Symantec NetBackup™ Cloud Administrator's Guide

Release 7.5

21220057

Symantec

Documentation version: 7.5

PN: 21220057

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Technical Support

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

Symantec's support offerings include the following:

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

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Chapter 1

About NetBackup Cloud storage

This chapter includes the following topics:

About Cloud Storage features and functionality

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

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

Table 1-1 Features and functionality

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

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

Feature	Details
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. ■ Maximum number of connections that are supported for each cloud provider at any given time. ■ Network bandwidth as a percent of total bandwidth. ■ Network bandwidth per block of time.
Metering	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 Cloud Storage 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 throttling plug-in On Windows, it is a standard service installed by NetBackup. On UNIX, it runs as a standard daemon.

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

Feature	Details
Storage providers	Symantec currently offers the following cloud storage providers: AT&T, Amazon, Nirvanix and Rackspace. More information is available about each of these vendors. See "About Nirvanix Cloud Storage Network" on page 55. See "About AT&T Synaptic" on page 54. See "About Amazon Simple Storage Service (S3)" on page 53. See "About Rackspace CloudFiles" on page 58.
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 seven days filtered on cloud-based storage. ■ **Cloud Metering**: Historical view of the data that is written to cloud per cloud provider. ■ **Average Data Transfer Rate**: Historical view of average data transfer rate to cloud per cloud provider. ■ **Cloud Metering Chargeback**: Ranking, forecast, and distribution view of the cost that is incurred on cloud-based storage per cloud provider.

About unsupported OpenStorage capabilities

None of the cloud providers support the following OpenStorage capabilities:

- Optimized duplication
- Direct to tape (by NDMP)
- Disk volume spanning of backup images

Legacy cloud storage considerations

If your NetBackup environment used NetBackup 7.1 Cloud storage through Nirvanix, this storage remains fully operational. You do not, however, have access to the new metering and throttling capabilities available in NetBackup 7.5. Legacy cloud storage is limited to Nirvanix provided cloud storage. The two legacy Nirvanix stypes are unencrypted (`nirvanix`) and encrypted (`nirvanix_e`). To take advantage of the new metering and throttling functionality in NetBackup 7.5, you

must create new Nirvanix cloud storage. For unencrypted Nirvanix, use the `nirvanix_raw` stype. For encrypted Nirvanix, us `nirvanix_crypt` stype.

More information about configuring these storage server types is available.

See "Using the Cloud Storage Configuration Wizard" on page 20.

Chapter 2

Planning your cloud deployment

This chapter includes the following topics:

Cloud installation requirements

When you develop a plan to implement a NetBackup Cloud solution, use Table 2-1 to assist with your plan.

Table 2-1 Required information

Requirement	Details
NetBackup media server platform support	Multiple NetBackup media server platforms support NetBackup Cloud Storage. ■ AIX ■ HP-UX ■ RedHat ■ Solaris 10 ■ SUSE ■ Windows 2008 R2 Please refer to the release notes for information on supported media servers before you configure NetBackup Cloud Storage.

Table 2-1 Required information *(continued)*

Requirement	Details
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 cloud storage providers" on page 53.
NetBackup Cloud Storage licensing	NetBackup Cloud Storage is enabled through the Enterprise Disk License. No additional cloud-specific license key is required for the basic cloud features. If you plan to use NetBackup Accelerator with NetBackup Cloud you must upgrade to the Data Protection Optimization Option which includes the NetBackup Accelerator feature.

Note:

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

Example:

```
ulimit -m unlimited

ulimit -d unlimited

ulimit -s unlimited
```

About changing media servers for a storage server

Once you have specified a media server for a storage server, you cannot change the media server. This behavior is the result of the current OST plugin design. Attempts to change the media server generate an authorization error.

Chapter 3

Configuring

This chapter includes the following topics:

About configuring the cloud feature

After planning your cloud deployment, use either the NetBackup Administrative Console or the command line to configure your cloud environment.

The following procedure outlines the process you need to configure cloud storage.

Table 3-1 Overview of the NetBackup Cloud configuration process

Step	Procedure	More information
1	Enable log files on the master and the media servers	More information about cloud specific logs is available. See "Enabling NetBackup logging" on page 68. For general information on NetBackup logs on how to set the debug level, see *Logging properties* in the *Symantec NetBackup Administrator's Guide, Volume I*. For details on both unified and legacy logging, see the *NetBackup Troubleshooting Guide*.
2	Launch the Cloud Storage Configuration Wizard	See "Using the Cloud Storage Configuration Wizard" on page 20.
3	Select the storage provider for the cloud connection you want to make.	See "Cloud storage provider selection panel" on page 20.
4	Specify the unique information for the specified vendor.	See "Cloud provider configuration panel for Amazon " on page 20. See "Cloud provider configuration panel for AT&T " on page 21. See "Cloud provider configuration panel for Nirvanix " on page 22. See "Cloud provider configuration panel for Rackspace " on page 22.
5	(Conditional) Enter any advanced settings as required in your environment.	See "Cloud provider advanced setting panel" on page 23.
6	Specify encryption settings	See "Cloud encryption panel" on page 23.
7	Review the cloud configuration summary panel.	See "Cloud storage configuration summary panel" on page 25.

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

Step	Procedure	More information
8	Monitor the configuration process.	See "Cloud storage configuration progress panel" on page 25.
9	Review the configuration completion panel.	See "Cloud storage configuration completion panel" on page 25.
10	Configure disk pool	See "Using the Disk Pool Configuration Wizard" on page 26.
11	Configure storage unit	See the *Configuring storage units* chapter in the *Symantec NetBackup Administrator's Guide, Volume I*.
12	(Conditional) Create a cloud storage volume for the cloud vendor specified.	See "Create buckets for Amazon" on page 26. See "Create cloud storage volume for AT&T" on page 26. See "Create cloud storage volume for Nirvanix" on page 27. See "Create cloud storage volume for Rackspace" on page 27.
13	Review and update the cloud host properties as necessary.	See "Cloud Host Properties" on page 27.
14	Test the environment	Confirm backup and restore operations work correctly.
15	Disable log files on the master and the media servers	Set the debug level to zero in the NetBackup Administrative Console to disable logs. For general information on NetBackup logs on how to set the debug level, see *Logging properties* in the *Symantec NetBackup Administrator's Guide, Volume I*. For details on both unified and legacy logging, see the *NetBackup Troubleshooting Guide*.

See "Using the Cloud Storage Configuration Wizard" on page 20.

Using the Cloud Storage Configuration Wizard

Cloud storage wizard welcome panel

Review the welcome information. Click **Next** to continue

See "Cloud storage provider selection panel" on page 20.

See "About configuring the cloud feature" on page 17.

Cloud storage provider selection panel

For the cloud provider panel, select the cloud provider you want to configure. Click **Next** to continue.

See "Cloud provider configuration panel for Nirvanix " on page 22.

See "Cloud provider configuration panel for Rackspace " on page 22.

See "Cloud provider configuration panel for Amazon " on page 20.

See "Cloud provider configuration panel for AT&T " on page 21.

See "About configuring the cloud feature" on page 17.

Cloud provider configuration panel for Amazon

On the cloud storage device panel, specify the required information for Amazon and click **Next**.

Table 3-2

Field name	Required content
Media server name	Select the name of your media server from the drop-down list. If your media server is not shown in the list, confirm it is displayed correctly in the NetBackup Administrative Console under **Host Properties > Media servers**. Additionally, confirm the cloud binaries are present in `ost-plugins` folder and the `nbcssc` service or daemon is running.
Checkbox	Select **I have an Amazon S3 account** to enter the required account and storage pool information.
Access ID	Enter your Amazon S3 Access ID. If you do not have an account, click **Create an account with the service provider** link.

Table 3-2 *(continued)*

Field name	Required content
Secure Access Token	Enter your Amazon S3 Secure Access Token.

Click **Advanced Settings** to specify the storage server name (if it is different from the default) or to make changes to the maximum network connections.

See "Cloud provider advanced setting panel" on page 23.

See "Create buckets for Amazon" on page 26.

See "About configuring the cloud feature" on page 17.

Cloud provider configuration panel for AT&T

On the cloud storage device panel, specify the required information for AT&T and click **Next**.

Table 3-3

Field name	Required content
Media server name	Select the name of your media server from the drop-down list. If your media server is not shown in the list, confirm it is displayed correctly in the NetBackup Administrative Console under **Host Properties > Media servers**. Additionally, confirm the cloud binaries are present in `ost-plugins` folder and the `nbcssc` service or daemon is running.
Checkbox	Select **I have an AT&T synaptic storage account** to enter the required account and storage pool 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 your AT&T password.

Click **Advanced Settings** to specify the storage server name (if it is different from the default) or to make changes to the maximum network connections.

See "Cloud provider advanced setting panel" on page 23.

See "Create cloud storage volume for AT&T" on page 26.

See "About configuring the cloud feature" on page 17.

Cloud provider configuration panel for Nirvanix

On the cloud storage device panel, specify the required information for Nirvanix and click **Next**.

Table 3-4

Field name	Required content
Media server name	Select the name of your media server from the drop-down list. If your media server is not shown in the list, confirm it is displayed correctly in the NetBackup Administrative Console under **Host Properties > Media servers**. Additionally, confirm the cloud binaries are present in `ost-plugins` folder and the `nbcssc` service or daemon is running.
Checkbox	Select **I have a Nirvanix Cloud Storage Network account** to enter the required account and storage pool information.
Master account name	Enter the Nirvanix provided master account name. If you do not have an account, click **Create an account with the service provider** link.
Password	Enter the password that is associated with the master account name.
Storage pool name	Enter the name for the storage pool. This name must be unique to the Nirvanix Cloud Storage Network storage space.

Click **Advanced** to specify the storage server name (if it is different from the default) or to make changes to the maximum network connections.

See "Cloud provider advanced setting panel" on page 23.

See "Create cloud storage volume for Nirvanix" on page 27.

See "About configuring the cloud feature" on page 17.

Cloud provider configuration panel for Rackspace

On the cloud storage device panel, specify the required information for Rackspace and click **Next**.

Table 3-5

Field name	Required content
Media server name	Select the name of your Media server from the drop-down list. If your media server is not shown in the list, confirm it is displayed correctly in the NetBackup Administrative Console under **Host Properties > Media servers**. Additionally, confirm the cloud binaries are present in `ost-plugins` folder and the `nbcssc` service or daemon is running.
Checkbox	Select **I have a Rackspace Cloud Files account** to enter the required account and storage pool information.
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 .

Click **Advanced** to specify the storage server name (if it is different from the default) or to make changes to the maximum network connections.

See "Cloud provider advanced setting panel" on page 23.

See "Create cloud storage volume for Rackspace" on page 27.

See "About configuring the cloud feature" on page 17.

Cloud provider advanced setting panel

The Advanced Server Configuration window lets you change the storage server name and the maximum number of network connections.

If the storage server name you use is different from the default, specify that information in this window.

Change the number of network connections in this window to limit how many simultaneous operations can take place on this server. If you do not set the value here, the global value from **Media server > Host properties** is used.

See "Cloud storage configuration summary panel" on page 25.

See "About configuring the cloud feature" on page 17.

Cloud encryption panel

When you select the encrypt data option your data is encrypted before it is sent to the cloud.

The NetBackup Key Management Service (KMS) encrypts the data before it is sent to the cloud. When you specify encryption, if encryption is already enabled, you see a summary screen with the required information displayed. The feature cannot be edited on this screen if encryption is already configured.

More information about the configuration of KMS is available. See the *NetBackup Security and Encryption Guide*.

If the KMS service is not enable, you are prompted for more information.

Table 3-6 Required encryption information

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 passphrase you want associated with your host master key. Refer to the *NetBackup Security and Encryption Guide* for details on password criteria and limitations.
Re-enter HMK Passphrase	Re-enter the passphrase you entered for the host master key.
Host Master Key ID	The tag that is used to identify the particular host master key. Enter an ID for your 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 passphrases that are associated with the files.
Key Protection Key (KPK) Passphrase	Enter the passphrase you want associated with your key protection key. Refer to the *NetBackup Security and Encryption Guide* for details on password criteria and limitations.
Re-enter KPK Passphrase	Re-enter the passphrase you entered for the key protection key.

Table 3-6 Required encryption information *(continued)*

Field Name	Required information
Key Protection Key ID	The tag that is used to identify the particular key protection key. Enter an ID for your 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 passphrases that are associated with the files.

More information about encryption is available.

See "About NetBackup Key Management Service" on page 33.

Cloud storage configuration summary panel

This panel summarizes the information you provided in the Cloud storage server wizard. Review the information that is contained in this panel. Click **Next** to continue or **Back** to return to previous panels and make changes.

See "Cloud storage configuration progress panel" on page 25.

See "About configuring the cloud feature" on page 17.

Cloud storage configuration progress panel

Monitor this panel to view the progress of the storage server creation.

See "Cloud storage configuration completion panel" on page 25.

See "About configuring the cloud feature" on page 17.

Cloud storage configuration completion panel

This panel reports the final status of the storage server creation. Click **Next** to create a Disk Pool or click **Close** to complete the wizard.

See "Create buckets for Amazon" on page 26.

See "Create cloud storage volume for AT&T" on page 26.

See "Create cloud storage volume for Nirvanix" on page 27.

See "Create cloud storage volume for Rackspace" on page 27.

See "About configuring the cloud feature" on page 17.

Using the Disk Pool Configuration Wizard

Disk pool creation for cloud storage is the same any other disk pool, with two exceptions.

1. You can create volumes with the **Add Volume** button on the **Select volume** panel.
2. When you create encrypted storage, you must enter a passphrase for each selected volume that uses encryption. The passphrase creates the encryption key for that volume.

Table 3-7 Create key record for each cloud storage volume dialog box

Property	Description
Use the same passphrase to create all key records	Uses the same passphrase to create the key record on each volume.
Use the different passphrase to create each key record	Uses different passphrases to create the key record on each volume. If you select this option, there is an option for **Passphrase** and **Re-enter Passphrase** for each volume.
Passphrase and Re-enter passphrase	Passphrase for the volume.

More information is available about the creation of disk pools.

See *Configuring disk storage* in the *Symantec NetBackup Administrator's Guide, Volume I*.

Create buckets for Amazon

Amazon uses the term bucket for the storage it creates. In the **Create Buckets** panel, enter a bucket name and click **Create**. Be sure to review and follow the restrictions for bucket names.

See "Cloud Host Properties" on page 27.

See "About configuring the cloud feature" on page 17.

Create cloud storage volume for AT&T

AT&T uses storage volume for the storage it creates. In the **Create Cloud Storage Volume** panel, enter a volume name and click **Create**. Be sure to review and follow the restrictions for volume names.

See "Cloud Host Properties" on page 27.

See "About configuring the cloud feature" on page 17.

Create cloud storage volume for Nirvanix

Nirvanix uses storage volume for the storage it creates. In the **Create Cloud Storage Volume** panel, enter a volume name, adjust the size limitation if desired, and click **Create**. Be sure to review and follow the restrictions for volume names.

See "Cloud Host Properties" on page 27.

See "About configuring the cloud feature" on page 17.

Create cloud storage volume for Rackspace

Rackspace uses storage volume for the storage it creates. In the **Create Cloud Storage Volume** panel, enter a volume name and click **Create**. Be sure to review and follow the restrictions for volume names.

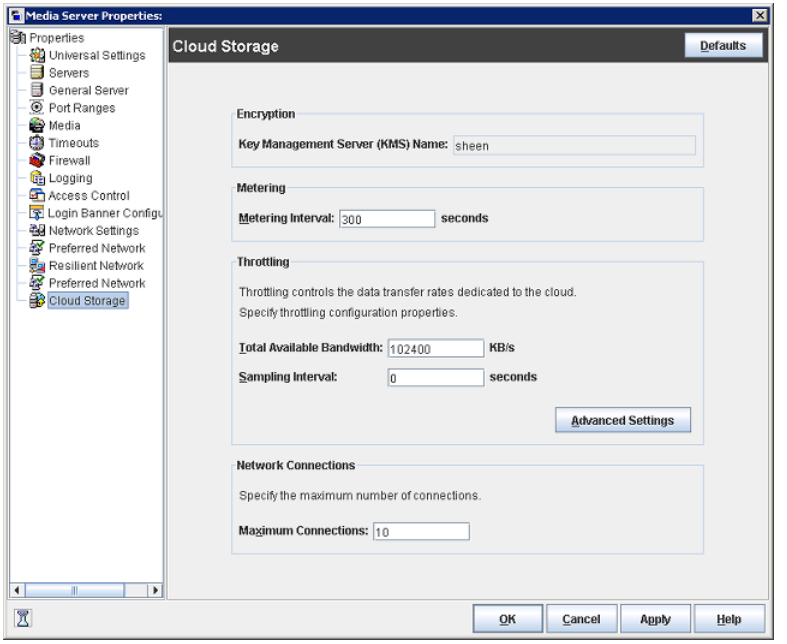
See "Cloud Host Properties" on page 27.

See "About configuring the cloud feature" on page 17.

Cloud Host Properties

The **Cloud Storage** properties apply to currently selected media servers. The **Cloud Storage** properties contain information about metering, bandwidth throttling, and network connections.

Figure 3-1 Cloud Storage dialog box



The **Cloud Storage** dialog box contains the following properties.

Table 3-8 Cloud Storage dialog box properties

Property	Description
Key Management Server (KMS) Name	The name of your site's KMS server. If you have not configured KMS, this displays as `<kms_server_name>`.
Metering Interval	Determines how often information is gathered for reporting purposes. OpsCenter uses the information that is collected to create reports. The value is set in seconds. The default setting is 300 seconds (5 minutes). If you set this value to zero, metering is disabled.
Total Available Bandwidth	Use this value to specify the speed of your connection to the cloud. The value is specified in kilobytes per second. The default value is 104857600 KB/sec.
Sampling interval	The time, in seconds, between measurements of bandwidth usage. The larger this value, the less often NetBackup checks to determine the bandwidth in use.

Table 3-8 Cloud Storage dialog box properties *(continued)*

Property	Description
Maximum connections	This value determines the maximum number of connections that are allowed for the cloud provider.

Click **Advanced Settings** to specify additional settings for throttling. The **Advanced Throttling Configuration** dialog box contains the following properties.

Figure 3-2 Advanced Throttling Configuration dialog box

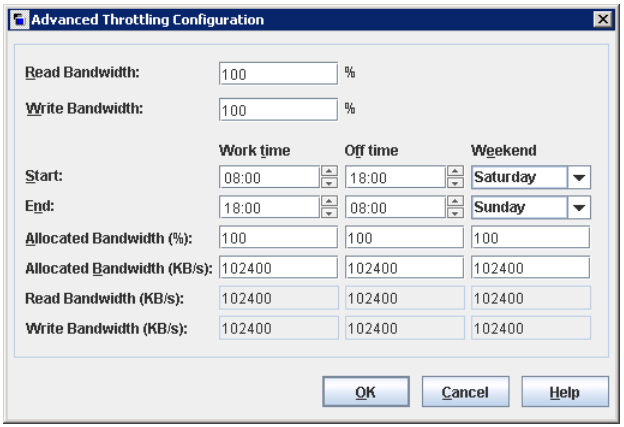


Table 3-9 Advanced Throttling Configuration dialog box

Property	Description
Read bandwidth	The read bandwidth value determines the size of the data packs transmitted from the cloud during each restore job. An increase in the value may increase performance when large amounts of contiguous data are accessed. If there is insufficient bandwidth to transmit the specified amount of data within a few minutes, restore failures may occur due to timeouts. Consider the total load of simultaneous jobs on multiple media servers when you calculate the required bandwidth.

Table 3-9 Advanced Throttling Configuration dialog box *(continued)*

Property	Description
Write bandwidth	The write bandwidth value determines the size of the data packs transmitted from the local computer to the cloud during each backup job. An increase in the value may increase performance when large amounts of contiguous data are accessed. If there is insufficient bandwidth to transmit the specified amount of data within a few minutes, restore failures may occur due to timeouts. Consider the total load of simultaneous jobs on multiple media servers when you calculate the required bandwidth.
Work time	Use this field to specify the time interval that is considered work time for the cloud connection. Specify a start and an 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 and an 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.

Using the command line for cloud configuration

You can use the NetBackup command line to configure your cloud deployment. Use the following procedure to configure cloud from the command line.

Note: For command line logging, see *About logging the command lines that the NetBackup interfaces use* in the *Symantec NetBackup Administrator's Guide, Volume I.*

To configure cloud from the command line

1 Configure the cloud server with the `nbdevconfig` command. The `nbdevconfig` command is found in the `/usr/openv/netbackup/bin/admincmd` directory on Linux/UNIX and the *`install_path`*`\NetBackup\bin\admincmd` directory on Windows.

```
nbdevconfig -creatests -storage_server cloud_provider_url -stype
cloud_storage_server_type -media_server hostname
```

In the preceding command

- *cloud_provider_url* is the correct URL for the cloud storage provider. For each cloud service you configure, set the storage server parameter to the URL of the cloud service. For private clouds, set this value to the URL of your private cloud.

Cloud provider	URL of the cloud service
Nirvanix	`nirvanix.com`
Rackspace	`rackspace.com`
AT&T	`storage.synaptic.att.com`
Amazon	`amazon.com`

- *cloud_storage_server_stype* defines the storage type and storage vendor created. The storage type is either encrypted or not encrypted. The vendor is the name of the cloud provider.

Cloud provider	Encryption disabled stype	Encryption enabled stype
Nirvanix	`nirvanix_raw`	`nirvanix_crypt`
Rackspace	`rackspace_raw`	`rackspace_crypt`

Cloud provider	Encryption disabled stype	Encryption enabled stype
AT&T	`att_raw`	`att_crypt`
Amazon	`amazon_raw`	`amazon_crypt`

2 Configure the credentials for the NetBackup cloud storage server using the `tpconfig` command.

Windows: *`NetBackup_install_path`*`\volmgr\bin\tpconfig`

UNIX/Linux: `/usr/openv/volmgr/bin/tpconfig`

The full command is:

```
tpconfig -add -storage_server cloud_provider_url -stype
cloud_storage_server_type -sts_user_id cloud_provider_account_name
-password cloud_provider_account_password
```

More information about this command is available. See the *Symantec NetBackup, Commands Reference Guide, UNIX, Windows, and Linux.*

3 (Optional) Configure encryption.

More information about encryption is available

See "About NetBackup Key Management Service" on page 33.

4 Configure a disk volume for the Cloud.

```
nbdevconfig -createdv -stype cloud_storage_server_type -dv
disk_volume_name -dp disk_pool_name -storage_server
cloud_provider_url
```

More information about this command is available. See the *Symantec NetBackup, Commands Reference Guide, UNIX, Windows, and Linux.*

5 Configure a disk pool with the `nbdevconfig -createdp` command. You use the command to create a disk pool from the specified list of disk volumes. You can specify additional properties like High Water Mark and comments with the command. More information about this command is available. See the *Symantec NetBackup, Commands Reference Guide, UNIX, Windows, and Linux.*

6 Configure a storage unit using the `bpstuadd` command. You use the command to create NetBackup storage unit or storage group. More information about this command is available. See the *Symantec NetBackup, Commands Reference Guide, UNIX, Windows, and Linux.*

About NetBackup Key Management Service

The NetBackup Key Management Service (KMS) feature is a symmetric Key Management Service. KMS is included as part of the NetBackup Enterprise Server and NetBackup Server software. It runs on the NetBackup master server. An additional license is not required to use the KMS functionality.

Be aware of the following points when configuring NetBackup KMS:

- KMS requires a Host Master Key passphrase and ID when you create the key management database. The Key Management Service can create a random passphrase for you.
- KMS requires a Key Protection Key passphrase and ID when you create the key management database. The Key Management Service can create a random passphrase for you.
- Each Cloud storage target you use for NetBackup storage requires a key group. KMS requires a name for each key group. Use the following format for the key group name: *cloud_provider_url*:*volume_name*.
- Unlike other storage types, the key group name does not require the `ENCR_` prefix.
- Each key group you create requires a key record. KMS requires a passphrase when you create the key record. A key record name is optional. If you use a key record name, you can use any name for the key record name. Symantec recommends that you use a descriptive name.
- You must activate the key to use it for encryption.

More information about how to configure NetBackup KMS though the NetBackup Administrative Console is available. See the *Data at rest key management* chapter in the *NetBackup Security and Encryption Guide*.

Using the command line to configure the NetBackup Key Management Service

If you do not have Key Management Service (KMS) configured, the Cloud Storage Server Configuration Wizard includes steps to create and enable KMS. You can also use the command line to configure KMS. Use the following procedure to configure KMS from the command line.

To configure NetBackup KMS from the command line

1. Create an empty KMS database.

   ```
   nbkms -createemptydb
   ```

2. Create a key group that is associated with the storage target. For each storage target you create, you must create a corresponding key group name.

   ```
   nbkmsutil -createkg -kgname cloud_provider_URL:volume_name
   ```

   The *storage_server_URL* variable is the name of the storage server that is configured during the cloud storage target configuration. More information is available.

   See "Using the command line for cloud configuration" on page 31.

3. Create a key associate to the key group. For each key group you create, you must create a corresponding key.

   ```
   nbkmsutil -createkey -kgname cloud_provider_URL:volume_name
   -keyname key_passphrase -activate
   ```

More information about how NetBackup KMS is available. See the *NetBackup Security and Encryption Guide*.

Cloud Storage Preferences

The cloud storage preferences are set at one of two times.

- If you use the NetBackup Cloud Storage Configuration Wizard, set the Storage Server Properties after you finish the wizard.
- If you use the command line, set the Storage Server Properties after you create the Storage Server.

To change storage server properties in the NetBackup Administration Console

1. Select **Management > Credentials > Storage Server NetBackup Administration Console Media and Device**.
2. Select the storage server.
3. From the **Edit** menu, select **Change**.
4. In the **Change Storage Server** dialog, select **Properties**.

All the available properties are displayed in list format. Values that are unavailable are fixed and you cannot change them. The properties are displayed using the following format:

```
prefix:property
```

For example:

NVX:USE_SSL where NVX is the prefix and USE_SSL is the Storage Server Property.

Table 3-10 Prefixes and their definition

Prefix	Prefix meaning
AMZ	Amazon
ATT	AT&T
CRYPT	Encrypted
METER	Metering
NVX	Nirvanix
RACKS	Rackspace
THR	Throttling

Note: Not all options apply to all plug-ins. For example USE_SSL applies only to the storage facing plug-ins (Amazon, Rackspace, Nirvanix and AT&T).

The intervening plug-ins (throttling, metering, and encryption) have their own options that only apply to their particular case.

The following storage server properties are specific to Nirvanix. You can only use the prefix NVX with them. You can edit these values from the storage server properties dialog.

Table 3-11 Nirvanix specific storage server properties

Property	Default value	Possible values	Description
NVX:CHILD_ACCOUNT_NAME	The name you give to your Nirvanix child account.	Any valid text string.	The NVX:CHILD_ACCOUNT_NAME is the disk volume where the backup images reside.

Table 3-11 Nirvanix specific storage server properties *(continued)*

Property	Default value	Possible values	Description
NVX:CHILD_ACCOUNT_SIZE	0	8192 PB	The total size for the Nirvanix child account. If you don't set this value, the size is shown as 0, but Nirvanix interprets the value as unlimited. You can specify the value in bytes by entering a number, or in megabytes or gigabytes by using either the MB or the GB suffix. The value 1048576000 is understood to be in bytes. If you enter 250GB, the value is understood as 250 gigabytes. This value is only used when you use a configuration file to create a child account. You must use the Nirvanix Web portal to modify this value after it is created.
NVX:RESTRICT_IP	YES	YES or NO	Determines if multiple hosts can upload and download with the same token. This value applies only to Nirvanix environments. The Nirvanix plug-in uses the token to group and validate multiple parts of large data transfers. The token is obtained during login. ■ If RESTRICT_IP is set to YES, only one host can use an upload-download token. By default,RESTRICT_IP is set to YES. This setting prevents any intrusions into the session by any other host. ■ If RESTRICT_IP is set to NO, multiple host addresses can upload and download using the same token. If the host's IP address changes, this setting allows the host to continue with the session. A host IP address may change because of network address translation (NAT) or proxies. Set RESTRICT_IP to NO for these environments.

Table 3-11 Nirvanix specific storage server properties *(continued)*

Property	Default value	Possible values	Description
NVX:STORAGE_POOL_NAME	The name you give to your Nirvanix storage pool.	Any valid text string.	A Nirvanix Application which contains one or more child accounts. The storage pool name must be unique across master accounts. Symantec recommends making the NVX:STORAGE_POOL_NAME as specific to your environment as possible.

The following storage server properties are common to all storage servers. Use the correct prefix for the desired cloud vendor. The prefixes are NVX for Nirvanix, AMZ for Amazon, ATT for AT&T, and RACKS for Rackspace. You can edit these values from the storage server properties dialog.

Table 3-12 Common cloud storage properties

Property	Default value	Possible values	Description
PREFIX: CURL_CONNECT_TIMEOUT	300	1 to 10000	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. The media server makes three attempts to connect out during the specified time. 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. In addition to the CURL_CONNECT_TIMEOUT that is a global value, you can set a cURL timeout value for each cloud vendor. If these values are set, they apply only to the specified vendor. The properties are: ■ Nirvanix: NVX:CURL_CONNECT_TIMEOUT ■ AT&T: ATT:CURL_CONNECT_TIMEOUT ■ Amazon: AMZ:CURL_CONNECT_TIMEOUT ■ Rackspace: RACKS:CURL_CONNECT_TIMEOUT If both the global value and the vendor-specific values are set, the vendor-specific value takes precedent.

Table 3-12 Common cloud storage properties *(continued)*

Property	Default value	Possible values	Description
PREFIX:CURL_TIMEOUT	900	1 to 10000	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). The media server attempts the operation up to three times. To disable this timeout, set the value to 0 (zero).
PREFIX:LOG_CURL	NO	NO (disabled) and YES (enabled)	Determines if cURL activity is logged. The default is NO which means log activity is disabled.
PREFIX:PROXY_IP	No default	Valid TCP/IP address	The TCP/IP address of the proxy server. If you do not use a proxy server, leave this field blank.
PREFIX:PROXY_PORT	70000	Valid port number	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.
PREFIX:PROXY_TYPE	NONE	NONE, HTTP, SOCKS, SOCKS4, SOCKS5, SOCKS4A	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.
PREFIX: READ_BUFFER_SIZE	0	524288 (512 KB) to 1073741824 (1 GB)	The size of the buffer to use for read operations. The default is 0 and the value is specified in bytes. To enable the use of the buffer, set this value to a non-zero number. Symantec recommends that this value be a multiple of 256. More information about READ_BUFFER_SIZE is available. See "About write buffer size, read buffer size, and download bandwidth" on page 44.

Table 3-12 Common cloud storage properties *(continued)*

Property	Default value	Possible values	Description
PREFIX:USE_SSL	YES	YES or NO	Determines if Secure Sockets Layer encryption is used for the control APIs. The default value is YES, meaning SSL is enabled.
PREFIX:USER_SSL_RW	YES	YES or NO	Determines if Secure Sockets Layer encryption is used for read and write operations. The default value is YES, meaning SSL is enabled.
PREFIX: WRITE_BUFFER_NUM	1	1	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.
PREFIX: WRITE_BUFFER_SIZE	10485760	10485760 (10 MB) to 1073741824 (1 GB)	The size of the buffer to use for write operations. The value is specified in bytes. The default is 10485760 (10 MBs). Valid values are 0 to 10487560 (1 GB). To disable the use of the buffer, set this value to 0 (zero). More information about WRITE_BUFFER_SIZE is available. See "About write buffer size, read buffer size, and download bandwidth" on page 44.

The following throttling-specific properties are common to all storage servers. You must specify the throttling (THR) prefix with these properties. Use the correct cloud provider URL for the desired cloud vendor. You can edit these values two different ways. You can edit these values from the **Host properties > Media servers (select the appropriate media server) > Cloud connect**. You can also edit these values from the command line using the `csconfig throttle` command.

Table 3-13 Throttling cloud storage properties

Property	Default value	Possible values	Description
THR:*storage_server*	Not applicable	See Description	Shows the storage server name for specified cloud storage server. Possible values for *storage_server* are: ■ Amazon: amazon.com ■ AT&T: storage.synaptic.att.com ■ Nirvanix: nirvanix.com ■ Rackspace: rackspace.com
THR:AVAIL_BANDWIDTH	104857600	Any positive integer	Changes 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.
THR: DEFAULT_MAX_CONNECTIONS	10	1 to 2147483647	Changes the maximum number of connections for each cloud provider. The option does not have a hard coded limit. In practice, you should not need to set this value higher than 100. The default value is 10.
THR: OFF_TIME_BANDWIDTH_PERCENT	100	0 to 100	Defines the bandwidth percent that is used during off time.
THR:OFF_TIME_END	8	0 to 2359	Defines 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.
THR:OFF_TIME_START	18	0 to 2359	Defines 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.
THR: READ_BANDWIDTH_PERCENT	100	0 to 100	Changes 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.

Table 3-13 Throttling cloud storage properties *(continued)*

Property	Default value	Possible values	Description
THR:SAMPLE_INTERVAL	0	1 to 2147483647	Specifies 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.
THR:WEEKEND_BANDWIDTH_PERCENT	100	0 to 100	Defines the bandwidth percent that is used during the weekend.
THR:WEEKEND_END	7	1 to 7	Defines the end of the weekend. The day value is specified with numbers, 1 for Monday, 2 for Tuesday, and so on.
THR:WEEKEND_START	6	1 to 7	Defines the start of the weekend. The day value is specified with numbers, 1 for Monday, 2 for Tuesday, and so on.
THR:WORK_TIME_BANDWIDTH_PERCENT	100	0 to 100	Defines the bandwidth percent that is used during the work time.
THR:WORK_TIME_END	18	0 to 2359	Defines 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.
THR:WORK_TIME_START	8	0 to 2359	Defines 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.
THR:WRITE_BANDWIDTH_PERCENT	100	0 to 100	Changes 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.

The following encryption-specific properties are common to all encrypted storage servers. You must specify the encryption (CRYPT) prefix with these properties. These values are for display purposes only and cannot be changed.

Table 3-14 Encryption cloud storage properties

Property	Default value	Possible values	Description
CRYPT:KMS_SERVER	*master server name*	N/A	The 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.
CRYPT:KMS_VERSION	16	N/A	The NetBackup Key Management Service version. You cannot change this value.
CRYPT:LOG_VERBOSE	NO	YES and NO	Determines if logs are enabled for encryption activities. The value is either YES for logging or NO for no logging.
CRYPT:VERSION	13107	N/A	The encryption version. You cannot change this value.

The following metering-specific properties are common to all storage servers. You must specify the metering (METER) prefix with these properties. Use the correct cloud provider URL for the desired cloud vendor. You can edit these values from the **Host properties > Media servers (select the appropriate media server) > Cloud connect**.

Table 3-15 Metering cloud storage properties

Property	Default value	Possible values	Description
METER:DIRECTORY	See Description	Valid directory locations.	The directory where metering information is stored. The default value for METER:DIRECTORY is /usr/openv/lib/ost-plugins/meter. You cannot change this value from the **Host Properties** window. You must use the csconfig meter command.

Table 3-15 Metering cloud storage properties *(continued)*

Property	Default value	Possible values	Description
METER:INTERVAL	300	0 to 86400 (24 hours)	Determines the metering interval. The value is specified in seconds. The METER:INTERVAL parameter is the time interval, in seconds, between persisted measurements. This parameter accepts interval values from 0 (zero) to 86400 (24 hours). The setting METER:INTERVAL=5 means a metering interval of every five seconds. Setting the metering interval to 0 (zero) disables metering.

About write buffer size, read buffer size, and download bandwidth

The WRITE_BUFFER_SIZE value determines the size of the data packs transmitted from the computer to the cloud during a backup. Similarly, the READ_BUFFER_SIZE values determines the size of the data packs transmitted from the cloud during each restore job. An increase in the value may increase performance when a large amount of contiguous data is accessed. If there is insufficient bandwidth to transmit the specified amount of data within a few minutes, backup and 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.

To adjust the write buffer size and the read buffer size

1. Launch the NetBackup Administration Console.
2. Select **Media and Device Management > Credentials > Storage Servers**.
3. Right-click the storage server you want to modify and select **Change**.
4. Modify the WRITE_BUFFER_SIZE and the READ_BUFFER_SIZE attributes as necessary for your environment.

About the NetBackup Cloud Storage Service Container

Cloud Storage Service Container is a web-based service container that runs on the media server that is configured for cloud. This container hosts different services such as the configuration service, the throttling service, and the metering data collector service.

The configuration service enables various cloud store configuration changes to things like throttling and metering. The throttling service acts as data collector for throttling related data. The throttling component uses this service to store relevant data. The metering service acts as a data collector for metering data. The metering component interacts with this service to store metering data. OpsCenter uses this data for monitoring and reporting purpose.

Configuration is done through the NetBackup Administrative Console or from the command line. In the NetBackup Administrative Console, configuration is part of the media server host properties, under **Cloud Storage**. From the command line, use the `csconfig` command to make changes.

The configuration settings for the NetBackup Cloud Storage Service Container are stored in an operating system specific location.

- UNIX and Linux: In the `/usr/openv/lib/ost-plugins/cloudstore.conf` file.
- Windows: In the `HKEY_LOCAL_MACHINE\SOFTWARE\Veritas\NetBackup\CurrentVersion\CloudStore` registry key.

The NetBackup Cloud Storage Service Container can be started in either secure or non-secure mode. The security mode determines how the clients communicate with the service. Use the `CSSC_IS_SECURE` attribute to set the security mode. The default value is 1, secure communication.

When the service is started in secure mode, the client components must authenticate before it communicates over a secure HTTPS channel. The server generates a self-signed certificate which lasts for 365 days and uses that certificate for authentication. The certificate is named `cssc.crt`. The file is located in the `/usr/openv/lib/ost-plugins` directory on UNIX/Linux and *`install_path`*`\Veritas\NetBackup\bin\ost-plugins` on Windows. If the certificate becomes corrupt or expires, delete the old certificate and restart the services to regenerate a new certificate.

If you change the `CSSC_IS_SECURE` value to zero, that indicates non-secure communication. The client communicates with the server over HTTP with no authentication required.

Configuring Cloud storage throttling and metering

The Cloud Storage throttling and metering configuration parameters are configured using the `csconfig` command. The `csconfig` is used to manage these configuration values from the local computer or from a remote host. To manage the values from a remote host, use the `-cshost` argument. If the service is running on a port other than the default port, use the `-csport` argument to specify the correct port. The `csconfig` command is located in the `/usr/openv/netbackup/bin/admincmd` for UNIX and Linux and *`install_path`*`\Veritas\NetBackup\bin\admincmd` for Windows.

The `csconfig` command and its output are logged. The log details are defined in the `cloudstore.conf` file for UNIX and Linux. The `cloudstore.conf` file is located in the `/usr/openv/lib/ost-plugins/` directory. The log details are defined in the registry for Windows. The registry key for Windows is `HKEY_LOCAL_MACHINE\SOFTWARE\Veritas\NetBackup\CurrentVersion\CloudStore`.

The log file location is specified with the `CSSC_LOG_DIR` attribute. The default log location is `/usr/openv/netbackup/logs/nbcssc` for UNIX and Linux and *`install_path`*`\Veritas\NetBackup\logs\nbcssc` for Windows. If the attribute is not present, the default location is used.

The `CSCONFIG_LOG_FILE` attribute defines the log file name. If the attribute is not present, the default name for the log file is `csconfig.log`.

The command usage is as follows:

`csconfig` *`option`* `[-n | -cshost cloud_connect_server_name] [-p | -csport cloud_connect_service_port] [arguements] [values]`

The options and arguments for throttling are shown in Table 3-16.

Table 3-16 Throttling options and their values

Option	Details
`throttle`	Retrieves the throttling configuration details from the master server.
`throttle -rbw | -readbw` *`value`*	Changes the read bandwidth percentage the cloud feature uses. Specify a value between 0 and 100. If you enter an incorrect value, an “Illegal value specified”error is generated.

Table 3-16 Throttling options and their values *(continued)*

Option	Details
`throttle -wbw | -writebw value`	Changes the write bandwidth percentage the cloud feature uses. Specify a value between 0 and 100. If you enter an incorrect value, an “Illegal value specified”error is generated.
`throttle -mxc | -maxconn value`	Changes the maximum number of connections for all cloud providers. The option does not have a hard coded limit. The default value is 10. If you specify a value of `20` and have both Amazon and Nirvanix, this value is for each vendor. This value indicates 20 connections for Amazon and 20 connections for Nirvanix. If you enter a negative value, an “Illegal value specified” error is generated.

`throttle -abw | -availablebw value`	Changes the total available bandwidth value for the cloud feature. The value is specified in either KB or MB. If you omit the units, the value is understood as being in KB. You must specify a number greater than zero. If you enter zero, an “Illegal value specified” error is generated.
	
	Example with 50 KB
	
	`throttle -availablebw 50KB`
	
	Example with 50 MB
	
	`throttle -availablebw 50MB`

`throttle -wkt | -worktime start_time, end_time, bandwidth_percentage`	Defines the bandwidth available for the defined work time. Specify the start and the end times in 24 hour format. For example, 8:00 A.M. is 8 and 6:30 P.M. is 1830. Specify the bandwidth value as a percentage between 0 and 100. Separate these values with a comma. Example shows start time 8:00 A.M., end time 8:00 P.M., and bandwidth limit of 30%. `throttle -worktime 8,20,30`

Table 3-16 Throttling options and their values *(continued)*

Option	Details
`throttle -oft | -offtime start_time, end_time, bandwidth_percentage`	Defines the bandwidth available for the specified off time. Specify the start and the end times in 24 hour format. For example, 8:00 A.M. is 8 and 6:30 P.M. is 1830. Specify the bandwidth value as a percentage between 0 and 100. Separate these values with a comma. Example shows start time 8:00 P.M., end time 8:00 A.M., and bandwidth limit of 80%. `throttle -offtime 20,8,80`
`throttle -wkd | -weekend first_day, last_day, bandwidth_percentage`	Specifies the beginning and end of the weekend and the percentage of the available bandwidth the cloud feature should use. The three values are separated with commas. The first and the last days are specified with numbers, 1 for Monday, 2 for Tuesday, and so on. Specify the bandwidth value as a percentage between 0 and 100. Separate these values with a comma. In the example, the weekend is defined as Saturday and Sunday. The bandwidth for the cloud feature is defined at 80% of the available bandwidth. Example: `throttle -weekend 6,7,80`
`throttle -i | -interval value`	Specifies the rate at which backup streams sample their utilization and adjust their bandwidth use. The value is specified in seconds. Acceptable values are 0 to 86400 (24 hours). If you specify 0, this value disables the feature.
`throttle -t | -stype value`	Specifies the storage server type. Acceptable values for the *stype* variable are: ■ Amazon: `amazon_raw` for unencrypted data and `amazon_crypt` for encrypted data. ■ AT&T: `att_raw` for unencrypted data and `att_crypt` for encrypted data. ■ Nirvanix: `nirvanix_raw` for unencrypted data and `nirvanix_raw` for encrypted data. ■ Rackspace: `rackspace_raw` for unencrypted data and `rackspace_raw` for encrypted data.

Table 3-16 Throttling options and their values *(continued)*

Option	Details
`throttle -r | -sserver value`	Specifies the storage server name. Acceptable values for the *sserver* variable are: ■ Amazon: `amazon.com` ■ AT&T: `storage.synaptic.att.com` ■ Nirvanix: `nirvanix.com` ■ Rackspace: `rackspace.com`
`throttle -pmc | -providermaxconn value`	Changes the maximum number of connections for a specific cloud provider. Enter a value between 1 and the maximum number of connections. You must specify both the `stype` and the `sserver` when you set this value. Example: `csconfig throttle -stype nirvanix_raw -sserver nirvanix.com -pmc 20`
`throttle -f | -force`	Forces the throttle value specified. Used for scripting to avoid the confirmation question.
`throttle -def | -setdefaults`	Returns all throttling parameters to the default.
`throttle -h | -help`	Displays the help information for the `throttle` command.

Examples:

- Retrieve the throttling configuration details:

```
csconfig throttle
```

- Set the read bandwidth, write bandwidth, available bandwidth, work time and the weekend configuration:

```
csconfig throttle -readbw 70 -writebw 80 -availablebw 512MB
-worktime 8,20,30 -weekend 6,7,80
```

- Set the read bandwidth to 30% and available bandwidth to 2 GB:

```
csconfig throttle -readbw 30 -availablebw 2147483648 -f
```

- Set the provider-specific maximum connection for Nirvanix to 5:

```
csconfig throttle -stype nirvanix_raw -sserver nirvanix.com
-providermaxconn 5
```

The options and arguments for metering are shown in Table 3-17.

Table 3-17 Metering options

Option	Details
`meter`	Display the metering information for the storage server.
`meter -i | -interval` *value*	Change the metering time interval. This value is specified in seconds. Acceptable values for `interval` are 0 to 86400 (24 hours). If you specify 0, this value disables this feature.
`meter -d | -directory` *value*	Specify the directory location the cloud feature uses to store the metering data.
`meter -def | -setdefaults`	Returns all metering parameters to the default.
`meter -f | -force`	Forces the throttle value specified. Used for scripting to avoid the confirmation question.
`meter -h | -help`	Displays the help information for the `meter` command.

Examples:

- Get the metering configuration details:

  ```
  csconfig meter
  ```

- Set the following metering parameters: Time interval = 500 seconds and the metering data storage location to `/tmp/metered_data`:

  ```
  csconfig meter -interval 500 -directory /tmp/metered_data
  ```

Additional media servers

You can add additional media servers to your cloud environment. This option allows you to adjust your cloud configuration as necessary. Use this procedure to properly add new media servers to your cloud environment.

Adding additional media servers to the 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 Server** tab
5. Select the media server or servers that you want to enable for Cloud backup. The operating system of any specified media servers must be a supported operating system. The media servers that are checked are configured as Cloud servers.
6. Click **OK**.
7. Copy `libstspinirvanix.conf` to the appropriate directory for your operating system.
   - UNIX and Linux: `/usr/openv/lib/ost-plugins`
   - Windows: `install_path\VERITAS\NetBackup\bin\ost-plugins`
8. Modify policies as desired.

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

Chapter 4

Cloud Storage Providers

This chapter includes the following topics:

About cloud storage providers

The following topics explain how to configure NetBackup to read and write backup data to each cloud service provider:

See "About Amazon Simple Storage Service (S3)" on page 53.

See "About AT&T Synaptic" on page 54.

See "About Nirvanix Cloud Storage Network" on page 55.

See "About Rackspace CloudFiles" on page 58.

About Amazon Simple Storage Service (S3)

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

Table 4-1 outlines the details and requirements of Amazon Simple Storage Service.

Table 4-1

Feature or requirement	Details
Amazon Simple Storage Service accounts	You must obtain an Amazon S3 account and the associated user name and password. You must also obtain an access ID and secure access token. These are required when you create the storage server.
Storage requirements	The following are the requirements for Amazon Simple Storage Service: ■ The bucket name must be between 3 and 255 characters ■ You can create a maximum of 100 buckets per Amazon account. You can delete empty buckets and then reuse the bucket name, but deleted buckets count toward the 100 bucket limit. ■ You must have a NetBackup Enterprise Disk license key. ■ You must have an Amazon Simple Storage Service account user name and password.
Maximum 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.

Note:

The information that is displayed for **Used Capacity** and **Available Space** for Amazon is inaccurate in the NetBackup Administrative Console. The values are found under **Disk Pool > Devices**. 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 Web site for accurate use information.

More information about Amazon S3 is available from Amazon.

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

About AT&T Synaptic

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

Table 4-2 outlines the details and requirements of AT&T Synaptic.

Table 4-2

Feature or requirement	Details
AT&T Synaptic accounts	You must obtain a user ID and password for an AT&T account. These are required when you create the Storage Server.
Storage requirements	The following are the requirements for AT&T cloud storage: ■ The logical storage unit (LSU) name must be 50 characters or less. ■ You must have a NetBackup Enterprise Disk license key. ■ You must have an AT&T Synaptic account user name and password.

Note:

The information that is displayed for **Used Capacity** and **Available Space** for AT&T is inaccurate in the NetBackup Administrative Console. The values are found under **Disk Pool > Devices**. 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 Web site for accurate use information.

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

http://www.business.att.com/enterprise/Service/hosting-services/cloud/storage/

About Nirvanix Cloud Storage Network

NetBackup Cloud Storage enables Symantec NetBackup to back up data and restore data from the Nirvanix Cloud Storage Network™. The Nirvanix Cloud Storage Network is a fully-managed, highly-secure cloud storage service. The Cloud Storage Network is comprised of standards-based access to Nirvanix storage nodes that are located in the United States, Europe, and Asia. The Cloud Storage Network stores, delivers, and processes storage requests in the best location for your enterprise.

Table 4-3 outlines the details and requirements of Nirvanix Cloud Storage Network.

Table 4-3

Feature or requirement	Details
Storage pool requirements	Be aware that Nirvanix uses the terms “application” and “storage pool” interchangeably in their documentation. Nirvanix Cloud Storage Network requirements: ■ The storage pool name must be 50 characters or less. ■ You must use only one Nirvanix storage pool for each NetBackup backup domain. ■ You must use unique Storage pool names among all users of Nirvanix Cloud Storage Network. ■ You must use NetBackup to create the Nirvanix storage pool for your NetBackup backups. The storage pools that NetBackup creates contain a required Symantec Partner Key. If you use the Nirvanix Management Portal to create the storage pool, it does not contain the partner key. Consequently, that storage pool cannot accept data from NetBackup. When you create the storage server and then set its properties, NetBackup creates the storage pool and the first child account. **Caution:** Never change the name of your Nirvanix storage pool after you configure Nirvanix storage in NetBackup. If you change the name of the storage pool, you risk being unable to backup and restore your data.
Child accounts	A Nirvanix child account represents storage on the Nirvanix Cloud Storage Network. In the Nirvanix Cloud Storage Network, a child account is subordinate to a storage pool. NetBackup creates a child account when you configure Nirvanix storage in NetBackup. You can create additional child accounts for your storage pool. Each child account must have a unique name. The child account name must be 100 characters or less. **Note:** The password for each child account you create must be the same as its name. For the child account that NetBackup creates, NetBackup uses the child account name for the password. A child account is exposed to NetBackup as a single volume through the OpenStorage API. If a Nirvanix storage pool has more than one child account, each is exposed as a volume. You add the volume or volumes to a NetBackup disk pool.

Table 4-3 *(continued)*

Feature or requirement	Details
Backup image representation in the Nirvanix cloud	The Nirvanix Management Portal shows the NetBackup backup images as follows in the Nirvanix Web Client: ■ Backup images appear as folders under the Storage Pool/Child Account view. ■ Every write operation for a new image creates a folder under the backup image folder. The folder names use a block image sequence number. For example, 0, 1, 2, and so on. ■ Each backup image folder contains a `block_map` file. The file maps the block images to individual files. ■ Backup image properties are added as metadata to the folders.
Storage requirements and limitations	The following are the requirements for Nirvanix cloud storage: ■ You must have a NetBackup Enterprise Disk license key. ■ You must have a Nirvanix Cloud Storage Network master account user name and password. ■ You must have a default node-replication policy setting for your Nirvanix account. New storage pools inherit the default policies. You can adjust these settings for each storage pool to fit your business needs. Contact Nirvanix customer support using the Nirvanix Management Portal for more information or to verify that your account has the proper settings. ■ You must use NetBackup to create the Nirvanix storage pool that you use for your NetBackup backups. The storage pools that NetBackup creates contain the required Symantec Partner Key. Do not use the Nirvanix Management Portal Planning to create the storage pool. The storage pools it creates do not contain the required Symantec partner key. If Nirvanix Management Portal Planning creates the storage pool, it cannot accept data from NetBackup. ■ You must use unique storage pool names. Storage pool names must be unique among all users of the Nirvanix Cloud Storage Network.

More information about Nirvanix Cloud Storage Network is available from Nirvanix.

http://www.nirvanix.com/products-services/index.aspx

Unable to change the Nirvanix storage pool name

After you upgrade to NetBackup 7.5, you cannot change the name of a Nirvanix storage pool.

About Rackspace CloudFiles

NetBackup Cloud Storage enables Symantec NetBackup to back up data to and restore data from Rackspace CloudFiles™.

Table 4-4 outlines the details and requirements of Rackspace CloudFiles.

Table 4-4

Feature or requirement	Details
Rackspace CloudFiles 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 Enterprise Disk license key. ■ You must have a Rackspace CloudFiles account user name and password.

More information about Rackspace CloudFiles is available from Rackspace.

http://www.rackspace.com/cloud/cloud_hosting_products/files/

Chapter 5

Support for NetBackup Accelerator and NetBackup Optimized Synthetic Backups

This chapter includes the following topics:

About Cloud and NetBackup Accelerator and NetBackup Optimized Synthetic backups

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

- *Symantec NetBackup Deduplication Guide UNIX, Windows, Linux*
- *Symantec NetBackup Administrator's Guide, Volume I UNIX and Linux*

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

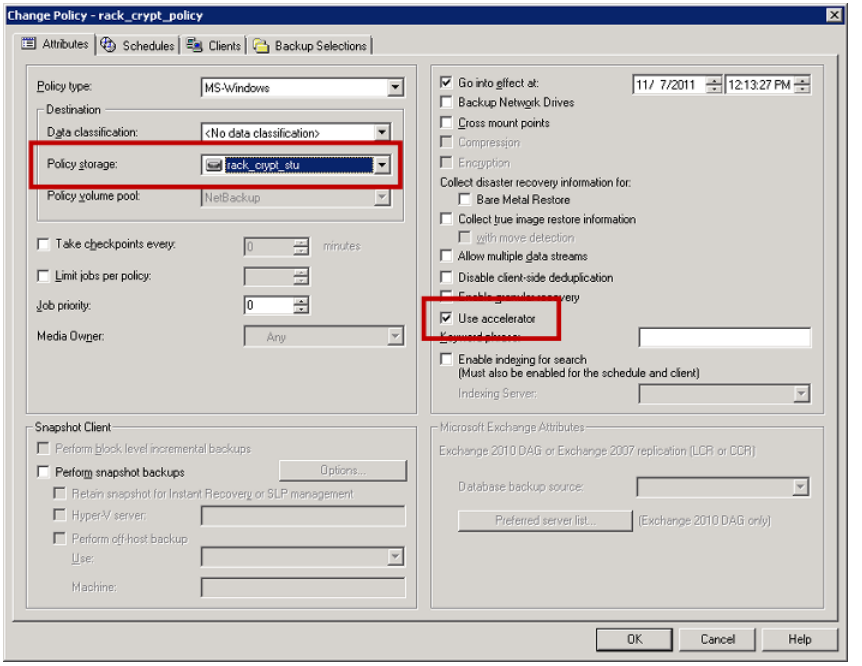
Enable Accelerator with Cloud

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**.

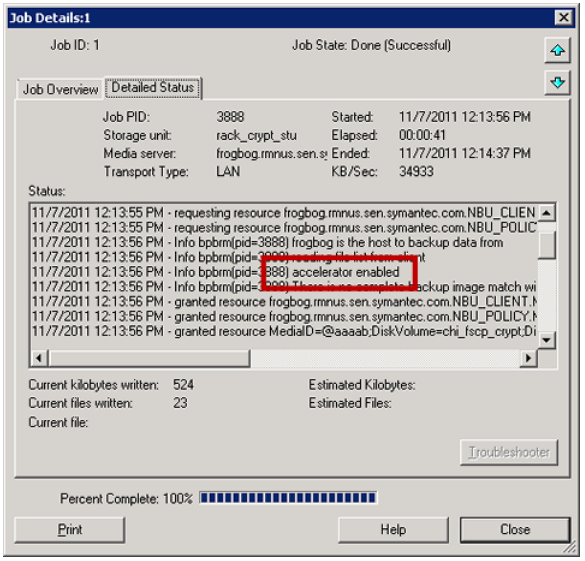
Figure 5-1 Enable Accelerator



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 5-2 Confirm Accelerator used during backup



Enable Optimized Synthetic backups with Cloud

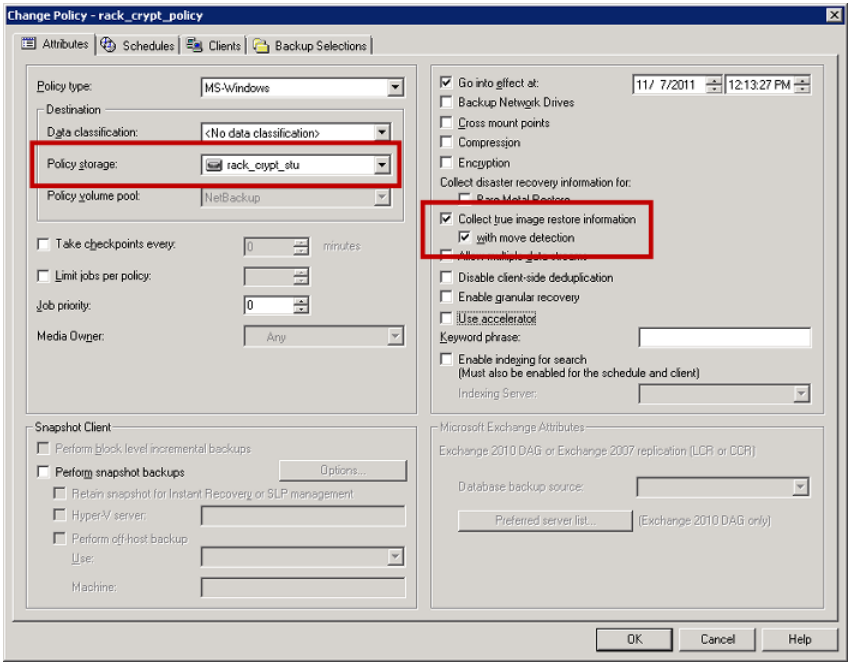
Optimized Synthetic backups require three backup schedules. You must have a **Full backup**, an **Incremental backup**, and a **Full Backup with Synthetic backup enabled**. You can use either a Differential incremental or a Cumulative incremental for the incremental backup. You must then perform a full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

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**.

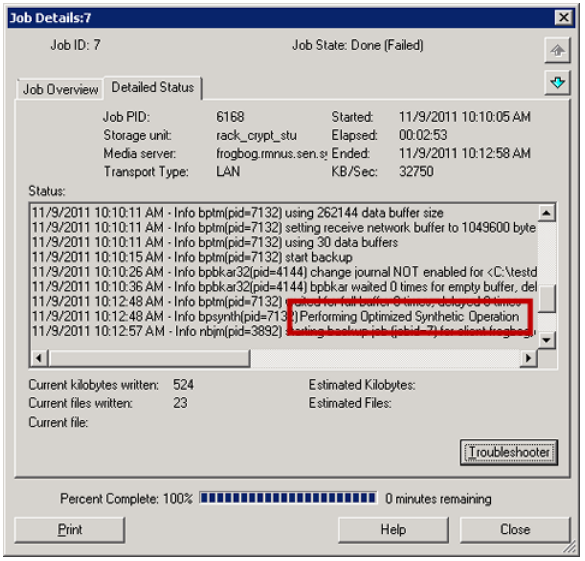
Figure 5-3 Enable Optimized Synthetic backups



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 5-4 Confirm backup was Optimized Synthetic



Chapter 6

Monitoring and Reporting

This chapter includes the following topics:

Reporting and monitoring cloud backups

All monitoring and reporting for NetBackup Cloud is handled through NetBackup OpsCenter. Please refer to the *NetBackup OpsCenter Administrator's Guide* for details on cloud monitoring and reporting.

Chapter 7

Troubleshooting

This chapter includes the following topics:

About NetBackup cloud storage log directories

NetBackup Cloud Storage logs to the same directories as OpenStorage. The following NetBackup processes log cloud activities:

- `bpbrm`: Back up and restore manager.
- `bpdbm`: Database manager.
- `bpdm`: Disk manager.

- bptm: Tape manager for backup and restore operations.
- bpstsinfo: A utility that writes information about connections to the cloud storage server.
- nbcssc: NetBackup Cloud Storage Service Container
  - For Windows: *install_path*\NetBackup\logs\nbcssc
  - For UNIX/Linux: /usr/openv/netbackup/logs/nbcssc
- tpconfig: The tpconfig utility logs connection operations. The tpconfig command writes log files to the tpcommand directory.
  UNIX/Linux: /usr/openv/volmgr/debug/tpcommand
  Windows *NetBackup_install_path*\veritas\volmgr\debug\tpcommand
  The tpcommand folder is not created as part of the mklogdir utility. It must be created manually.

Enabling NetBackup logging

To enable NetBackup log collection, set the global log level to 5 in the NetBackup Administration Console. Set the global log level under **Host Properties > Master server > Logging**.

Note: The log directory must exist for logging to work. You can either create the log directory manually or use the NetBackup utility mklogdir to make it for you.

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:

- NVX for Nirvanix
- AMZ for Amazon
- ATT for AT&T
- RACKS for Rackspace

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

Start and stop the NetBackup Cloud Storage Service Container service

You can use the command line or the NetBackup Administrative Console to start and stop the NetBackup Cloud Store Service Container (nbcssc) service.

- From the NetBackup Administrative Console:
  You can start and stop the service though the **Services** option in control panel.
- From the command line, start and stop the nbcssc service:
  Start the service: `nbcssc -a NetBackup` (Windows) or `nbcssc -s` (UNIX or Linux).
  Stop the service: `nbcssc -t` (Windows, UNIX, and Linux)
- From the command line, start and stop all NetBackup services:
  Windows: Use the `bpup` and `bpdown` commands. These commands are located in the *`install_path`*`\NetBackup\bin` directory.
  UNIX/Linux: Use the `bp.start_all` and `bp.kill_all` commands. These commands are located in the `/usr/openv/netbackup/bin/` directory.

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

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.

Setting the NetBackup Cloud Storage Server Configuration service port to a value other than the default causes the NetBackup Administrative Console to fail to open.

By default, the NetBackup Cloud Storage Server Configuration service port is 5637. This value is specified in either the `cloudstorewin.conf` or the `cloudstorejava.conf` file. The configuration file has an `NBCSSC_PORT` value.

Example that shows default value:

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

The files are in the following locations:

For Windows: `C:\Program Files\Veritas\NetBackup\bin\cloudstorewin.conf`

For UNIX/Linux: `/usr/openv/java/cloudstorejava.conf`

The value in the `conf` file must match what is in the operating system's `services` file. The `services` file is in the following locations:

Windows: `C:\WINDOWS\system32\drivers\etc\services`

UNIX/Linux: `/etc/services`

If the value in the `services` file does not match the value in the `conf`, the NetBackup Administration Console fails to launch.

Backups fail with NetBackup Status Code 84 (media write error)

A number of issues can cause a media write error message (NetBackup Status Code 84). Among the causes for Cloud storage backups is an incorrectly set `WRITE_BUFFER_SIZE` value.

If the `WRITE_BUFFER_SIZE` is increased to a value that exceeds the total swap space of the computer, backups can fail with a NetBackup Status Code 84. Adjust the `WRITE_BUFFER_SIZE` size to a value lower than the computer's total swap space to resolve this issue.

Nirvanix backup attempts fail with Disk volume is down error messages

When performing a full system recovery of a computer using the Nirvanix plug in, you must restore the `libstspinirvanix.conf` and the `libstspinirvanix.pref` files. Failure to restore these files results in "Disk volume is down" error messages when you attempt a Nirvanix backup.

Restore these files to the `/usr/openv/libs/ost-plugins/` directory for UNIX and Linux computers and to the *`install_path`*`\Veritas\NetBackup\bin\ost-plugins\` for Windows computers.

Connection to the NetBackup Cloud Storage Service Container fails

The `csconfig` command makes three attempts to connect to the NetBackup Cloud Storage Service Container with a 60-second timeout for each connection attempt. If the connection attempt fails, verify the following information:

- Make sure that your firewall settings are appropriate or firewall is disabled.
- Check the security mode as defined by the `CSSC_IS_SECURE` attribute in the CloudStore configuration file (for UNIX or Linux) or the registry (for Windows). The current mode should be same as that when the Service was started.
- If the `CSSC_IS_SECURE` value equals `1` and the service fails to start, the server certificate may be corrupt or expired. Review the cssc log file for error messages similar to the following (bold added for emphasis):
  `[1326119109] [error] [client unknown host] set_ssl_option:` **`cannot open C:\Program Files\Veritas\NetBackup\bin\ost-plugins\cssc.crt`**`: error:0906D064 EM routines EM_read_bio:bad base64 decode.`
  One of the causes of this error message is a corrupt or an expired server certificate file. The server certificate file is `cssc.crt`. It is in the `/usr/openv/lib/ost-plugins` directory on UNIX or Linux and *`install_path`*`\Veritas\Netbackup\bin\ost-plugins` on Windows. To recreate this file, delete the file and restart the service.
  More information about the cssc log file is available.
  See "About the NetBackup Cloud Storage Service Container" on page 45.

NetBackup Cloud Storage Service Container startup and shutdown troubleshooting

Do not change the security mode of the NetBackup Cloud Storage 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.

More information is available if the NetBackup Cloud Storage Service Container service does not start.

See "Connection to the NetBackup Cloud Storage Service Container fails" on page 71.

If the NetBackup Cloud Storage Service Container fails during service shutdown, check the `CSSC_IS_SECURE` attribute. You can find this value in the CloudStore configuration file for UNIX or Linux or the registry for Windows. Determine if

the CSSC_IS_SECURE attribute is the same as the current mode of the service. Be sure to stop the service in the same mode it was started.

Chapter 8

Known issues

This chapter includes the following topics:

About using the bpstsinfo to list storage server information

When using the `bpstsinfo` command to list storage server information, use either the `-stype` option or the `-storageserverprefix` option. If you do not use one of these two options, the command attempts to find the storage server name in all providers. This action frequently takes too long to complete and causes the command to fail.

Encrypted and non-encrypted storage units displayed in bpstsinfo command output

When using the `bpstsinfo` command to display the encrypted logical storage unit (LSU) information, the output shows both encrypted and non-encrypted LSUs.

Example:

```
bpstsinfo -lsuinfo -storage_server nirvanix.com -stype nirvanix_crypt
```

Displaying both encrypted and non-encrypted LSUs is an 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. As such, when you use the `bpstsinfo` command with the `-lsuinfo` operation, all potential LSUs on that level are returned, regardless of their use within NetBackup.

About inconsistencies when image information is displayed

Due to the nature of the cloud plugins, each plugin returns image information on the basis of its own interpretation of the image. When using commands to list image properties, be aware the plugin that requested the information affects the information that is returned. When using the `bpstsinfo` command to list images, specify the same option for `-stype` that was used at the time of backup.

About deleting storage servers

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 login 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 the `.conf` and `.pref` files from `lib/ost-plugins` or `bin/ost-plugins` directory.

Special characters and the csconfig command

Do not specify a directory with special characters when issuing the `csconfig meter -directory` command. The operating system's shell may incorrectly interpret the directory path which leads to unexpected results.

Directory length exceeds maximum path length for csconfig command

The `csconfig meter -directory` *`dir`* command sets the metering directory path and creates the directory if it does not exist. The directory creation fails if directory value exceeds the maximum path length limit for the system or if there are permission issues. If the directory creation fails, NetBackup uses the default directory. The default directory is `/usr/openv/netbackup/bin/ost-plugins` for UNIX and Linux. The default directory is *`install_path`*`\NetBackup\bin` for Windows.

Unexpected results for csconfig throttle command

Do not use `cloud_global` as the `stype` when you set the maximum connections with the `csconfig throttle` command. This term is a reserved keyword and can lead to unexpected results. The `stype` value should be one of the acceptable values that is listed in the *Throttling options and their values* table.

See Table 3-16 on page 46.

Different cloud provider information provided to the csconfig throttle command

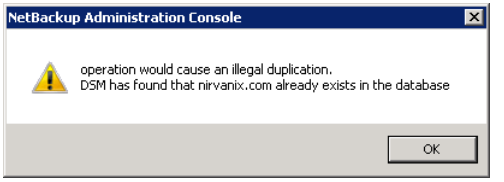
When setting the maximum connections using `csconfig throttle` command, make sure the cloud provider for the `stype` and the `sserver` are the same. If you provide two different providers, the provider name that is passed with the `sserver` command is used.

Attempts to set available bandwidth with the csconfig command fail

The `csconfig throttle` command accepts large values for the available bandwidth option. The maximum allowed value varies with the operating system where the NetBackup Cloud Storage Service Container resides. Refer to the `csconfig` log file if the command fails.

Unable to configure additional media servers

If you attempt to run the Cloud wizard on a second media server that uses the same master server as the first media server, you receive an `illegal duplication` error.



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 on this topic.

See "Adding additional media servers to the Cloud environment" on page 51.

Cloud configuration may fail if NetBackup Access Control is enabled

When you attempt to configure Cloud in an environment that uses NetBackup Access Control, you may receive an error. The error is `Error creating Key Group and Keyscannot connect on socket`. This error is generated because the user trying to configure Cloud does not have sufficient rights within NetBackup Access Control. The user account that configures Cloud must be a member of the NBU_KMS Admin Group if you use NetBackup Access Control. See the *NetBackup Security and Encryption Guide* for more information on NetBackup Access Control and account setup.

Index