value to **AE256**, every object that Amazon S3 cloud storage receives is encrypted before it is stored in the cloud. Amazon S3 server-side encryption uses one of the strongest block ciphers available, that is AE256 to encrypt your data. Additionally, it encrypts the key itself with a master key that it regularly rotates. **Note:** If you have already enabled the encryption option while creating Amazon S3 cloud storage server, you do not need to enable this option. Because, the data is already encrypted before NetBackup sends it over the network. ■ **x-amz-storage-class**. Select an Amazon S3 storage class that you want to assign to your data backups or objects. Amazon S3 stores objects according to their storage class. You can select any of the following storage classes: **STANDARD** or **STANDARD_IA**. The default value of the **x-amz-storage-class** HTTP header is **STANDARD**. **Note:** The **x-amz-storage-class** HTTP header is applicable only for the Amazon S3 and AmazonGov cloud provider. See "About Amazon S3 storage classes" on page 36. ■ Storage class is configured at the time of creating the storage server. Once configured, storage class is non-editable.

Table 2-10 Proxy Settings tab options

Option	Description
Use Proxy Server	**Use Proxy Server** option to use proxy server and provide proxy server settings. Once you select the **Use Proxy Server** option, you can specify the following details: ■ **Proxy Host**–Specify IP address or name of the proxy server. ■ **Proxy Port**–Specify port number of the proxy server. ■ **Proxy Type**– You can select one of the following proxy types: ■ **HTTP** **Note:** You need to provide the proxy credentials for HTTP proxy type. ■ **SOCKS** ■ **SOCKS4** ■ **SOCKS5** ■ **SOCKS4A**
Use Proxy Tunneling	You can enable proxy tunneling for HTTP proxy type. After you enable **Use Proxy Tunneling**, HTTP CONNECT requests are send from the cloud media server to the HTTP proxy server and the TCP connection is directly forwarded to the cloud back-end storage. The data passes through the proxy server without reading the headers or data from the connection.
Authentication Type	You can select one of the following authentication types if you are using HTTP proxy type. ■ **None**– Authentication is not enabled. Username and password is not required. ■ **NTLM**–Username and password needed. ■ **Basic**–Username and password needed. **Username** is the username of the proxy server **Password** can be empty. You can use maximum 256 characters.

Amazon S3 credentials broker details

Figure 2-2 shows the **Cloud Storage Configuration Wizard** credentials broker panel for Amazon GovCloud cloud storage. You add the credentials broker details when you configure a cloud storage server in NetBackup.

See "Configuring a storage server for cloud storage" on page 105.

The credentials broker details also appear in a **Cloud Storage Server Configuration** dialog box in which you can change the details.

See "Changing cloud storage host properties" on page 86.

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

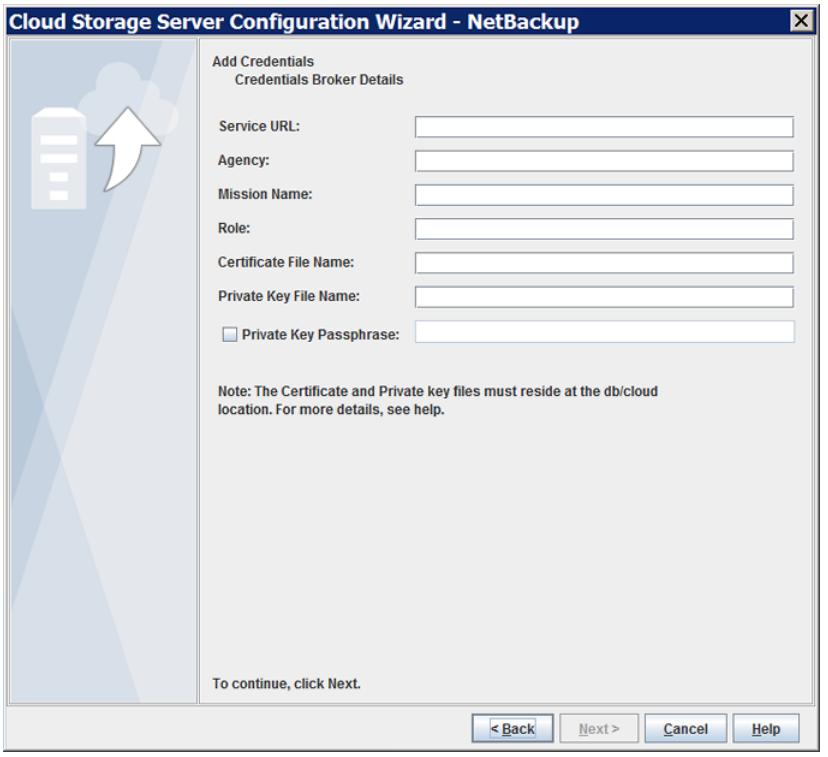


Table 2-11 describes the credential broker options for Amazon GovCloud.

Table 2-11 Credential broker details

Field	Description
Service URL	Enter the service URL. For example: `https://hostname:port_number/service_path`
Agency	Enter the agency name.
Mission Name	Enter the mission name.
Role	Enter the role.

Table 2-11 Credential broker details *(continued)*

Field	Description
Certificate File Name	Enter the certificate file name.
Private Key File Name	Enter the private key file name.
Private Key Passphrase	Select the check box to specify the private key pass phrase. It must be 100 or fewer characters. The **Private Key Passphrase** is optional.

Note: The certificate file and the private key file must reside at the following location:

On UNIX - `/usr/openv/netbackup/db/cloud`

On Windows - *`install_dir`*`\NetBackup\db\cloud`

Note: For more details on the credentials broker parameters, contact the Veritas Technical Support team.

About private clouds from Amazon S3-compatible cloud providers

NetBackup supports the private clouds or cloud instances from the following Amazon S3-compatible cloud providers:

- Amazon GovCloud
- Cloudian HyperStore
- Hitachi
- Verizon

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 fails 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.

About Amazon S3 storage classes

NetBackup supports Amazon S3 and AmazonGov storage classes. While you configure a cloud storage, you can select a specific storage class that you want to assign to your objects or data backups. The objects are stored according to their storage classes.

NetBackup supports the following Amazon S3 storage classes: or

- **STANDARD**
- **STANDARD_IA** (IA stands for Infrequent Access.)
- **GLACIER** See "Protecting data in Amazon Glacier for long-term retention" on page 38.

In the following scenarios, NetBackup assigns the default STANDARD storage class to the backups or objects:

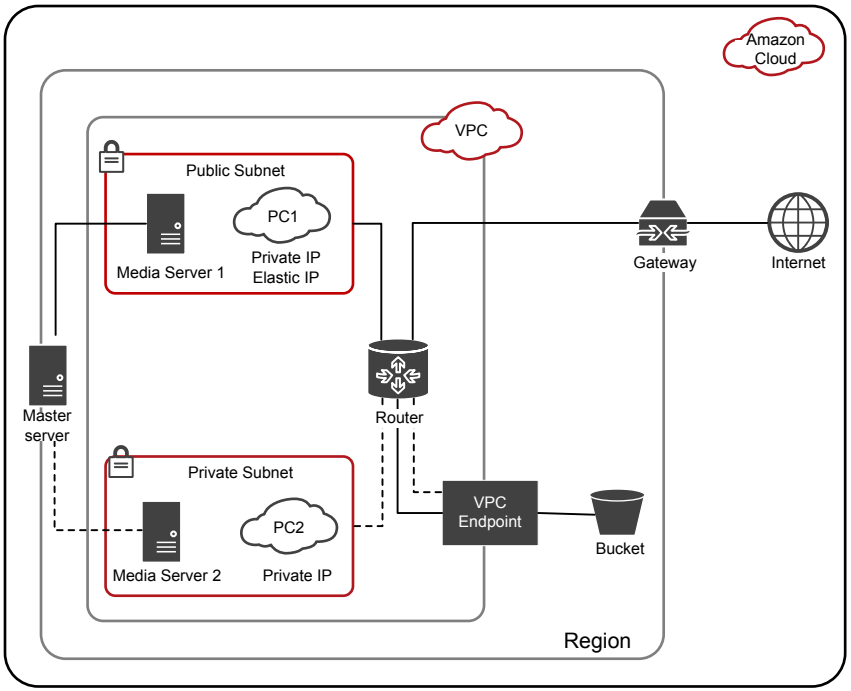
- If you do not select a specific storage class while you configure the Amazon S3 cloud storage
- If the backups were configured in an earlier NetBackup version

See "Assigning a storage class to Amazon cloud storage" on page 109.

Amazon virtual private cloud support with NetBackup

Using NetBackup you can add a new cloud storage in an Amazon virtual private cloud (VPC) environment.

The following diagram illustrates how NetBackup integrates with VPC.



The diagram illustrates the following points:

- You must deploy the media servers within the VPC environment.
- You can deploy the master server locally or in the VPC environment. Ensure that the master server is able to communicate with the media servers.
- In the public subnet, PC1 uses both private and elastic IP and has access to the Internet. The media server 1, also has access to the Internet. In a public subnet, you can authenticate and access the storage bucket over Internet or using the VPC endpoint.
- In the private subnet, PC2 uses only private IP and has no access to the Internet. The media server 2, also has no access to the Internet. In a private subnet, you can authenticate and access the storage bucket using the VPC endpoint.
- A VPC is restricted to a specific region.

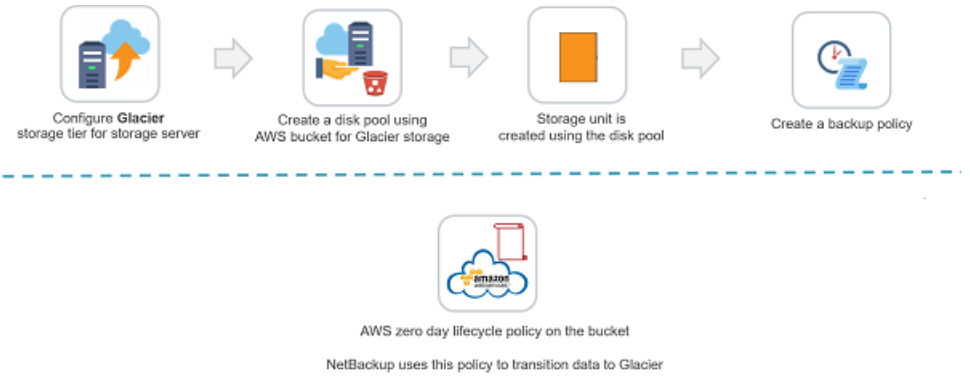
Considerations for configuring cloud storage server in an Amazon virtual private cloud (VPC) environment

- You need to add a new cloud storage server for the specific region.
  See “Amazon S3 cloud storage options” on page 28.

- Do not configure multiple regions for one service host.
- When you configure a region for a service host, it must be same as the VPC region; you cannot configure a different region. For example, if you want to add a cloud storage for Singapore region VPC environment, you must configure the service host region to Singapore.
- For VPC in the default (**US East (N. Virginia)**) AWS region, use **external-1.amazonaws.com** as the service host and **US-east-1** as the location identifier.
- Configure the NetBackup policy to use the media server within the VPC environment.

Protecting data in Amazon Glacier for long-term retention

To protect your data for long-term retention you can back up the data to Amazon (AWS) Glacier using NetBackup. Using NetBackup, you can create a storage server with Glacier storage class. During the backup process, NetBackup internally uses the Amazon's zero-day lifecycle policy to transition data to Glacier. AWS lifecycle policy is a lifecycle rule defined to transition objects to the Glacier storage class in 0 (zero) days after creation. The following diagram illustrates the configuration process:



To configure a cloud storage server for Amazon GLACIER storage class

1. Configure the GLACIER storage class for *amazon_glacier* cloud storage server using the following command:

   ```
   ./csconfig cldinstance -as -in amazon.com -sts amazon_glacier
   -storage_class GLACIER
   ```

   For information on the command, see *Veritas NetBackup Commands Reference Guide*.

2. Configure the Amazon GLACIER cloud storage server.

   See "Configuring a storage server for cloud storage" on page 105.

3. Create a disk pool using the Amazon bucket for GLACIER storage.

   See "Configuring a disk pool for cloud storage" on page 124.

4. Create a backup policy.

   See "Creating a backup policy" on page 145.

Best practices

When you configure a storage server to transition data to Amazon Glacier, consider the following:

- Ensure that Amazon Glacier is supported for the region to which the bucket belongs.
- Ensure that the selected bucket does not have any existing Amazon lifecycle policy.
- For restores, set the retrieval retention period to minimum 3 days.
- You can reduce restore time by parallel restores. For this, you must backup using multi-streaming that creates multiple images at logical boundaries.
- Workload Granular Revovery (GRT) or VMware Single File Restore (SFR), increases the timeout on the master, media, and client to more than 5 hours.

Limitations

Consider the following limitations:

- NetBackup Accelerator feature is not supported for policies of the storage units that are created for Amazon Glacier. Do not select the **Accelerator** check box.
- CloudCatalyst with Glacier is not supported.
- When you run parallel restores from same set of data, critical info is displayed only for one restore job.
- You can configure the GLACIER storage class only using the CLI.

- During import of images:
  - Phase 1: Each image takes around 4 hours.
    The total image duration = Number of images X 4 hours (approx).
  - Phase 2: For images without TIR fragments:
    Time required for import = Number of fragments X 4 hours (approx).

Permissions

You must have the following permissions:

- Life cycle policy related permissions:
  - s3:PutLifecycleConfiguration
  - s3:GetLifecycleConfiguration
- Object tagging permissions
  - s3:PutObjectTagging

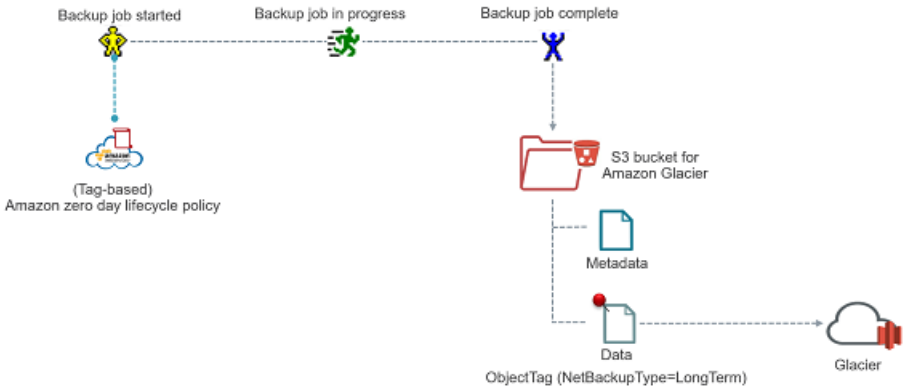
Note: The bucket owner has these permissions, by default. The bucket owner can grant these permissions to others by writing an access policy.

- Also ensure that you also have the required IAM USER permissions. See "Permissions required for Amazon IAM user" on page 43.

Backing up data to Amazon Glacier

When a NetBackup backup job is run to backup data in to Amazon Glacier, NetBackup internally uses the Amazon zero day lifecycle policy. The data objects are tagged as **NetBackupType=LongTerm**. Only the data objects are backed up to Glacier storage, while the metadata objects reside in the Standard storage.

The following diagram illustrates the high-level backup process.



To duplicate tape data to Amazon Glacier

Use the `bpduplicate` command to duplicate tape data to Amazon Glacier storage.

For information on the command, see *Veritas NetBackup Commands Reference Guide*.

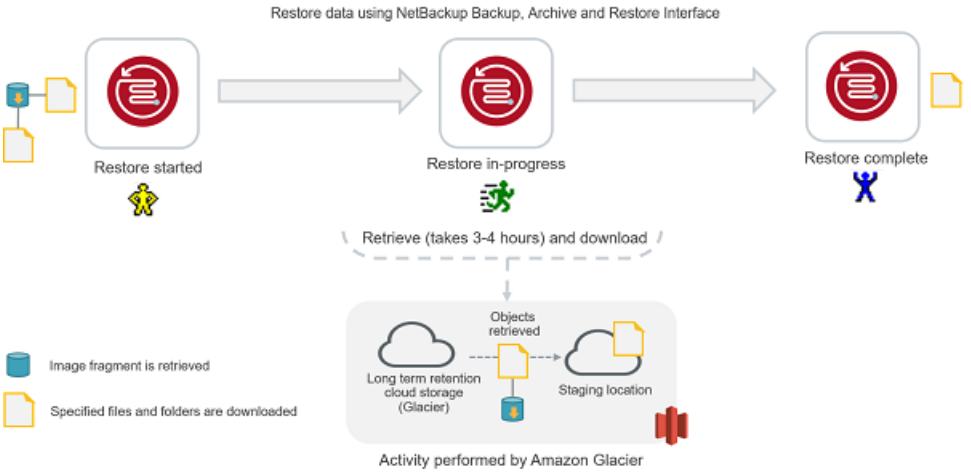
Restoring data from Amazon Glacier

NetBackup image is stored as set of objects with specified storage class, in this case, Glacier storage class. Restore from Amazon Glacier happens in two phases. The objects are first retrieved at an internal staging location that is maintained by Amazon and from there the data are restored at the destination location. The entire restore operation takes minimum 3 – 5 hours. The objects are available at the Amazon staging location depending on the retrieval retention period you have specified. Veritas recommends that you set the retrieval retention period to minimum 3 days. After the retrieval retention period expires, the data is transitioned back to Amazon Glacier.

Note: NetBackup supports Amazon Standard retrievals, which complete within minimum 3 – 5 hours.

When you perform a restore, the entire image fragment is restored while only the selected objects are downloaded.

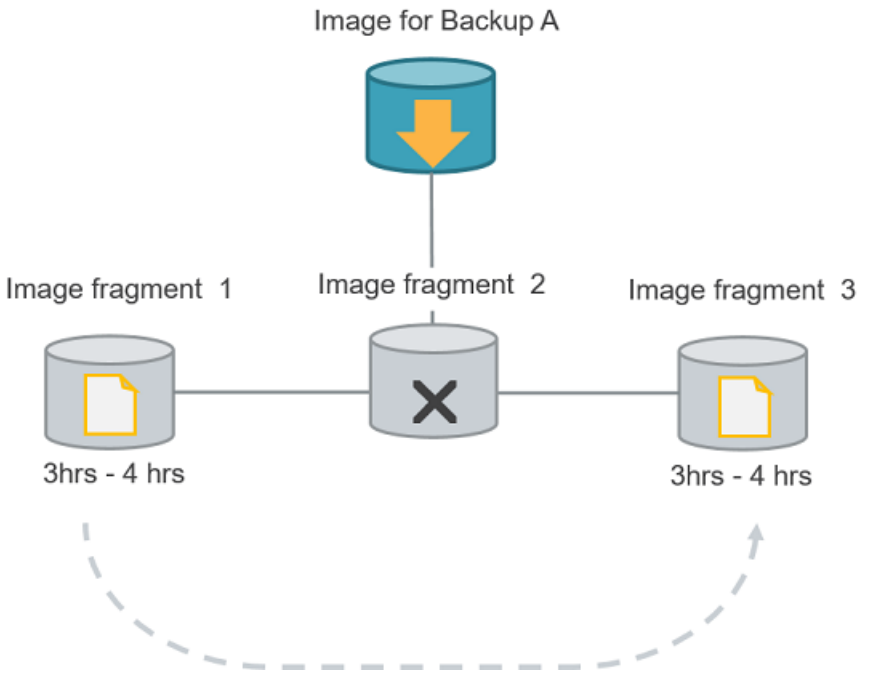
The following diagram illustrates the high-level restore process.



Considerations with Restore of Image Fragments

If the files and folders, you want to restore belong to multiple image fragment consider the following:

- One image fragment is retrieved at a time. Only after the selected files and folders part of the first image fragment are downloaded, the next image fragment is retrieved.
- The restore time must be considered depending on the number of image fragments. For example, if the files you want to restore are part of two fragments, the additional 6hrs - 10 hrs will be added to the complete restore time.



Note: If you cancel a job after the restore retrieval is initiated, cost is incurred for all the objects that are retrieved on the staging location till the point of cancellation.

Permissions required for Amazon IAM user

With the Amazon (S3) cloud vendor, if you have configured an IAM user, it should have following minimum permissions to work with NetBackup:

- s3:CreateBucket
- s3:ListAllMyBuckets
- s3:ListBucket
- s3:GetBucketLocation
- s3:GetObject
- s3:PutObject
- s3:DeleteObject

For more information refer to the *AWS Identity and Access Management* documentation.

For Amazon Glacier, you need additional permissions. See “Protecting data in Amazon Glacier for long-term retention” on page 38.

About NetBackup character restrictions for Amazon S3 cloud connector

NetBackup S3 cloud connector on the S3 compliant cloud storage does not support VMware and Hyper-V backups if the virtual machine display name contains unsupported characters. The unsupported characters are listed in the Object Key Naming guidelines from Amazon S3.

Characters to avoid as per Amazon S3 Object Key Naming guidelines:

The virtual machine display name maps to the key name in Amazon S3 context. Therefore, avoid the following set of characters in a virtual machine display name:

- Backslash \
- Left curly brace {
- Right curly brace }
- Non-printable ASCII characters (128–255 decimal characters)
- Caret ^
- Percent character %
- Grave accent or back tick `
- Right square bracket]
- Left square bracket [
- Quotation marks "
- Tilde ~
- Less Than symbol <
- Greater Than symbol >
- Pound character #
- Vertical bar or pipe |

Characters to avoid as per NetBackup S3 connector guidelines:

Avoid the following set of characters in a virtual machine display name:

- Ampersand &

- Dollar $
- ASCII character ranges 00–1F hex (0–31 decimal) and 7F (127 decimal)
- At symbol @
- Equals =
- Semicolon ;
- Colon :
- Plus +
- Space (Significant sequences of spaces may be lost in some uses, especially multiple spaces)
- Comma ,
- Question mark ?
- Right round parenthesis)
- Left round parenthesis (

Note: For an updated list of characters to avoid, refer to Amazon S3 documentation.

About EMC Atmos cloud storage API type

NetBackup Cloud Storage enables Veritas NetBackup to backup data to and restore data from vendors that use the EMC Atmos storage API. Information about the requirements and configuration options for the EMC Atmos storage API vendors is provided as follows:

Table 2-12 EMC Atmos storage API type information and topics

Information	Topic
Certified vendors	See "EMC Atmos cloud storage vendors certified for NetBackup" on page 46.
Requirements	See "EMC Atmos storage type requirements" on page 46.
Storage server configuration options	See "EMC Atmos cloud storage provider options" on page 47.
Storage server name and network connection options	See "EMC Atmos advanced server configuration options" on page 50.

Note: NetBackup also supports provide clouds from EMC ATMOS using the Amazon S3 cloud storage API.

See "About the Amazon S3 cloud storage API type" on page 17.

EMC Atmos cloud storage vendors certified for NetBackup

Table 2-13 identifies the vendors who are certified for NetBackup cloud storage using the EMC Atmos storage API as of the NetBackup 8.1 release. Vendors achieve certification by participating in the Veritas Technology Partner Program (VTPP). NetBackup can send backups to the storage that these vendors provide.

Table 2-13 Vendors who support the EMC Atmos storage type for NetBackup

Vendor	Notes
AT&T	AT&T also allows for private cloud storage. See "About private clouds from AT&T" on page 51.

Note: Veritas may certify vendors between NetBackup releases. If your cloud storage vendor is not listed in this table, see the following webpage for the most up-to-date list of supported cloud vendors:

http://www.veritas.com/docs/000115793

EMC Atmos storage type requirements

Table 2-14 describes the details and requirements for vendors that use the EMC Atmos storage API.

Table 2-14 AT&T Synaptic requirements

Requirement	Details
User account	An AT&T Synaptic user ID and password are required to create the storage server.

Table 2-14 AT&T Synaptic requirements *(continued)*

Requirement	Details
Storage requirements	The following are the requirements for AT&T cloud storage: ■ You must have a NetBackup license that allows for cloud storage. ■ You must use NetBackup to create the volume for your NetBackup backups. The volume that NetBackup creates contain a required Veritas 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: ■ 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 51.

EMC Atmos cloud storage provider options

Figure 2-3 shows the **Cloud Storage Server Configuration Wizard** panel for a vendor that uses the EMC Atmos storage API.

Figure 2-3 Cloud Storage Server Configuration Wizard panel for AT&T

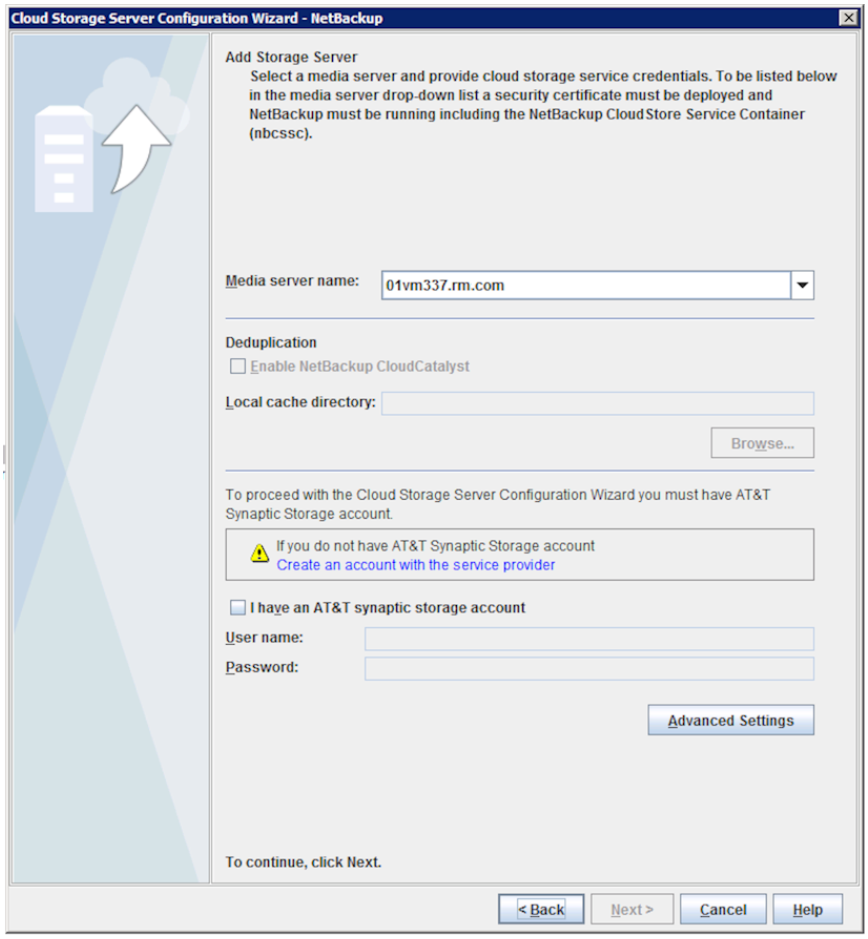


Table 2-15 describes the storage server configuration options for vendors who use the EMC Atmos storage API.

Table 2-15 EMC Atmos storage API configuration options

Field name	Required content
Media Server Name	Select a NetBackup media server from the drop-down lis5. Only the media servers that conform to the requirements for cloud storage appear in the drop-down list. The requirements are described in the following topic: See "About the NetBackup media servers for cloud storage" on page 102. 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.
Deduplication	Enabling this option creates a CloudCatalyst storage server that can be used to upload deduplicated data to the cloud. This option is grayed out if any of the following cases are true: ■ The selected media server does not have NetBackup 8.1 or later installed. ■ CloudCatalyst does not support the media server operating system. ■ CloudCatalyst does not support the cloud vendor. See the NetBackup compatibility lists for support information: http://www.netbackup.com/compatibility For information about CloudCatalyst, see the *NetBackup Deduplication Guide*: http://www.veritas.com/docs/DOC5332
Local cache directory	Enter the mount path to be used as the storage path on the CloudCatalyst storage server. For example: `/space/mnt/esfs` The deduplicated data is written to this local cache directory before it is uploaded to the cloud. The larger the cache, the more likely that NetBackup can service requests locally, avoiding cloud access to read and write. Notes: ■ This path should be to a file system which is dedicated for CloudCatalyst cache use. Inaccurate cache eviction occurs if the path shares any storage with other data or applications. ■ NetBackup manages the files in the local cache directory. Users should not manually delete files in this directory.

Table 2-15 EMC Atmos storage API configuration options *(continued)*

Field name	Required content
Create an account with the service provider	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.
I have an AT&T Synaptic storage account	Select **I have an AT&T Synaptic storage account** to enter the required account information.
User Name	Enter your AT&T user name. If you do not have an account, click **Create an account with the service provider** link.
Password	Enter the password for the **User Name** account. It must be 100 or fewer characters.
Advanced	To change the default storage server for your cloud vendor or specify the maximum number of network connections, click **Advanced**. See "EMC Atmos advanced server configuration options" on page 50. See "About private clouds from AT&T" on page 51.

EMC Atmos advanced server configuration options

The following table describes the storage server name and the maximum number of network connections you can configure. These options appear in the **Advanced Server Configuration** dialog box.

Table 2-16 Advanced configuration options for EMC Atmos storage type

Option	Description
Override storage server	To change the storage server, click and then enter the storage server name. You can use this option to specify an internal host for a private cloud. See "About private clouds from AT&T" on page 51.
Maximum Concurrent Jobs	To limit the number of simultaneous network connections to the storage server, enter the value in the **Maximum Concurrent Jobs** box. If you do not set the value here, NetBackup uses the global value from the **Scalable Storage** host properties. See "Scalable Storage properties" on page 78.

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/openv/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 105.

About Microsoft Azure cloud storage API type

NetBackup supports cloud storage from the vendors that use the Microsoft Azure storage API for their storage. Information about the requirements and configuration options for the Microsoft Azure storage API vendors is provided as follows:

Table 2-17 Microsoft Azure storage API type information and topics

Information	Topic
Certified vendors	See "Microsoft Azure cloud storage vendors certified for NetBackup" on page 52.
Requirements	See "Microsoft Azure storage type requirements" on page 53.
Storage server configuration options	See "Microsoft Azure cloud storage provider options" on page 53.
SSL and proxy options	See "Microsoft Azure advanced server configuration options" on page 57.

Microsoft Azure cloud storage vendors certified for NetBackup

Table 2-18 identifies the vendors who are certified for NetBackup cloud storage using the Microsoft Azure storage API as of theNetBackup 8.1 release. Vendors achieve certification by participating in the Veritas Technology Partner Program (VTPP).

Table 2-18 Vendors who support the Microsoft Azure storage type for NetBackup

Vendor	Notes
Microsoft	None.
Microsoft Azure Government	None.

Note: Veritas may certify vendors between NetBackup releases. If your cloud storage vendor is not listed in this table, see the following webpage for the most up-to-date list of supported cloud vendors:

http://www.veritas.com/docs/000115793

Microsoft Azure storage type requirements

Table 2-19 describes the details and requirements of Microsoft Azure cloud storage in NetBackup.

Table 2-19 Microsoft Azure cloud storage requirements

Requirement	Details
License requirement	You must have a NetBackup license that allows for cloud storage.
Microsoft Azure account requirements	You must obtain a Microsoft Azure storage account and at least one storage access key (primary access key or secondary access key).
Container names	Veritas recommends that you use NetBackup to create the container that you use with NetBackup. The following are the NetBackup requirements for container names: ■ Container names must be from 3 through 63 characters long. ■ Container names must start with a letter or number, and can contain only letters, numbers, and the dash (-) character. ■ Every dash (-) character must be immediately preceded and followed by a letter or number; consecutive dashes are not permitted in container names. ■ All letters in a container name must be lowercase. You can refer to the following link: https://msdn.microsoft.com/en-us/library/azure/dd135715.aspx

Microsoft Azure cloud storage provider options

Figure 2-4 shows the **Cloud Storage Configuration Wizard** panel for Microsoft Azure cloud storage.

Figure 2-4 Cloud Storage Server Configuration Wizard panel for Microsoft Azure

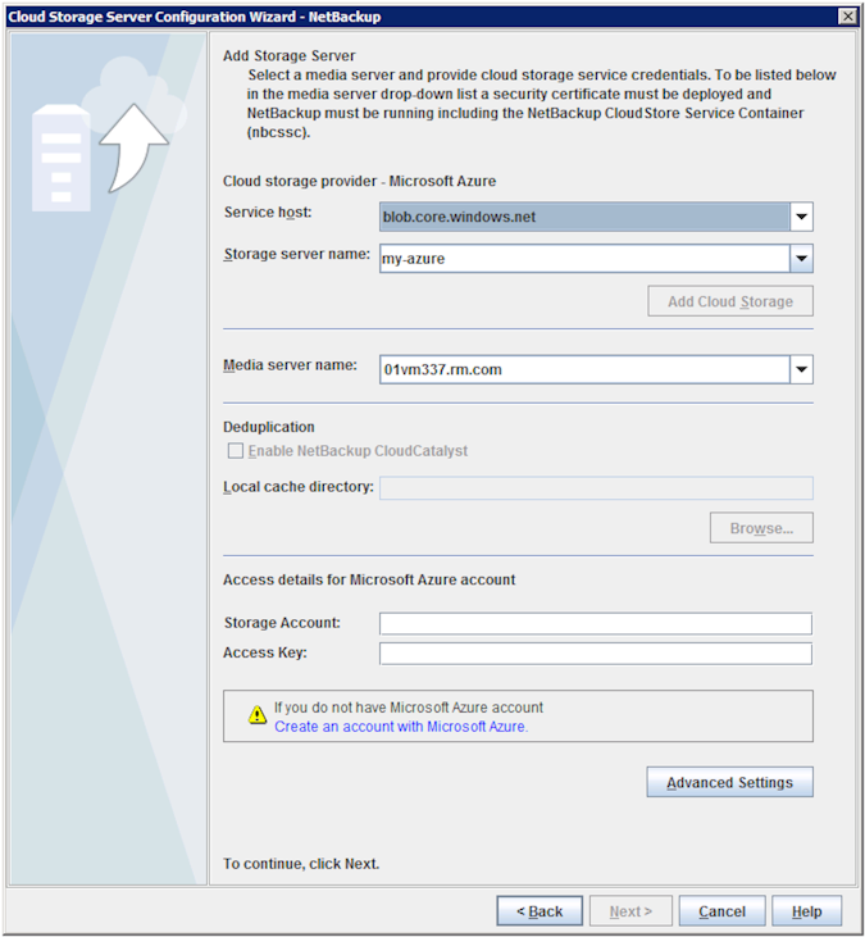


Table 2-20 describes the storage server configuration options for Microsoft Azure.

Table 2-20 Microsoft Azure storage server configuration options

Field name	Required content
Service host	Service host is the host name of the cloud service end point of Microsoft Azure. The **Service host** drop-down list displays part of the service host URL that also comprises **Storage Account**. Example of a service host URL: *storage_account*.blob.core.windows.net **Note:** Based on the region where you have created your storage account - default or China - you should select the service host from the drop-down list.
Storage server name	Displays the default Azure storage server, which is my-azure. You can select a storage server other than the default one. The drop-down list displays only those names that are available for use. 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 different names that refer to the same physical service host for Azure. 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. **Note:** Veritas recommends that a storage server name that you add while configuring an Azure cloud storage should be a logical name and should not match a physical host name. For example: While you add an Azure storage server, avoid using names like ‘azure.com’ or ‘azure123.com’. These servers may be physical hosts, which can cause failures during cloud storage configuration. Instead, use storage server names like ‘azure1’ or ‘azureserver1’ and so on.

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

Field name	Required content
Deduplication	Enabling this option creates a CloudCatalyst storage server that can be used to upload deduplicated data to the cloud. This option is grayed out if any of the following cases are true: ■ The selected media server does not have NetBackup 8.1 or later installed. ■ CloudCatalyst does not support the media server operating system. ■ CloudCatalyst does not support the cloud vendor. See the NetBackup compatibility lists for support information: http://www.netbackup.com/compatibility For information about CloudCatalyst, see the *NetBackup Deduplication Guide*: http://www.veritas.com/docs/DOC5332
Local cache directory	Enter the mount path to be used as the storage path on the CloudCatalyst storage server. For example: `/space/mnt/esfs` The deduplicated data is written to this local cache directory before it is uploaded to the cloud. The larger the cache, the more likely that NetBackup can service requests locally, avoiding cloud access to read and write. Notes: ■ This path should be to a file system which is dedicated for CloudCatalyst cache use. Inaccurate cache eviction occurs if the path shares any storage with other data or applications. ■ NetBackup manages the files in the local cache directory. Users should not manually delete files in this directory.
Media server name	Select a NetBackup media server from the drop-down list. Only the media servers that conform to the requirements for cloud storage appear in the drop-down list. The requirements are described in the following topic: See "About the NetBackup media servers for cloud storage" on page 102. 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.

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

Field name	Required content
Storage Account	Enter the storage account that you want to use for your cloud backups. For more information about Microsoft Azure storage service, refer to the Microsoft Azure documentation. http://azure.microsoft.com Create the storage account using the following URL: https://portal.azure.com
Access key	Enter your Azure access key. You can enter the primary access key or the secondary access key. It must be 100 or fewer characters. Refer to the following URL for the access key: https://portal.azure.com
Advanced Settings	To change SSL or proxy settings for Azure, click **Advanced Settings**. See "Microsoft Azure advanced server configuration options" on page 57.

Microsoft Azure advanced server configuration options

The following table describes the SSL and proxy options that are specific to all Microsoft Azure compatible cloud providers. These options appear on the **Advanced Server Configuration** dialog box.

Table 2-21 General settings options

Option	Description
Use SSL	Select this option if you want to use the SSL (Secure Sockets Layer) protocol for user authentication or data transfer between NetBackup and cloud storage provider. ■ **Authentication only** - Select this option, if you want to use SSL only at the time of authenticating users while they access the cloud storage. ■ **Data Transfer** - Select this option, if you want to use SSL to authenticate users and transfer the data from NetBackup to the cloud storage. **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 fails in the SSL mode.

Table 2-22 Proxy Settings tab options

Option	Description
Use Proxy Server	**Use Proxy Server** option to use proxy server and provide proxy server settings. Once you select the **Use Proxy Server** option, you can specify the following details: ■ **Proxy Host**–Specify IP address or name of the proxy server. ■ **Proxy Port**–Specify port number of the proxy server. ■ **Proxy Type**– You can select one of the following proxy types: ■ **HTTP** **Note:** You need to provide the proxy credentials for HTTP proxy type. ■ **SOCKS** ■ **SOCKS4** ■ **SOCKS5** ■ **SOCKS4A**
Use Proxy Tunneling	You can enable proxy tunneling for HTTP proxy type. After you enable **Use Proxy Tunneling**, HTTP CONNECT requests are send from the cloud media server to the HTTP proxy server and the TCP connection is directly forwarded to the cloud back-end storage. The data passes through the proxy server without reading the headers or data from the connection.

Table 2-22 Proxy Settings tab options *(continued)*

Option	Description
Authentication Type	You can select one of the following authentication types if you are using HTTP proxy type. ■ **None**– Authentication is not enabled. Username and password is not required. ■ **NTLM**–Username and password needed. ■ **Basic**–Username and password needed. **Username** is the username of the proxy server **Password** can be empty. You can use maximum 256 characters.

About OpenStack Swift cloud storage API type

NetBackup supports cloud storage from the vendors that use the OpenStack Swift storage API for their storage. Information about the requirements and configuration options for the OpenStack Swift storage API vendors is provided as follows:

Table 2-23 OpenStack Swift storage API type information and topics

Information	Topic
Certified vendors	See "OpenStack Swift cloud storage vendors certified for NetBackup" on page 60.
Requirements	See "OpenStack Swift storage type requirements" on page 60.
Storage server configuration options	See "OpenStack Swift cloud storage provider options" on page 61.
Region and host configuration options	See "OpenStack Swift storage region options" on page 65.
Cloud instance configuration options	See "OpenStack Swift add cloud storage configuration options" on page 67.
Proxy connection options	See "OpenStack Swift proxy settings" on page 67.

Rackspace Cloud Files is a special case, described in the following topics:

- See "About Rackspace Cloud Files storage requirements" on page 68.
- See "Rackspace storage server configuration options" on page 69.

- See "About private clouds from Rackspace" on page 72.

OpenStack Swift cloud storage vendors certified for NetBackup

Table 2-24 identifies the OpenStack Swift compliant cloud vendors who are certified for NetBackup as of the NetBackup 8.1 release. The cloud vendors achieve certification by participating in the Veritas Technology Partner Program (VTPP).

Table 2-24 OpenStack Swift compliant cloud vendors that NetBackup supports

Cloud vendor	Notes
Oracle	As of this release of NetBackup, NetBackup supports only authentication V1.
Rackspace Cloud Files	Rackspace Cloud Files is a special case, described in the following topics: ■ See "About Rackspace Cloud Files storage requirements" on page 68. ■ See "Rackspace storage server configuration options" on page 69. ■ See "About private clouds from Rackspace" on page 72.
SwiftStack	No notes for OpenStack Swift. NetBackup also supports SwiftStack with Amazon S3 storage API type. See "About the Amazon S3 cloud storage API type" on page 17.
IBM Softlayer	No notes.
FUJITSU Cloud Service K5	No notes.

Note: Veritas may certify vendors between NetBackup releases. If your cloud storage vendor is not listed in this table, see the following webpage for the most up-to-date list of supported cloud vendors:

http://www.veritas.com/docs/000115793

OpenStack Swift storage type requirements

The following table provides links to the details and requirements of OpenStack Swift compatible cloud.

Table 2-25 OpenStack Swift compatible cloud storage requirements

Requirement	Details
License requirement	You must have a NetBackup license that allows for cloud storage.
Storage account requirements	You must obtain the credentials required to access the cloud storage account. If you use authentication V1, only the user name and password are required to validate the user to access the cloud storage. If you use authentication version Identity V2, the user name, password, and either tenant ID or tenant name is required to validate the user to access the cloud storage.
Containers	The containers for OpenStack Swift compliant cloud providers cannot be created in NetBackup. You must use the native cloud tools to create a container. The container names must conform to the following requirements: ■ The container name must be between 3 and 255 characters. ■ Any of the 26 lowercase (small) letters of the International Standards Organization (ISO) Latin-script alphabet. These are the same lowercase (small) letters as the English alphabet. ■ Any integer from 0 to 9, inclusive. ■ Any of the following characters (you cannot use these as the first character in the container name): Period (.), underscore (_), and dash (-). *Exception*: If you use SSL for communication, you cannot use a period. By default, NetBackup uses SSL for communication. See "NetBackup cloud storage server connection properties" on page 117. **Note:** Only those containers are listed in NetBackup that follow these naming conventions.

OpenStack Swift cloud storage provider options

Figure 2-5 shows the cloud storage provider wizard panel for OpenStack Swift-compliant cloud storage. The panel includes cloud provider and access information.

Figure 2-5 Cloud Storage Server Configuration Wizard panel

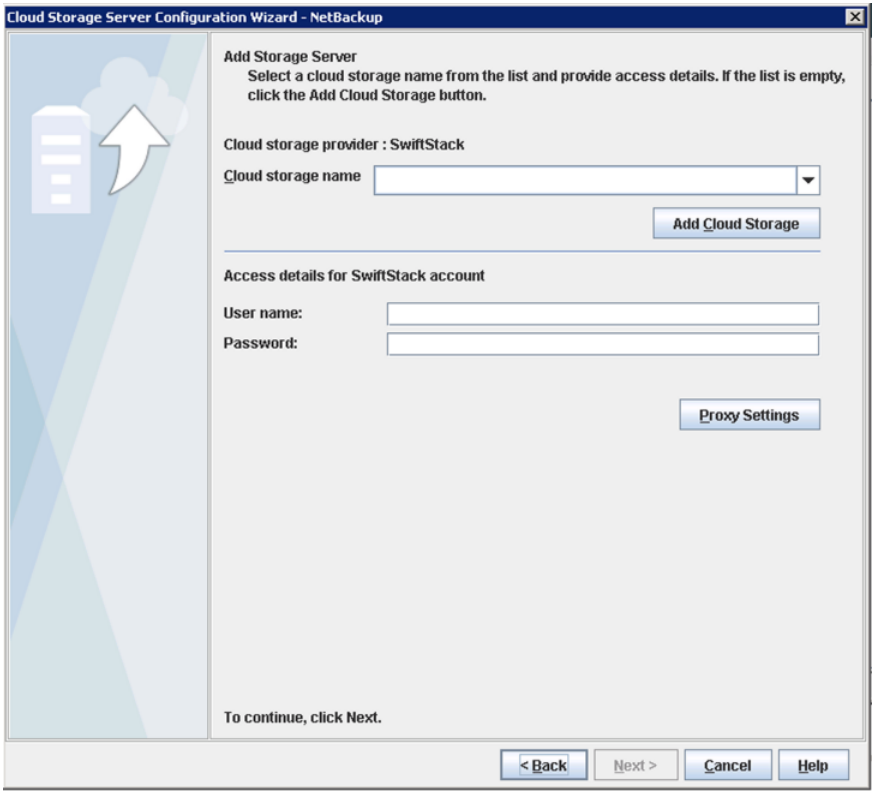


Table 2-26 describes configuration options for OpenStack Swift cloud storage.

Table 2-26 OpenStack Swift provider and access details

Field name	Required content
Cloud storage provider	Displays the name of the selected cloud provider.
Cloud storage name	Select the cloud storage name from the list. If the list is empty, you must add a cloud storage instance. See the **Add Cloud Storage** option description.
Add Cloud Storage	Click the add cloud storage option, then add, select, or enter the required information. See "OpenStack Swift add cloud storage configuration options" on page 67.

Table 2-26 OpenStack Swift provider and access details *(continued)*

Field name	Required content
Tenant ID / Tenant Name	Based on the selection, enter either the tenant ID or tenant name that is associated with your cloud storage credentials. **Note:** This field is visible only if you selected the **Identity v2 Authentication version** in the **Add Cloud Storage** dialog box. See "OpenStack Swift add cloud storage configuration options" on page 67.
User name	Enter the user name that is required to access the cloud storage.
Password	Enter the password that is required to access the cloud storage. It must be 100 or fewer characters.
Proxy Settings	To change the default storage server for your cloud vendor or specify the maximum number of network connections, click **Advanced Settings**.
User ID	Based on the selection, enter either the User ID or the User Name that is associated with your cloud storage credentials. When you provide User ID, User Name and Domain information is not required. **Note:** This field is visible only if you selected the Identity v3 Authentication version in the **Authentication version** dialog box. See "OpenStack Swift add cloud storage configuration options" on page 67.
Domain ID / Domain name (for user details)	Based on the selection, enter either the user's Domain ID or Domain Name that is associated with your cloud storage credentials. **Note:** This field is visible only if you selected the Identity v3 Authentication version in the **Authentication version** dialog box. See "OpenStack Swift add cloud storage configuration options" on page 67.
Project ID / Project Name	Based on the selection, enter either the Project ID or Project Name that is associated with your cloud storage credentials. When you provide Project ID, Project Name and Domain information is not required. **Note:** This field is visible only if you selected the Identity v3 Authentication version in the **Authentication version** dialog box. See "OpenStack Swift add cloud storage configuration options" on page 67.

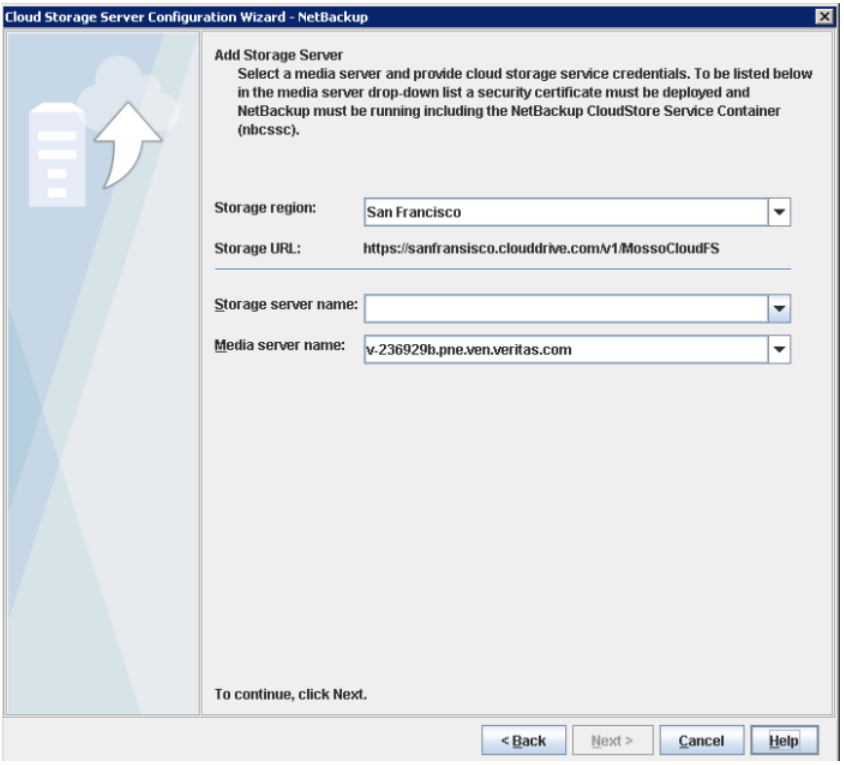
Table 2-26 OpenStack Swift provider and access details *(continued)*

Field name	Required content
Domain ID / Domain name(for project details)	Based on the selection, enter either the project's Domain ID or Domain Name that is associated with your cloud storage credentials. **Note:** This field is visible only if you selected the Identity v3 Authentication version in the **Authentication version** dialog box. See "OpenStack Swift add cloud storage configuration options" on page 67.
Deduplication	Enabling this option creates a CloudCatalyst storage server that can be used to upload deduplicated data to the cloud. This option is grayed out if any of the following cases are true: ■ The selected media server does not have NetBackup 8.1 or later installed. ■ CloudCatalyst does not support the media server operating system. ■ CloudCatalyst does not support the cloud vendor. See the NetBackup compatibility lists for support information: http://www.netbackup.com/compatibility For information about CloudCatalyst, see the *NetBackup Deduplication Guide*: http://www.veritas.com/docs/DOC5332
Local cache directory	Enter the mount path to be used as the storage path on the CloudCatalyst storage server. For example: `/space/mnt/esfs` The deduplicated data is written to this local cache directory before it is uploaded to the cloud. The larger the cache, the more likely that NetBackup can service requests locally, avoiding cloud access to read and write. Notes: ■ This path should be to a file system which is dedicated for CloudCatalyst cache use. Inaccurate cache eviction occurs if the path shares any storage with other data or applications. ■ NetBackup manages the files in the local cache directory. Users should not manually delete files in this directory.

OpenStack Swift storage region options

Figure 2-6 shows the storage region wizard panel for OpenStack Swift-compliant cloud storage. The panel includes storage region and storage host information.

Figure 2-6 Cloud Storage Server Configuration Wizard panel



Provider and access details are used to map the cloud storage settings to NetBackup storage settings. The cloud storage region is mapped to the NetBackup storage server. All the backups that are targeted to the NetBackup storage server use the cloud storage region to which it is mapped.

Note: One cloud storage region is mapped to one NetBackup storage server.

Table 2-27 describes configuration options for OpenStack Swift cloud storage.

Table 2-27 OpenStack Swift region and host details

Field name	Description
Storage region	Select the cloud storage region. You may use the cloud storage region that is geographically closest to the NetBackup media server that sends the backups to the cloud. Contact your storage administrator for more details. **Note:** This field is visible only if you selected the **Identity v2 Authentication version** in the **Add Cloud Storage** dialog box. See "OpenStack Swift add cloud storage configuration options" on page 67.
Storage URL	The cloud storage URL is auto-populated based on the storage region selection. This field is non-editable and is only for your reference. **Note:** This field is visible only if you selected the **Identity v2 Authentication version** in the **Add Cloud Storage** dialog box. See "OpenStack Swift add cloud storage configuration options" on page 67.
Storage server name	Enter a unique name for the storage server. **Note:** Veritas recommends that a storage server name that you add while configuring an OpenStack Swift compatible cloud provider should be a logical name and should not match a physical host name. For example: When you add an Oracle storage server, avoid using names like 'oracle.com' or 'oracle123.com'. These servers may be physical hosts, which can cause failures during cloud storage configuration. Instead, use storage server names like 'oracle1' or 'oracleserver1' and so on.
Media server name	Select a NetBackup media server from the drop-down list. The drop-down list displays only NetBackup 8.1 and later media servers. In addition, only the media servers that conform to the requirements for cloud storage appear in the drop-down list. The requirements are described in the following topic: See "About the NetBackup media servers for cloud storage" on page 102. 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.

OpenStack Swift add cloud storage configuration options

The following table describes the configuration options for the **Add Cloud Storage** dialog box. It appears when you click **Add Cloud Storage** on the wizard panel for OpenStack providers.

Table 2-28 Add Cloud Storage

Field	Description
Cloud storage provider	The cloud storage provider from the previous wizard panel is displayed.
Cloud storage name	Enter a unique name to identify the authentication service endpoint. You can reuse the same authentication service endpoint for another storage server.
Authentication location	This field is not visible for cloud providers with custom authentication URLs. Select the authentication location of the cloud storage, otherwise, select **Other**. **Note:** If you select **Other**, you must enter the authentication URL.
Authentication version	Select the authentication version that you want to use. Select **Do not use identity service** if you do not want to authenticate using the OpenStack's Identity APIs.
Authentication URL	Enter the authentication URL that your cloud vendor provided. Authentication URL comprises of either HTTP or HTTPS and port number. For example, http://mycloud.example.com:5000/v2.0/tokens

OpenStack Swift proxy settings

For security purpose, you can use a proxy server to establish communication with the cloud storage.

The following table describes the options of the **Proxy Settings** dialog box.

Table 2-29 Proxy settings for OpenStack Swift

Option	Description
Use Proxy Server	**Use Proxy Server** option to use proxy server and provide proxy server settings. Once you select the **Use Proxy Server** option, you can specify the following details: ■ **Proxy Host**–Specify IP address or name of the proxy server. ■ **Proxy Port**–Specify port number of the proxy server. Possible values: 1-65535 ■ **Proxy Type**– You can select one of the following proxy types: ■ **HTTP** **Note:** You need to provide the proxy credentials for HTTP proxy type. ■ **SOCKS** ■ **SOCKS4** ■ **SOCKS5** ■ **SOCKS4A**
Use Proxy Tunneling	You can enable proxy tunneling for HTTP proxy type. After you enable **Use Proxy Tunneling**, HTTP CONNECT requests are send from the cloud media server to the HTTP proxy server and the TCP connection is directly forwarded to the cloud back-end storage. The data passes through the proxy server without reading the headers or data from the connection.
Authentication Type	You can select one of the following authentication types if you are using HTTP proxy type. ■ **None**– Authentication is not enabled. Username and password is not required. ■ **NTLM**–Username and password needed. ■ **Basic**–Username and password needed. **Username** is the username of the proxy server **Password** can be empty. You can use maximum 256 characters.

About Rackspace Cloud Files storage requirements

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

Table 2-30 describes the details and requirements of Rackspace CloudFiles.

Table 2-30 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.
Storage requirements	The following are the requirements for Rackspace CloudFiles: ■ You must have a NetBackup license that allows for cloud storage. ■ 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 Veritas 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: ■ 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: `~!@#$%^&*()- _+=|\\[]{}':;?><.,

See “Rackspace storage server configuration options” on page 69.

NetBackup supports the private clouds from the supported cloud providers.

See “About private clouds from Rackspace” on page 72.

Rackspace storage server configuration options

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

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

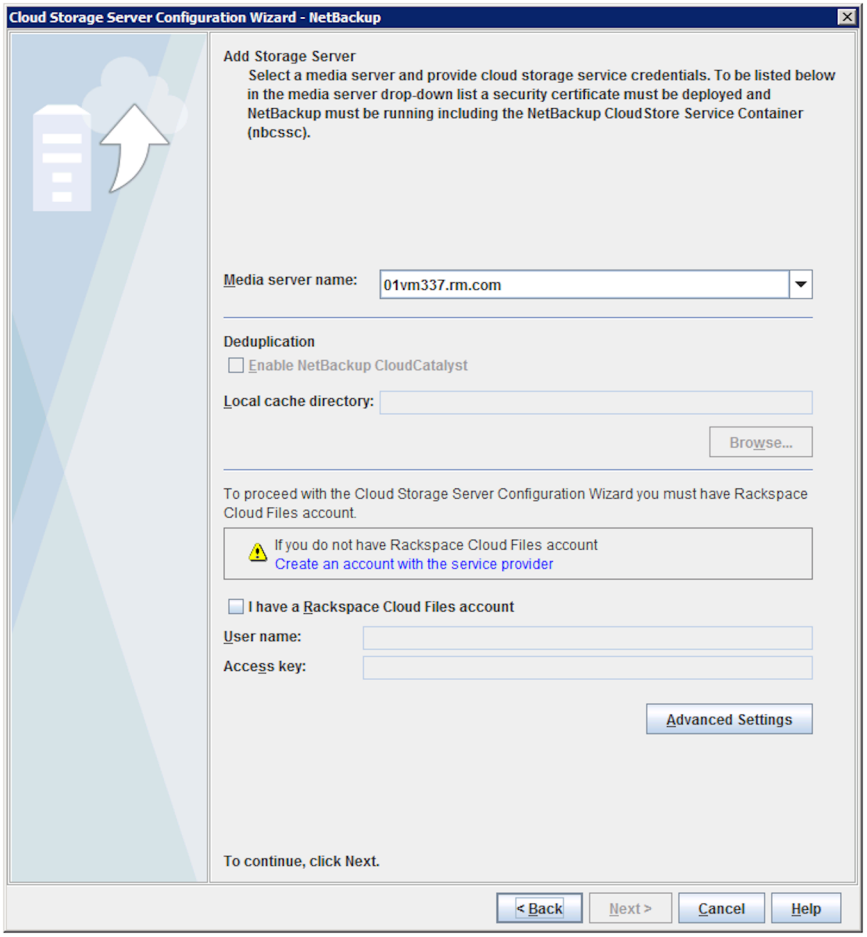


Table 2-31 describes the configuration options for Rackspace cloud storage.

Table 2-31 Rackspace storage server configuration options

Field name	Required content
Media Server Name	Select a NetBackup media server from the drop-down list. Only the media servers that conform to the requirements for cloud storage appear in the drop-down list. The requirements are described in the following topic: See "About the NetBackup media servers for cloud storage" on page 102. 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.
Deduplication	Enabling this option creates a CloudCatalyst storage server that can be used to upload deduplicated data to the cloud. This option is grayed out if any of the following cases are true: ■ The selected media server does not have NetBackup 8.1 or later installed. ■ CloudCatalyst does not support the media server operating system. ■ CloudCatalyst does not support the cloud vendor. See the NetBackup compatibility lists for support information: http://www.netbackup.com/compatibility For information about CloudCatalyst, see the *NetBackup Deduplication Guide*: http://www.veritas.com/docs/DOC5332
Local cache directory	Enter the mount path to be used as the storage path on the CloudCatalyst storage server. For example: `/space/mnt/esfs` The deduplicated data is written to this local cache directory before it is uploaded to the cloud. The larger the cache, the more likely that NetBackup can service requests locally, avoiding cloud access to read and write. Notes: ■ This path should be to a file system which is dedicated for CloudCatalyst cache use. Inaccurate cache eviction occurs if the path shares any storage with other data or applications. ■ NetBackup manages the files in the local cache directory. Users should not manually delete files in this directory.
Create an account with the service provider	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.
I have a Rackspace Cloud Files account	Select **I have a Rackspace Cloud Files account** to enter the required account information.

Table 2-31 Rackspace storage server configuration options *(continued)*

Field name	Required content
User Name	Enter your Rackspace Cloud Files account user name. If you do not have an account, click **Create an account with the service provider** link.
Access Key	Enter your Rackspace Cloud Files account access key. It must be 100 or fewer characters.
Advanced Settings	To change the default storage server for your cloud vendor or specify the maximum number of network connections, click **Advanced Settings**. See "About private clouds from Rackspace" on page 72.

About private clouds from Rackspace

NetBackup supports the private clouds from Rackspaces. 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/openv/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 105.

Chapter 3

Configuring cloud storage in NetBackup

This chapter includes the following topics:

- NetBackup cloud storage server properties
- About cloud storage disk pools
- Configuring a disk pool for cloud storage
- 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
- Managing Certification Authorities (CA) for NetBackup Cloud

Before you begin to configure cloud storage in NetBackup

Veritas recommends that you do the following before you begin to configure cloud storage in NetBackup:

- Review the NetBackup configuration options for your cloud storage vendor.
  NetBackup supports cloud storage based on the storage API type, and Veritas organizes the information that is required to configure cloud storage by API type. The API types, the vendors who use those API types, and links to the required configuration information are in the following topic:
  See "About the cloud storage vendors for NetBackup" on page 15.

  Note: Veritas may certify vendors between NetBackup releases. If your cloud storage vendor is not listed in the NetBackup product documentation, see the following webpage for the most up-to-date list of supported cloud vendors:

  http://www.veritas.com/docs/000115793

- Collect the information that is required to configure cloud storage in NetBackup. If you have the required information organized by the NetBackup configuration options, the configuration process may be easier than if you do not.

Configuring cloud storage in NetBackup

This topic describes how to configure cloud storage in NetBackup. Table 3-1 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.veritas.com/docs/DOC5332

Table 3-1 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 167. See "Creating NetBackup log file directories for cloud storage" on page 167.
Step 2	Review the cloud installation requirements	See "Cloud installation requirements" on page 77.
Step 3	Determine the requirements for provisioning and configuring your cloud storage provider in NetBackup	See "About the cloud storage vendors for NetBackup" on page 15.
Step 4	Configure the global cloud storage host properties as necessary	See "Scalable Storage properties" on page 78.
Step 5	Configure the Cloud Storage properties	Optionally, add a cloud storage service host using the NetBackup host properties. See "Cloud Storage properties" on page 83.
Step 6	Understand the role of the CloudStore Service Container	See "About the NetBackup CloudStore Service Container" on page 88.
Step 7	Provision a security certificate for authentication on the media servers	See "NetBackup CloudStore Service Container security certificates" on page 89. See "Deploying host name-based certificates" on page 93.
Step 8	Understand key management for encryption	Encryption is optional. See "About data encryption for cloud storage" on page 97. See "About key management for encryption of NetBackup cloud storage" on page 98.

Table 3-1 Overview of the NetBackup cloud configuration process *(continued)*

Step	Task	More information
Step 9	Configure the storage server	See "About cloud storage servers" on page 99. See "Adding a cloud storage instance" on page 85. See "Configuring a storage server for cloud storage" on page 105. See "About object size for cloud storage" on page 100.
Step 10	Configure the disk pool	See "About cloud storage disk pools" on page 123. See "Configuring a disk pool for cloud storage" on page 124.
Step 11	Configure additional storage server properties	See "NetBackup cloud storage server properties" on page 112. See "Changing cloud storage server properties" on page 110.
Step 12	Add additional media servers	Adding additional media servers is optional. See "About the NetBackup media servers for cloud storage" on page 102. See "Adding backup media servers to your cloud environment" on page 135.
Step 13	Configure a storage unit	See "Configuring a storage unit for cloud storage" on page 136.
Step 14	Configure NetBackup Accelerator and optimized synthetic backups	Accelerator and optimzed synthetic backups are optional. See "About NetBackup Accelerator and NetBackup Optimized Synthetic backups" on page 141. See "Enabling NetBackup Accelerator with cloud storage" on page 141. See "Changing cloud storage server properties" on page 110.
Step 15	Configure a backup policy	See "Creating a backup policy" on page 145.

Cloud installation requirements

When you develop a plan to implement a NetBackup Cloud solution, use Table 3-2 to assist with your plan.

Table 3-2 Cloud installation requirements

Requirement	Details
NetBackup media server platform support	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 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.
Cloud storage provider account	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. You can create this account in the Cloud Storage Configuration Wizard. See "About the cloud storage vendors for NetBackup" on page 15.
NetBackup cloud storage licensing	NetBackup cloud storage is licensed separately from base NetBackup. The license also enables the **Use Accelerator** feature on the NetBackup policy **Attributes** tab. Accelerator increases the speed of full backups for files systems.

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 the host is supported for cloud storage. See the NetBackup hardware compatibility list for your release available through the following URL:

http://www.netbackup.com/compatibility

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

Figure 3-1 Scalable Storage Cloud Settings host properties

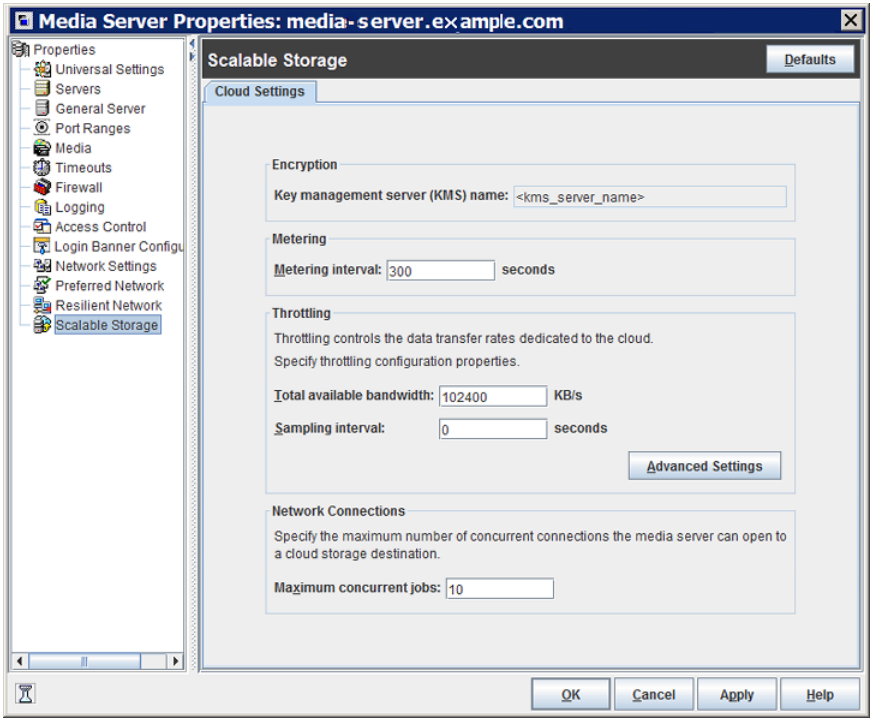


Table 3-3 describes the properties.

Table 3-3 Scalable Storage Cloud Settings 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 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. If this value is zero, throttling is disabled.

Table 3-3 Scalable Storage Cloud Settings host properties *(continued)*

Property	Description
Advanced Settings	Click **Advanced Settings** to specify additional settings for throttling. See "Configuring advanced bandwidth throttling settings" on page 80. See "Advanced bandwidth throttling settings" on page 81.
Maximum concurrent jobs	The default maximum number of concurrent jobs that the media server can run for the cloud storage server. 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. 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. You can configure job limits per backup policy and per storage unit. **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. If the media server is not a CloudCatalyst storage server, a value over 100 is generally not needed. If the media server is a CloudCatalyst storage server, change the value to 160 or more.

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 78.

To configure advanced bandwidth throttling settings

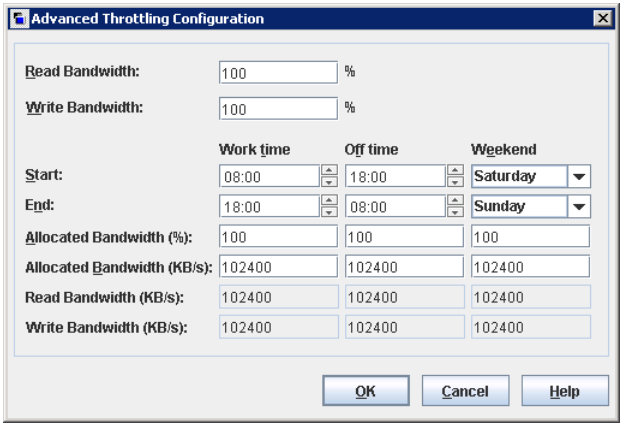
1. In the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > Media Servers** in the left pane.
2. In the right pane, select the host on which to specify properties.

3 Click **Actions** > **Properties**.

4 In the properties dialog box left pane, select **Scalable Storage**.

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

The following is an example of the dialog box:



6 Configure the settings and then click **OK**.

See “Advanced bandwidth throttling settings” on page 81.

Advanced bandwidth throttling settings

The following table describes the advanced bandwidth throttling settings.

Table 3-4 Advanced Throttling Configuration settings

Property	Description
Read Bandwidth	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. 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. Consider the total load of simultaneous jobs on multiple media servers when you calculate the required bandwidth. Default value: `100` Possible values: `0` to `100`

Table 3-4 Advanced Throttling Configuration settings *(continued)*

Property	Description
Write Bandwidth	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. If there is insufficient bandwidth to transmit the specified amount of data within a few minutes, backup failures may occur due to timeouts. Consider the total load of simultaneous jobs on multiple media servers when you calculate the required bandwidth. Default value: `100` Possible values: `0` to `100`
Work time	Use this field to specify the time interval that is considered work time for the cloud connection. Specify a start time and end time in 24-hour format. For example, 2:00 P.M. is 14:00. 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.
Off time	Use this field to specify the time interval that is considered off time for the cloud connection. Specify a start time and end time in 24-hour format. For example, 2:00 P.M. is 14:00. 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.
Weekend	Specify the start and stop time for the weekend. 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.

Table 3-4 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.

Cloud Storage properties

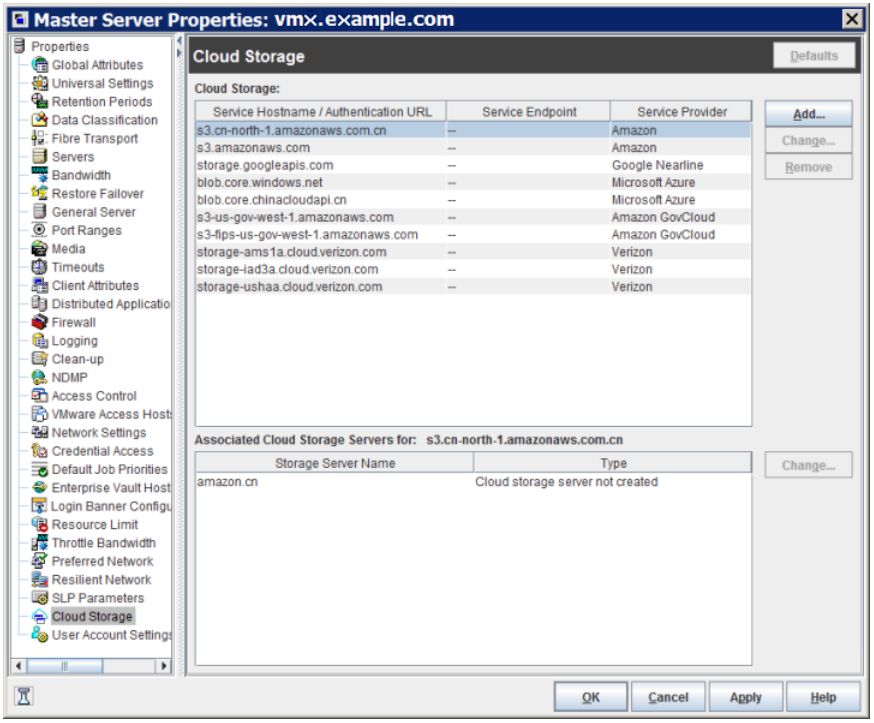
The NetBackup **Cloud Storage** properties in the **NetBackup Administration Console** apply to the currently selected master server.

The hosts that appear in this **Cloud Storage** list are available to select when you configure a storage server. The **Service Provider** type of your cloud vendor determines whether a service host is available or required.

NetBackup includes service hosts for some cloud storage providers. You can add a new host to the **Cloud Storage** list if the **Service Provider** type allows it. If you add a host, you also can change its properties or delete it from the **Cloud Storage** list. (You cannot change or delete the information that is included with NetBackup.)

If you do not add a service host to this **Cloud Storage** list, you can add one when you configure the storage server. The **Service Provider** type of your cloud vendor determines whether a **Service Hostname** is available or required.

Figure 3-2 Cloud Storage host properties



Cloud Storage host properties contain the following properties:

Table 3-5 Cloud Storage

Property	Description
Cloud Storage	The cloud storage that corresponds to the various cloud service providers that NetBackup supports are listed here. See "Adding a cloud storage instance" on page 85. See "Changing cloud storage host properties" on page 86. See "Deleting a cloud storage host instance" on page 87.
Associated Storage Servers for	The cloud storage servers that correspond to the selected cloud storage are displayed. See "Changing cloud storage host properties" on page 86.

Note: Changes that you make in the **Cloud Storage** dialog box are applied before you click **OK** in the **Host Properties** dialog box.

Adding a cloud storage instance

You may have to add a custom cloud storage instance before you configure a NetBackup cloud storage server. A custom cloud storage allows customization, such as a different service host or other properties. A custom cloud storage instance appears in the **Cloud Storage Server Configuration Wizard** when you configure a storage server.

The cloud storage provider type determines if you have to add a custom cloud storage instance.

See "About the cloud storage vendors for NetBackup" on page 15.

You can add a custom cloud storage instance as follows:

By using NetBackup **Master Server Properties**	With this method, you add the cloud storage instance before you configure the storage server in NetBackup. Then, the wizard that configures the storage is populated with the instance details. You select the instance when you configure the storage server. See "To add a cloud storage instance in Cloud Storage host properties" on page 85.
By using the **Cloud Storage Server Configuration Wizard**	With this method, you add the instance at the same time as when you configure the storage server in NetBackup. The wizard that configures the storage is *not* populated with the instance details until you add them in the wizard itself. See "Configuring a storage server for cloud storage" on page 105.

To add a cloud storage instance in Cloud Storage host properties

1. In the **NetBackup Administration Console**, expand **NetBackup Management** > **Host Properties** > **Master Servers** in the left pane.
2. In the right pane, select the master server on which to add the cloud storage instance.
3. On the **Actions** menu, click **Properties**.
4. In the properties dialog box left pane, select **Cloud Storage**.
5. In the right pane, click **Add**.

6 In the **Add Cloud Storage** dialog box, configure the settings.

See "Amazon S3 cloud storage options" on page 28.

7 After you configure the settings, click **OK**.

Changing cloud storage host properties

From the **Cloud Storage Master Server Properties**, you can change the following properties:

Cloud Storage properties	You can change the properties of a host that you add. (You cannot change or delete the properties of the cloud storage providers that are included with NetBackup.) See "To change cloud storage host properties" on page 86.
Associated cloud storage server properties	See "To change associated cloud storage server host properties" on page 86.

How to change cloud storage *server* properties is described in a different topic.

See "Changing cloud storage server properties" on page 110.

To change cloud storage host properties

1 In the **NetBackup Administration Console**, expand **NetBackup Management** > **Host Properties** > **Master Servers** in the left pane.

2 In the right pane, select the master server on which to specify properties.

3 On the **Actions** menu, click **Properties**.

4 In the left pane of the **Master Server Properties** dialog box, select **Cloud Storage**.

5 In the **Cloud Storage** list in the right pane, select the wanted cloud storage.

6 Click **Change** adjacent to the **Cloud Storage** list.

7 In the **Change Cloud Storage** dialog box, change the properties.

See "Amazon S3 cloud storage options" on page 28.

8 Click **OK** in the **Change Cloud Storage** dialog box.

9 Click **OK** to close the **Master Server Properties** dialog box.

To change associated cloud storage server host properties

1 In the **NetBackup Administration Console**, expand **NetBackup Management** > **Host Properties** > **Master Servers** in the left pane.

2 In the right pane, select the master server on which to specify properties.

3 On the **Actions** menu, click **Properties**.

4 In the left pane of the **Master Server Properties** dialog box, select **Cloud Storage**.

5 In the **Associated Cloud Storage Servers for** list in the right pane, select the wanted storage server.

6 Click **Change** adjacent to the **Associated Cloud Storage Servers for** list.

7 In the **Cloud Storage Server Configuration** dialog box, change the properties.

See "Amazon S3 advanced server configuration options" on page 30.

See "Amazon S3 credentials broker details" on page 33.

8 Click **OK** in the **Change Cloud Storage** dialog box.

9 Click **OK** to close the **Master Server Properties** dialog box.

Deleting a cloud storage host instance

You can delete your custom cloud storage (cloud instance) by using the **Cloud Storage Master Server Properties**. You cannot delete the cloud storage instances that were delivered with NetBackup.

See "Cloud Storage properties" on page 83.

To delete a cloud storage host instance

1 In the **NetBackup Administration Console**, expand **NetBackup Management** > **Host Properties** > **Master Servers** in the left pane.

2 In the right pane, select the master server on which to specify properties.

3 On the **Actions** menu, click **Properties**.

4 In the left pane of the **Master Server Properties** dialog box, select **Cloud Storage**.

5 In the **Cloud Storage** list in the right pane, select the wanted cloud storage.

6 Click **Remove**.

7 In the **Remove the Cloud Storage** dialog box, click **Yes**.

8 Click **OK** to close the **Master Server Properties** dialog box.

About the NetBackup CloudStore Service Container

The NetBackup CloudStore Service Container (`nbcssc`) is a web-based service container that runs on the following NetBackup hosts:

- The NetBackup master server.
  In a NetBackup master server cluster environment, the NetBackup CloudStore Service Container is a highly available service. In case of a NetBackup resource group failover, this service fails over to another node.
- The NetBackup media servers that are 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 NetBackup CloudStore Service Container behavior by using the **Scalable Storage** host properties in the **NetBackup Administration Console**.

See "Scalable Storage properties" on page 78.

The default port number for the NetBackup CloudStore Service Container service is 5637.

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

Security certificates	The NetBackup hosts on which the NetBackup CloudStore Service Container runs must be provisioned with a security certificate or certificates. See "NetBackup CloudStore Service Container security certificates" on page 89. **Note:** You do not need to generate a security certificate, if you have already generated it before configuring the cloud storage.
Security modes	The NetBackup CloudStore Service Container can run in different security modes. See "NetBackup CloudStore Service Container security modes" on page 90.

See "About the NetBackup media servers for cloud storage" on page 102.

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 8.0 and later	The NetBackup hosts that run the CloudStore Service Container require both a host ID-based certificate and a host name-based certificate. You may have to install the certificates on those hosts. See "Deploying host name-based certificates" on page 93. See "Deploying host ID-based certificates" on page 94. If the NetBackup master server is clustered, you must ensure that the active node and the passive nodes have both host named-based and host-ID based certificates. See the *NetBackup Security and Encryption Guide* for NetBackup 8.0 or later: http://www.veritas.com/docs/DOC5332
NetBackup 7.7 and 7.7.*x*	The NetBackup hosts that run the CloudStore Service Container require a host name-based certificate. You must use a command to install it on a media server. See "Deploying host name-based certificates" on page 93. **Note:** You do not need to generate a security certificate, if you have already generated it before configuring the cloud storage. The host name-based security certificates expire after one year. NetBackup automatically replaces existing certificates with new ones as needed. **Note:** The security certificates that are provisioned for other NetBackup features or purposes satisfy the certificate requirement for the NetBackup CloudStore Service Container. The NetBackup Access Control feature uses security certificates, and the NetBackup Administration Console requires security certificates for interhost communication. If the NetBackup master server is clustered, you must ensure that the active node and the passive node have host named-based certificates. See the 7.7.*x* version of the *NetBackup Security and Encryption Guide*

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/openv/var/vxss/credentials` ■ Windows: *`install_dir`*`\Veritas\NetBackup\var\VxSS\credentials`

See "About the NetBackup CloudStore Service Container" on page 88.

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 64, secure communication.

See "NetBackup cloudstore.conf configuration file" on page 90.

See "About the NetBackup CloudStore Service Container" on page 88.

NetBackup cloudstore.conf configuration file

Table 3-6 describes the `cloudstore.conf` configuration file parameters.

The `cloudstore.conf` file is available on the master server and all the media servers that are installed on the platforms that NetBackup cloud supports.

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/openv/netbackup/db/cloud`

- Windows: *install_path*\Netbackup\db\cloud

Table 3-6 `cloudstore.conf` configuration file parameters and descriptions

Parameter	Description
`CSSC_VERSION`	Veritas recommends that you do not modify this value. Specifies the version of `cloudstore.conf` file. The default value is 2.
`CSSC_PLUGIN_PATH`	Veritas 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: *install_path*\Veritas\NetBackup\bin\ost-plugins On UNIX: `/usr/openv/lib/ost-plugins`
`CSSC_PORT`	Specifies the port number for the CloudStore Service Container (`nbcssc`). The default value is 5637.
`CSSC_LOG_DIR`	Specifies the directory path where `nbcssc` generates log files. The default path is as follows: On Windows: *install_path*\Veritas\NetBackup\logs\nbcssc On UNIX: `/usr/openv/netbackup/logs/nbcssc`
`CSSC_LOG_FILE`	Specifies the file name that the `nbcssc` 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 `nbcssc` service runs in secure (value 64) or non-secure mode (value 0). The default value is 64.

Table 3-6 `cloudstore.conf` configuration file parameters and descriptions *(continued)*

Parameter	Description
`CSSC_CIPHER_LIST`	Specifies the cipher list that NetBackup uses for the following purpose: ■ The cloud master host's cipher is used for communicating with the `nbcssc` service and for communication with the cloud service provider. ■ The media server cipher is used for communicating with the cloud master host's `nbcssc` service. Veritas recommends that you do not modify this value. However, if you want to customize the cipher list, depending on the purpose, you must modify the cipher list in the `cloudstore.conf` on the master server and the media servers. **Note:** If the cipher list is invalid, the customized cipher list is replaced by the default cipher list. The default value is `AES:!aNULL:@STRENGTH`.
`CSSC_LOG_LEVEL`	Specifies the log level for `nbcssc` 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 `nbcssc` service runs. The default value is 5637.
`CSSC_MASTER_NAME`	Specifies the NetBackup master server name. This entry indicates that the `nbcssc` service runs on this host. It processes all cloud provider-specific requests based on the `CloudProvider.xml` and `CloudInstance.xml` files that reside at the following location: On Windows: *`install_path`*`\Netbackup\db\cloud` On UNIX: `/usr/openv/netbackup/db/cloud`
`CSSC_MASTER_IS_SECURE`	Specifies if the `nbcssc` service is running in secure (value 64) or non-secure mode (value 0) on the NetBackup master server. The default value is 64.

Table 3-6 `cloudstore.conf` configuration file parameters and descriptions *(continued)*

Parameter	Description
`CSSC_LEGACY_AUTH_ENABLED`	Specifies if the `nbcssc` service has the legacy authentication enabled (value 1) or disabled (0). The default value is 0. **Note:** Starting from NetBackup 8.1, the `CSSC_LEGACY_AUTH_ENABLED` option is deprecated. To communicate with legacy media servers, use the **Enable insecure communication with 8.0 and earlier hosts** option on the NetBackup master server. The option is available in the **NetBackup Administration Console** on the **Security Management > Global Security Settings > Secure Communication** tab.

Deploying host name-based certificates

You can deploy the required host name-based security certificate for the NetBackup media servers that you use for cloud storage. Each media server that you use for cloud storage runs the NetBackup CloudStore Service Container.

See "About the NetBackup CloudStore Service Container" on page 88.

You can deploy a certificate for an individual media server or for all media servers. Media servers that you use for cloud storage must have a host name-based security certificate.

Note: Deploying a host name-based certificate is a one-time activity for a host. If a host name-based certificate was deployed for an earlier release or for a hotfix, it does not need to be done again.

Ensure the following before you deploy a host-name based certificate:

- All nodes of the cluster have a host ID-based certificate.
- All Fully Qualified Domain Names (FQHN) and short names for the cluster nodes are mapped to their respective host IDs.

Deploying a host name-based certificate on media servers

This procedure works well when you deploy host name-based security certificates to many hosts at one time. As with NetBackup deployment in general, this method assumes that the network is secure.

To deploy a host name-based security certificate for media servers

1. Run the following command on the master server, depending on your environment. Specify the name of an individual media server or specify `-AllMediaServers`.

   On Windows: *install_path*`\NetBackup\bin\admincmd\bpnbaz -ProvisionCert` *host_name*`|-AllMediaServers`

   On UNIX: `/usr/openv/netbackup/bin/admincmd/bpnbaz -ProvisionCert` *host_name*`|-AllMediaServers`

   NetBackup appliance (as a `NetBackupCLI` user): `bpnbaz -ProvisionCert` *Media_server_name*

2. Restart the NetBackup Service Layer (`nbsl`) service on the media server.

Note: In you use dynamic IPs on the hosts (DHCP), ensure that the host name and the IP address are correctly listed on the master server. To do so, run the following NetBackup `bpclient` command on the master server:

On Windows: *Install_path*`\NetBackup\bin\admincmd\bpclient -L -All`

On UNIX: `/usr/openv/netbackup/bin/admincmd/bpclient -L -All`

Deploying host ID-based certificates

Depending on the certificate deployment security level, a non-master host may require an authorization token before it can obtain a host ID-based certificate from the Certificate Authority (master server). When certificates are not deployed automatically, they must be deployed manually by the administrator on a NetBackup host using the `nbcertcmd` command.

The following topic describes the deployment levels and whether the level requires an authorization token.

Deploying when no token is needed

Use the following procedure when the security level is such that a host administrator can deploy a certificate on a non-master host without requiring an authorization token.

To generate and deploy a host ID-based certificate when no token is needed

1. The host administrator runs the following command on the non-master host to establish that the master server can be trusted:

   ```
   nbcertcmd -getCACertificate
   ```

2 Run the following command on the non-master host:

```
nbcertcmd -getCertificate
```

Note: To communicate with multiple NetBackup domains, the administrator of the host must request a certificate from each master server using the `-server` option.

Run the following command to get a certificate from a specific master server:

```
nbcertcmd -getCertificate -server master_server_name
```

3 To verify that the certificate is deployed on the host, run the following command:

```
nbcertcmd -listCertDetails
```

Deploying when a token is needed

Use the following procedure when the security level is such that a host requires an authorization token before it can deploy a host ID-based certificate from the CA.

To generate and deploy a host ID-based certificate when a token is required

1 The host administrator must have obtained the authorization token value from the CA before proceeding. The token may be conveyed to the administrator by email, by file, or verbally, depending on the various security guidelines of the environment.

2 Run the following command on the non-master host to establish that the master server can be trusted:

```
nbcertcmd -getCACertificate
```

3 Run the following command on the non-master host and enter the token when prompted:

```
nbcertcmd -getCertificate -token
```

Note: To communicate with multiple NetBackup domains, the administrator of the host must request a certificate from each master server using the `-server` option.

If the administrator obtained the token in a file, enter the following:

```
nbcertcmd -getCertificate -file authorization_token_file
```

4 To verify that the certificate is deployed on the host, run the following command:

```
nbcertcmd -listCertDetails
```

Use the `-cluster` option to display cluster certificates.

About data compression for cloud backups

In NetBackup, you can compress your data before you send it to cloud storage server.

You can enable data compression on the NetBackup media server while you configure your cloud storage server using the **Cloud Storage Server Configuration Wizard**.

See "Configuring a storage server for cloud storage" on page 105.

Note: After you have enabled the data compression during the cloud storage configuration, you cannot disable it.

Important notes about data compression in NetBackup

- NetBackup media servers that are older than the 7.7.3 version do not support data compression. Therefore, if you have selected an older media server while you configure the cloud storage server, the compression option does not appear on the **Cloud Storage Server Configuration Wizard**.
- NetBackup uses a third-party library, LZO Pro, with compression level 3. The `bptm` logs provide information of the compression ratio of your data after the backup is taken in the cloud storage.
  See "Viewing the compression ratio" on page 154.
- NetBackup compresses the data in chunks of 256 KB.

- NetBackup Accelerator and True Image Restore (TIR) with move detection is supported with compression.
- The backup data is compressed before it is transmitted to the cloud storage server. If both the compression and the encryption options are selected, the data is compressed before it is encrypted.
- Data compression reduces the backup time and the data size based on how much the data is compressible. Although you may notice reduced bandwidth utilization when you compare it with the data without compression.
- Performance of the data compression is reduced, if the data is incompressible. Therefore, Veritas recommends not to enable compression for backing up incompressible data such as policy data and so on.
- Veritas recommends not to use the same bucket with storage servers of different types.
- You must not use client-side compression along with storage server-side compression.
- You cannot change the compression configuration settings (enable/disable) after the storage server is created.

About data encryption for cloud storage

You can encrypt your data before you send it to the cloud. The NetBackup **Cloud Storage Server Configuration Wizard** and the **Disk Pool Configuration Wizard** include the steps that configure key management and encryption.

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 98.

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

See the *NetBackup Security and Encryption Guide*:

http://www.veritas.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 97.

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 3-7 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 specify 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 3-8 Encryption keys and key records for each storage server and volume combination

Item	Description
Key group key	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: For cloud storage, the following is the format: *storage_server_name*:*volume_name* The following items describe the requirements for the key group name components for cloud storage: ■ *storage_server_name*: 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 *storage_server_name*. ■ *volume_name*: You must specify the LSU name that the storage vendor exposes to NetBackup. The **Disk Pool Configuration Wizard** conforms to this format when it creates a key group.
Key record	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. A name for the key record is optional. If you use a key name, you can use any name. Veritas 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.

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

http://www.veritas.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 not a NetBackup host. Usually, it is a host that your cloud storage vendor exposes to the Internet and 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 78.

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

See "Changing cloud storage server properties" on page 110.

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

NetBackup media servers back up the clients and send the data to the storage server.

See "About the NetBackup media servers for cloud storage" on page 102.

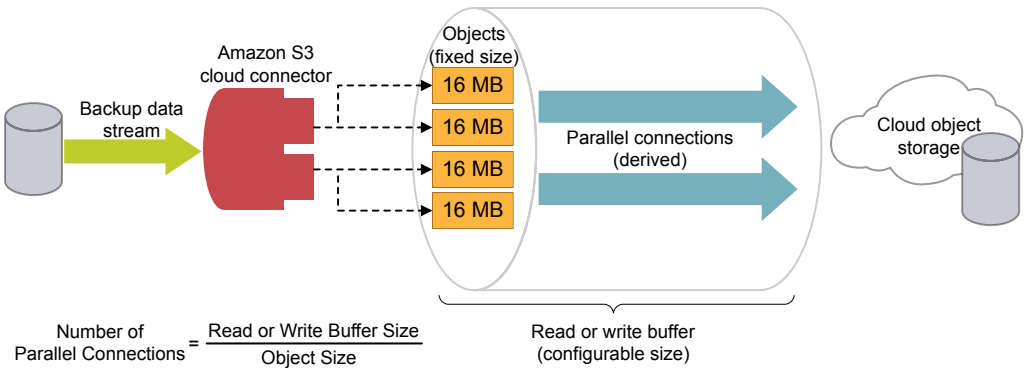
About object size for cloud storage

Overview

The performance of NetBackup in cloud is driven by the combination of object size, number of parallel connections, and the read or write buffer size.

The following diagram illustrates how these factors are related:

Figure 3-3 NetBackup Cloud Performance Considerations



The parameters are described as follows:

- Object Size: The backup data stream is divided into fixed size chunks. These chunks are stored as objects in the cloud object storage. The backup related metadata gets written in variable sizes.
- Read or write buffer size: You can configure the read or write buffer size to tune the performance of the backup and restore operations.

  Note: If you increase the read or write buffer size, the number of parallel connections increase. Similarly, if you want lesser number of parallel connections, you can reduce the read or write buffer size. However, you must consider the network bandwidth and the system memory availability.

- Parallel connections (Derived): To enhance the performance of backup and restore operations, NetBackup uses multiple parallel connections into the cloud storage. The performance of NetBackup depends on the number of parallel connections.

  Number of parallel connections is derived from the read or write buffer size and the object size.

  Number of Parallel Connections = Read or Write Buffer Size / Object Size

  Consider the following factors when deciding the number of parallel connections:

  - Maximum number of parallel connections permitted by the cloud storage provider.
  - Network bandwidth availability between NetBackup and the cloud storage environment.
  - System memory availability on the NetBackup host.

Current default settings

The default settings are as follows:

Table 3-9 Current default settings

Cloud storage provider	CloudCatalyst storage		Classic Cloud storage	
	Object size	Default read/write buffer size	Object size	Default read/write buffer size
Amazon S3/Amazon GovCloud	64 MB (fixed)	64 MB (fixed)	16 MB (fixed)	400 MB (configurable between 16 MB to 1 GB)
Azure	64 MB (fixed)	64 MB (fixed)	4 MB (fixed)	400 MB (configurable between 4 MB to 1 GB)

Considerations

In case of temporary failures on network with data transfer, NetBackup performs multiple retries for transferring the failed objects. In such case, if the failures persist, the complete object is transferred again. Also, with higher latency and higher packet loss, the performance might reduce. To handle the latency and packet loss issues, increasing the number of parallel connections can be helpful.

NetBackup has some timeouts on the client side. If the upload operation takes more time (due to big object size) than the minimum derived NetBackup data transfer rate, there can be failures with NetBackup.

Consider the following for legacy environments without deduplication support:

While restoring from back-level images (8.0 and earlier), where the object size is 1MB, the buffer of 16 MB (for one connection) is not completely utilized while also consuming memory. With the increased object size, there is a restriction on number of connections due to the available memory.

If the number of connections are less, parallel downloads would be less compared to older number of connections.

About the NetBackup media servers for cloud storage

The NetBackup media servers that you use for cloud storage backup the NetBackup clients and then send that backup data to the cloud storage server. The storage server then writes the data to storage.

See “About cloud storage servers” on page 99.

The NetBackup media servers also can move data back to primary storage (the client) during restores and from secondary storage to tertiary storage during duplication. These media servers are also known as *data movers*. They host a software plug in that they use to communicate with the storage implementation.

When you configure a cloud storage server, the media server that you specify in the wizard or on the command line becomes a cloud storage data mover.

See “Configuring a storage server for cloud storage” on page 105.

You can add additional media servers to backup clients. They can help balance the load of the backups that you send to the cloud storage.

See “Adding backup media servers to your cloud environment” on page 135.

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 136.

You can configure a cloud media server as a cloud master host.

See “Using media server as NetBackup Cloud master host” on page 103.

To support cloud storage, a media server must conform to the following items:

- The 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 (`nbcssc`) must be running.
  See “About the NetBackup CloudStore Service Container” on page 88.
- The NetBackup media servers that you use for cloud storage must be the same NetBackup version as the master server.

Using media server as NetBackup Cloud master host

You must perform this procedure for all the operating systems those are not supported by NetBackup cloud.

See the NetBackup hardware compatibility list for your release available through the following URL:

http://www.netbackup.com/compatibility

For disaster recovery, you must take a manual backup of the following files from the media server that you have configured as NetBackup cloud master host:

- `CloudProvider.xml`
- `CloudInstance.xml`

To use media server as NetBackup cloud master host

1. Identify one of the NetBackup cloud media servers as a cloud master host.

   Choose a media server that has same NetBackup master server version. Do not use a media server with different version.

   Note: The media server does not hold the master copy of the `CloudProvider.xml` file which all the media servers require while configuring the cloud storage and for running operations such as backup, restore, and so on.

   ---

2. Run the following commands on all the NetBackup cloud media servers including the one that is selected as the cloud master host:

   ```
   nbcssc -t -a NetBackup
   ```

   ```
   nbcssc -s -a NetBackup -m cloud_master_host -f
   ```

   For information on the command, see *Veritas NetBackup Commands Reference Guide*.

3. Ensure that the values of **CSSC_PORT** and **CSSC_IS_SECURE** as mentioned in `cloudstore.conf` file from cloud master host are copied as **CSSC_MASTER_PORT** and **CSSC_MASTER_IS_SECURE** in `cloudstore.conf` file on all other NetBackup cloud media servers.

After you select a cloud master host, do not change the name again to point to another media server. If you need to do so, contact Veritas Technical Support.

Additional task post disaster recovery

For a cloud storage server that uses proxy server , you must update the proxy credentials.

- To perform the task using the NetBackup Administrators Console, see See "Changing cloud storage host properties" on page 86.
- To perform the task using the commands, run the following:

  ```
  csconfig cldinstance -us -in instance_name -sts storage_server_name
  -pxtype proxy_type -pxhost proxy_host -pxport proxy_port
  -pxautth_type proxy_auth_type -pxtunnel proxytunnel_usage
  ```

  For information on the command, see *Veritas NetBackup Commands Reference Guide*.

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 service endpoint and selects the appropriate host for the storage server.

See "About cloud storage servers" on page 99.

The wizard also lets you enable encryption and configure corresponding parameters for the NetBackup Key Management Service.

See "About data encryption for cloud storage" on page 97.

If you configure encryption, Veritas 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 133.

If you configure a storage server by using CLI, you must run `csconfig` command before running `nbdevconfig` and `tpconfig` commands.

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

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

The NetBackup media server that you select during the configuration process must conform to the requirements for cloud storage.

See "About the NetBackup media servers for cloud storage" on page 102.

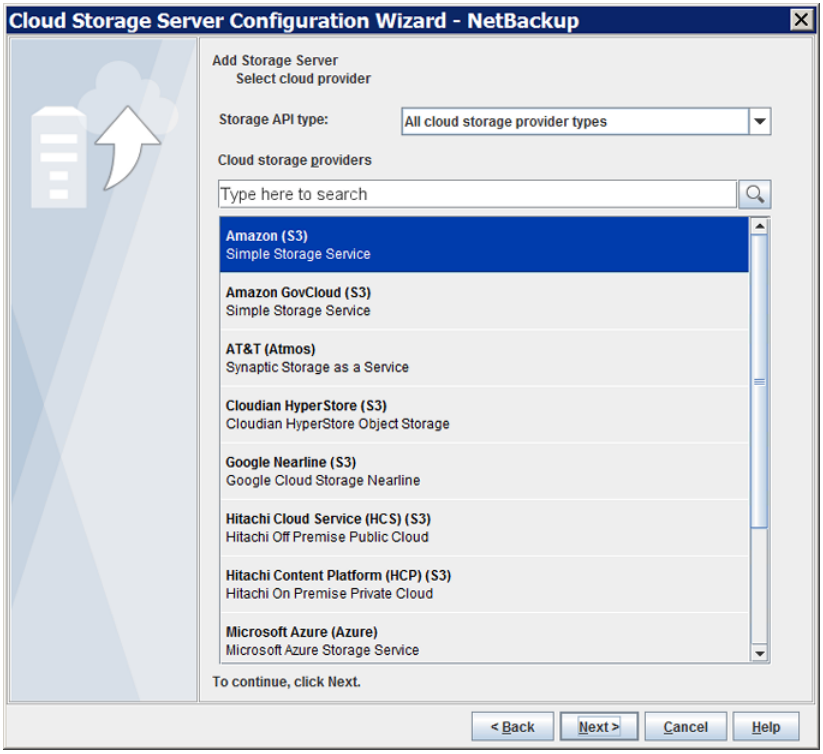
To configure a cloud storage server by using the wizard

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.

The **Select cloud provider** panel appears.

The following is an example of the panel:



4 On the **Select cloud provider** panel, perform one of the following:

- Select the cloud provider from the **Cloud storage providers** list of cloud providers.
- Sort the list of cloud providers by selecting the cloud storage API type from the **Storage API type** drop-down list and then selecting the cloud provider.
- In the **Cloud storage providers** search box, type the cloud provider name that you want to select. A cloud provider may support multiple cloud storage API types. Select an appropriate provider.

5 Click **Next**. A wizard panel for the selected cloud provider appears.

6 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, based on the storage type API. Those topics also include examples of the wizard panels.

See "About the Amazon S3 cloud storage API type" on page 17.

See "About EMC Atmos cloud storage API type" on page 45.

See "About Microsoft Azure cloud storage API type" on page 52.

See "About OpenStack Swift cloud storage API type" on page 59.

Rackspace Cloud Files is a special case, described in the following topic:

See "About Rackspace Cloud Files storage requirements" on page 68.

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.

---

7 Specify the following settings on the **Specify compression and encryption settings** panel.

Note: NetBackup media servers that are older than the 7.7.3 version do not support data compression. Therefore, if you have selected an older media server, the compression option does not appear on the panel.

Caution: If you use NetBackup commands to add a NetBackup 7.7.3 or earlier media server to a cloud storage environment that uses compression, cloud backups may fail. Ensure that all media servers that you add to a cloud storage configuration with the compression are NetBackup 7.7.3 or later.

- To compress your backup data, select **Compress data before writing to cloud storage**.
  See "About data compression for cloud backups" on page 96.
- To encrypt the data that would go on cloud storage , select **Encrypt data using AES-256 before writing to cloud storage**. Then, enter the information to protect the KMS database.
  See "KMS database encryption settings" on page 108.

Click **Next**. If you entered the compression and the encryption information, a dialog box appears that explains that you cannot change the settings after configuration. Click **Yes** to proceed or click **No** to cancel. If you click **Yes**, the **Cloud Storage Server Configuration Summary** panel appears.

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

If you need to make corrections, click **Back** until you reach the panel on which you need to make corrections.

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

9 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 124.
- To exit from the wizard, click **Finish**.
  If you exit, you can still create a disk pool.
  See "Configuring a disk pool for cloud storage" on page 124.

KMS database encryption settings

Table 3-10 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 3-10 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 **<kms_server_name>**.
Host Master Key (HMK) Passphrase	Enter the key that protects the database. In KMS terminology, the key is called a *passphrase*.
Re-enter HMK Passphrase	Re-enter the host master key.

Table 3-10 Required information for the encryption database *(continued)*

Field Name	Required information
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.
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 *passphrase*.
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, Veritas 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 133.

Assigning a storage class to Amazon cloud storage

In NetBackup, you can assign a storage class to cloud storage while you configure a new storage server.

See "About Amazon S3 storage classes" on page 36.

See "Configuring a storage server for cloud storage" on page 105.

To assign a storage class

1. In the NetBackup **Administration Console** > **Cloud Storage Configuration** wizard, select **Amazon**.
2. On the **Add Storage Server** screen, specify the Amazon S3 configuration details such as, service host, storage server name, and access details.

3 Click **Advanced Settings** and specify the appropriate value for the selected HTTP header. Click the **Value** column to see the drop-down list and select the value.

4 On the **Advanced Server Configuration** screen, the **x-amz-storage-class** header shows the Amazon S3 storage classes that NetBackup supports.

Click the **Value** column to select any of the available storage classes - **STANDARD** or **STANDARD_IA**.

Note: x-amz-storage-class is referred as **AMZ:STORAGE_CLASS** in the list of storage server properties.

---

5 Click **Ok**.

Note: Veritas recommends that you do not modify the storage class of a cloud storage server, after you have assigned it.

---

6 Configure a new disk pool.

See "Configuring a disk pool for cloud storage" on page 124.

Note: Veritas recommends that you use different buckets for different storage classes.

---

7 Configure a new storage unit by accessing **NetBackup Administration Console** > **NetBackup Management** > **Storage** > **Storage Units**.

8 Modify the existing policy or SLP (or create new policy or SLP) to use the new storage unit by accessing the respective user interfaces:

- To access policy, do the following: In the **NetBackup Administration Console**, expand **NetBackup Management**, and click **Policies**.
- To access SLP, do the following: In the **NetBackup Administration Console**, expand **NetBackup Management**, expand **Storage**, and click **Storage Life Cycle Policies**.

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 76.

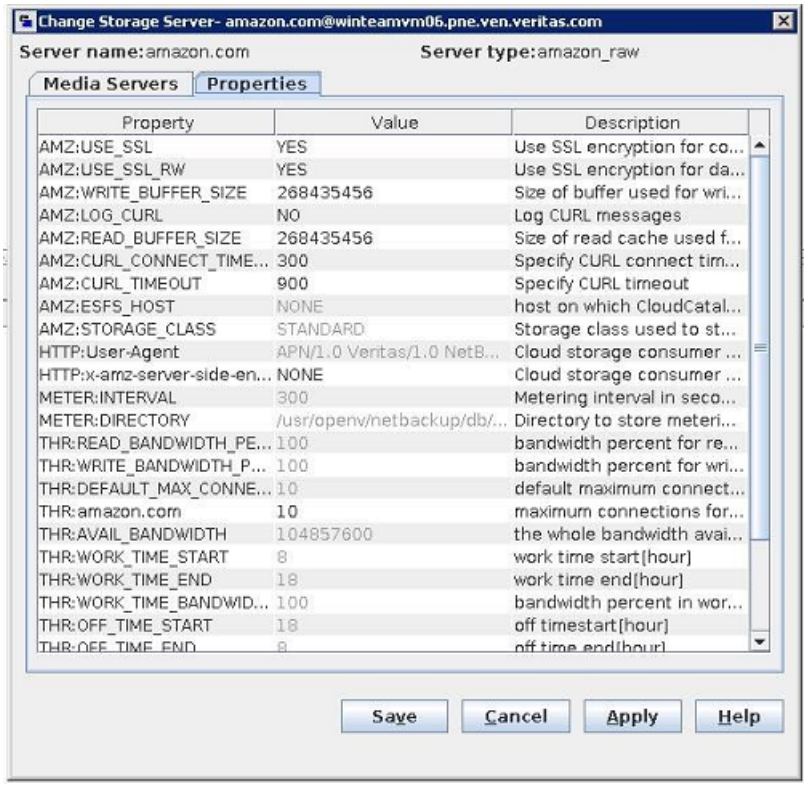
How to change cloud storage host properties is described in a different topic.

See "Changing cloud storage host properties" on page 86.

To change cloud 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 112.

See “NetBackup cloud storage server connection properties” on page 117.

See “NetBackup cloud storage server encryption properties” on page 123.

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. The following table describes the prefixes that NetBackup uses to categorize the properties.

Not all properties apply to all storage vendors.

Table 3-11 Prefix definitions

Prefix	Definition	For more information
`AMZ`	Amazon	See “NetBackup cloud storage server connection properties” on page 117.
`AMZGOV`	Amazon GovCloud	See “NetBackup cloud storage server connection properties” on page 117.
`ATT`	AT&T	See “NetBackup cloud storage server connection properties” on page 117.
`AZR`	Microsoft Azure	See “NetBackup cloud storage server connection properties” on page 117.
`CLD`	Cloudian Hyperstore	See “NetBackup cloud storage server connection properties” on page 117.
`CRYPT`	Encryption	See “NetBackup cloud storage server encryption properties” on page 123.
`GOOG`	Google Nearline	See “NetBackup cloud storage server connection properties” on page 117.

Table 3-11 Prefix definitions *(continued)*

Prefix	Definition	For more information
HT	Hitachi	See "NetBackup cloud storage server connection properties" on page 117.
HTTP	HTTP headers	See "NetBackup cloud storage server connection properties" on page 117. **Note:** This field applies to Amazon S3-compatible cloud providers.
METER	Metering	See "NetBackup cloud storage server connection properties" on page 117.
MSDPCLD	CloudCatalyst deduplication to the cloud	See "NetBackup CloudCatalyst storage server properties" on page 122.
ORAC	Oracle Cloud	See "NetBackup cloud storage server connection properties" on page 117.
RACKS	Rackspace	See "NetBackup cloud storage server connection properties" on page 117.
SWSTK-SWIFT	SwiftStack (Swift)	See "NetBackup cloud storage server connection properties" on page 117.
THR	Throttling	See "NetBackup cloud storage server bandwidth throttling properties" on page 113.
VER	Verizon	See "NetBackup cloud storage server connection properties" on page 117.

See "Changing cloud storage server properties" on page 110.

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 78.

Table 3-12 Cloud storage server bandwidth throttling properties

Property	Description
THR:*storage_server*	Shows maximum number of concurrent jobs that can be run for a specific cloud storage server. If configuring throttling for a media server that is a CloudCatalyst cloud storage server: ■ Change this value to 160 or more. ■ This value should be the same as the **Maximum concurrent jobs** media server property in the **Scalable Storage** host properties. See "Scalable Storage properties" on page 78. Default value: Not applicable Possible values: See the **Description** column
THR:AVAIL_BANDWIDTH	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. Default value: 104857600 Possible values: Any positive integer

Table 3-12 Cloud storage server bandwidth throttling properties *(continued)*

Property	Description
THR:DEFAULT_MAX_CONNECTIONS	The default maximum number of concurrent jobs that the media server can run for the cloud storage server. If THR:*storage_server* is set, NetBackup uses THR:*storage_server* instead of THR:DEFAULT_MAX_CONNECTIONS. This is a read-only field. 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. 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. You can configure job limits per backup policy and per storage unit. See the *NetBackup Administrator's Guide, Volume I*: http://www.veritas.com/docs/DOC5332 **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. In practice, you should not need to set this value higher than 100. Default value: 10 Possible values: 1 to 2147483647
THR:OFF_TIME_BANDWIDTH_PERCENT	This read-only field displays the bandwidth percent that is used during off time. Default value: 100 Possible values: 0 to 100

Table 3-12 Cloud storage server bandwidth throttling properties *(continued)*

Property	Description
THR:OFF_TIME_END	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. Default value: 8 Possible values: 0 to 2359
THR:OFF_TIME_START	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. Default value: 18 Possible values: 0 to 2359
THR:READ_BANDWIDTH_PERCENT	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. Default value: 100 Possible values: 0 to 100
THR:SAMPLE_INTERVAL	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. Default value: 0 Possible values: 1 to 2147483647
THR:WEEKEND_BANDWIDTH_PERCENT	This read-only field displays the bandwidth percent that is used during the weekend. Default value: 100 Possible values: 0 to 100
THR:WEEKEND_END	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. Default value: 7 Possible values: 1 to 7
THR:WEEKEND_START	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. Default value: 6 Possible values: 1 to 7

Table 3-12 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 110.

See "NetBackup cloud storage server properties" on page 112.

NetBackup cloud storage server connection properties

All or most of the cloud storage servers use the storage server properties in Table 3-13. The following are the prefixes for the currently supported cloud vendors:

- Amazon: AMZ
- Amazon GovCloud: AMZGOV
- AT&T: ATT
- Cloudian: CLD
- Google Nearline: GOOG
- Hitachi: HT
- Microsoft Azure: AZR

- Rackspace: `RACKS`
- Verizon: `VER`

Table 3-13 Storage server cloud connection properties

Property	Description
`METER:DIRECTORY`	This read-only field displays the directory in which to store data stream metering information. Default value: `/usr/openv/netbackup/db/cloud` (UNIX) or *`install_path`*`\VERITAS\NetBackup\db\cloud\` (Windows)
`METER:INTERVAL`	The interval at which 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 To change this property, use the **Cloud Settings** tab of the **Scalable Storage** host properties. See "Scalable Storage properties" on page 78. Default value: `300` Possible values: `1` to `10000`
`PREFIX``:CURL_CONNECT_TIMEOUT`	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. 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. This value cannot be disabled. If an invalid number is entered, the `CURL_CONNECT_TIMEOUT` returns to the default value of 300. Default value: `300` Possible values: `1` to `10000`
`PREFIX``:CURL_TIMEOUT`	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). Default value: `900` Possible values: `1` to `10000`

Table 3-13 Storage server cloud connection properties *(continued)*

Property	Description
PREFIX:ESFS_HOST	Identifies the host that contains the ESFS cache. The ESFS cache is used by a CloudCatalyst storage server for deduplication to the cloud. This property is set internally and cannot be changed by the user.
PREFIX:LOG_CURL	Determines if cURL activity is logged. The default is NO which means log activity is disabled. Default value: NO Possible values: NO (disabled) and YES (enabled)
PREFIX:PROXY_IP	The TCP/IP address of the proxy server. If you do not use a proxy server, leave this field blank. Default value: No default Possible values: Valid TCP/IP address This parameter is applicable only for EMC Atmos and Rackspace.
PREFIX:PROXY_PORT	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. Default value: 70000 Possible values: Valid port number This parameter is applicable only for EMC Atmos and Rackspace.
PREFIX:PROXY_TYPE	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. Default value: NONE Possible values: NONE, HTTP, SOCKS, SOCKS4, SOCKS5, SOCKS4A This parameter is applicable only for EMC Atmos and Rackspace.

Table 3-13 Storage server cloud connection properties *(continued)*

Property	Description
PREFIX:READ_BUFFER_SIZE	The size of the buffer to use for read operations. READ_BUFFER_SIZE is specified in bytes. To enable the use of the buffer, set this value to a non-zero number. The READ_BUFFER_SIZE 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. See "About object size for cloud storage" on page 100.
PREFIX:USE_SSL	Determines if Secure Sockets Layer encryption is used for the control APIs. The default value is YES, meaning SSL is enabled. Default value: YES Possible values: YES or NO
PREFIX:USE_SSL_RW	Determines if Secure Sockets Layer encryption is used for read and write operations. The default value is YES, meaning SSL is enabled. Default value: YES Possible values: YES or NO
PREFIX: WRITE_BUFFER_NUM	This parameter is not applicable for Amazon S3-compatible cloud providers. This read-only field displays the total number of write buffers that are used by the plug-in. The WRITE_BUFFER_SIZE value defines the size of the buffer. The value is set to 1 and cannot be changed. Default value: 1 Possible values: 1

Table 3-13 Storage server cloud connection properties *(continued)*

Property	Description
PREFIX:WRITE_BUFFER_SIZE	The size of the buffer to use for write operations. WRITE_BUFFER_SIZE is specified in bytes. To disable the use of the buffer, set this value to 0 (zero). The WRITE_BUFFER_SIZE 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. See "About object size for cloud storage" on page 100.
HTTP:User-Agent	This is applicable only for Amazon S3-compatible cloud providers. This property is set internally and cannot be changed by the user.
HTTP:x-amz-server-side-encryption	This is applicable only for the following cloud providers: Amazon S3 and Amazon GovCloud Use this property to enable the server-side encryption of the data that you need to transfer to the cloud storage. AES-256 is a server-side encryption standard. Set this property to NONE to disable the server-side encryption for the cloud provider. **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.
AMZ:RETRIEVAL RETENTION PERIOD	This is applicable only for Amazon Glacier. Use this property to specify the retrieval retention period in days.
AMZ:STORAGE_CLASS	This is applicable only for the Amazon S3 cloud providers. Displays the storage class used by the cloud storage server. This property is set internally and cannot be changed by the user.

See "Changing cloud storage server properties" on page 110.

See "NetBackup cloud storage server properties" on page 112.

NetBackup CloudCatalyst storage server properties

The `MSDPCLD` prefix specifies a deduplication storage property in the **Properties** tab of the **Change Storage Server dialog** box. The following table describes the properties.

Table 3-14 CloudCatalyst storage server properties

Property	Description
MSDPCLD:storagepath	Storage Path
MSDPCLD:spalogpath	Storage Pool Log Path
MSDPCLD:dbpath	Database Path
MSDPCLD:required_interface	Required Interface
MSDPCLD:spalogretention	Storage Pool Log Retention
MSDPCLD:verboselevel	Storage Pool Verbose Level (Range 0 - 5)
MSDPCLD:replication_target(s)	Replication Target(s)
MSDPCLD:dedupetocloud	Dedupe To Cloud
MSDPCLD:Storage Pool Raw Size	Storage Pool Raw Size
MSDPCLD:Storage Pool Reserved Space	Storage Pool Reserved Space
MSDPCLD:Storage Pool Size	Storage Pool Size
MSDPCLD:Storage Pool Used Space	Storage Pool Used Space
MSDPCLD:Storage Pool Available Space	Storage Pool Available Space
MSDPCLD:Catalog Logical Size	Catalog Logical Size
MSDPCLD:Catalog files Count	Catalog files Count
MSDPCLD:Deduplication Ratio	Deduplication Ratio

See “NetBackup cloud storage server properties” on page 112.

See “Changing cloud storage server properties” on page 110.

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 3-15 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 "NetBackup cloud storage server properties" on page 112.

See "Changing cloud storage server properties" on page 110.

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 124.

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.veritas.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

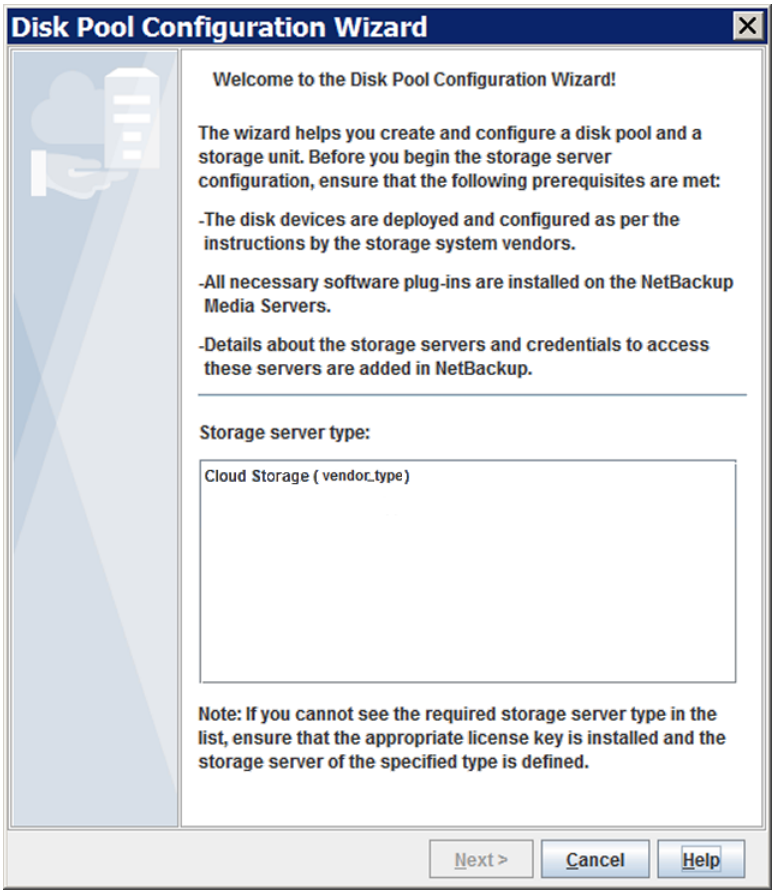
1. If the **Disk Pool Configuration Wizard** was launched from the **Storage Server Configuration Wizard**, go to step 5.

   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:

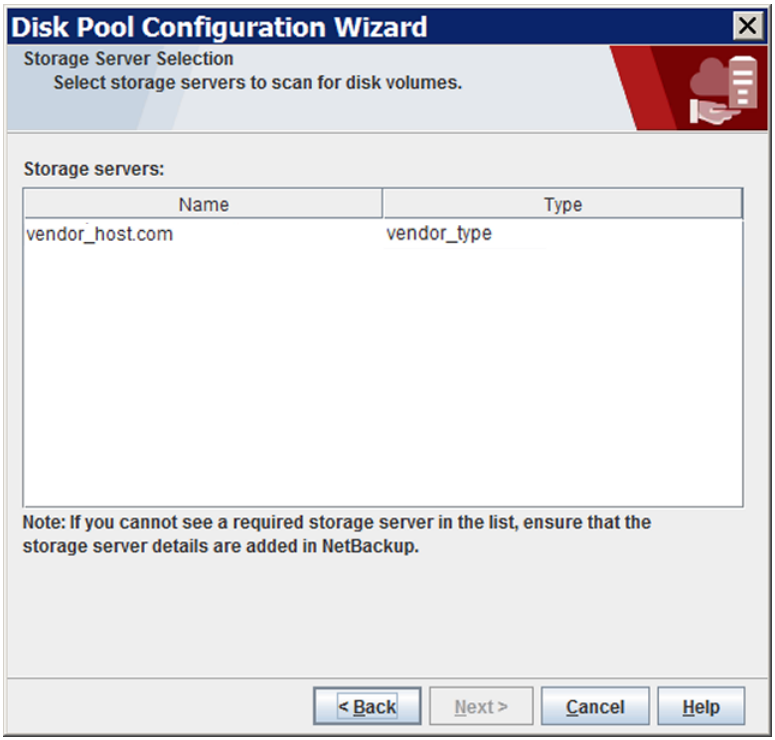


Read the information on the welcome panel of the wizard. Then, select the appropriate storage server type and click **Next**.

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.

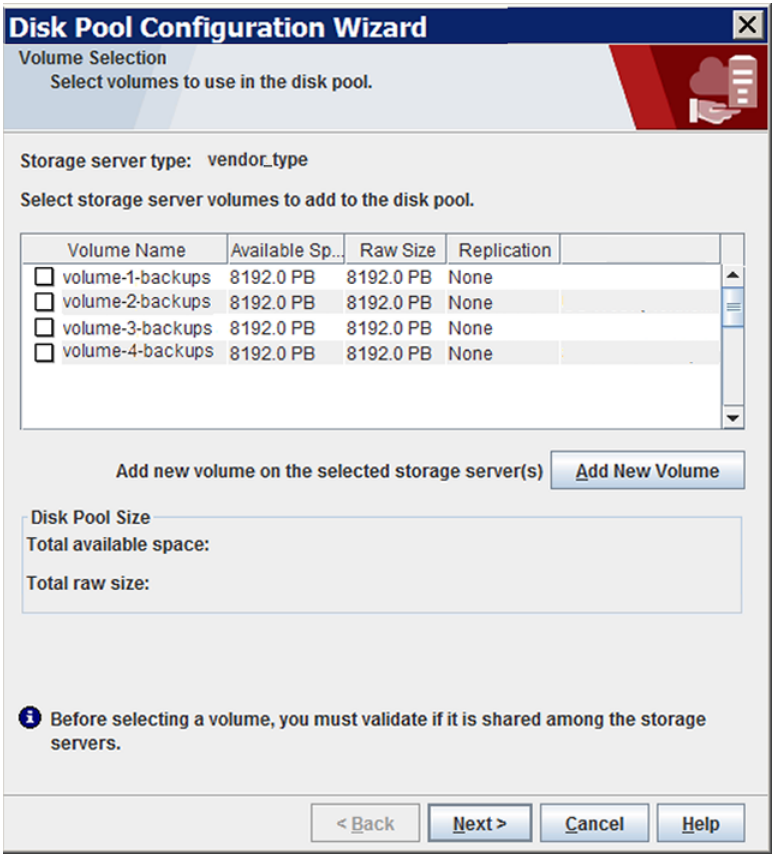
After you select the cloud storage server, click **Next**. The **Volume Selection** wizard panel appears.

5 The **Volume Selection** panel displays the volumes that have been created already under your account within the vendor's cloud storage.

Note: The following properties do not apply to cloud storage disk pools: **Total available space**, **Total raw size**, **Low water mark**, and **High water mark**.

All these values are derived from the storage capacity, which cannot be fetched from the cloud provider.

The 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. Use the following link to find the information about the requirements for the volume names.

See "About the cloud storage vendors for NetBackup" on page 15.

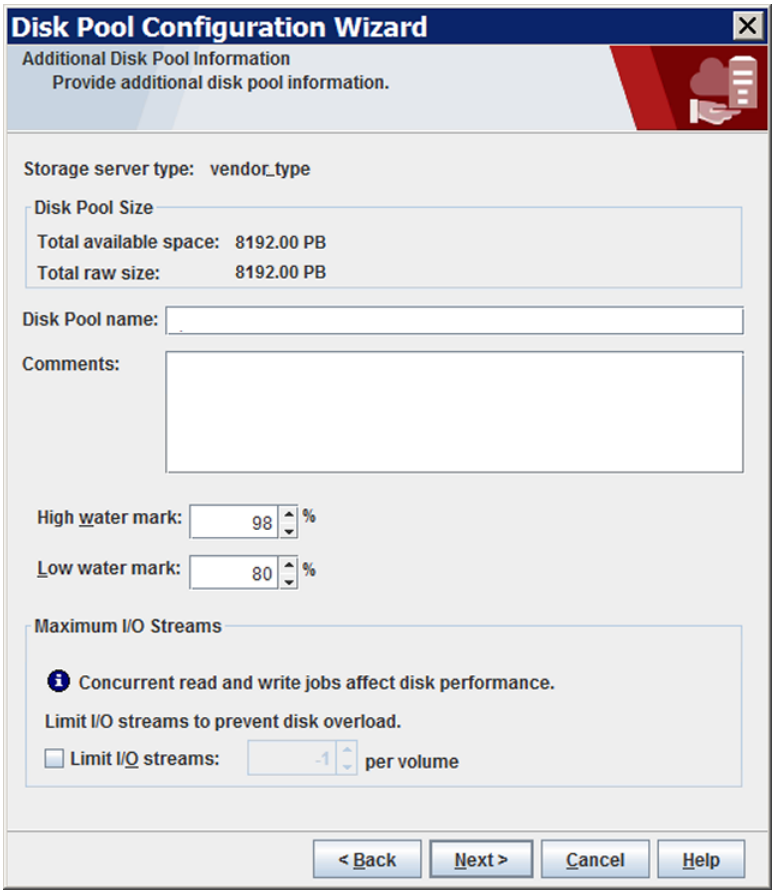
To select a volume, click the check box for the volume. You can select one volume only.

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 selected a volume on a storage destination that does not require encryption, the **Additional Disk Pool Information** panel appears. Go to the next step, step 6.
Encryption	If you selected a volume on a storage destination that requires encryption, a **Settings** 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. See "About key management for encryption of NetBackup cloud storage" on page 98. After you enter a pass phrase and then click **OK** in the **Settings** dialog box, the dialog box closes. Click **Next** in the **Volume Selection** wizard panel to continue to the **Additional Disk Pool Information** wizard panel. Continue to the next step, step 6.

6 On the **Additional Disk Pool Information** panel, enter or select the properties for this disk pool.

The following is an example of the wizard panel:



See "Cloud storage disk pool properties" on page 147.

After you enter the additional disk pool information, click **Next**. The **Summary** panel appears.

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

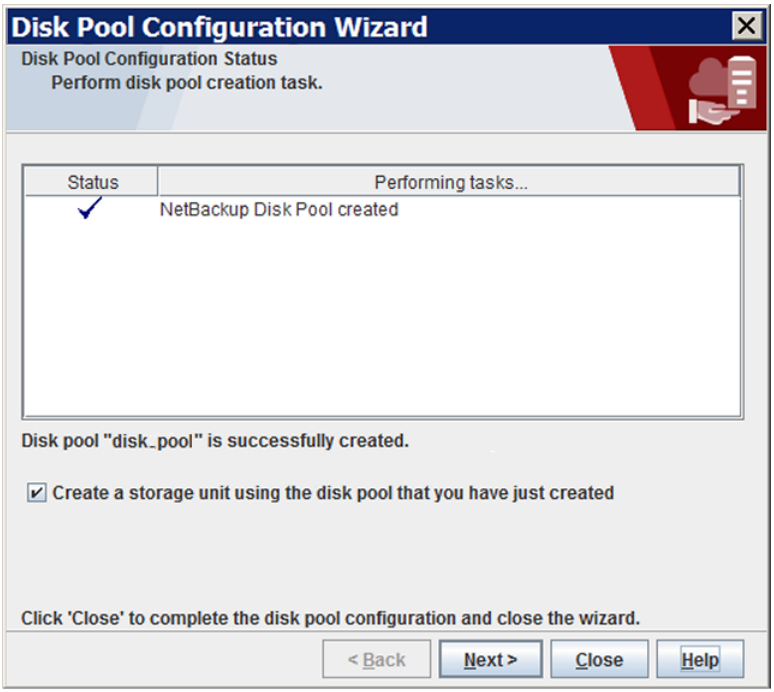
If the summary shows your selections accurately, click **Next**.

Veritas 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 133.

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

The following is an example of the wizard panel:

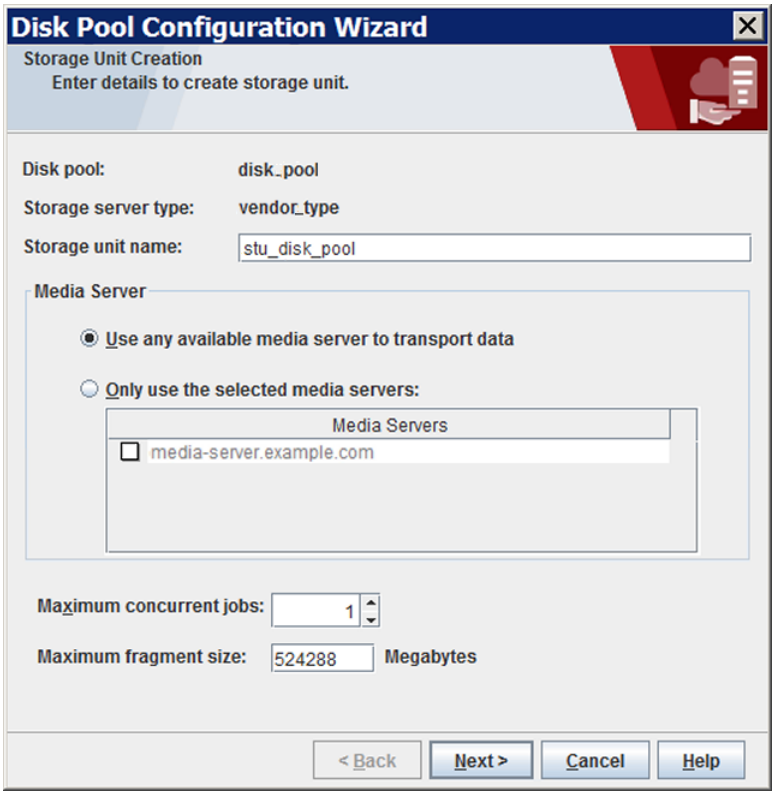


After NetBackup creates the disk pool, you can do the following:

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 136.

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

The following is an example of the wizard panel:



See "Cloud storage unit properties" on page 138.

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 140.

See "Control backup traffic to the media servers" on page 141.

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

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

Veritas 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 97.

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/openv/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/openv/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*. 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.

A NetBackup media server must conform to the requirements for cloud storage.

See "About the NetBackup media servers for cloud storage" on page 102.

To add 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.
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:

      `libstspi`*`VendorName`*`.conf`

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

      - UNIX and Linux: `/usr/openv/netbackup/db/cloud/`
      - Windows: `install_path\VERITAS\NetBackup\db\cloud\`

   b. Save the file to the appropriate directory on the media server or servers that you added, as follows:

      - UNIX and Linux: `/usr/openv/netbackup/db/cloud/`
      - Windows: `install_path\VERITAS\NetBackup\db\cloud\`

   Caution: If you do not copy the `libstspi`*`VendorName`*`.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.

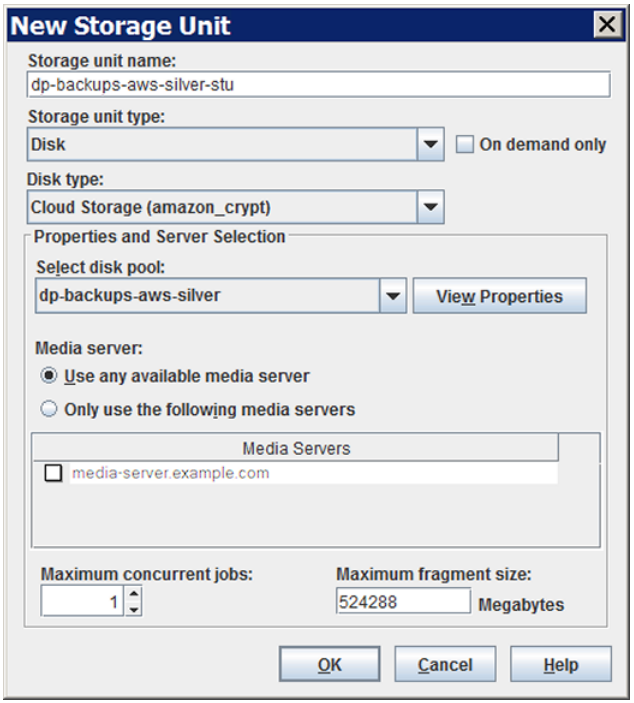
You can use storage unit properties to control your backup traffic.

See “Configure a favorable client-to-server ratio” on page 140.

See “Control backup traffic to the media servers” on page 141.

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 138.

Cloud storage unit properties

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

Table 3-16 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 3-16 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. *type* represents the disk pool type, based on storage vendor, encryption, and so on.
Disk pool	Select the disk pool that contains the storage for this storage unit. 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.
Media server	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. Specify the media server or servers as follows: ■ 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. NetBackup selects the media server to use when the policy runs.
Maximum concurrent jobs	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. 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. **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. The number to enter depends on the available disk space and the server's ability to run multiple backup processes. **Warning:** A **Maximum concurrent jobs** setting of 0 disables the storage unit.

Table 3-16 Cloud storage unit properties *(continued)*

Property	Description
Maximum fragment size	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. For a FlashBackup policy, Veritas recommends that you use the default, maximum fragment size to ensure optimal duplication performance.

Configure a favorable client-to-server ratio

You can use storage unit settings to configure a favorable client-to-server ratio. Uou 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.

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

These guides are available through the following URL:

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

Enabling NetBackup Accelerator with cloud storage

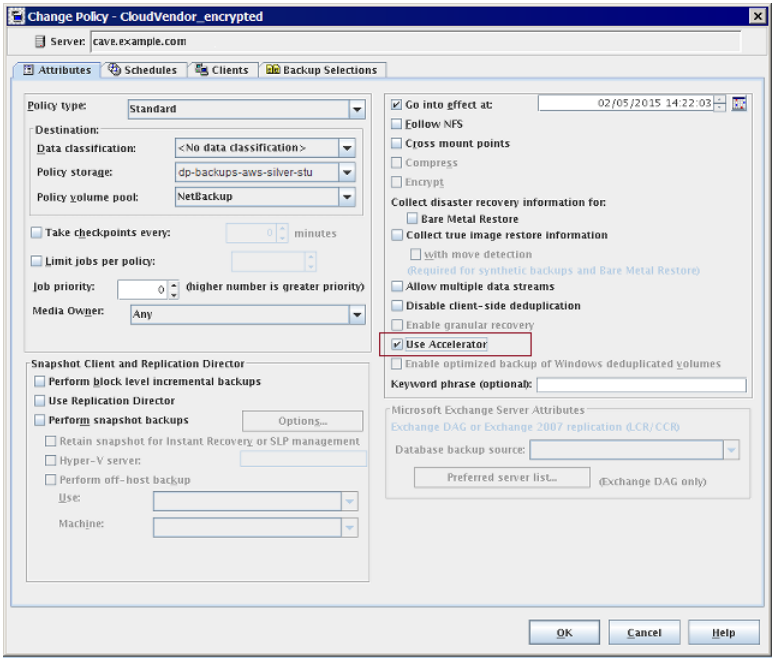
Use the following procedure to enable NetBackup Accelerator for use with NetBackup cloud storage.

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**.

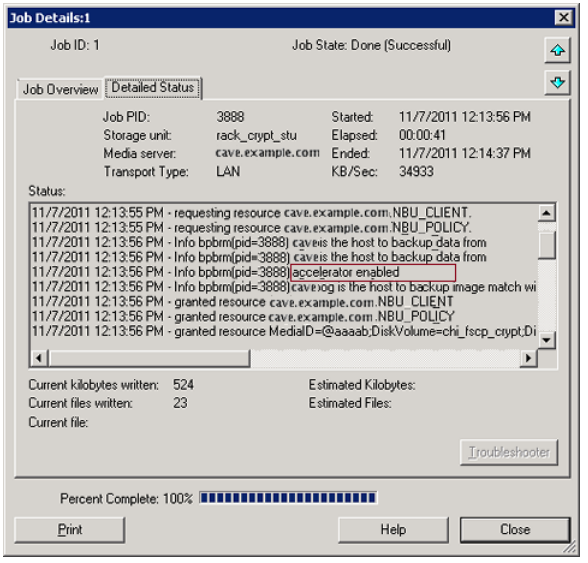
Figure 3-4 Enable Accelerator



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 3-5 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.

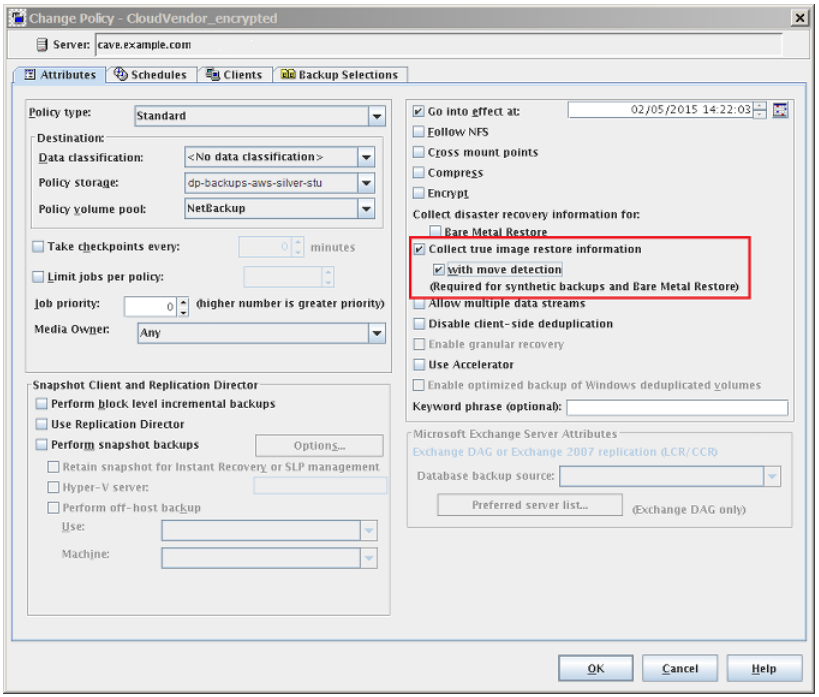
Note: In the case of Hitachi cloud configuration, the True Image Restore (TIR) or synthetic backups do not work, if you have enabled the encryption option. To successfully run the TIR or synthetic backups, you need to enable the versioning option for buckets (or namespaces) through the Hitachi cloud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

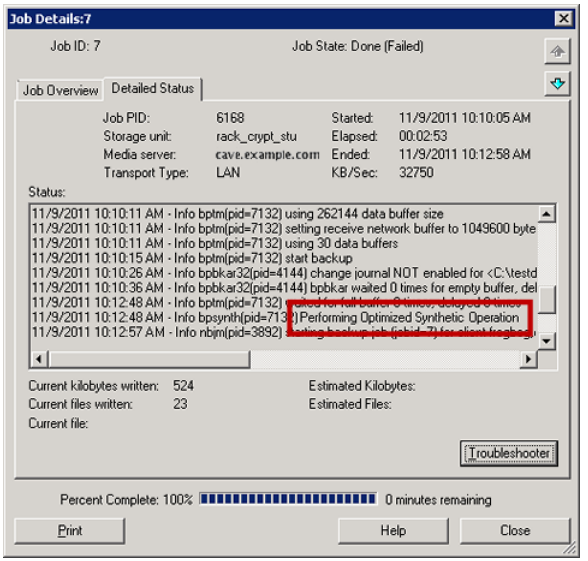
Figure 3-6 Enable Optimized Synthetic backups



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 3-7 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.

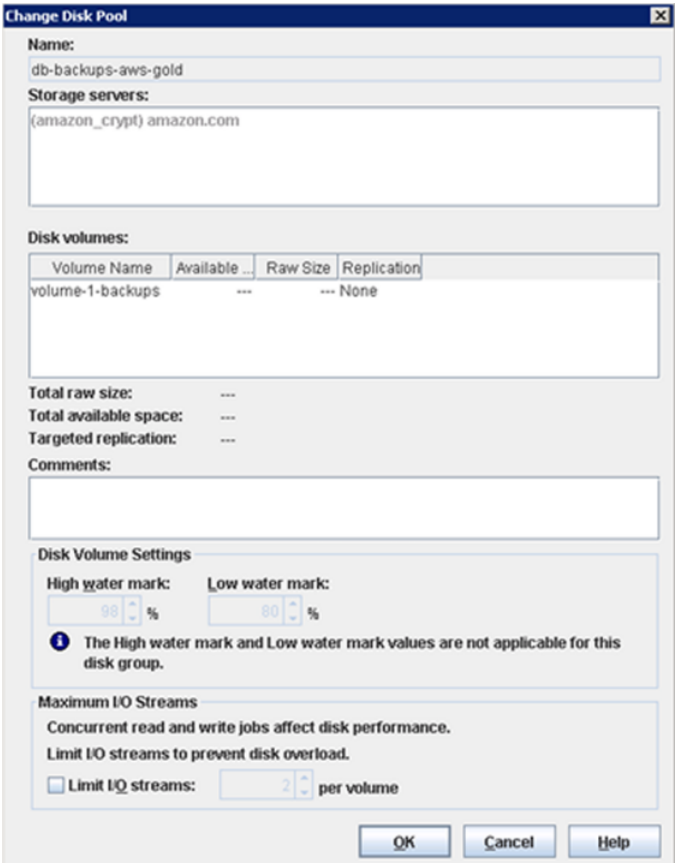
Changing cloud storage disk pool properties

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**.



4 Change the properties as necessary.

See “Cloud storage disk pool properties” on page 147.

5 Click **OK**.

Cloud storage disk pool properties

The properties of a disk pool may vary depending on the purpose the disk pool.

Note: The following properties do not apply to cloud storage disk pools: **Total available space**, **Total raw size**, **Usable Size**, **Low water mark**, and **High water mark**.

All these values are derived from the storage capacity, which cannot be fetched from the cloud provider.

The following table describes the possible properties:

Table 3-17 Cloud storage disk pool properties

Property	Description
Name	The disk pool name.
Storage servers	The storage server name.
Disk volumes	The disk volume that comprises 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. **Note:** **Total raw size** does not apply to cloud storage disk pools.
Total available space	The total amount of space available in the disk pool. **Note:** **Total available space** does not apply to cloud storage disk pools.
Comments	A comment that is associated with the disk pool.
High water mark	The **High water mark**, is a threshold at which the volume or the disk pool is considered full. **Note:** **High water mark** does not apply to cloud storage disk pools.
Low water mark	The **Low water mark** is a threshold at which NetBackup stops image cleanup. **Low water mark** does not apply to cloud storage disk pools.

Table 3-17 Cloud storage disk pool properties *(continued)*

Property	Description
Limit I/O streams	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. 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. 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. 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.
per volume	Select or enter the number of read and write streams to allow per volume. Many factors affect the optimal number of streams. Factors include but are not limited to disk speed, CPU speed, and the amount of memory. For the disk pools that are configured for **Snapshot** and that have a **Replication source** property: ■ 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.

Managing Certification Authorities (CA) for NetBackup Cloud

NetBackup cloud supports only X.509 certificates in .PEM (Privacy-enhanced Electronic Mail) format.

You can find the details of the Certification Authorities (CAs) in the `cacert.pem` bundle at following location:

- Windows: *install-path*\NetBackup\db\cloud\cacert.pem
- UNIX: /usr/openv/netbackup/db/cloud/cacert.pem

Note: In a cluster deployment, NetBackup database path points to the shared disk, which is accessible from the active node.

You can add or remove a CA from the cacert.pem bundle.

After you complete the changes, when you upgrade to a new version of NetBackup, the cacert.pem bundle is overwritten by the new bundle. All the entries that you may have added or removed are lost. As a best practice, keep a local copy of the edited cacert.pem file. You can use the local copy to override the upgraded file and restore your changes.

To add a CA

You must get a CA certificate from the required cloud provider and update it in the cacert.pem file. The certificate must be in .PEM format.

1. Open the cacert.pem file.
2. Append the self-signed CA certificate on a new line and at the beginning or the end of the cacert.pem file.

   Add the following information block:

   ```
   Certificate Authority Name

   ==========================

   -----BEGIN CERTIFICATE-----

   <Certificate content>

   -----END CERTIFICATE-----
   ```

3. Save the file.

To remove a CA

Before you remove a CA from the cacert.pem file, ensure that none of the cloud jobs are using the related certificate.

1. Open the `cacert.pem` file.
2. Remove the required CA. Remove the following information block:

```
Certificate Authority Name

==========================

-----BEGIN CERTIFICATE-----

<Certificate content>

-----END CERTIFICATE-----
```

3. Save the file.

List of CAs approved by NetBackup

- Baltimore CyberTrust Root
- Cybertrust Global Root
- DigiCert Assured ID Root CA
- DigiCert Assured ID Root G2
- DigiCert Assured ID Root G3
- DigiCert Global Root CA
- DigiCert Global Root G2
- DigiCert Global Root G3
- DigiCert High Assurance EV Root CA
- DigiCert Trusted Root G4
- GeoTrust Global CA
- GeoTrust Global CA 2
- GeoTrust Primary Certification Authority
- GeoTrust Primary Certification Authority - G2
- GeoTrust Primary Certification Authority - G3
- GeoTrust Universal CA
- GeoTrust Universal CA 2
- RSA Security 2048 v3
- Starfield Services Root Certificate Authority - G2
- Thawte Primary Root CA

- Thawte Primary Root CA - G2
- Thawte Primary Root CA - G3
- VeriSign Class 1 Public Primary Certification Authority - G3
- VeriSign Class 2 Public Primary Certification Authority - G3
- Verisign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G4
- VeriSign Class 3 Public Primary Certification Authority - G5
- VeriSign Universal Root Certification Authority

Chapter 4

Monitoring and Reporting

This chapter includes the following topics:

About monitoring and reporting for cloud backups

Veritas 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.veritas.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. **Note:** Where Amazon is the cloud service provider, OpsCenter cannot report on the data that MSDP cloud storage servers upload to the cloud. See "Connection to the NetBackup CloudStore Service Container fails" on page 172.

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. **Note:** The information that is displayed for **Used Capacity** and **Available Space** for Amazon is inaccurate in the NetBackup Administration Console. The values are found under **Media and Device Management > Devices > Disk Pool**. Even if there is information 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 155.

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 the compression ratio

The bptm logs provide information of the compression ratio of your data after the backup is taken in the cloud storage. The compression ratio is calculated by dividing the original size with the compressed size. For example, if the original data is of 15302918144 bytes and is compressed to 7651459072, then the compression ratio is 2.00.

To view the compression ratio

1. Note down the bptm PID of the backup job.

   See "Viewing cloud storage job details" on page 154.

2. Open the `bptm.log` file. The log file resides in the following directories:

   UNIX `/usr/openv/netbackup/logs/`

   Windows *install_path*`\NetBackup\logs\`

3. Search for the bptm PID instance.

   The following lines provide the compression ratio information according to the image format:

   date:time <PID> <4> 35:bptm:<PID>:
   media_server_IP: compress: image *image_name*_C1_F1
   compressed from *data in bytes* to *data in bytes* bytes,
   compression ratio *ratio_value*

   date:time <PID> <4> 35:bptm:<PID>:
   media_server_IP: compress: image *image_name*_C1_HDR
   compressed from *data in bytes* to *data in bytes* bytes,
   compression ratio *ratio_value*

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 4-1 describes the disk reports available.

Table 4-1 Disk reports

Report	Description
Images on Disk	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. 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.

Table 4-1 Disk reports *(continued)*

Report	Description
Disk Logs	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.
Disk Storage Unit Status	The Disk Storage Unit Status report displays the state of disk storage units in the current NetBackup configuration. 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.
Disk Pool Status	The Disk Pool Status report displays the state of disk pool storage units. This report displays only when a license is installed that enables a NetBackup disk feature.

See "About monitoring and reporting for cloud backups" on page 153.

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: Veritas 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/openv/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           : -
```

Chapter 5

Operational notes

This chapter includes the following topics:

NetBackup bpstsinfo command operational notes

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

Table 5-1 `bpstsinfo` command operational notes

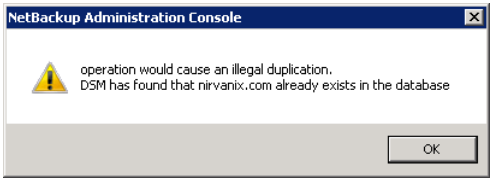
Note	Description
Use either the `-stype` option or the `-storageserverprefix`	Use either the `-stype` option or the `-storageserverprefix` option to constrain the `bpstsinfo` command to list storage server information. If you do not, the command searches all providers, which may be time consuming and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

Table 5-1 `bpstsinfo` command operational notes *(continued)*

Note	Description
Encrypted and non-encrypted storage units are displayed in `bpstsinfo` command output	When you use the `bpstsinfo` 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 `bpstsinfo` command operates on the level of the storage plug-in, which is not aware of any higher-level detail, such as encryption. The following is an example of a command that specifies encrypted storage: `bpstsinfo -lsuinfo -storage_server amazon.com -stype amazon_crypt`

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 "To add backup media servers to your cloud environment" on page 136.

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.veritas.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 `.pref` files from `db/cloud` directory.

Chapter 6

Troubleshooting

This chapter includes the following topics:

About unified logging

Unified logging and legacy logging are the two forms of debug logging used in NetBackup. All NetBackup processes use one of these forms of logging. Server processes and client processes use unified logging.

Unified logging creates log file names and messages in a standardized format. These logging files cannot be easily viewed with a text editor. They 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.

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/openv/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:

`vxlogcfg`	Modifies the unified logging configuration settings. for more information about the `vxlogcfg` command.
`vxlogmgr`	Manages the log files that the products that support unified logging generate. for more information about the `vxlogmgr` command.
`vxlogview`	Displays the logs that unified logging generates. See "Examples of using vxlogview to view unified logs" on page 164. for more information about the `vxlogview` command.

These commands are located in the following directory:

Windows *install_path*\NetBackup\bin

UNIX `/usr/openv/netbackup/bin`

See the NetBackup Commands Reference Guide for a complete description about these commands.

More information about legacy logging is available.

See "About legacy logging" on page 165.

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/openv/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 6-1 Example uses of the vxlogview command

Item	Example
Display all the attributes of the log messages	`vxlogview -p 51216 -d all`
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: `vxlogview --prodid 51216 --display D,T,m,x`
Display the latest log messages	Display the log messages for originator 116 (`nbpem`) that were issued during the last 20 minutes. Note that you can specify `-o nbpem` instead of `-o 116`: `# vxlogview -o 116 -t 00:20:00`
Display the log messages from a specific time period	Display the log messages for `nbpem` that were issued during the specified time period: `# vxlogview -o nbpem -b "05/03/15 06:51:48 AM" -e "05/03/15 06:52:48 AM"`

Table 6-1 Example uses of the vxlogview command *(continued)*

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

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

http://www.veritas.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 162.

In legacy debug logging, each process creates log files of debug activity in its own logging directory. The NetBackup legacy debug log directories are located in the following directories:

Windows	*install_path*\NetBackup\logs *install_path*\Volmgr\debug
UNIX	/usr/openv/netbackup/logs /usr/openv/volmgr/debug

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. For example, the following directories are created by default on UNIX servers:

- nbfp
- nbliveup
- nblogadm
- user_ops

To enable logging for all of the NetBackup processes that use legacy logging, you must create the log file directories that do not already exist, unless you use the Logging Assistant. For more information about the Logging Assistant, see the *NetBackup Administrator's Guide, Volume I*. The guide is available at the following location:

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

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/openv/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.veritas.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. Each log file grows to a certain size before the NetBackup process closes it and creates a new log file.

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

Windows	*install_path*\Volmgr\debug\vmscd\
UNIX	/usr/openv/volmgr/debug/vmscd

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

Creating NetBackup log file directories for cloud storage

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/openv/netbackup/logs/
- Windows:*install_path*\NetBackup\logs\

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

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

To create log directories for NetBackup commands

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

  UNIX: /usr/openv/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/openv/volmgr/debug/tpcommand

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

NetBackup cloud storage log files

NetBackup cloud storage exists within the Veritas 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.

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 log files is available. See the *NetBackup Logging Reference Guide*:

http://www.veritas.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 Veritas 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 6-2.

Table 6-2 describes the logs.

Table 6-2 NetBackup logs for cloud storage

Activity	OID	Processes
Backups and restores	N/A	Messages appear in the log files for the following processes: ■ The `bpbrm` backup and restore manager. ■ The `bpdbm` database manager. ■ The `bpdm` disk manager. ■ The `bptm` tape manager for I/O operations. The log files reside in the following directories: ■ UNIX: `/usr/openv/netbackup/logs/` ■ Windows:*`install_path`*`\NetBackup\logs\`
Backups and restores	117	The `nbjm` Job Manager.
Image cleanup, verification, import, and duplication	N/A	The `bpdbm` database manager log files. The log files reside in the following directories: ■ UNIX: `/usr/openv/netbackup/logs/bpdbm` ■ Windows:*`install_path`*`\NetBackup\logs\bpdbm`
Cloud connection operations	N/A	The `bpstsinfo` 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 (`nbcssc`) writes log files to the following directories: ■ For Windows: *`install_path`*`\Veritas\NetBackup\logs\nbcssc` ■ For UNIX/Linux: `/usr/openv/netbackup/logs/nbcssc`
Credentials configuration	N/A	The `tpconfig` utility. The `tpconfig` command writes log files to the `tpcommand` directory.
Device configuration	111	The `nbemm` process.
Device configuration	178	The Disk Service Manager process that runs in the Enterprise Media Manager (EMM) process.

Table 6-2 NetBackup logs for cloud storage *(continued)*

Activity	OID	Processes
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.

See "Troubleshooting cloud storage operational issues" on page 178.

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	Amazon
AMZGOV	Amazon GovCloud
ATT	AT&T
AZR	Microsoft Azure
CLD	Cloudian HyperStore
GOOG	Google Nearline
HT	Hitachi
ORAC	Oracle Cloud
RACKS	Rackspace
SWSTK-SWIFT	SwiftStack (Swift)
VER	Verizon

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

See "Changing cloud storage server properties" on page 110.

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/openv/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 172.

Troubleshooting cloud storage configuration issues

The following sections may help you troubleshoot configuration issues.

See "NetBackup Scalable Storage host properties unavailable" on page 172.

See "Connection to the NetBackup CloudStore Service Container fails" on page 172.

See "Cannot create a cloud storage disk pool" on page 174.

See "Cannot create a cloud storage" on page 174.

See "NetBackup Administration Console fails to open" on page 171.

See "Data transfer to cloud storage server fails in the SSL mode" on page 175.

See “Amazon GovCloud cloud storage configuration fails in non-SSL mode” on page 176.

See “Data restore from the Google Nearline storage class may fail” on page 176.

See “Fetching storage regions fails with authentication version V2” on page 177.

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 184.

See “Stopping and starting the NetBackup CloudStore Service Container” on page 183.

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 time-out for each connection attempt. The NetBackup OpsCenter also connects to the NetBackup CloudStore Service Container to obtain data for reporting.

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

- The NetBackup CloudStore Service Container is active.
  See “NetBackup CloudStore Service Container startup and shutdown troubleshooting” on page 184.
  See “Stopping and starting the NetBackup CloudStore Service Container” on page 183.
- Your firewall settings are appropriate.
- The **Enable insecure communication with 8.0 and earlier hosts** option on the NetBackup master server is selected if the media server is of the version 8.0 or earlier. The option is available in the **NetBackup Administration Console** on the **Security Management > Global Security Settings > Secure Communication** tab.

- The `cacert.pem` file is present on both NetBackup master and media server in following locations:
  - UNIX/Linux - `/usr/openv/var/webtruststore`
  - Windows - `<install_path>/var/webtruststore`

  If the `cacert.pem` file is not present on the master server or a media server, run the `nbcertcmd -getCACertificate` command on that host. After running this command, restart the NetBackup CloudStore Service Container on that host. See the *NetBackup Commands Reference Guide* for a complete description of the command.

  Note: This `cacert.pem` file contains the CA certificates that the NetBackup authorization service generates.

- The `cacert.pem` file is same on the NetBackup master and media server.
- The security certificate is present in following locations:
  - UNIX/Linux - `/usr/openv/var/vxss/credentials`
  - Windows - `<install_path>/var/vxss/credentials`

  If the security certificate is not present, run the `bpnbaz -ProvisionCert` on the master server. After running this command, restart the NetBackup CloudStore Service Container on the master server and the media servers.
  See "Deploying host name-based certificates" on page 93.
- If the master server runs on an operating system that does not support NetBackup cloud configurations: You can choose to use the NetBackup CloudStore Service Container on a media server as the master service container. To do so, update the `CSSC_MASTER_NAME` parameter of the `cloudstore.conf` file on all the cloud-supported media servers with the media server name you chose earlier. However, communication from other media servers to the media server that now functions as the master configuration for the `nbcssc` service and vice versa fails. The failure happens because both these media servers verify if a trusted host has made the communication request.

  Note: The media server that now functions as the master configuration for the `nbcssc` service must run the same NetBackup version as the NetBackupmaster server.

  For the operating systems that NetBackup supports for cloud storage, see the NetBackupoperating system compatibility list available through the following URL:

http://www.netbackup.com/compatibility

See “About the NetBackup CloudStore Service Container” on page 88.

To fix this issue, add the authorized host entries on the media and the master servers that support cloud configurations.

See the 'Adding a server to a servers list' topic in the *NetBackup™ Administrator's Guide, Volume I* for detailed steps.

- On the media server, if the certificate deployment security level if set to Very High, automatic certificate deployment is disabled. An authorization token must accompany every new certificate request. Therefore, you must create an authorization token before deploying the certificates.

  See the 'Creating authorization tokens' topic in the *NetBackup™ Security and Encryption Guide* for detailed steps.

Cannot create a cloud storage disk pool

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

Table 6-3 Cannot create disk pool solutions

Error	Description
`The wizard is not able to obtain Storage Server information. Cannot connect on socket. (25)`	The error message appears in the **Disk Configuration Wizard**. 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. To resolve the issue, use the NetBackup `nbdevconfig` command to configure the disk pool. Unlike the wizard, the `nbdevconfig` command does not monitor the command response times. See the *NetBackup Commands Reference Guide* for a complete description of the commands. The guide is available at the following location: http://www.veritas.com/docs/DOC5332

Cannot create a cloud storage

If you cannot create a cloud storage in NetBackup, verify the following:

- The `cacert.pem` file is present on both NetBackup master and media server in following locations:
  - UNIX/Linux - `/usr/openv/var/webtruststore`
  - Windows - `<install_path>/var/webtruststore`

If the `cacert.pem` file is not present, run the `nbcertcmd -getCACertificate` on the master server. After running this command, restart the NetBackup CloudStore Service Container.
See the *NetBackup Commands Reference Guide* for a complete description of the command.

Note: This cacert.pem file is a NetBackup-specific file. This file includes the CA certificates generated by the NetBackup authorization service.

- The `cacert.pem` file is same on the NetBackup master and media server.
- The machine certificate is present in following locations:
  - UNIX/Linux - `/usr/openv/var/vxss/credentials`
  - Windows - `<install_path>/var/vxss/credentials`

  If the security certificate is not present, run the `bpnbaz -ProvisionCert` on the master server. After running this command, restart the NetBackup CloudStore Service Container on the master and media server.
  See "Deploying host name-based certificates" on page 93.
- The NetBackup CloudStore Service is active.
  See "Stopping and starting the NetBackup CloudStore Service Container" on page 183.
- The **Enable insecure communication with 8.0 and earlier hosts** option on the NetBackup master server is selected if the media server is of the version 8.0 or earlier. The option is available in the **NetBackup Administration Console** on the **Security Management > Global Security Settings > Secure Communication** tab.
- On the media server, if the certificate deployment security level if set to Very High, automatic certificate deployment is disabled. An authorization token must accompany every new certificate request. Therefore, you must create an authorization token before deploying the certificates.
  See the 'Creating authorization tokens' topic in the *NetBackup™ Security and Encryption Guide* for detailed steps.

Data transfer to cloud storage server fails 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 fails 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.veritas.com/docs/DOC5332

Data restore from the Google Nearline storage class may fail

Data restore from the Google Nearline storage class may fail, if your `READ_BUFFER_SIZE` in NetBackup is set to a value that is greater than the allotted read throughput. Google allots the read throughput based on the total size of the data that you have stored in the Google Nearline storage class.

Note: The default `READ_BUFFER_SIZE` is 100 MB.

The NetBackup bptm logs show the following error after the data restore from Google Nearline fails:

```
HTTP status: 429, Retry type: RETRY_EXHAUSTED
```

Google provides 4 MB/s of read throughput per TB of data that you store in the Google Nearline storage class per location. You should change the READ_BUFFER_SIZE value in NetBackup to match it to the read throughput that Google allots.

For example, if the data that you have stored in the Google Nearline storage class is 5 TB, you should change the `READ_BUFFER_SIZE` value to match it to the allotted read throughput, which equals to 20 MB.

Refer to the Google guidelines, for more information:

https://cloud.google.com/storage/docs/nearline?hl=en

See “Changing cloud storage server properties” on page 110.

See “NetBackup cloud storage server connection properties” on page 117.

Backups may fail for cloud storage configurations with Frankfurt region

NetBackup 7.7.1 and later versions support configuring cloud storage using the Frankfurt region. NetBackup media servers that are older than the 7.7.1 version do not support configuring cloud storage using the Frankfurt region.

Cloud backups may fail in the following scenario:

You have configured cloud storage server with a media server that is older than NetBackup 7.7.1. You have created a disk pool in the Frankfurt region using an existing bucket.

To avoid such cloud backup failures, ensure that when you configure cloud storage using the Frankfurt region, the cloud media server is NetBackup 7.7.1 or later version.

Backups may fail for cloud storage configurations with the cloud compression option

The NetBackup cloud data compression option requires all cloud media servers that are associated with the cloud storage configuration to be NetBackup 7.7.3 or later version.

Cloud backups may fail in the following cloud compression scenario:

You have configured cloud storage server using the **NetBackup Administration Console** or the command-line interface with the compression option enabled, with a media server that is compatible. You then add a media server of a version that is older than NetBackup 7.7.3 using the command-line interface, to the same cloud configuration.

To avoid such cloud backup failures, ensure that all media servers that you add to the cloud storage configuration with the compression option to be NetBackup 7.7.3 or later version.

Fetching storage regions fails with authentication version V2

When you use authentication version V2, if fetching storage regions step fails with pop-up error `Unable to process request (228)`, perform the following troubleshooting steps:

Ensure that `nbsl` and `nbcssc` services are up and running.

Enable `nbcssc` logs and increase verbosity to highest level. Try fetching regions once again.

See “NetBackup cloudstore.conf configuration file” on page 90.

If the issue persists, look for cURL error in `nbcssc` logs. The cURL error code helps you to find the root cause of the issue.

Some of the erroneous configuration scenarios can be:

- If the cURL error indicates that issue is caused due to invalid authentication URL, ensure that identity API version 2 endpoint (v2.0/tokens) is used for authentication.
  For example, http://mycloud.xyz.com.com:5000/**v2.0/tokens** must be used to authenticate instead of https://mycloud.xyz.com:5000.
- If the cURL error indicates that the issue is caused due to non-CA signed certificate, add a self-signed certificate to `cacert.pem` for *authentication* as well as *storage endpoint* (in case they are hosted separately).

nbcssc service does not start after installation in clustered environment

This issue arises because the certificates are not available on the inactive nodes of the clustered master server. After finishing a clustered master server installation, you must generate a certificate on the inactive nodes.

For steps to generate certificate on the inactive nodes, see the *Veritas NetBackup Security and Encryption Guide*.

Troubleshooting cloud storage operational issues

The following sections may help you troubleshoot operational issues.

See "NetBackup Scalable Storage host properties unavailable" on page 172.

See "Cloud storage backups fail" on page 178.

See "A restart of the nbcssc process reverts all cloudstore.conf settings" on page 184.

See "NetBackup CloudStore Service Container startup and shutdown troubleshooting" on page 184.

See "NetBackup Administration Console fails to open" on page 171.

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

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 Veritas 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 154.

See "NetBackup cloud storage log files" on page 167.

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 184.

Backups may fail if the Use any available media server option is selected

While you configure a cloud storage server, you must ensure that the media server and the master server are of the same version.

Note: This limitation does not apply to the existing cloud storage servers.

Cloud backups may fail in the following scenario:

You selected **Use any available media server** while you configured the storage unit and NetBackup uses a media server with version different than the master server version during cloud storage configuration.

To resolve this issue, do the following:

Select **Only use the following media servers** while you configure the storage unit and select the media server with a version same as master server from the **Media Servers** pane.

Cloud backup and restore operations fail with error code 83 or error code 2106

The cloud backups and restore operations failing with error code 83 or error code 2106 may occur due to any one of the following reasons:

- The media server's date and time settings are skewed (not in sync with the GMT/UTC time).
- The storage server credentials that are provided are incorrect.

Perform the following:

Change the media server's date and time settings so that it is in sync with the GMT/UTC time.

Update the storage server credentials. Use the `tpconfig` command to update the credentials. For more information, see the *NetBackup Commands Reference Guide*.

Cloud storage backup fails for certificate issues

If the cloud storage backups fails because of certificate issues, verify the following:

- The `cacert.pem` file is present on both NetBackup master and media server in following locations:
  - UNIX/Linux - `/usr/openv/var/webtruststore`
  - Windows - `<install_path>/var/webtruststore`

  If the `cacert.pem` file is not present, run the `nbcertcmd -getCACertificate` on the master server. After running this command, restart the NetBackup CloudStore Service Container.
  See the *NetBackup Commands Reference Guide* for a complete description of the command.

  Note: This cacert.pem file is a NetBackup-specific file. This file includes the CA certificates generated by the NetBackup authorization service.

- The `cacert.pem` file is same on the NetBackup master and media server.
- That the machine certificate is present in following locations:
  - UNIX/Linux - `/usr/openv/var/vxss/credentials`
  - Windows - `<install_path>/var/vxss/credentials`

  If the security certificate is not present, run the `bpnbaz -ProvisionCert` on the master server. After running this command, restart the NetBackup CloudStore Service Container on the master and media server.
  See "Deploying host name-based certificates" on page 93.
- The NetBackup CloudStore Service is active.
  See "Stopping and starting the NetBackup CloudStore Service Container" on page 183.
- The **Enable insecure communication with 8.0 and earlier hosts** option on the NetBackup master server is selected if the media server is of the version 8.0 or earlier. The option is available in the **NetBackup Administration Console** on the **Security Management > Global Security Settings > Secure Communication** tab.
- On the media server, if the certificate deployment security level if set to Very High, automatic certificate deployment is disabled. An authorization token must accompany every new certificate request. Therefore, you must create an authorization token before deploying the certificates.
  See the 'Creating authorization tokens' topic in the *NetBackup™ Security and Encryption Guide* for detailed steps.

Backup jobs to Amazon S3 complaint cloud storage fail with status 41

NetBackup consumes the available bandwidth to it's maximum potential and pushes the requests accordingly, however the Amazon S3 complaint cloud is not able to process the number requests.

The cloud vendor returns error 503 to slow down the requests and the backup job fails with the following errors:

- In the media server `bptm` logs:

  ```
  bptm:4940:<media_server_name>: AmzResiliency:
  AmzResiliency::getRetryType cURL error: 0, multi cURL error: 0,
  HTTP status: 503, XML response: SlowDown, RetryType:
  RETRY_EXHAUSTED
  ```

- In the media server `bpbrm` logs:

  ```
  bpbrm Exit: client backup EXIT STATUS 41: network connection timed
  out
  ```

This issue arises only if higher bandwidth is available between NetBackup and the cloud storage.

To troubleshoot you can perform one of the following:

- Configure bandwidth throttling to reduce the number of requests.
  See "NetBackup cloud storage server connection properties" on page 117.
- Reduce the number of read/write buffers.
  See "NetBackup cloud storage server bandwidth throttling properties" on page 113.
- Talk to your cloud vendor to increase the number of parallel requests limit. This might incur extra cost.

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 88.

See "NetBackup CloudStore Service Container startup and shutdown troubleshooting" on page 184.

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
- CloudStore Service Container fails to start in a clustered environment

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 89.

NetBackup 7.7 and later	If a certificate does not exist, create one from the NetBackup master server. See “NetBackup CloudStore Service Container security certificates” on page 89.

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 90.

See “Stopping and starting the NetBackup CloudStore Service Container” on page 183.

CloudStore Service Container fails to start in a clustered environment

If the NetBackup master server is in a cluster environment, the required certificates for nbcssc are not deployed automatically on the passive node. Thus, the `nbcssc` service does not start on failover of the active node. This scenario happens mostly on a UNIX cluster environment, or on a Microsoft Windows Server Failover Cluster (WSFC) setup, if you add a new node after the NetBackup push installation.

Perform the following steps before the failover:

1. Run the following command on the active node of the master server cluster:

   On Windows: `Install_path\NetBackup\bin\admincmd\bpnbaz -setupat`

   On UNIX: `/usr/openv/netbackup/bin/admincmd/bpnbaz -setupat`

   See the *NetBackup Commands Reference Guide* for a complete description of the command.

2. Restart all services on the active node of the master server.

Index

O

P

R

S

T

U

V

W