

Symantec NetBackup™ Cloud Administrator's Guide

Release 7.6 Draft

DRAFT

Symantec NetBackup™ Cloud Administrator's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version:

PN:

Legal Notice

Copyright © 2013 Symantec Corporation. All rights reserved.

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

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

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

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

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

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.com>

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

DRAFT

Technical Support

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

Symantec's support offerings include the following:

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

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

DRAFT

Contents

Technical Support	4
Chapter 1	About NetBackup Cloud storage 11
	About cloud storage features and functionality 11
	About unsupported OpenStorage capabilities 13
	Legacy cloud storage considerations 13
Chapter 2	Configuring cloud storage in NetBackup 15
	Configuring cloud storage in NetBackup 16
	Cloud installation requirements 18
	About the cloud storage providers 19
	About the Amazon Simple Storage Service (S3) requirements 19
	About AT&T Synaptic requirements 21
	About the Nirvanix Cloud Storage Network requirements 22
	About Rackspace Cloud Files requirements 25
	Scalable Storage properties 26
	Cloud Settings tab of the Scalable Storage properties 27
	About the NetBackup CloudStore Service Container 32
	About key management for encryption of NetBackup cloud storage 33
	Configuring key management for NetBackup cloud storage encryption 34
	Setting up the KMS database for NetBackup cloud storage encryption 35
	Creating a KMS key group for NetBackup cloud storage encryption 37
	Creating a KMS key for NetBackup cloud storage encryption 38
	Saving a record of the KMS key names for NetBackup cloud storage encryption 39
	About cloud storage servers 41
	Configuring a storage server for cloud storage 42
	Amazon S3 storage server configuration options 47
	AT&T storage server configuration options 47

	Nirvanix storage server configuration options	48
	Rackspace storage server configuration options	50
	KMS database encryption settings	50
	About cloud storage disk pools	52
	Configuring a disk pool for cloud storage	52
	About cloud storage server properties	59
	Storage server cloud connection properties	59
	Storage server bandwidth throttling properties	63
	Storage server encryption properties	67
	Nirvanix storage server properties	68
	Configuring storage server properties in NetBackup	70
	About cloud storage data movers	71
	Adding backup media servers to your cloud environment	72
	Configuring a storage unit for cloud storage	73
	Cloud storage unit properties	74
	Configure a favorable client-to-server ratio	76
	Control backup traffic to the media servers	77
	About NetBackup Accelerator and NetBackup Optimized Synthetic backups	77
	Enabling NetBackup Accelerator with cloud storage	78
	Enabling optimized synthetic backups with cloud storage	80
	Creating a backup policy	82
	Changing cloud storage disk pool properties	83
	Cloud storage disk pool properties	85
Chapter 3	Monitoring and Reporting	87
	Viewing cloud storage job details	87
	Reporting and monitoring cloud backups	87
	Reporting on Auto Image Replication jobs	88
	Displaying KMS key information for cloud storage encryption	88
Chapter 4	Troubleshooting	91
	About unified logging	91
	About using the vxlogview command to view unified logs	92
	Examples of using vxlogview to view unified logs	93
	About legacy logging	94
	Creating NetBackup log file directories	95
	About NetBackup cloud storage log files	96
	Enable libcurl logging	98
	NetBackup CloudStore Service Container startup and shutdown troubleshooting	99

	Connection to the NetBackup CloudStore Service Container fails	99
	Stopping and starting the NetBackup CloudStore Service Container	100
	Troubleshooting cloud storage configuration issues	100
	Cloud storage: cannot create a storage server	100
	Troubleshooting cloud storage operational issues	101
	Cloud storage backups fail with status code 84 or 87	101
	Nirvanix backup attempts fail with Disk volume is down error messages	102
	A restart of the nbcssc process reverts all cloudstore.conf settings	103
	NetBackup Administration Console fails to open	103
Chapter 5	Known issues	105
	About using the bpstsinfo to list storage server information	105
	Encrypted and non-encrypted storage units displayed in bpstsinfo command output	106
	About inconsistencies when image information is displayed	106
	About deleting storage servers	106
	Special characters and the csconfig command	107
	Directory length exceeds maximum path length for csconfig command	107
	Unexpected results for csconfig throttle command	107
	Different cloud provider information provided to the csconfig throttle command	107
	Attempts to set available bandwidth with the csconfig command fail	107
	Unable to configure additional media servers	108
	Cloud configuration may fail if NetBackup Access Control is enabled	108
Chapter 6	Cloud Storage Server Configuration Wizard	109
	Reviewers: about these wizard help topics	123
	About the Cloud Storage Server Configuration Wizard panel	110
	Select Cloud Provider panel	111
	Amazon S3 Cloud Provider Configuration panel	112
	AT&T Cloud Provider Configuration panel	113
	Nirvanix Cloud Provider Configuration panel	114
	Rackspace Cloud Provider Configuration panel	115
	Advanced Server Configuration dialog box	116
	Specify Deduplication Settings panel	116

	Specifying Encryption Settings panel	118
	Cloud Storage Server Configuration Summary panel	119
	Cloud storage configuration progress panel	120
	Cloud storage configuration completion panel	121
Chapter 7	Disk Pool Configuration Wizard	123
	Reviewers: about these wizard help topics	123
	About the Disk Pool Configuration Wizard	124
	Disk Pool panel	126
	Select Storage Server panel	128
	Select Volumes panel	130
	Create Buckets for Amazon dialog box	131
	Create Cloud Storage Volume for AT&T dialog box	132
	Create Cloud Storage Volume for Nirvanix dialog box	133
	Create Cloud Storage Volume for Rackspace dialog box	134
	Settings dialog box	134
	Disk Pool Properties panel	135
	Summary panel	136
	Confirmation panel	137
	Storage Unit Option panel	138
	Create Storage Unit panel	139
	Finish panel	139
Index		141

About NetBackup Cloud storage

This chapter includes the following topics:

- [About cloud storage features and functionality](#)
- [About unsupported OpenStorage capabilities](#)
- [Legacy cloud storage considerations](#)

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 Cloud Storage Server Configuration Wizard is incorporated to facilitate the cloud storage setup and storage provisioning. Cloud storage provisioning now happens entirely through the NetBackup interface.
Encryption	<p>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.</p> <p>The encryption feature uses an AES 256 cipher feedback (CFB) mode encryption.</p>

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

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

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

Feature	Details
Storage providers	<p>Symantec currently offers the following cloud storage providers: AT&T, Amazon, Nirvanix and Rackspace. More information is available about each of these vendors.</p> <p>See “About the Nirvanix Cloud Storage Network requirements” on page 22.</p> <p>See “About AT&T Synaptic requirements” on page 21.</p> <p>See “About the Amazon Simple Storage Service (S3) requirements” on page 19.</p> <p>See “About Rackspace Cloud Files requirements” on page 25.</p>
OpsCenter Reporting	<p>Monitoring and reporting of the data that is sent to cloud storage is available through new cloud reports in OpsCenter. The cloud reports include:</p> <ul style="list-style-type: none"> ■ Job Success Rate: Success rate by backup job level across domains, clients, policies, and business level views filtered on cloud-based storage. ■ Data Expiring In Future: Data that expires each day for the next seven days filtered on cloud-based storage. ■ Cloud Metering: Historical view of the data that is written to cloud per cloud provider. ■ Average Data Transfer Rate: Historical view of average data transfer rate to cloud per cloud provider. ■ Cloud Metering Chargeback: Ranking, forecast, and distribution view of the cost that is incurred on cloud-based storage per cloud provider.

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` type. For encrypted Nirvanix, use `nirvanix_crypt` type.

More information about configuring these storage server types is available.

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

DRAFT

Configuring cloud storage in NetBackup

This chapter includes the following topics:

- [Configuring cloud storage in NetBackup](#)
- [Cloud installation requirements](#)
- [About the cloud storage providers](#)
- [Scalable Storage properties](#)
- [About the NetBackup CloudStore Service Container](#)
- [About key management for encryption of NetBackup cloud storage](#)
- [Configuring key management for NetBackup cloud storage encryption](#)
- [About cloud storage servers](#)
- [Configuring a storage server for cloud storage](#)
- [About cloud storage disk pools](#)
- [Configuring a disk pool for cloud storage](#)
- [About cloud storage server properties](#)
- [Configuring storage server properties in NetBackup](#)
- [About cloud storage data movers](#)
- [Adding backup media servers to your cloud environment](#)
- [Configuring a storage unit for cloud storage](#)

- [About NetBackup Accelerator and NetBackup Optimized Synthetic backups](#)
- [Enabling NetBackup Accelerator with cloud storage](#)
- [Enabling optimized synthetic backups with cloud storage](#)
- [Creating a backup policy](#)
- [Changing cloud storage disk pool properties](#)

Configuring cloud storage in NetBackup

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

The NetBackup administrator's guide describes how to configure a base NetBackup environment.

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

Table 2-1 Overview of the NetBackup cloud configuration process

Step	Task	More information
Step 1	Create NetBackup log file directories on the master server and the media servers	See “About NetBackup cloud storage log files” on page 96. See “Creating NetBackup log file directories” on page 95.
Step 2	Review the cloud installation requirements	See “Cloud installation requirements” on page 18.
Step 3	Determine the requirements for provisioning and configuring your cloud storage provider in NetBackup	See “About the cloud storage providers” on page 19.
Step 4	Understand the role of the Cloud Storage Service Container	See “About the NetBackup CloudStore Service Container” on page 32.
Step 5	Configure the global cloud storage host properties as necessary	See “Scalable Storage properties” on page 26.
Step 6	Understand key management for encryption	Encryption is optional. See “About key management for encryption of NetBackup cloud storage” on page 33.

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

Step	Task	More information
Step 7	Configure key management manually	<p>You can configure key management manually by using NetBackup commands.</p> <p>See “Configuring key management for NetBackup cloud storage encryption” on page 34.</p> <p>Alternatively, you can configure key management if you use NetBackup wizards:</p> <ul style="list-style-type: none"> ■ The Cloud Storage Server Configuration Wizard lets you configure the key database key and the key record key. ■ The Disk Pool Configuration Wizard configures key groups and key names. <p>Note: Regardless of how you configure key management, record your keys and store them in a safe place.</p> <p>See “Saving a record of the KMS key names for NetBackup cloud storage encryption” on page 39.</p>
Step 8	Configure the storage server	<p>See “About cloud storage servers” on page 41.</p> <p>See “Configuring a storage server for cloud storage” on page 42.</p>
Step 9	Configure the disk pool	<p>See “About cloud storage disk pools” on page 52.</p> <p>See “Configuring a disk pool for cloud storage” on page 52.</p>
Step 10	Configure additional storage server properties	<p>See “About cloud storage server properties” on page 59.</p> <p>See “Configuring storage server properties in NetBackup” on page 70.</p>
Step 11	Add additional media servers	<p>Adding additional media servers is optional.</p> <p>See “About cloud storage data movers” on page 71.</p> <p>See “Adding backup media servers to your cloud environment” on page 72.</p>
Step 12	Configure a storage unit	<p>See “Configuring a storage unit for cloud storage” on page 73.</p>

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

Step	Task	More information
Step 13	Configure NetBackup Accelerator and optimized synthetic backups	<p>Accelerator and optimized synthetic backups are optional.</p> <p>See “About NetBackup Accelerator and NetBackup Optimized Synthetic backups” on page 77.</p> <p>See “Enabling NetBackup Accelerator with cloud storage” on page 78.</p> <p>See “Configuring storage server properties in NetBackup” on page 70.</p>
Step 14	Configure a backup policy	See “Creating a backup policy” on page 82.

Cloud installation requirements

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

Table 2-2 Cloud installation requirements

Requirement	Details
NetBackup media server platform support	<p>NetBackup cloud storage is supported on the following operating systems for media servers:</p> <ul style="list-style-type: none"> ■ AIX ■ HP-UX ■ RedHat Linux ■ Solaris 10 ■ SUSE Linux ■ Windows Server 2008 R2
Cloud storage provider account	<p>You must have an account created with your preferred cloud storage provider before you configure NetBackup Cloud Storage. Please refer to the list of available NetBackup cloud storage providers.</p> <p>You can create this account in the Cloud Storage Configuration Wizard.</p> <p>See “About the cloud storage providers” on page 19.</p>

Table 2-2 Cloud installation requirements (*continued*)

Requirement	Details
NetBackup cloud storage licensing	NetBackup cloud storage is enabled through the Enterprise Disk License. To use NetBackup Accelerator with NetBackup cloud storage, you must install the Data Protection Optimization Option. that license key activates the NetBackup Accelerator feature.

About the cloud storage providers

The information that is required to configure cloud storage in NetBackup varies according to each cloud storage provider's requirements. Separate topics describe the requirements for each provider.

See [“About the Amazon Simple Storage Service \(S3\) requirements”](#) on page 19.

See [“About AT&T Synaptic requirements”](#) on page 21.

See [“About the Nirvanix Cloud Storage Network requirements”](#) on page 22.

See [“About Rackspace Cloud Files requirements”](#) on page 25.

About the Amazon Simple Storage Service (S3) requirements

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

[Table 2-3](#) describes the details and requirements of Amazon Simple Storage Service.

Table 2-3 Amazon Simple Storage Service requirements

Requirement	Details
User account	You must obtain an Amazon Simple Storage Service (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 configure the storage server in NetBackup.

Table 2-3 Amazon Simple Storage Service requirements (*continued*)

Requirement	Details
Storage requirements	<p>The following are the requirements for Amazon Simple Storage Service:</p> <ul style="list-style-type: none"> ■ The bucket name must be between 3 and 255 characters. <p>You can use the following characters for the bucket name:</p> <ul style="list-style-type: none"> ■ 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 any of these as the first character in the bucket name) <ul style="list-style-type: none"> ■ 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. ■ You must use NetBackup to create the bucket for your NetBackup backups. <p>The bucket that NetBackup creates contain a required Symantec Partner Key. If you use the Amazon S3 interface to create the volume, it does not contain the partner key. Consequently, that bucket cannot accept data from NetBackup.</p>
Number of disk pools	<p>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.</p>

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 Web site for accurate use information.

More information about Amazon S3 is available from Amazon.

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

About AT&T Synaptic requirements

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

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

Table 2-4 AT&T Synaptic requirements

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

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 2-5](#) outlines the details and requirements of Nirvanix Cloud Storage Network.

DRAFT

Table 2-5 Nirvanix Cloud Storage Network requirements

Requirement	Details
Storage pool and volume requirements	<p>Be aware that Nirvanix uses the terms “application” and “storage pool” interchangeably in their documentation.</p> <p>The following items describe the Nirvanix Cloud Storage Network requirements:</p> <ul style="list-style-type: none"> ■ The storage pool name must be 50 characters or less. You can use the following characters in the storage pool name: <ul style="list-style-type: none"> ■ Any of the 26 letters of the International Standards Organization (ISO) Latin-script alphabet, both uppercase (capital) letters and lowercase (small) letters. These are the same letters as the English alphabet. ■ Any integer from 0 to 9, inclusive. ■ Any of the following characters: ~`!@#\$\$%^&()_-=+{ } ; ' , ■ You must use only one Nirvanix storage pool for each NetBackup backup domain. ■ You must use unique names for your storage pools and volumes. The names must be unique 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. ■ You can use the following characters in the volume name: <ul style="list-style-type: none"> ■ Any of the 26 letters of the International Standards Organization (ISO) Latin-script alphabet, both uppercase (capital) letters and lowercase (small) letters. These are the same letters as the English alphabet. ■ Any integer from 0 to 9, inclusive. ■ Any of the following characters: `#\$ _ - ' , <p>Warning: 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.</p>

Table 2-5 Nirvanix Cloud Storage Network requirements (*continued*)

Requirement	Details
Child accounts	<p>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.</p> <p>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.</p> <p>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.</p>
Storage requirements	<p>The following are the requirements for Nirvanix cloud storage:</p> <ul style="list-style-type: none"> ■ 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. <p>You must use NetBackup to create the storage pool. The storage pools that the Nirvanix Management Portal creates do not contain the required Symantec partner key. Such storage pools cannot accept data from NetBackup.</p> <ul style="list-style-type: none"> ■ You must use unique storage pool names. Storage pool names must be unique among all users of the Nirvanix Cloud Storage Network. ■ After you upgrade to NetBackup 7.5, you cannot change the name of a Nirvanix storage pool.
Limitations	<p>The following OpenStorage capabilities are not supported for Nirvanix storage:</p> <ul style="list-style-type: none"> ■ Optimized duplication. ■ Optimized synthetics. ■ Direct to tape (by NDMP). ■ Disk volume spanning of backup images.

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

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

About 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.

About Rackspace Cloud Files requirements

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

[Table 2-6](#) describes the details and requirements of Rackspace CloudFiles.

Table 2-6 Rackspace Cloud Files requirements

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

Table 2-6 Rackspace Cloud Files requirements (continued)

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

Note: The information that is displayed for **Used Capacity** and **Available Space** for Rackspace 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 Web site for accurate use information.

More information about Rackspace Cloud Files is available from Rackspace.
http://www.rackspace.com/cloud/cloud_hosting_products/files/

Scalable Storage properties

The **Scalable Storage** properties apply to currently selected media servers. The **Scalable Storage** properties appear only if a cloud storage server or a SureScale storage server is configured.

The **Scalable Storage** properties contain the following two tabs:

Cloud Settings tab	<p>The Cloud Settings properties control the communication and bandwidth between the NetBackup media servers and the cloud storage.</p> <p>The Cloud Settings tab appears only if a cloud storage server is configured.</p> <p>See “Cloud Settings tab of the Scalable Storage properties” on page 27.</p>
SureScale Settings tab	<p>The SureScale Settings tab appears only if a cloud storage server is configured and that storage is a target for SureScale deduplication.</p> <p>SureScale is described in a different guide.</p> <p>See the <i>NetBackup SureScale Guide</i>.</p>

Cloud Settings tab of the Scalable Storage properties

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

The **Cloud Settings** tab appears only if a cloud storage server is configured.

Figure 2-1 Scalable Storage Cloud Settings host properties

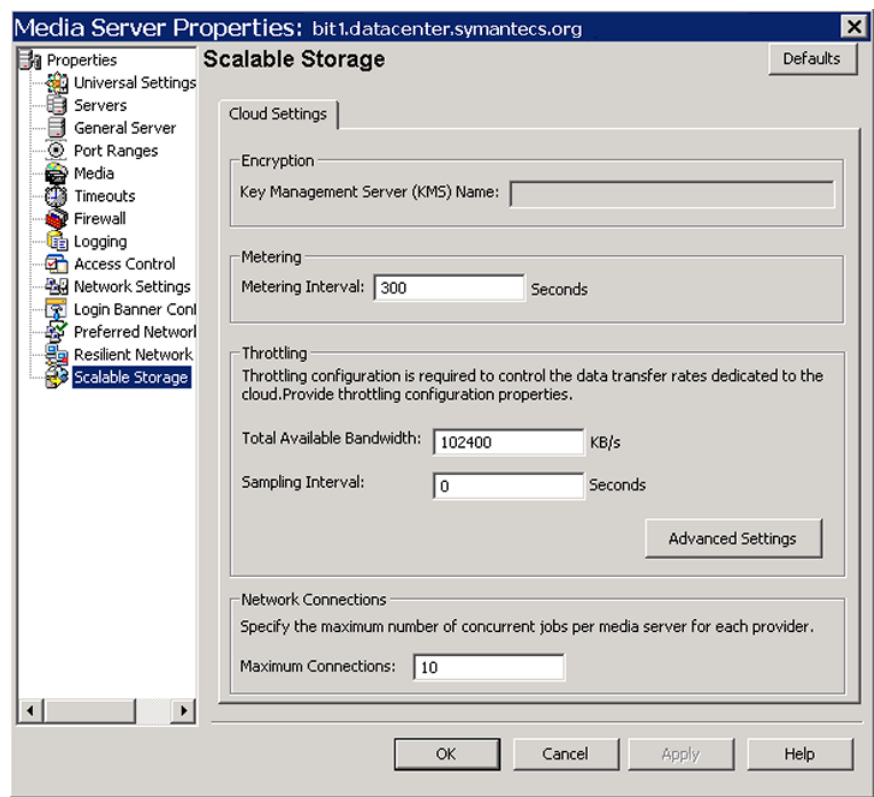


Table 2-7 describes the properties.

Table 2-7 Cloud storage host properties

Property	Description
Key Management Server (KMS) Name	If you configured the NetBackup Key Management Service (KMS), the name of the KMS server.
Metering Interval	Determines how often NetBackup gathers connection information for reporting purposes. . NetBackup OpsCenter uses the information that is collected to create reports. The value is set in seconds. The default setting is 300 seconds (5 minutes). If you set this value to zero, metering is disabled.
Total Available Bandwidth	Use this value to specify the speed of your connection to the cloud. The value is specified in kilobytes per second. The default value is 104857600 KB/sec.

Table 2-7 Cloud storage host properties (*continued*)

Property	Description
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.
Advanced Settings	Click Advanced Settings to specify additional settings for throttling. See “ Configuring advanced bandwidth throttling settings ” on page 29. See “ Advanced bandwidth throttling settings ” on page 30.
Maximum connections	<p>The maximum number of concurrent connections that the media server can open to 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. <i>Exception:</i> For a NetBackup 5400 appliance, this value applies to every compute node (that is, media server) in the appliance. Therefore, to determine the total number of connections to the cloud storage server, add the values from each media server.</p> <p>If NetBackup is configured to allow more jobs than the number of connections, NetBackup fails any jobs that start after the number of maximum connections is reached. NetBackup retries the failed jobs. If a connection is available when NetBackup retries a failed job, the job does not fail because of a lack of connections. Jobs include both backup and restore jobs.</p> <p>Note: NetBackup must account for many factors when it starts jobs: the number of concurrent jobs, the number of connections per media server, the number of media servers, and the job load-balancing logic. Therefore, NetBackup may not fail jobs exactly at the maximum number of connections. NetBackup may fail a job when the connection number is slightly less than the maximum, exactly the maximum, or slightly more than the maximum.</p> <p>In practice, you should not need to set this value higher than 100.</p> <p>You can apply a global maximum concurrent job limit in the master server host properties and a maximum concurrent job limit on each storage unit.</p>

Configuring advanced bandwidth throttling settings

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

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

See “[Scalable Storage properties](#)” on page 26.

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:

Advanced Throttling Configuration

Read Bandwidth:

100

%

Write Bandwidth:

100

%

Start:

Work time

08:00

▲

▼

Off time

18:00

▲

▼

Weekend

Saturday

▼

End:

18:00

▲

▼

08:00

▲

▼

Sunday

▼

Allocated Bandwidth (%):

100

100

100

Allocated Bandwidth (KB/s):

102400

102400

102400

Read Bandwidth (KB/s):

102400

102400

102400

Write Bandwidth (KB/s):

102400

102400

102400

OK

Cancel

Help

- 6 Configure the settings and then click **OK**.
See “[Advanced bandwidth throttling settings](#)” on page 30.

Advanced bandwidth throttling settings

The following table describes the advanced bandwidth throttling settings.

Table 2-8 Advanced Throttling Configuration settings

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

Table 2-8 Advanced Throttling Configuration settings (*continued*)

Property	Description
Off time	<p>Use this field to specify the time interval that is considered off time for the cloud connection.</p> <p>Specify a start time and end time in 24-hour format. For example, 2:00 P.M. is 14:00.</p> <p>Indicate how much bandwidth the cloud connection can use in the Allocated bandwidth field. This value determines how much of the available bandwidth is used for cloud operations in this time window. The value is expressed as a percentage or in kilobytes per second.</p>
Weekend	<p>Specify the start and stop time for the weekend.</p> <p>Indicate how much bandwidth the cloud connection can use in the Allocated bandwidth field. This value determines how much of the available bandwidth is used for cloud operations in this time window. The value is expressed as a percentage or in kilobytes per second.</p>
Read Bandwidth (KB/s)	This field displays how much of the available bandwidth the cloud storage server transmits to a NetBackup media server during each restore job. The value is expressed in kilobytes per second.
Write Bandwidth (KB/s)	This field displays how much of the available bandwidth the NetBackup media server transmits to the cloud storage server during backup jobs. The value is expressed in kilobytes per second.

About the NetBackup CloudStore Service Container

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

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

See “[Scalable Storage properties](#)” on page 26.

The NetBackup CloudStore 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.

In secure mode, the client components must authenticate with the CloudStore Service Container. After authentication, communication occurs 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/opensv/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, the CloudStore Service Container uses non-secure communication. The client communicates with the server over HTTP with no authentication required.

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

See [“Stopping and starting the NetBackup CloudStore Service Container”](#) on page 100.

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.

The following table describes the encryption keys that are required for the KMS database.

Table 2-9 Encryption keys required for the KMS database

Key	Description
Host Master Key	The host master key protects the key database. You can enter a key (a passphrase in KMS terminology) A Host Master Key and an ID.
Key Protection Key	A Key Protection Key passphrase and ID. The key protection key protects individual records in the key database.

The following table describes the encryption keys that are required for each storage server and volume combination.

Table 2-10 Encryption keys required for each storage server and volume combination

Key	Description
A key group	<p>Each storage server and volume combination requires a key group. The key group name must use the following format:</p> <p><code>storage_server_name:volume_name</code></p> <p>The following is the criteria for the key group name:</p> <ul style="list-style-type: none">■ For <code>storage_server_name</code>, you must use the same name that you used when you configured the storage server. If you used a short name, use the same short name. If you used the fully-qualified domain name, use the same fully-qualified domain name.■ The <code>volume_name</code> must be the last directory name in the pathname to the volume. For example, if the pathname is <code>/mnt/disk/hdd1</code>, the <code>volume_name</code> must be <code>hdd1</code>.■ The <code>volume_name</code> must not contain forward or backward slash characters. Therefore, on Windows hosts you must specify a directory name not a drive letter.
A key record	<p>Each key group you create requires a key record. A key record stores the actual key.</p>

See “[Configuring key management for NetBackup cloud storage encryption](#)” on page 34.

See “[Displaying KMS key information for cloud storage encryption](#)” on page 88.

More information about KMS is available.

See the *NetBackup Security and Encryption Guide*.

Configuring key management for NetBackup cloud storage encryption

This topic is an overview of how to configure key management manually by using NetBackup commands.

For cloud storage, encryption is optional. If you do not use encryption, you do not have to configure key management. If you do use encryption, two method exist to configure key management, as follows:

- NetBackup wizards

Symantec recommends that you use the **Cloud Storage Server Configuration Wizard** and the **Disk Pool Configuration Wizard**. The wizards include steps that configure key management.

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

See [Table 2-11](#) on page 35.
- NetBackup commands

You can configure key management manually by using NetBackup commands.

See [“Configuring key management for NetBackup cloud storage encryption”](#) on page 34.

Encryption is optional for on-premises storage.

Table 2-11 Configure key management manually

Step	Task	Instructions
Step 1	Learn about NetBackup key management	See “About key management for encryption of NetBackup cloud storage” on page 33.
Step 2	Set up the KMS database	See “Setting up the KMS database for NetBackup cloud storage encryption” on page 35.
Step 3	Create the key groups	Each storage server and volume combination requires a key group. See “Creating a KMS key group for NetBackup cloud storage encryption” on page 37.
Step 4	Create the key records	Each key group requires a key record. The key record contains the encryption key. See “Creating a KMS key for NetBackup cloud storage encryption” on page 38.
Step 5	Save a record of the key names	The record of the key names lets you recreate the keys if they are lost. See “Saving a record of the KMS key names for NetBackup cloud storage encryption” on page 39.

See [“Displaying KMS key information for cloud storage encryption”](#) on page 88.

Setting up the KMS database for NetBackup cloud storage encryption

Setting up the KMS database is the first task in the process of configuring the NetBackup Key Management Service manually.

See [“Configuring key management for NetBackup cloud storage encryption”](#) on page 34.

See [“KMS database encryption settings”](#) on page 50.

To set up the KMS database

- 1 On the NetBackup master server, create the KMS database by running the `nbkms` command with the `-createemptydb` option, as follows:

UNIX: `/usr/opensv/netbackup/bin/nbkms -createemptydb`

Windows: `install_path\Veritas\NetBackup\bin\nbkms.exe -createemptydb`

The following prompt appears:

Enter the Host Master Key (HMK) passphrase (or hit ENTER to use a randomly generated HMK). The passphrase will not be displayed on the screen.

Enter passphrase :

- 2 Enter a passphrase for the host master key (HMK) or press **Enter** to create a randomly generated key.

After you enter the Host Master Key passphrase, the following prompt appears:

An ID will be associated with the Host Master Key (HMK) just created. The ID will assist you in determining the HMK associated with any key store.

Enter HMK ID :

- 3 Enter an ID for the HMK. This ID can be anything descriptive that you want to use to identify the HMK.

After you enter the Host Master Key ID, the following prompt appears:

Enter the Key Protection Key (KPK) passphrase (or hit ENTER to use a randomly generated KPK). The passphrase will not be displayed on the screen.

Enter passphrase :

- 4 Enter a passphrase for the key protection key.

After you enter the Key Protection Key passphrase, the following prompt appears:

An ID will be associated with the Key Protection Key (KPK) just created. The ID will assist you in determining the KPK associated with any key store.

Enter KPK ID :

- 5 Enter an ID for the KPK. The ID can be anything descriptive that you want to use to identify the KPK.
- 6 Start the NetBackup Key Management Service on the master server. You can do so in the **Activity Monitor** of the **NetBackup Administration Console**.
After you start the service, the initial database setup is complete.
- 7 After you set up the database, create key groups for the volumes in the disk pool.

Creating a KMS key group for NetBackup cloud storage encryption

Creating a KMS key group is the second task in the process of configuring the NetBackup Key Management Service manually.

See [“Configuring key management for NetBackup cloud storage encryption”](#) on page 34.

See [“KMS database encryption settings”](#) on page 50.

A key group is a container for key records. Each storage server and volume combination requires a key group in the following format:

storage_server_name:volume_name

To create a KMS key group

- 1 On the NetBackup master server, create a key group by using the `nbkmsutil` command and the `-createkg` option. The following is the command syntax:

UNIX: `/usr/opensv/netbackup/bin/admincmd/nbkmsutil -createkg -kgname storage_server_name:volume_name`

Windows: `install_path\Veritas\NetBackup\bin\admincmd\nbkmsutil -createkg -kgname storage_server_name:volume_name`

The following is the criteria for the key group name:

- For *storage_server_name*, you must use the same name that you used when you configured the storage server. If you used a short name, use the

same short name. If you used the fully-qualified domain name, use the same fully-qualified domain name.

- The `volume_name` must be the last directory name in the path name to the volume. For example, if the pathname is `/mnt/disk/hdd1`, the `volume_name` must be `hdd1`.
- The `volume_name` must not contain forward or backward slash characters. Therefore, on Windows hosts you must specify a directory name not a drive letter.

The following is an example:

```
nbkmsutil -createkg -kgname  
CloudStorageVendor.com:symc_volume_for_backups
```

- 2 After you create the key groups, create a key record for each group.
See [“Creating a KMS key for NetBackup cloud storage encryption”](#) on page 38.

Creating a KMS key for NetBackup cloud storage encryption

Creating a KMS key is the third and the final task in the process of configuring the NetBackup Key Management Service manually. A KMS key is also known as a *key record*.

See [“Configuring key management for NetBackup cloud storage encryption”](#) on page 34.

See [“KMS database encryption settings”](#) on page 50.

Each key group requires at least one key record. The key record contains the encryption key itself and information about the key. The key is used to encrypt and decrypt data.

For the key name, Symantec recommends that you use the volume name that you used in the key group name. (A key name is optional. If you use a key name, you can use any name for the key name.)

Note: If you create more than one key for a key group, only the last key remains active.

To create a KMS key

- 1 On the NetBackup master server, create a key record by using the `nbkmsutil` command and the `-createkey` option.

UNIX: `/usr/opensv/netbackup/bin/admincmd/nbkmsutil -createkey
 -keyname keyname -kname storage_server_name:volume_name -activate`

Windows: `install_path\Veritas\NetBackup\bin\admincmd\nbkmsutil
 -createkey -keyname keyname -kname
 storage_server_name:volume_name -activate`

You are prompted to enter a passphrase. The following is an example:

```
nbkmsutil -createkey -keyname symc_volume_for_backups -kname
CloudStorageVendor.com:symc_volume_for_backups -activate
```

Enter a passphrase:

- 2 Enter and then re-enter a passphrase; this passphrase should differ from any passphrases you entered already.
 Save a record of the passphrase.

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

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

To save a record of the key names

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

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

Windows: `install_path\Program`

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

The following is example output:

```
Key Group Name       : 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          : CloudStorageVendor.com:symc_volume_for_backups
```

DRAFT

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

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

Windows: `install_path\Program`

`Files\Veritas\NetBackup\bin\admincmd\nbkmsutil.exe -listkeys -kname keyname > filename.txt`

The following is example output for a key group named
CloudStorageVendor.com:symc_volume_for_backups:

`nbkmsutil.exe -listkeys -kname keyname >
keys_for_AdvDiskServer1.symantecs.org:AdvDisk_Volume.txt`

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 group to protect cloud volume

Key Tag : 532cf41cc8b3513a13c1c26b5128731e5ca0b9b01e0689cc38ac2b7596bbae3c
Key Name : symc_volume_for_backups
Current State : Active
Creation Time : Tues Jan 01 01:02:00 2013
Last Modification Time: Tues Jan 01 01:02:00 2013
Description : Key to protect cloud volume

Number of Keys: 1

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

About cloud storage servers

A storage server is an entity that writes data to and reads data from the storage. For cloud storage, it is usually a host on the Internet to which you send the backup data. Your storage vendor provides the name of the storage server. Use that name when you configure cloud storage in NetBackup.

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

If you share the backup images on a cloud vendor's storage, you must configure a storage server in each NetBackup domain that shares the backup images.

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

See “[About cloud storage data movers](#)” on page 71.

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 **Cloud Storage Server Configuration Wizard** communicates with your cloud storage vendor's network and selects the appropriate host for the storage server. The wizard also lets you configure the NetBackup Key Management Service for encryption.

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

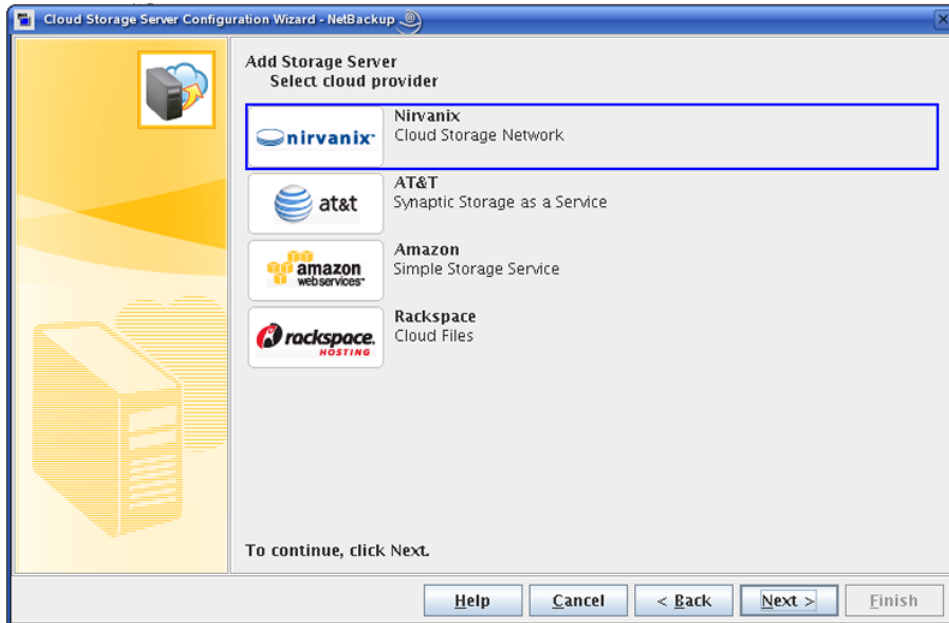
- The media server operating system must be supported for cloud storage. For the operating systems that NetBackup supports for cloud storage, see the NetBackup operating system compatibility list on the [Symantec NetBackup Support Landing Page](#).
- The NetBackup Cloud Storage Service Container (`nbcssc`) must be running.
- The cloud storage binary files must be present in the `ost-plugins` directory.

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

To configure a cloud storage server by using the wizard

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

- 3 Click **Next** on the welcome panel of the wizard.
The **Select Cloud Provider** panel appears.
The following is an example of the wizard panel:



- 4 On the **Select Cloud Provider** panel, select your cloud storage provider and then click **Next**.

After you click **Next**, a cloud storage provider configuration panel appears.

The following is an example of a configuration panel.



- 5 If you do not have a storage provider account, click **Create an account with service provider** on the storage provider configuration panel.

If you have a storage provider account, click **I have a VendorName account**.

The options that you have to configure depend on the storage provider. Select or specify the configuration options.

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

See “[AT&T storage server configuration options](#)” on page 47.

See “[Nirvanix storage server configuration options](#)” on page 48.

See “[Rackspace storage server configuration options](#)” on page 50.

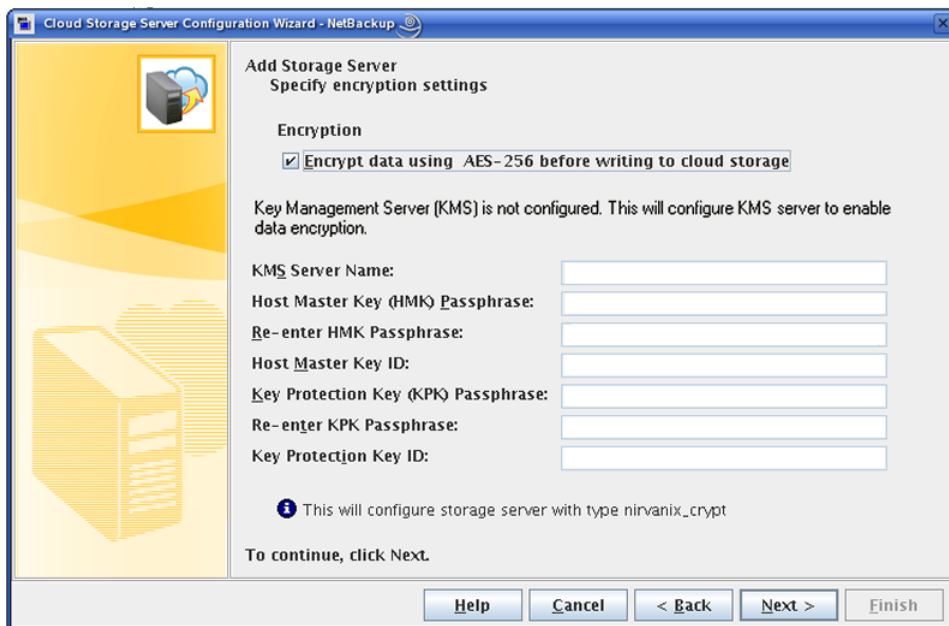
To change the default storage server for your cloud vendor or specify the maximum number of network connections, click **Advanced** then do the following:

- To change the storage server, click **Override storage server** and then enter the storage server name.
- To limit the number of simultaneous network connections to the storage server, enter the value in the **Maximum Connections** box. If you do not set the value here, NetBackup uses the global value from the Cloud Storage host properties.

After you configure the options, click **Next**.

The **Specify Encryption Settings** panel appears.

The following is an example of the panel:



Cloud Storage Server Configuration Wizard - NetBackup

Add Storage Server
Specify encryption settings

Encryption

☒ **Encrypt data using AES-256 before writing to cloud storage**

Key Management Server (KMS) is not configured. This will configure KMS server to enable data encryption.

KMS Server Name:

Host Master Key (HMK) Passphrase:

Re-enter HMK Passphrase:

Host Master Key ID:

Key Protection Key (KPK) Passphrase:

Re-enter KPK Passphrase:

Key Protection Key ID:

i This will configure storage server with type nirvanix_crypt

To continue, click Next.

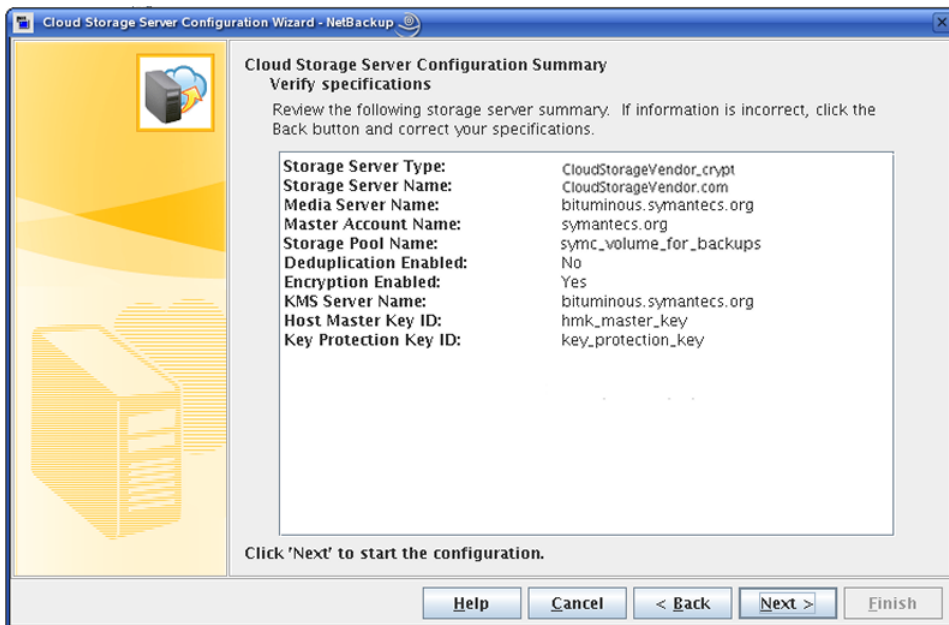
Help **Cancel** **< Back** **Next >** **Finish**

- 6 On the **Specify Encryption Settings** panel, select or enter the encryption settings.

See “[KMS database encryption settings](#)” on page 50.

After you click **Next**, the **Cloud Storage Server Configuration Summary** panel appears.

The following is an example of the panel:



- 7 On the **Cloud Storage Server Configuration Summary** panel, verify the selections. If OK, click **Next**. If not OK, click **Back** until you reach the panel on which you need to make corrections.
- 8 After the wizard creates the storage server, click **Next**.
The **Storage Server Creation Confirmation** panel appears.
- 9 On the **Completion** 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 52.
To exit from the wizard, click **Close**.

Amazon S3 storage server configuration options

The following table describes the storage server configuration options for Amazon S3.

Table 2-12 Amazon S3 storage server configuration options

Field name	Required content
Media Server Name	<p>Select NetBackup media server from the drop-down list.</p> <p>Only those media servers that are enabled for cloud storage appear in the list, as follows:</p> <ul style="list-style-type: none">■ The media server operating system must be supported for cloud storage. See the NetBackup operating system compatibility list for your release on the NetBackup Landing Page.■ The NetBackup Cloud Storage Service Container (nbcssc) must be running.■ The cloud storage binary files must be present in the <code>ost-plugins</code> directory. <p>The host that you select queries the storage vendor's network for its capabilities and for the available storage. The media server also becomes a data mover for your backups and restores.</p> <p>See “About cloud storage data movers” on page 71.</p> <p>After you configure the storage server, you cannot change the media server that you specify here. This behavior is the result of the OpenStorage plugin design. Attempts to change the media server generate an authorization error.</p>
I have an Amazon S3 account	Select I have a Amazon S3 account (Cloud Storage Network) to enter the required account information.
Access ID	<p>Enter your Amazon S3 Access ID.</p> <p>If you do not have an account, click Create an account with the service provider link.</p>
Secure Access Token	Enter your Amazon S3 Secure Access Token.
Advanced	To change the default storage server for your cloud vendor or specify the maximum number of network connections, click Advanced .

AT&T storage server configuration options

The following table describes the storage server configuration options for AT&T.

Table 2-13 AT&T Storage server configuration options

Field name	Required content
Media Server Name	<p>Select NetBackup media server from the drop-down list.</p> <p>Only those media servers that are enabled for cloud storage appear in the list, as follows:</p> <ul style="list-style-type: none"> ■ The media server operating system must be supported for cloud storage. See the NetBackup operating system compatibility list for your release on the NetBackup Landing Page. ■ The NetBackup Cloud Storage Service Container (<code>nbcssc</code>) must be running. ■ The cloud storage binary files must be present in the <code>ost-plugins</code> directory. <p>The host that you select queries the storage vendor's network for its capabilities and for the available storage. The media server also becomes a data mover for your backups and restores.</p> <p>See “About cloud storage data movers” on page 71.</p> <p>After you configure the storage server, you cannot change the media server that you specify here. This behavior is the result of the OpenStorage plugin design. Attempts to change the media server generate an authorization error.</p>
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	<p>Enter your AT&T user name.</p> <p>If you do not have an account, click Create an account with the service provider link.</p>
Password	Enter the password for the User Name account.
Advanced	To change the default storage server for your cloud vendor or specify the maximum number of network connections, click Advanced .

Nirvanix storage server configuration options

The following table describes the storage server configuration options for Nirvanix.

Table 2-14 Storage server configuration options

Field name	Required content
Media Server Name	<p>Select a NetBackup media server from the drop-down list.</p> <p>Only those media servers that are enabled for cloud storage appear in the list, as follows:</p> <ul style="list-style-type: none"> ■ The media server operating system must be supported for cloud storage. See the NetBackup operating system compatibility list for your release on the NetBackup Landing Page. ■ The NetBackup Cloud Storage Service Container (<code>nbcssc</code>) must be running. ■ The cloud storage binary files must be present in the <code>ost-plugins</code> directory. <p>The host that you select queries the storage vendor's network for its capabilities and for the available storage. The media server also becomes a data mover for your backups and restores.</p> <p>See “About cloud storage data movers” on page 71.</p> <p>After you configure the storage server, you cannot change the media server that you specify here. This behavior is the result of the OpenStorage plugin design. Attempts to change the media server generate an authorization error.</p>
I have a Nirvanix CSN account	Select I have a Nirvanix CSN account (Cloud Storage Network) to enter the required account and storage pool information.
Master Account Name	<p>Enter the Nirvanix provided master account name.</p> <p>If you do not have an account, click Create an account with the service provider link.</p>
Password	Enter the password that is associated with the master account name.
Storage Pool Name	<p>Enter the name for the storage pool. This is also known as the Application Name in the Nirvanix Cloud Storage Network. This name must be unique to the Nirvanix Cloud Storage Network storage space.</p> <p>You can use the following characters in the storage pool name:</p> <ul style="list-style-type: none"> ■ Any of the 26 letters of the International Standards Organization (ISO) Latin-script alphabet, both uppercase (capital) letters and lowercase (small) letters. These are the same letters as the English alphabet. ■ Any integer from 0 to 9, inclusive. ■ Any of the following characters: <code>~`!@#\$%^&()_ -+={} ; ' ,</code>
Advanced	To change the default storage server for your cloud vendor or specify the maximum number of network connections, click Advanced .

Rackspace storage server configuration options

The following table describes the storage server configuration options for Rackspace.

Table 2-15 Rackspace storage server configuration options

Field name	Required content
Media Server Name	<p>Select a NetBackup media server from the drop-down list.</p> <p>Only those media servers that are enabled for cloud storage appear in the list, as follows:</p> <ul style="list-style-type: none"> ■ The media server operating system must be supported for cloud storage. See the NetBackup operating system compatibility list for your release on the NetBackup Landing Page. ■ The NetBackup Cloud Storage Service Container (nbcssc) must be running. ■ The cloud storage binary files must be present in the <code>ost-plugins</code> directory. <p>The host that you select queries the storage vendor's network for its capabilities and for the available storage. The media server also becomes a data mover for your backups and restores.</p> <p>See “About cloud storage data movers” on page 71.</p> <p>After you configure the storage server, you cannot change the media server that you specify here. This behavior is the result of the OpenStorage plug-in design. Attempts to change the media server generate an authorization error.</p>
I have a Rackspace Cloud Files account	Select I have a Rackspace Cloud Files account to enter the required account information.
User Name	<p>Enter your Rackspace Cloud Files account user name.</p> <p>If you do not have an account, click Create an account with the service provider link.</p>
Access Key	Enter your Rackspace Cloud Files account access key.
Advanced	To change the default storage server for your cloud vendor or specify the maximum number of network connections, click Advanced .

KMS database encryption settings

The following table describes the settings to configure the NetBackup Key Management Service database.

Table 2-16 Required information for the encryption database

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

Key groups and key records also are required for encryption. If you use the NetBackup wizards to configure cloud storage, the **Disk Pool Configuration Wizard** configures them for you. If you use the

See [“Configuring key management for NetBackup cloud storage encryption”](#) on page 34.

See [“About key management for encryption of NetBackup cloud storage”](#) on page 33.

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.

If you share NetBackup images among multiple NetBackup domains, you do not have to use the same disk pool name in each domain. However, you must use the same volume that you configured in the primary sharing domain.

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

See [“Configuring a disk pool for cloud storage”](#) on page 52.

Configuring a disk pool for cloud storage

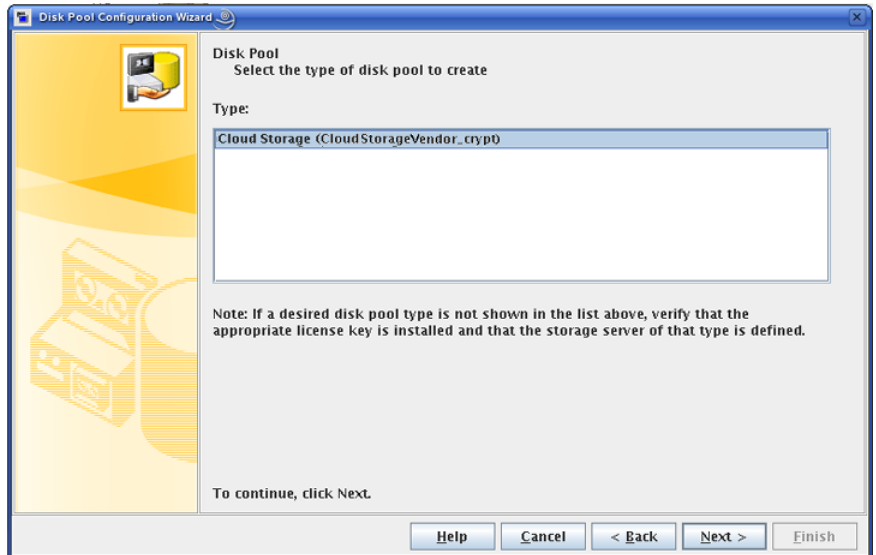
Use the following procedure to configure a disk pool.

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.

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 6.
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 Click **Next** on the welcome panel of the wizard.
- The **Disk Pool** panel appears.
- The following is an example of the wizard panel:

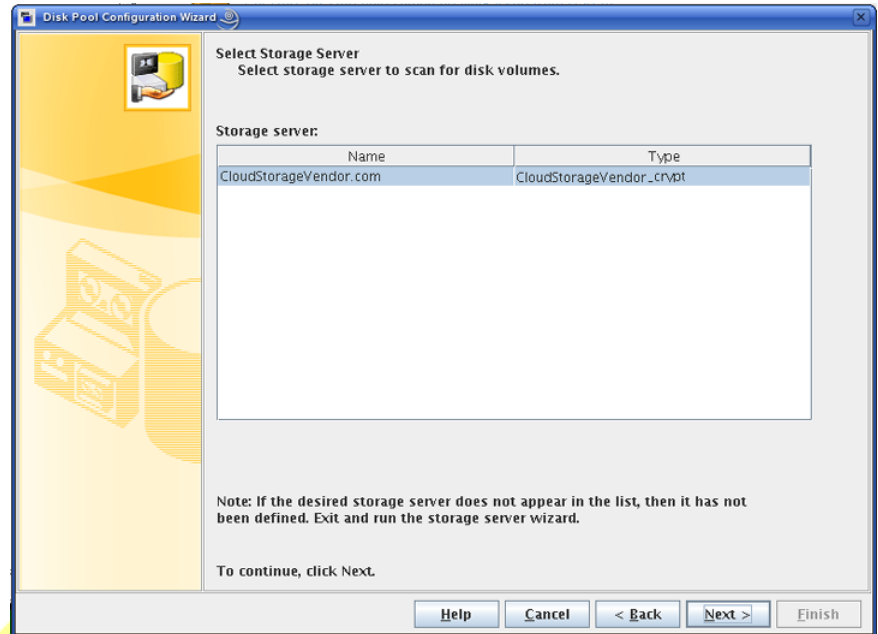


- 4 On the **Disk Pool** panel, select your storage vendor disk pool type, as follows:

The types of disk pools that you can configure depend on the options for which you are licensed.

Click **Next**. The **Select Storage Server** wizard panel appears.

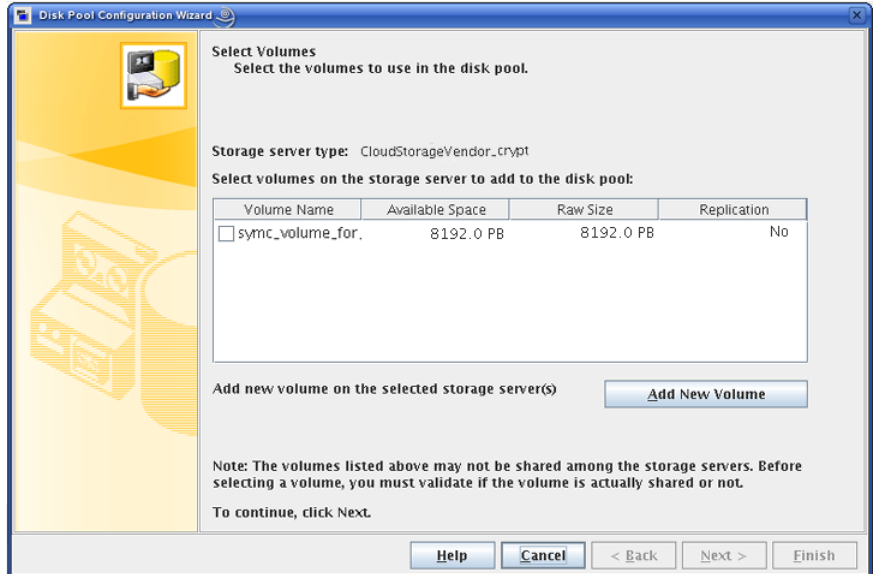
The following is an example of the wizard panel:



- 5 On the **Select Storage Server** panel, select the storage server for this disk pool. The wizard displays the deduplication storage servers that are configured in your environment.

Click **Next**. A wizard panel that lets you create storage volumes appears.

The following is an example of the wizard panel:



- 6 On the **Create Volumes** panel, select the volume for this disk pool. You must select only one volume for a disk pool.

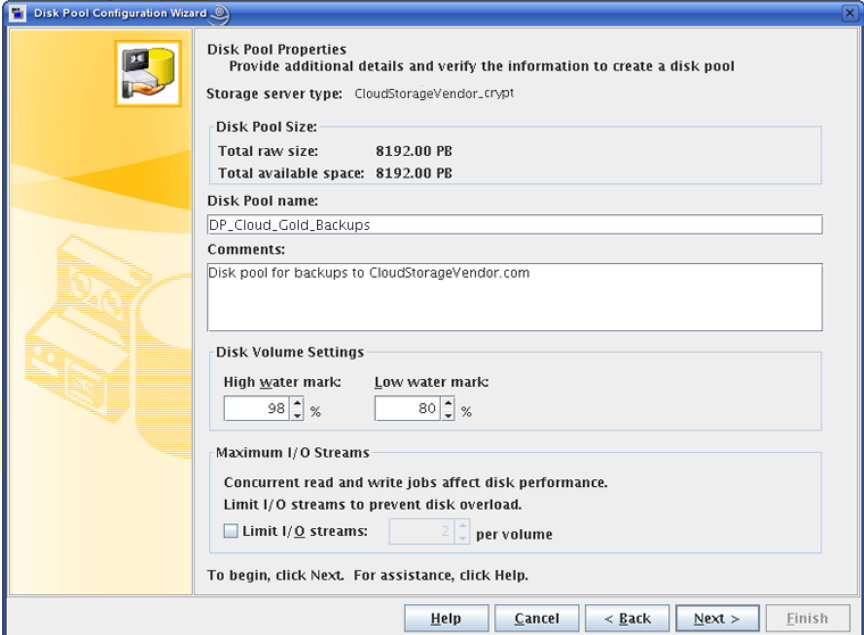
If no volumes are available, click **Add New Volume**. A **Create Cloud Storage Volume** dialog box appears. The information required for the new volume depends on your storage provider.

After you create the new volume, select the volume and then click **Next**.

If you select a volume on a storage destination that requires encryption, a dialog box appears in which you must enter the encryption passphrase. Enter the passphrase in that dialog box.

Click **Next**. The **Disk Pool Properties** wizard panel appears.

The following is an example of the wizard panel:



The screenshot shows the 'Disk Pool Configuration Wizard' window, specifically the 'Disk Pool Properties' step. The window has a blue title bar and a yellow sidebar on the left with a disk icon. The main area is white and contains the following sections:

- Disk Pool Properties**
Provide additional details and verify the information to create a disk pool
- Storage server type:** CloudStorageVendor_crypt
- Disk Pool Size:**
Total raw size: 8192.00 PB
Total available space: 8192.00 PB
- Disk Pool name:**
DP_Cloud_Gold_Backups
- Comments:**
Disk pool for backups to CloudStorageVendor.com
- Disk Volume Settings**
High water mark: 98%
Low water mark: 80%
- Maximum I/O Streams**
Concurrent read and write jobs affect disk performance.
Limit I/O streams to prevent disk overload.
☐ Limit I/O streams: 2 per volume
- To begin, click Next. For assistance, click Help.**

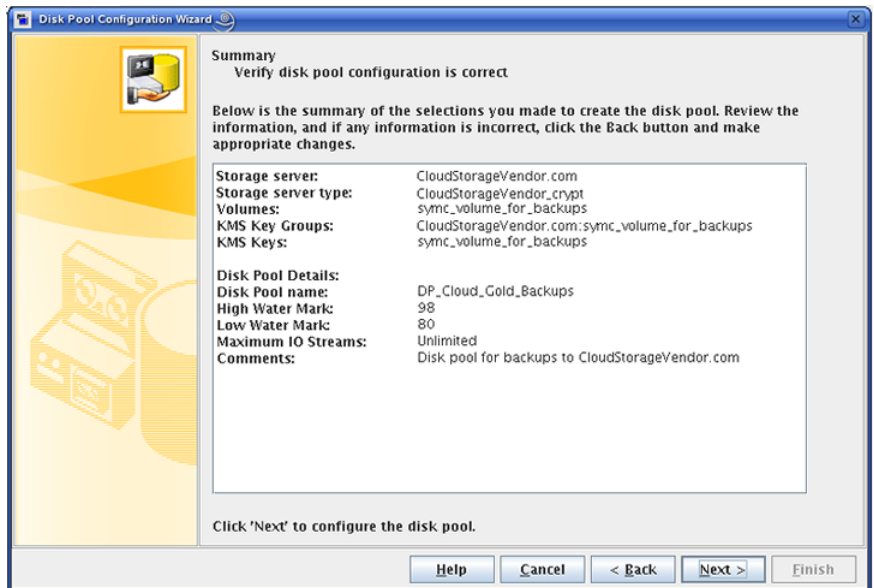
At the bottom right, there are five buttons: Help, Cancel, < Back, Next >, and Finish.

- 7 On the **Disk Pool Properties** panel, enter the values for this disk pool.

See “[Cloud storage disk pool properties](#)” on page 85.

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

The following is an example of the wizard panel:



- 8 On the **Summary** panel, verify the selections. Also, 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 39.

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

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

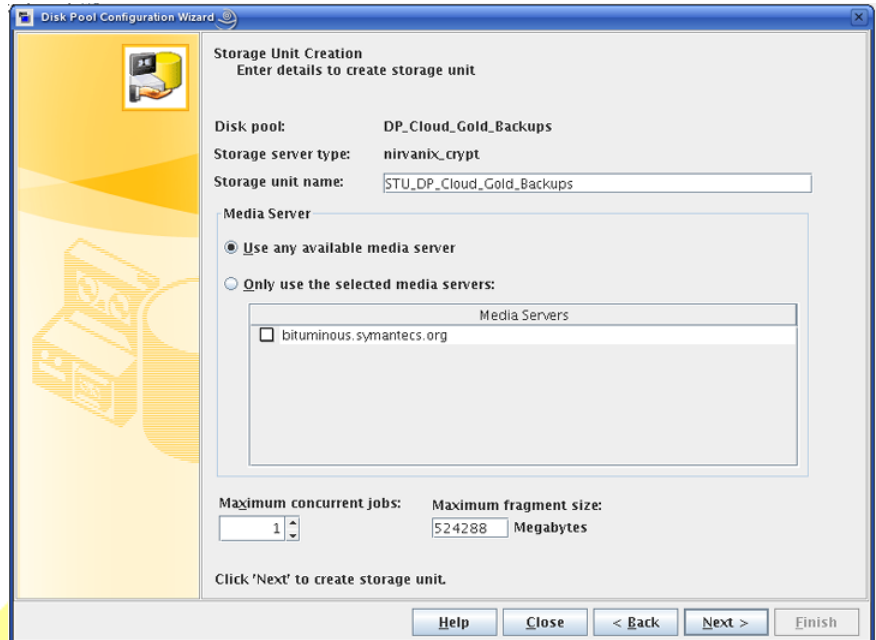
To continue, click **Next**.

The **Storage Unit Creation** wizard panel appears.

- 10 To configure a storage unit for the disk pool, ensure that **Create a storage unit that uses *disk_pool_name*** is selected, then click **Next**. Otherwise, click **Close** to exit from the wizard.

If you click **Next**, a wizard panel appears in which you enter the details about the storage unit.

The following is an example of the wizard panel:



The screenshot shows the 'Disk Pool Configuration Wizard' window, specifically the 'Storage Unit Creation' step. The title bar reads 'Disk Pool Configuration Wizard'. The main heading is 'Storage Unit Creation' with the subtitle 'Enter details to create storage unit'. The form contains the following fields and options:

- Disk pool:** DP_Cloud_Gold_Backups
- Storage server type:** nirvanix_crypt
- Storage unit name:** STU_DP_Cloud_Gold_Backups
- Media Server:**
 - ☒ Use any available media server
 - ☐ Only use the selected media servers:
 - Media Servers:** A list box containing 'bituminous.symantecs.org' with an unchecked checkbox next to it.
- Maximum concurrent jobs:** 1 (in a spinner box)
- Maximum fragment size:** 524288 Megabytes

At the bottom, there is a text prompt: 'Click 'Next' to create storage unit.' and a row of buttons: 'Help', 'Close', '< Back', 'Next >', and 'Finish'.

- 11 Enter the appropriate information for the storage unit.

See [“Cloud storage unit properties”](#) on page 74.

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 76.

See [“Control backup traffic to the media servers”](#) on page 77.

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

About cloud storage server properties

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

Not all properties apply to all storage vendors.

[Table 2-17](#) describes the prefixes for the various properties.

Table 2-17 Prefix definitions

Prefix	Prefix meaning
AMZ	Amazon
ATT	AT&T
COMPR	Data compression
CRYPT	Encryption
METER	Metering
NVX	Nirvanix
RACKS	Rackspace
THR	Throttling

See [“Storage server cloud connection properties”](#) on page 59.

See [“Storage server bandwidth throttling properties”](#) on page 63.

See [“Storage server encryption properties”](#) on page 67.

See [“Nirvanix storage server properties”](#) on page 68.

Storage server cloud connection properties

All or most of the storage vendors use the storage server properties in [Table 2-18](#). The following are the prefixes for the currently supported cloud vendors:

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

Table 2-18 Storage server cloud connection properties

Property	Description
METER:DIRECTORY	<p>This read-only field displays the directory in which to store data stream metering information.</p> <p>Default value: /usr/openv/lib/ost-plugins/meter (UNIX) or <i>install_path</i>\VERITAS\NetBackup\bin\ost-plugins\ (Windows)</p>
METER:INTERVAL	<p>The interval at which NetBackup gathers connection information for reporting purposes.</p> <p>NetBackup OpsCenter uses the information that is collected to create reports. The value is set in seconds. The default setting is 300 seconds (5 minutes). If you set this value to zero, metering is disabled</p> <p>To change this property, use the Cloud Settings tab of the Scalable Storage host properties.</p> <p>See “Cloud Settings tab of the Scalable Storage properties” on page 27.</p> <p>Default value: 300</p> <p>Possible values: 1 to 10000</p>
PREFIX:CURL_CONNECT_TIMEOUT	<p>The amount of time that is allocated for the media server to connect to the cloud storage server. This value is specified in seconds. The default is 300 seconds or five minutes. The media server makes three attempts to connect out during the specified time.</p> <p>This only limits the connection time, not the session time. If the media server cannot connect to the cloud storage server in the specified time, the job fails.</p> <p>This value cannot be disabled. If an invalid number is entered, the <code>CURL_CONNECT_TIMEOUT</code> returns to the default value of 300.</p> <p>In addition to the <code>CURL_CONNECT_TIMEOUT</code> 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.</p> <p>If both the global value and the vendor-specific values are set, the vendor-specific value takes precedent.</p> <p>Default value: 300</p> <p>Possible values: 1 to 10000</p>

Table 2-18 Storage server cloud connection properties (*continued*)

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

Table 2-18 Storage server cloud connection properties (*continued*)

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

Table 2-18 Storage server cloud connection properties (continued)

Property	Description
<code>PREFIX:WRITE_BUFFER_SIZE</code>	<p>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 1073741824 (1 GB). To disable the use of the buffer, set this value to 0 (zero).</p> <p>The <code>WRITE_BUFFER_SIZE</code> value determines the size of the data packs transmitted from the data mover to the storage server during a backup. An increase in the value may increase performance when a large amount of contiguous data is accessed. If insufficient bandwidth exists to transmit the specified amount of data within a few minutes, backup failures may occur due to timeouts. When you calculate the required bandwidth, consider the total load of simultaneous backup jobs and restore jobs on multiple media servers.</p> <p>Default value: 10485760</p> <p>Possible values: 10485760 (10 MB) to 1073741824 (1 GB)</p>

See [“Configuring storage server properties in NetBackup”](#) on page 70.

See [“About cloud storage server properties”](#) on page 59.

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 [“Cloud Settings tab of the Scalable Storage properties”](#) on page 27.

Table 2-19

Cloud storage server bandwidth throttling properties

Property	Description
THR:storage_server	<p>Shows the storage server name for specified cloud storage server. Possible values for <i>storage_server</i> are:</p> <ul style="list-style-type: none"> ■ Amazon: amazon.com ■ AT&T: storage.synaptic.att.com ■ Nirvanix: nirvanix.com ■ Rackspace: rackspace.com <p>Default value: Not applicable</p> <p>Possible values: See Description</p>
THR:AVAIL_BANDWIDTH	<p>This read-only field displays the total available bandwidth value for the cloud feature. The value is displayed in bytes per second. You must specify a number greater than zero. If you enter zero, an error is generated.</p> <p>Default value: 104857600</p> <p>Possible values: Any positive integer</p>

Table 2-19 Cloud storage server bandwidth throttling properties (*continued*)

Property	Description
THR:DEFAULT_MAX_CONNECTIONS	<p>This read-only field displays the maximum number of concurrent connections that the media server can open to 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. <i>Exception:</i> For a NetBackup 5400 appliance, this value applies to every compute node (that is, media server) in the appliance. Therefore, to determine the total number of connections to the cloud storage server, add the values from each media server.</p> <p>If NetBackup is configured to allow more jobs than the number of connections, NetBackup fails any jobs that start after the number of maximum connections is reached. NetBackup retries the failed jobs. If a connection is available when NetBackup retries a failed job, the job does not fail because of a lack of connections. Jobs include both backup and restore jobs.</p> <p>Note: NetBackup must account for many factors when it starts jobs: the number of concurrent jobs, the number of connections per media server, the number of media servers, and the job load-balancing logic. Therefore, NetBackup may not fail jobs exactly at the maximum number of connections. NetBackup may fail a job when the connection number is slightly less than the maximum, exactly the maximum, or slightly more than the maximum.</p> <p>You can apply a global maximum concurrent job limit in the master server host properties and a maximum concurrent job limit on each storage unit.</p> <p>In practice, you should not need to set this value higher than 100.</p> <p>Default value: 10</p> <p>Possible values: 1 to 2147483647</p>
THR:OFF_TIME_BANDWIDTH_PERCENT	<p>This read-only field displays the bandwidth percent that is used during off time.</p> <p>Default value: 100</p> <p>Possible values: 0 to 100</p>
THR:OFF_TIME_END	<p>This read-only field displays the end of off time. Specify the time in 24 hour format. For example, 8:00 A.M. is 8 and 6:30 P.M. is 1830.</p> <p>Default value: 8</p> <p>Possible values: 0 to 2359</p>

Table 2-19

Cloud storage server bandwidth throttling properties (*continued*)

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

Table 2-19 Cloud storage server bandwidth throttling properties (*continued*)

Property	Description
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 [“Configuring storage server properties in NetBackup”](#) on page 70.

See [“About cloud storage server properties”](#) on page 59.

Storage server encryption properties

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

Table 2-20 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

Table 2-20 Encryption cloud storage server properties (*continued*)

Property	Description
CRYPT:KMS_VERSION	<p>This read-only field displays the NetBackup Key Management Service version. You cannot change this value.</p> <p>Default value: 16</p> <p>Possible values: N/A</p>
CRYPT:LOG_VERBOSE	<p>This read-only field displays if logs are enabled for encryption activities. The value is either YES for logging or NO for no logging.</p> <p>Default value: NO</p> <p>Possible values: YES and NO</p>
CRYPT:VERSION	<p>This read-only field displays the encryption version. You cannot change this value.</p> <p>Default value: 13107</p> <p>Possible values: N/A</p>

See [“Configuring storage server properties in NetBackup”](#) on page 70.

See [“About cloud storage server properties”](#) on page 59.

Nirvanix storage server properties

The following storage server properties are specific to Nirvanix. You must use the prefix NVX for these properties.

Table 2-21 Nirvanix specific storage server properties

Property	Description
NVX:CHILD_ACCOUNT_NAME	<p>The NVX:CHILD_ACCOUNT_NAME is the disk volume where the backup images reside.</p> <p>Default value: The name of your Nirvanix child account.</p> <p>Possible values: Any valid text string.</p>

Table 2-21 Nirvanix specific storage server properties (*continued*)

Property	Description
NVX:CHILD_ACCOUNT_SIZE	<p>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.</p> <p>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.</p> <p>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.</p> <p>Default value: 0</p> <p>Possible values: 8 PB</p>
NVX:RESTRICT_IP	<p>Determines if multiple hosts can upload and download with the same token.</p> <p>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.</p> <ul style="list-style-type: none"> ■ 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. <p>Default value: YES</p> <p>Possible values: YES or NO</p>
NVX:STORAGE_POOL_NAME	<p>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.</p> <p>Default value: The name you give to your Nirvanix storage pool.</p> <p>Possible values: Any valid text string.</p>

See [“Configuring storage server properties in NetBackup”](#) on page 70.

See [“About cloud storage server properties”](#) on page 59.

Configuring storage server properties in NetBackup

You can configure and change the properties of your storage server. Normally, you should not have to change the properties.

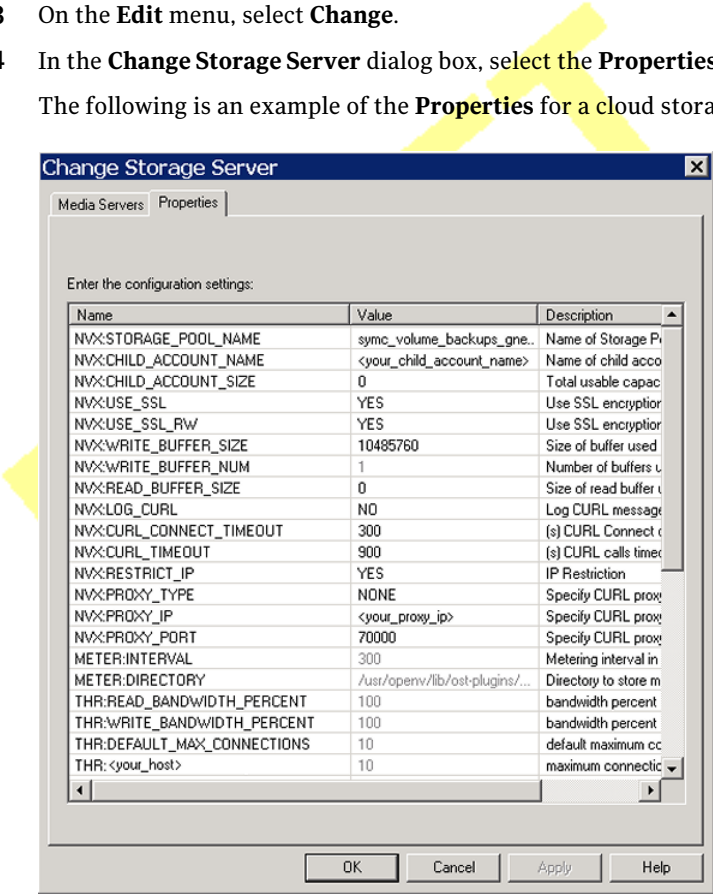
The storage vendor exposes the properties that you can change.

See [“Configuring cloud storage in NetBackup”](#) on page 16.

To change storage server properties

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

The following is an example of the **Properties** for a cloud storage server:



- 5 To change a property, select its value in the **Value** column and then change it.
See [“About cloud storage server properties”](#) on page 59.
See [“Storage server cloud connection properties”](#) on page 59.
See [“Storage server encryption properties”](#) on page 67.
See [“Nirvanix storage server properties”](#) on page 68.
- 6 Repeat step 5 until you have finishing changing properties.
- 7 Click **OK**.
- 8 Restart the `nbrmmms` service by using the **NetBackup Administration Console Activity Monitor**.

About cloud storage data movers

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

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

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

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

See [“Adding backup media servers to your cloud environment”](#) on page 72.

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 73.

Adding backup media servers to your cloud environment

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

See “[About cloud storage data movers](#)” on page 71.

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 the appropriate configuration file from the media server that you specified when you configured the storage server. The file name depends on your storage vendor. The following is the format:

```
libstspiVendorName.conf
```

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

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

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

- 9 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 76.

See [“Control backup traffic to the media servers”](#) on page 77.

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**.

New Storage Unit

Storage unit name: STU_DP_Cloud_Silver

Storage unit type: Disk ☒ On demand only

Disk type: Cloud Storage (CloudStorageVendor_crypt)

Properties and Server Selection

Storage unit configured for: Backup

A storage unit inherits the properties of its disk pool. If properties are specified, only those disk pools that match the specified properties will be available below.

☐ Replication source

☐ Replication target

Select disk pool: DP_Cloud [View Properties](#)

Media server:

☒ Use any available media server

☐ Only use the following media servers

Media Servers

☐ bituminous.symantecs.org

Maximum concurrent jobs: 1

Maximum fragment size: 524288 Megabytes

[OK](#) [Cancel](#) [Help](#)

- 3 Complete the fields in the **New Storage Unit** dialog box.
See [“Cloud storage unit properties”](#) on page 74.

Cloud storage unit properties

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

Table 2-22 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.
Storage unit type	Select Disk as the storage unit type.
Disk type	Select Cloud Storage (<i>type</i>) for the disk type. <i>type</i> represents the disk pool type, based on storage vendor, encryption, and so on.
Storage unit configured for	Select either Backup or Replication .
Primary	Applies to snapshot replication only. Indicates that the storage unit can be used for snapshot creation.
Replication source	Indicates that the storage unit is a source for replication.
Replication target	Indicates that the storage unit is a target for replication.
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 deduplicate the data for this storage unit. Only the deduplication storage server and the load balancing servers appear in the media server list. Specify the media server or servers as follows: <ul style="list-style-type: none">■ To allow any server in the media server list to deduplicate data, select Use any available media server.■ To use specific media servers to deduplicate the data, select Only use the following media servers. Then, select the media servers to allow. NetBackup selects the media server to use when the policy runs.

Table 2-22 Cloud storage unit properties (*continued*)

Property	Description
Maximum fragment size	<p>For normal backups, NetBackup breaks each backup image into fragments so it does not exceed the maximum file size that the file system allows. You can enter a value from 20 MBs to 51200 MBs.</p> <p>For a FlashBackup policy, Symantec recommends that you use the default, maximum fragment size to ensure optimal deduplication performance.</p>
Maximum concurrent jobs	<p>The Maximum concurrent jobs setting specifies the maximum number of jobs that NetBackup can send to a disk storage unit at one time. (Default: one job. The job count can range from 0 to 256.) This setting corresponds to the Maximum concurrent write drives setting for a Media Manager storage unit.</p> <p>NetBackup queues jobs until the storage unit is available. If three backup jobs are scheduled and Maximum concurrent jobs is set to two, NetBackup starts the first two jobs and queues the third job. If a job contains multiple copies, each copy applies toward the Maximum concurrent jobs count.</p> <p>Maximum concurrent jobs controls the traffic for backup and duplication jobs but not restore jobs. The count applies to all servers in the storage unit, not per server. If you select multiple media servers in the storage unit and 1 for Maximum concurrent jobs, only one job runs at a time.</p> <p>The number to enter depends on the available disk space and the server's ability to run multiple backup processes.</p> <p>Warning: A Maximum concurrent jobs setting of 0 disables the storage unit.</p>

Configure a favorable client-to-server ratio

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

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

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

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

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

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

Control backup traffic to the media servers

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

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

About NetBackup Accelerator and NetBackup Optimized Synthetic backups

NetBackup Cloud Storage supports NetBackup Accelerator and NetBackup Optimized Synthetics. Encryption, metering, and throttling are functional and

supported when you enable NetBackup Accelerator or NetBackup Optimized Synthetic backups. You enable both NetBackup Accelerator and NetBackup Optimized Synthetic backups in the same way as non-Cloud backups. More information about NetBackup Accelerator and NetBackup Optimized Synthetic backups is available.

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

Enabling NetBackup Accelerator with cloud storage

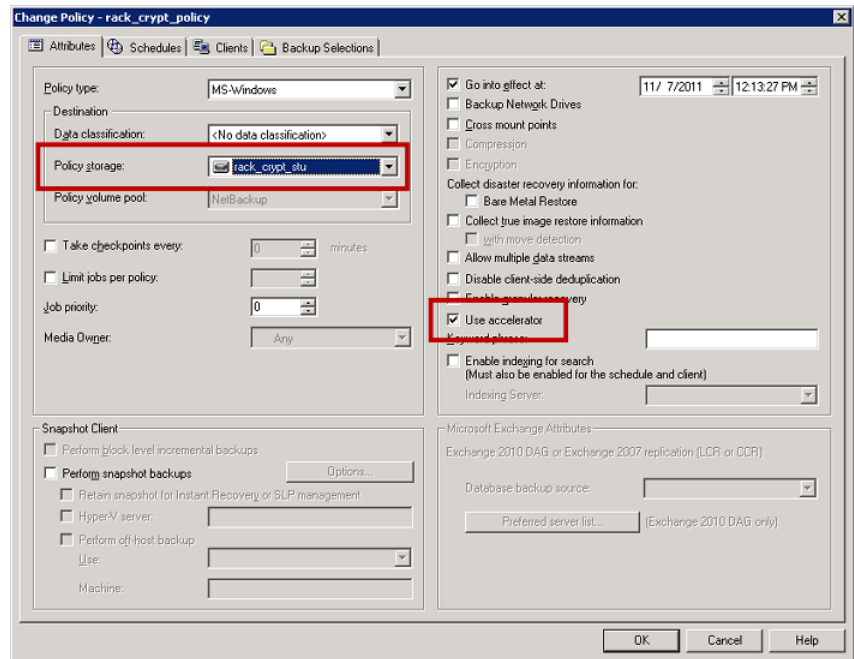
Use the following procedure to enable NetBackup Accelerator for use with NetBackup cloud storage.

Enabling Accelerator for use with NetBackup cloud storage

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

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

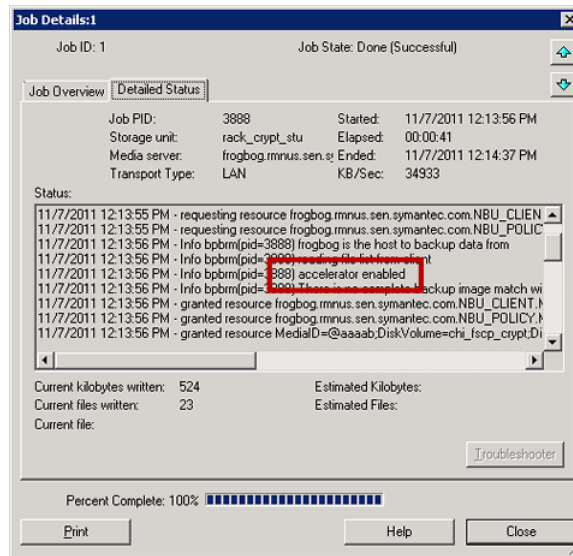
Figure 2-2 Enable Accelerator



Determining if NetBackup Accelerator was used during a backup operation

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

Figure 2-3 Confirm Accelerator used during backup



Enabling optimized synthetic backups with cloud storage

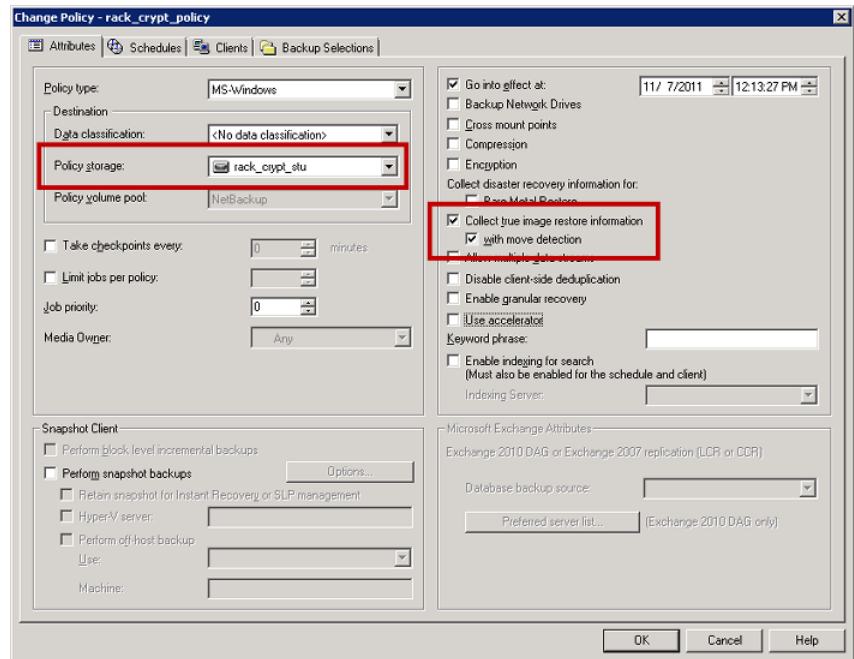
Optimized Synthetic backups require three backup schedules. You must have a **Full backup**, an **Incremental backup**, and a **Full Backup with Synthetic backup enabled**. You can use either a Differential incremental or a Cumulative incremental for the incremental backup. You must then perform a full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

Enabling Optimized Synthetic backups for use with NetBackup Cloud Storage

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

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

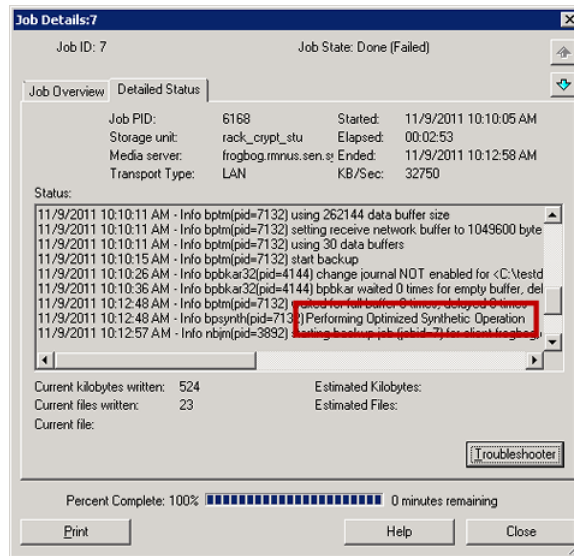
Figure 2-4 Enable Optimized Synthetic backups



Determining if a backup was an Optimized Synthetic backup

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

Figure 2-5 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.

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

To create a 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, or applications**.
- 4 Click **Next** to start the wizard and follow the prompts.

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

Use the following procedure to create a policy 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** checkbox.
- 5 Click **OK**.
- 6 Configure the attributes, the schedules, the clients, and the backup selections for the new policy.

Changing cloud storage disk pool properties

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

To change disk pool properties

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

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

Change Disk Pool

Name: DP_Cloud

Storage servers:

(CloudStorageVendor_crypt) CloudStorageVendor.com

Change

Disk volumes:

Volume Name	Available Space	Raw Size	Replication
sync_volume_backups.	8192.0 PB	8192.0 PB	None

Refresh

Total raw size: 8192.00 PB Total available space: 8192.00 PB

Comments: Disk pool for backups to CloudStorageVendor.com

Disk Volume Settings

High water mark: 98 % Low water mark: 80 %

Maximum I/O Streams

Concurrent read and write jobs affect disk performance.
Limit I/O streams to prevent disk overload.

☐ Limit I/O streams: 2 per volume

OK **Cancel** **Help**

- 4 To add or remove storage servers, click **Change** and then change the servers.
- 5 To update the disk pool replication properties, click **Refresh** in the **Change Disk Pool** dialog box.
- 6 Change the other properties as necessary.
See [“Cloud storage disk pool properties”](#) on page 85.

- 7 Click **OK**.
- 8 If you clicked **Refresh** and the **Replication** value for the **PureDiskVolume** changed, refresh the view in the **Administration Console**.

Cloud storage disk pool properties

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

Table 2-23 OpenStorage disk pool properties

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

Table 2-23 OpenStorage disk pool properties (*continued*)

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

Monitoring and Reporting

This chapter includes the following topics:

- [Viewing cloud storage job details](#)
- [Reporting and monitoring cloud backups](#)
- [Reporting on Auto Image Replication jobs](#)
- [Displaying KMS key information for cloud storage encryption](#)

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.

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.

Reporting on Auto Image Replication jobs

The Activity Monitor displays both the **Replication** job and the **Import** job in a configuration that replicates to a target master server domain.

Table 3-1 Auto Image Replication jobs in the Activity Monitor

Job type	Description
Replication	<p>The job that replicates a backup image to a target master displays in the Activity Monitor as a Replication job. The Target Master label displays in the Storage Unit column for this type of job.</p> <p>Similar to other Replication jobs, the job that replicates images to a target master can work on multiple backup images in one instance.</p> <p>The detailed status for this job contains a list of the backup IDs that were replicated.</p>
Import	<p>The job that imports a backup copy into the target master domain displays in the Activity Monitor as an Import job. An Import job can import multiple copies in one instance. The detailed status for an Import job contains a list of processed backup IDs and a list of failed backup IDs.</p> <p>Note: If the master servers in the source and target domains are not at the same NetBackup version, the following error can occur under certain circumstances: Failed to auto create data classification.</p> <p>This error occurs if the master server in the source domain is at a NetBackup version earlier than 7.6 and the data classification of Any is used. If the master server in the target domain is at NetBackup 7.6, use a different data classification in the source domain or the Import job fails.</p> <p>Note that a successful replication does not confirm that the image was imported at the target master.</p> <p>If the data classifications are not the same in both domains, the Import job fails and NetBackup does not attempt to import the image again.</p> <p>Failed Import jobs fail with a status 191 and appear in the Problems report when run on the target master server.</p> <p>The image is expired and deleted during an Image Cleanup job. Note that the originating domain (Domain 1) does not track failed imports.</p>

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
- Keys

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

The following are the directories in which the `nbkmsutil` command resides:

- UNIX: `/usr/opensv/netbackup/bin/admincmd`
- Windows: `install_path\Veritas\NetBackup\bin\admincmd`

To display KMS key group information

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

```
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         : Key group to protect cloud volume
```

To display KMS key information

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

```
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 group to protect cloud volume
```

```
Key Tag            : 532cf41cc8b3513a13c1c26b5128731e5ca0b9b01e0689cc38ac2b7596bbae3c
Key Name           : symc_volume_for_backups
Current State      : Active
Creation Time      : Tues Jan 01 01:02:00 2013
Last Modification Time: Tues Jan 01 01:02:00 2013
Description        : Key to protect cloud volume
```

DRAFT

Troubleshooting

This chapter includes the following topics:

- [About unified logging](#)
- [About legacy logging](#)
- [About NetBackup cloud storage log files](#)
- [Enable libcurl logging](#)
- [NetBackup CloudStore Service Container startup and shutdown troubleshooting](#)
- [Stopping and starting the NetBackup CloudStore Service Container](#)
- [Troubleshooting cloud storage configuration issues](#)
- [Troubleshooting cloud storage operational issues](#)

About unified logging

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

Unlike the files that are written in legacy logging, unified logging files cannot be 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.

See [“About legacy logging”](#) on page 94.

Server processes and client processes use unified logging.

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

UNIX	<code>/usr/opensv/logs</code>
Windows	<code>install_path\NetBackup\logs</code>

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

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

<code>vxlogcfg</code>	Modifies the unified logging configuration settings. For more information about this command, see the <i>NetBackup Troubleshooting Guide</i> .
<code>vxlogmgr</code>	Manages the log files that the products that support unified logging generate. For more information about this command, see the <i>NetBackup Troubleshooting Guide</i> .
<code>vxlogview</code>	Displays the logs that unified logging generates. See “Examples of using vxlogview to view unified logs” on page 93.

A complete description of the `vxlogcfg`, `vxlogmgr`, and `vxlogview` commands are provided in the *NetBackup Commands Reference Guide*.

These commands are located in the following directory:

UNIX	<code>/usr/opensv/netbackup/bin</code>
Windows	<code>install_path\NetBackup\bin</code>

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	<code>/usr/opensv/logs</code>
Windows	<code>install_path\logs</code>

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.
- Specify the PBX product ID by entering `-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.

See [“Examples of using vxlogview to view unified logs”](#) on page 93.

Examples of using vxlogview to view unified logs

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

Table 4-1 Example uses of the `vxlogview` command

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

Table 4-1 Example uses of the vxlogview command (continued)

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

About legacy logging

Legacy logging and unified logging are the two forms of debug logging used in NetBackup. In legacy debug logging, each process creates logs of debug activity in its own logging directory. All NetBackup processes use either unified logging or legacy logging.

See “[About unified logging](#)” on page 91.

To enable legacy debug logging on NetBackup servers, you must first create the appropriate directories for each process.

UNIX `/usr/opensv/netbackup/logs`
 `/usr/opensv/volmgr/debug`

Windows `install_path\NetBackup\logs`
 `install_path\Volmgr\debug`

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

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

As an alternative, you can stop and restart `nbemm` after creating the following directory:

UNIX `/usr/opensv/volmgr/debug/reqlib`
Windows `install_path\Volmgr\debug\reqlib\`

Tables are available that list the log directories that you must create.

Note: On a Windows server, you can create the debug log directories at once, under `install_path\NetBackup\Logs`, by running the following batch file:
`install_path\NetBackup\Logs\mklogdir.bat`.

Media servers have only the `bpbm`, `bpcd`, `bpdm`, and `bptm` debug logs.

Creating NetBackup log file directories

Before you configure a feature that uses the OpenStorage framework, create the directories into which NetBackup commands write log files. Create the directories on the master server and on each media server that you use for OpenStorage. The log files reside in the following directories:

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

More information about NetBackup logging is available.

See the *NetBackup Troubleshooting Guide*.

See “[About NetBackup cloud storage log files](#)” on page 96.

To create log directories for NetBackup commands

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

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

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

To create the `tpconfig` command log directory

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

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

Windows: `install_path\Volmgr\debug\tpcommand`

About NetBackup cloud storage log files

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

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

See [“Creating NetBackup log file directories”](#) on page 95.

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

More information about how to view and manage VxUL log files is available.

See the *NetBackup Troubleshooting Guide*.

The following are the component identifiers for log messages:

- An `sts_` prefix relates to the interaction with the storage vendor software plug-in.
- A cloud storage server prefix (for example, `nirvanix.com`) relates to interaction with the cloud storage network.
- An `encrypt` prefix relates to interaction with the encryption plug-in.
- A `KMSCLIB` prefix relates to interaction with the NetBackup Key Management Service.

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

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

Specify the NetBackup log levels in the **Logging** host properties on the NetBackup master server. The log levels for some processes specific to certain options are set in configuration files as described in [Table 4-2](#).

[Table 4-2](#) describes the logs.

Table 4-2 NetBackup logs

Activity	OID	Processes
Backups and restores	N/A	<p>Messages appear in the log files for the following processes:</p> <ul style="list-style-type: none"> ■ The <code>bpbrm</code> backup and restore manager. ■ The <code>bpdbm</code> database manager. ■ The <code>bpdm</code> disk manager. ■ The <code>bptm</code> tape manager for I/O operations. <p>The log files reside in the following directories:</p> <ul style="list-style-type: none"> ■ UNIX: <code>/usr/opensv/netbackup/logs/</code> ■ Windows: <code>install_path\NetBackup\logs\</code>
Backups and restores	117	<p>The <code>nbjm</code> Job Manager.</p>
Image cleanup, verification, import, and duplication	N/A	<p>The <code>bpdbm</code> database manager log files.</p> <p>The log files reside in the following directories:</p> <ul style="list-style-type: none"> ■ UNIX: <code>/usr/opensv/netbackup/logs/bpdbm</code> ■ Windows: <code>install_path\NetBackup\logs\bpdbm</code>
Connection operations	N/A	<p>The <code>bpstsinfo</code> utility writes information about connections to the storage server in its log files.</p>
Cloud account configuration	222	<p>The the Remote Manager and Monitor Service is the process that creates the cloud storage accounts. RMMS runs on media servers.</p>

Table 4-2 NetBackup logs (*continued*)

Activity	OID	Processes
Cloud Storage Service Container	N/A	The NetBackup Cloud Storage Service Container (<i>nbcssc</i>) writes log files to the following directories: <ul style="list-style-type: none"> ■ For Windows: <i>install_path\NetBackup\logs\nbcssc</i> ■ For UNIX/Linux: <i>/usr/opensv/netbackup/logs/nbcssc</i>
Credentials configuration	N/A	The <i>tpconfig</i> utility. The <i>tpconfig</i> command writes log files to the <i>tpcommand</i> directory.
Device configuration	111	The <i>nbemm</i> process.
Device configuration	178	The Disk Service Manager process that runs in the Enterprise Media Manager (EMM) process.
Device configuration	202	The Storage Server Interface process that runs in the Remote Manager and Monitor Service. RMMS runs on media servers.
Device configuration	230	The Remote Disk Service Manager interface (RDSM) that runs in the Remote Manager and Monitor Service. RMMS runs on media servers.

Enable libcurl logging

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

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

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

See [“Configuring storage server properties in NetBackup”](#) on page 70.

NetBackup CloudStore Service Container startup and shutdown troubleshooting

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.

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

See [“Connection to the NetBackup CloudStore Service Container fails”](#) on page 99.

If the NetBackup CloudStore 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.

See [“Stopping and starting the NetBackup CloudStore Service Container”](#) on page 100.

Connection to the NetBackup CloudStore Service Container fails

The `csconfig` command makes three attempts to connect to the NetBackup CloudStore 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/opensv/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 CloudStore Service Container”](#) on page 32.

See [“Stopping and starting the NetBackup CloudStore Service Container”](#) on page 100.

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 32.

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).

Troubleshooting cloud storage configuration issues

The following sections may help you troubleshoot configuration issues.

See [“Cloud storage: cannot create a storage server”](#) on page 100.

Cloud storage: cannot create a storage server

The following table describes potential solutions if you cannot create a storage server.

Table 4-3 Cannot create storage server solutions

Error	Description
Unauthorized storage pool creation due to node access	<p>The error message appears in the Remote Disk Service Manager interface (RDSM) logs. RDSM runs in the Remote Manager and Monitor Service.</p> <p>See “About NetBackup cloud storage log files” on page 96.</p> <p>For Nirvanix cloud storage, the storage you specified when you tried to create the storage server does not contain the Symantec partner ID.</p> <p>To resolve this issue, contact your Nirvanix support representative and request that they add the Symantec partner ID to the storage node.</p>

Troubleshooting cloud storage operational issues

The following sections may help you troubleshoot operational issues.

See [“Cloud storage backups fail with status code 84 or 87”](#) on page 101.

See [“Nirvanix backup attempts fail with Disk volume is down error messages”](#) on page 102.

See [“A restart of the nbcssc process reverts all cloudstore.conf settings”](#) on page 103.

See [“NetBackup Administration Console fails to open”](#) on page 103.

Cloud storage backups fail with status code 84 or 87

The following table describes backup failures indicated by status code 84 or 87.

Table 4-4 Media write error solutions

Error	Description
<p>A message similar to the following is in the job details:</p> <pre>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. Errno = 32: Broken pipe Info bptm(pid=xxxx) EXITING with status 84</pre> <p>The message in the bptm log file:</p> <pre>rackspace: Container jstage_systemtest is not Symantec container or tag data error, fail to create image. Please make sure that the LSU is created by means of NBU.</pre>	<p>For Rackspace cloud storage, the volume was not created by using the NetBackup Disk Pool Configuration Wizard.</p> <p>You must use the Disk Pool Configuration Wizard to create the volume on the cloud storage. The wizard applies a required partner ID to the Rackspace volume. If you use the Rackspace interface to create the container, the partner ID is not applied.</p> <p>Using the Rackspace interface, delete the container. Delete the disk pool in NetBackup, then recreate it using the Disk Pool Configuration Wizard.</p> <p>See “Viewing cloud storage job details” on page 87.</p> <p>See “About NetBackup cloud storage log files” on page 96.</p> <p>See “About Rackspace Cloud Files requirements” on page 25.</p>
WRITE_BUFFER_SIZE problem	<p>If the <code>WRITE_BUFFER_SIZE</code> 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 <code>WRITE_BUFFER_SIZE</code> size to a value lower than the computer's total swap space to resolve this issue.</p>
Large files backed up to an AIX media server	<p>When you back up large files to an AIX media server, 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 <code>ulimit</code> size to unlimited to resolve this issue. Be sure to stop and restart the NetBackup services or daemons after you change the <code>ulimit</code> value.</p> <p>Example:</p> <pre>ulimit -m unlimited ulimit -d unlimited ulimit -s unlimited</pre>

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 `libstspnirvanix.conf` and the `libstspnirvanix.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/opensv/libs/ost-plugins/` directory for UNIX and Linux computers and to the `install_path\Veritas\NetBackup\bin\ost-plugins\` for Windows computers.

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 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:

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

DRAFT

Known issues

This chapter includes the following topics:

- About using the `bpstsinfo` to list storage server information
- Encrypted and non-encrypted storage units displayed in `bpstsinfo` command output
- About inconsistencies when image information is displayed
- About deleting storage servers
- Special characters and the `csconfig` command
- Directory length exceeds maximum path length for `csconfig` command
- Unexpected results for `csconfig throttle` command
- Different cloud provider information provided to the `csconfig throttle` command
- Attempts to set available bandwidth with the `csconfig` command fail
- Unable to configure additional media servers
- Cloud configuration may fail if NetBackup Access Control is enabled

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/opensv/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.

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.

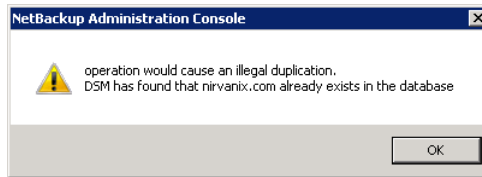
Attempts to set available bandwidth with the `csconfig` command fail

The `csconfig throttle` command accepts large values for the available bandwidth option. The maximum allowed value varies with the operating system where the

NetBackup CloudStore 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 72.

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 Keys cannot 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.

Cloud Storage Server Configuration Wizard

This chapter includes the following topics:

- [Reviewers: about these wizard help topics](#)
- [About the Cloud Storage Server Configuration Wizard panel](#)
- [Select Cloud Provider panel](#)
- [Amazon S3 Cloud Provider Configuration panel](#)
- [AT&T Cloud Provider Configuration panel](#)
- [Nirvanix Cloud Provider Configuration panel](#)
- [Rackspace Cloud Provider Configuration panel](#)
- [Advanced Server Configuration dialog box](#)
- [Specify Deduplication Settings panel](#)
- [Specifying Encryption Settings panel](#)
- [Cloud Storage Server Configuration Summary panel](#)
- [Cloud storage configuration progress panel](#)
- [Cloud storage configuration completion panel](#)

Reviewers: about these wizard help topics

The topics in this chapter are the actual help screens that users see when they click a Help button on a wizard screen. Please review these topics.

These wizard help topics are included in this guide only for review purposes.

*These wizard help topics will ***never*** appear in any guide that customers see.*

Also, the screen shots are not included in the wizard deliverable; they are included here for reference only. Please tell me if a wizard panel has been updated.

About the Cloud Storage Server Configuration Wizard panel

Figure 6-1 Writer and reviewer reference only. Mockup from 7.6 Titan.



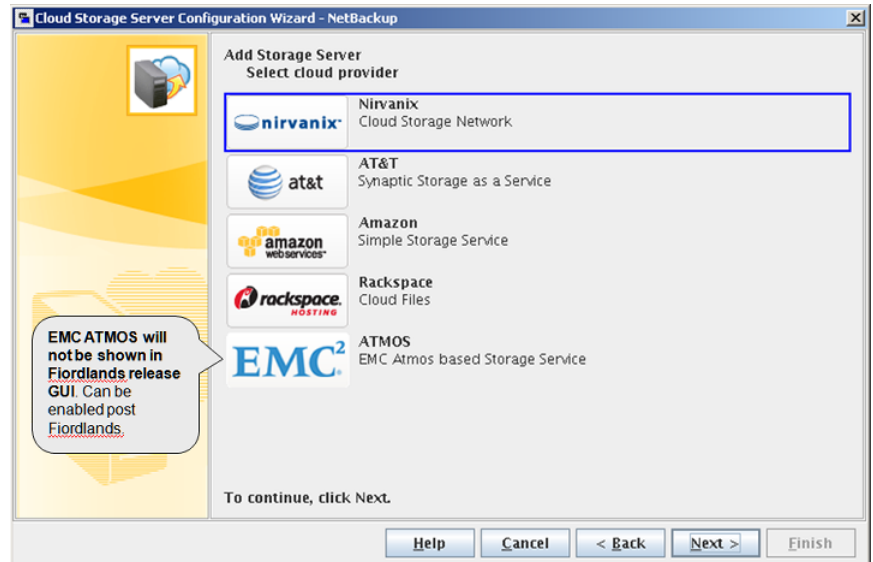
Review the welcome information. Click **Next** to continue.

See [“Select Cloud Provider panel”](#) on page 111.

See [“Configuring cloud storage in NetBackup”](#) on page 16.

Select Cloud Provider panel

Figure 6-2 Writer and reviewer reference only. Mockup from 7.6 Titan.



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

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

- The media server operating system must be supported for cloud storage. See the [NetBackup operating system compatibility list](#) for your release on the [NetBackup Landing Page](#).
- The NetBackup CloudStore Service Container (`nbcssc`) must be running. See [“About the NetBackup CloudStore Service Container”](#) on page 32.
- The cloud storage binary files must be present in the `ost-plugins` directory.

See [“Nirvanix Cloud Provider Configuration panel”](#) on page 114.

See [“Rackspace Cloud Provider Configuration panel”](#) on page 115.

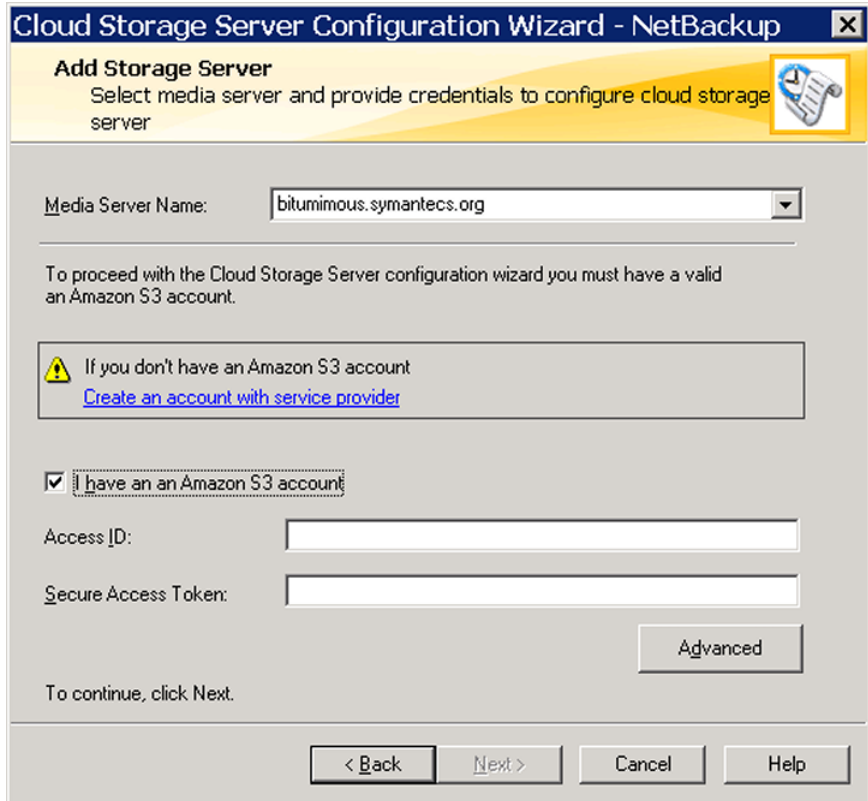
See [“Amazon S3 Cloud Provider Configuration panel”](#) on page 112.

See [“AT&T Cloud Provider Configuration panel”](#) on page 113.

See [“Configuring cloud storage in NetBackup”](#) on page 16.

Amazon S3 Cloud Provider Configuration panel

Figure 6-3 Writer and reviewer reference only. Mockup from 7.6 Titan.



The screenshot shows a window titled "Cloud Storage Server Configuration Wizard - NetBackup". The main heading is "Add Storage Server" with the instruction "Select media server and provide credentials to configure cloud storage server". A dropdown menu for "Media Server Name:" is set to "bitumimous.symantecs.org". A message states: "To proceed with the Cloud Storage Server configuration wizard you must have a valid an Amazon S3 account." Below this is a warning box: "If you don't have an Amazon S3 account" with a link "Create an account with service provider". A checkbox "I have an an Amazon S3 account" is checked. There are input fields for "Access ID:" and "Secure Access Token:". An "Advanced" button is located to the right of the "Secure Access Token" field. At the bottom, it says "To continue, click Next." and there are buttons for "< Back", "Next >", "Cancel", and "Help".

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

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

See “[About the Amazon Simple Storage Service \(S3\) requirements](#)” on page 19.

To change the default storage server for your cloud vendor or specify the maximum number of network connections, click **Advanced**.

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

AT&T Cloud Provider Configuration panel


Figure 6-4 Writer and reviewer reference only. Mockup from 7.6 Titan.

Cloud Storage Server Configuration Wizard - NetBackup

Add Storage Server
Select media server and provide credentials to configure cloud storage server

Media Server Name: bitumimous.symantecs.org

To proceed with the Cloud Storage Server configuration wizard you must have a valid AT&T synaptic storage account.

 If you don't have AT&T synaptic storage account
[Create an account with service provider](#)

☒ I have an AT&T synaptic storage account

User Name:

Password:

Advanced

To continue, click Next.

< Back Next > Cancel Help

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

See “[AT&T storage server configuration options](#)” on page 47.

See “[About AT&T Synaptic requirements](#)” on page 21.

To change the default storage server for your cloud vendor or specify the maximum number of network connections, click **Advanced**.

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

Nirvanix Cloud Provider Configuration panel


Figure 6-5 Writer and reviewer reference only. Mockup from 7.6 Titan.

Cloud Storage Server Configuration Wizard - NetBackup

Add Storage Server
Select media server and provide credentials to configure cloud storage server

Media Server Name:

To proceed with the Cloud Storage Server configuration wizard you must have a valid a Nirvanix CSN account.

 If you don't have an a Nirvanix CSN account
[Create an account with service provider](#)

☐ I have an a Nirvanix CSN account

Master Account Name:

Password:

Storage Pool Name:

Advanced

To continue, click Next.

< Back Next > Cancel Help

Specify the required information for Nirvanix.

See [“Nirvanix storage server configuration options”](#) on page 48.

See [“About the Nirvanix Cloud Storage Network requirements”](#) on page 22.

To change the default storage server for your cloud vendor or specify the maximum number of network connections, click **Advanced**.

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

Rackspace Cloud Provider Configuration panel

Figure 6-6 Writer and reviewer reference only. Mockup from 7.6 Titan.

Cloud Storage Server Configuration Wizard - NetBackup

Add Storage Server
Select media server and provide credentials to configure cloud storage server

Media Server Name:

To proceed with the Cloud Storage Server configuration wizard you must have a valid a Rackspace Cloud Files account.

If you don't have a Rackspace Cloud Files account
[Create an account with service provider](#)

☒ I have an a Rackspace Cloud Files account

User Name:

Access Key:

To continue, click Next.

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

See “[Rackspace storage server configuration options](#)” on page 50.

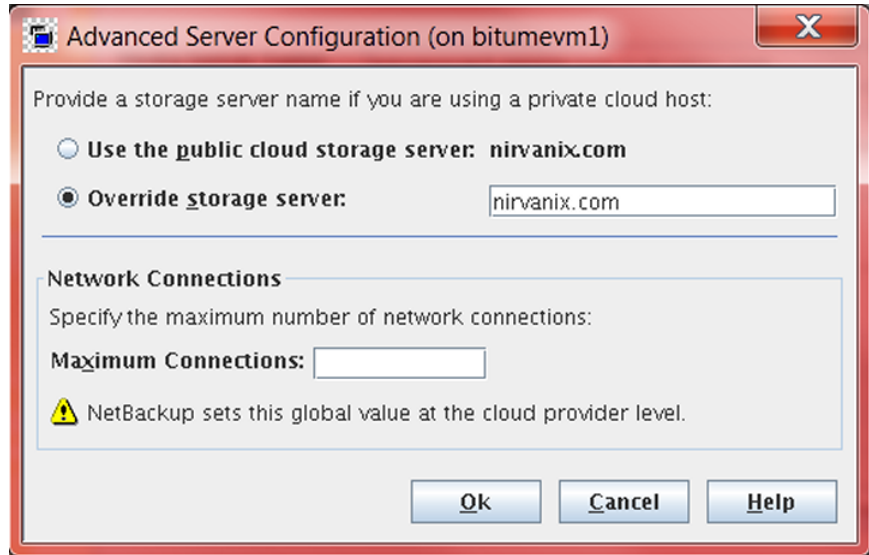
See “[About Rackspace Cloud Files requirements](#)” on page 25.

To change the default storage server for your cloud vendor or specify the maximum number of network connections, click **Advanced**.

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

Advanced Server Configuration dialog box

Figure 6-7 Screen shot for reference only; does not appear in the deliverable



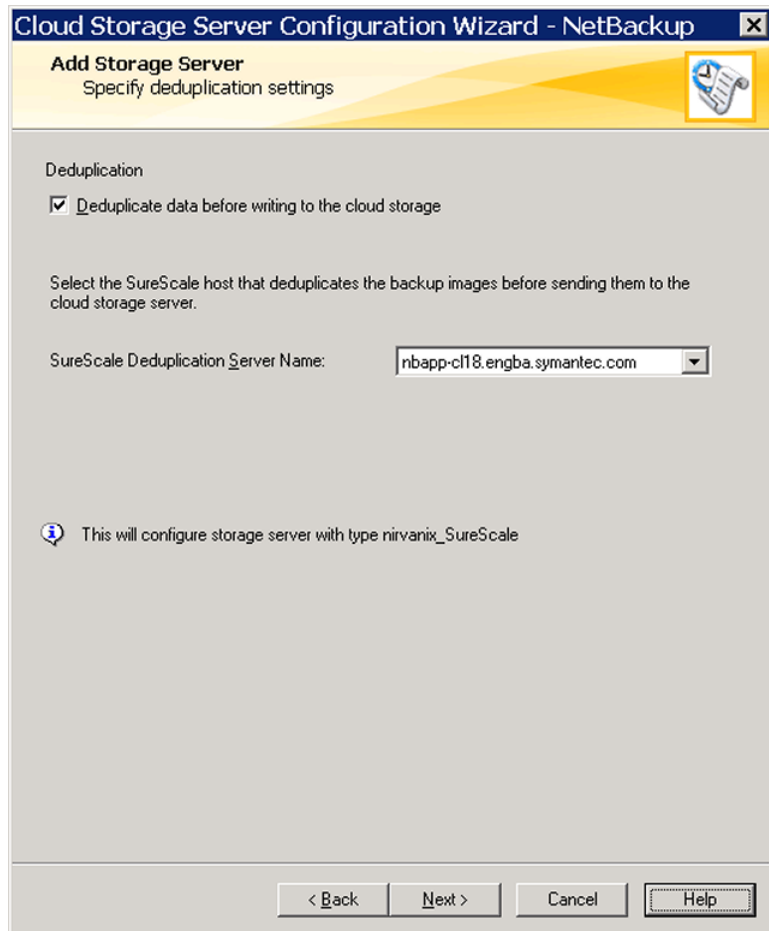
The **Advanced Server Configuration** dialog box lets you change the storage server name and the maximum number of network connections, as follows:

- To change the storage server, click **Override storage server** and then enter the storage server name.
- To limit the number of simultaneous network connections to the storage server, enter the value in the **Maximum Connections** 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 26.

Specify Deduplication Settings panel

Reviewer: This wizard will change to the Scalable Storage Server Configuration Wizard some time after 7.6.

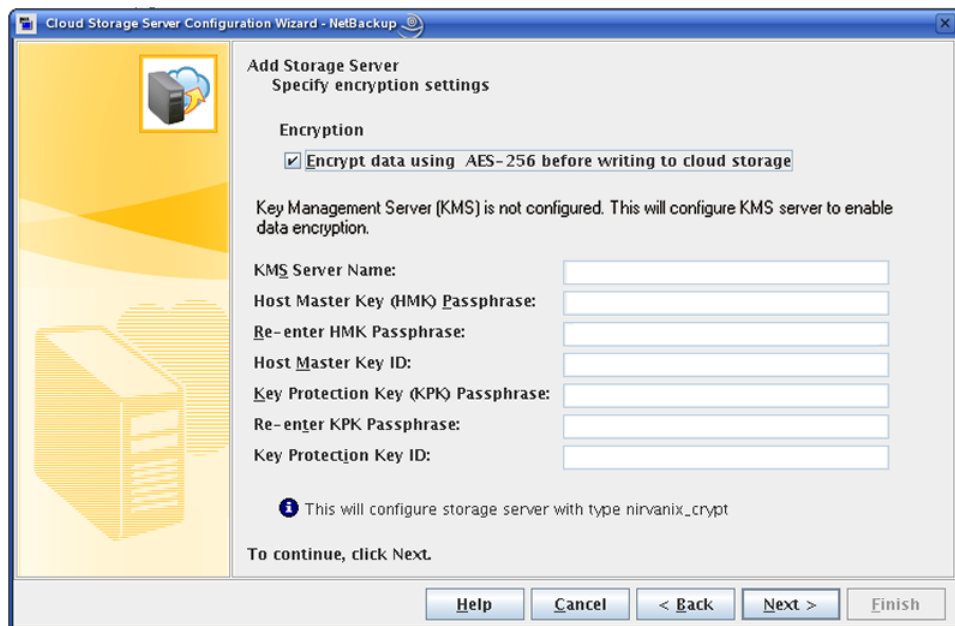
Figure 6-8 Writer and reviewer reference only

To configure deduplication for your data, do the following:

- Select **Deduplicate data before writing to scalable storage**. A **Deduplication Server Name** list box appears.
- For the **Deduplication Server Name**, select the SureScale host that performs the deduplication. If you have a NetBackup 5400 appliance, select the appliance virtual host name.
If you selected a SureScale host in the **Cloud Provider** panel, that host is selected automatically.
- Click **Next**.

Specifying Encryption Settings panel

Figure 6-9 Writer and reviewer reference only. Mockup from 7.6 Titan.



To encrypt the data, select **Encrypt data using AES-256 before writing to scalable storage**. For SureScale cloud storage, this option is selected by default and cannot be changed.

If encryption is configured already, a read-only summary of the database protection information is displayed.

If encryption is not enabled and configured, configure the key management settings for the database.

See [“About key management for encryption of NetBackup cloud storage”](#) on page 33.

See [“KMS database encryption settings”](#) on page 50.

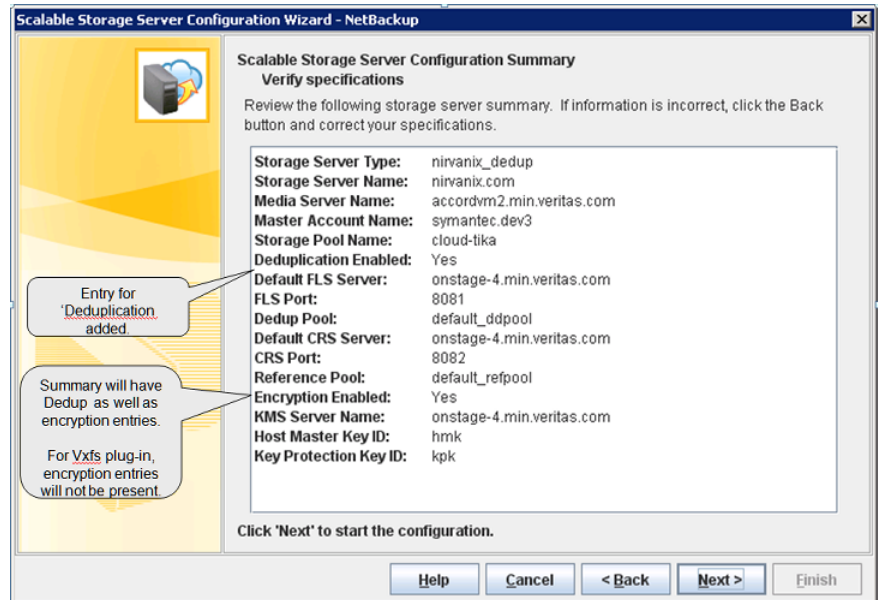
Encryption keys are also required for the volumes that contain the data. If you use the NetBackup wizards to configure cloud storage, the **Disk Pool Configuration Wizard** configures the volume keys for you.

More information about the configuration of KMS is available.

See the *NetBackup Security and Encryption Guide*.

Cloud Storage Server Configuration Summary panel

Figure 6-10 Writer and reviewer reference only. Mockup from 7.6 Titan.



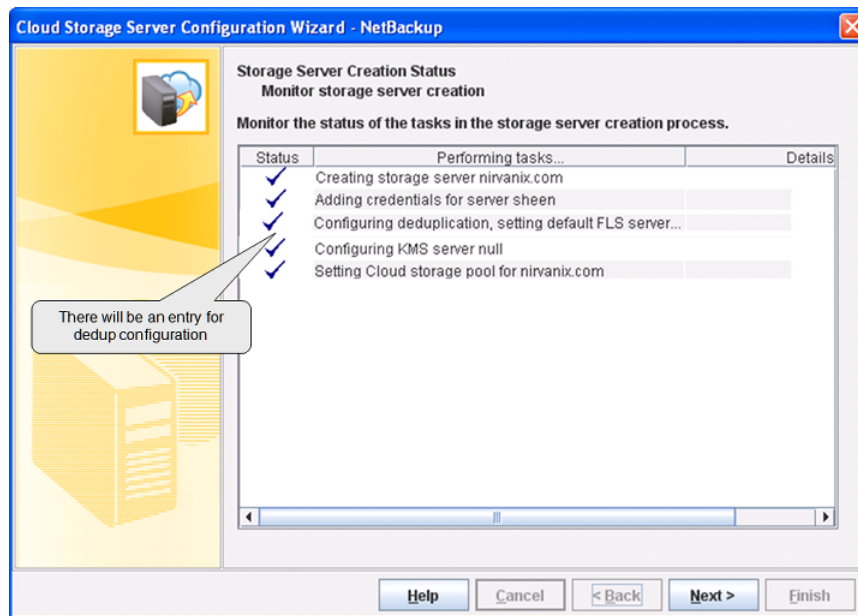
This panel summarizes the information you provided in the Cloud storage server wizard. Review the information that is contained in this panel. Click **Next** to continue or **Back** to return to previous panels and make changes.

See “Cloud storage configuration progress panel” on page 120.

See “Configuring cloud storage in NetBackup” on page 16.

Cloud storage configuration progress panel

Figure 6-11 Writer and reviewer reference only. Mockup from 7.6 Titan.



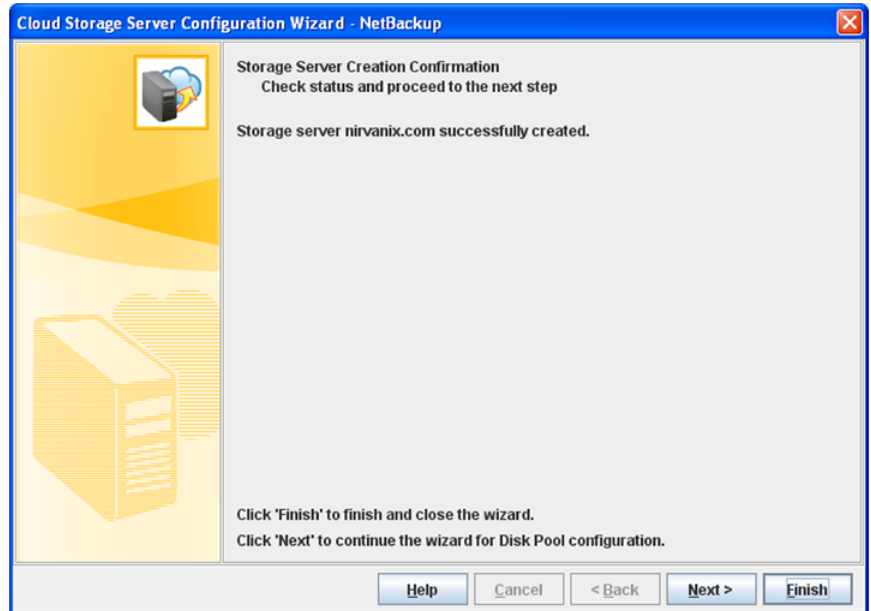
Monitor this panel to view the progress of the storage server creation.

See [“Cloud storage configuration completion panel”](#) on page 121.

See [“Configuring cloud storage in NetBackup”](#) on page 16.

Cloud storage configuration completion panel

Figure 6-12 Writer and reviewer reference only. Mockup from 7.6 Titan.



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 dialog box”](#) on page 131.

See [“Create Cloud Storage Volume for AT&T dialog box”](#) on page 132.

See [“Create Cloud Storage Volume for Nirvanix dialog box”](#) on page 133.

See [“Create Cloud Storage Volume for Rackspace dialog box”](#) on page 134.

See [“Configuring cloud storage in NetBackup”](#) on page 16.

DRAFT

Disk Pool Configuration Wizard

This chapter includes the following topics:

- [Reviewers: about these wizard help topics](#)
- [About the Disk Pool Configuration Wizard](#)
- [Disk Pool panel](#)
- [Select Storage Server panel](#)
- [Select Volumes panel](#)
- [Disk Pool Properties panel](#)
- [Summary panel](#)
- [Confirmation panel](#)
- [Storage Unit Option panel](#)
- [Create Storage Unit panel](#)
- [Finish panel](#)

Reviewers: about these wizard help topics

The topics in this chapter are the actual help screens that users see when they click a Help button on a wizard screen. Please review these topics.

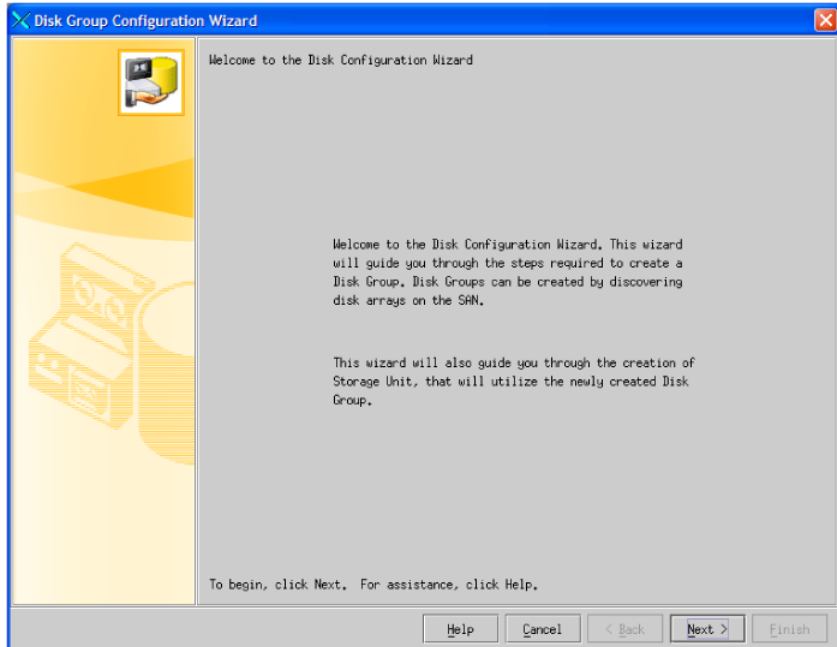
These wizard help topics are included in this guide only for review purposes.

*These wizard help topics will **never** appear in any guide that customers see.*

Also, the screen shots are not included in the wizard deliverable; they are included here for reference only. Please tell me if a wizard panel has been updated.

About the Disk Pool Configuration Wizard

Figure 7-1 [Writer's reference only]



Use the **Disk Pool Configuration Wizard** to create pools of disk volumes for backups by one or more media servers.

The wizard action depends on the NetBackup disk type, as follows:

AdvanceDisk

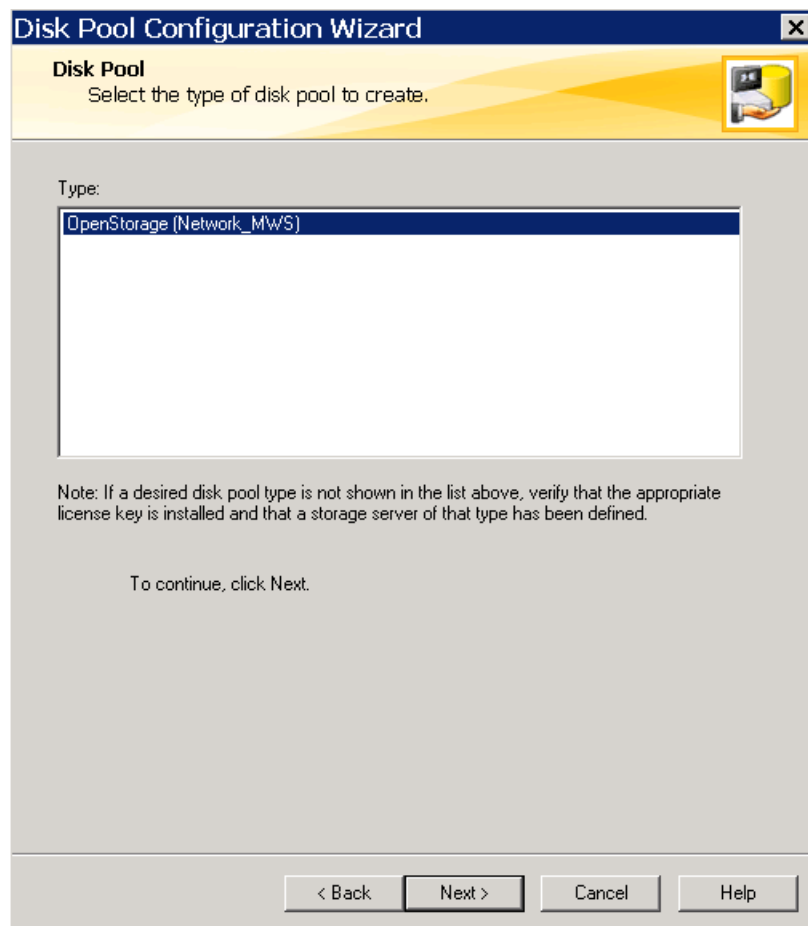
The wizard discovers the disk volumes that are attached to a NetBackup media server. (Attached means a file system mount on the storage.)

Use this wizard for AdvancedDisk

Cloud Storage	<p>The wizard discovers the disk volumes that are exposed to NetBackup by the vendor's host. The host is configured as a storage server in NetBackup.</p> <p>See “About cloud storage disk pools” on page 52.</p> <p>See “Configuring a disk pool for cloud storage” on page 52.</p>
OpenStorage (AdvancedDisk_crypt)	<p>For this type of disk pool, you must use the <code>nbdevconfig</code> command to configure disk pools.</p>
OpenStorage	<p>The wizard discovers the disk volumes that are used for the following purposes:</p> <ul style="list-style-type: none">■ For backups to NetBackup SureScale storage.■ For backups to disk appliance storage.■ For snapshots to disk appliance storage using the NetBackup Replication Director.
PureDisk	<p>The wizard discovers the storage for one of the following disk pool types:</p> <ul style="list-style-type: none">■ A Media Server Deduplication Pool on the disk storage that is attached to a NetBackup deduplication media server.■ A PureDisk Deduplication Pool, which represents a PureDisk storage pool.

Disk Pool panel

Figure 7-2 [Writer's reference only]



Select the type of disk pool to create from the following types. A disk pool type is available only if a storage server of that type exists.

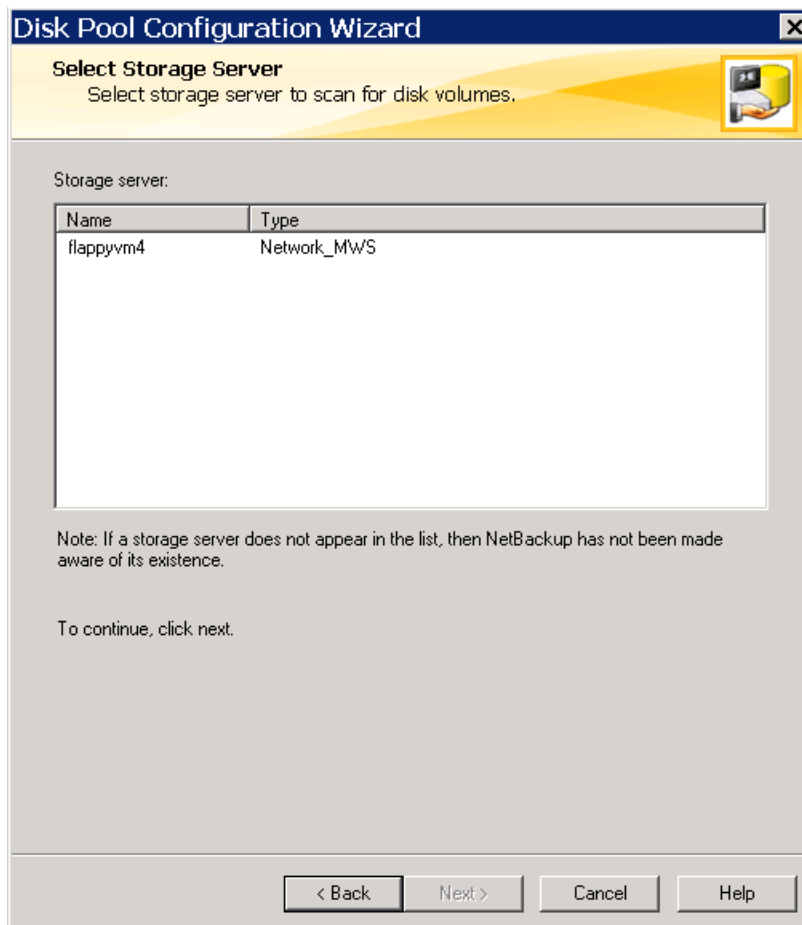
AdvancedDisk

Select this option to create a disk pool on the disk storage that is attached to a NetBackup media server. (Attached means a file system mount on the storage.)

Cloud Storage (Solution)	<p>Select this option for backups to cloud storage. <i>Solution</i> represents the string that identifies your cloud storage provider. If you configured the storage server for encryption, _crypt is appended to the string.</p> <p>The wizard discovers the disk volumes that are exposed to NetBackup by the vendor's host. The host is configured as a storage server in NetBackup.</p> <p>See “About cloud storage disk pools” on page 52.</p> <p>See “Configuring a disk pool for cloud storage” on page 52.</p>
OpenStorage (AdvancedDisk_crypt)	<p>For an AdvancedDisk disk pool with encryption, you must use the <code>nbdevconfig</code> command to configure the disk pool.</p>
OpenStorage (Solution)	<p>Select the OpenStorage (Solution) type for disk pools for backups or snapshots to disk appliance storage.</p> <p><i>Solution</i> represents one of the following strings:</p> <ul style="list-style-type: none">■ For backups, the vendor provides the string for <i>Solution</i>. The string may represent the vendor, the vendor device, or something else that is meaningful.■ For the snapshots that use the NetBackup Replication Director, the string is the Network_ prefix and a string that identifies the vendor, such as NTAP.■ For NetBackup SureScale storage, select one of the following:<ul style="list-style-type: none">■ For non-encrypted storage, select the Type that includes SureScale or SureScale_crypt.■ For encrypted storage, select the Type that includes SureScale_crypt.
PureDisk	<p>Select this option to create one of the following disk pool types:</p> <ul style="list-style-type: none">■ A Media Server Deduplication Pool on the disk storage that is attached to a NetBackup deduplication media server.■ A PureDisk Deduplication Pool, which represents a PureDisk storage pool.

Select Storage Server panel

Figure 7-3 [Writer's reference only]



You configured the storage server earlier in the configuration process.

What you select for the storage server depends on the disk type, as follows:

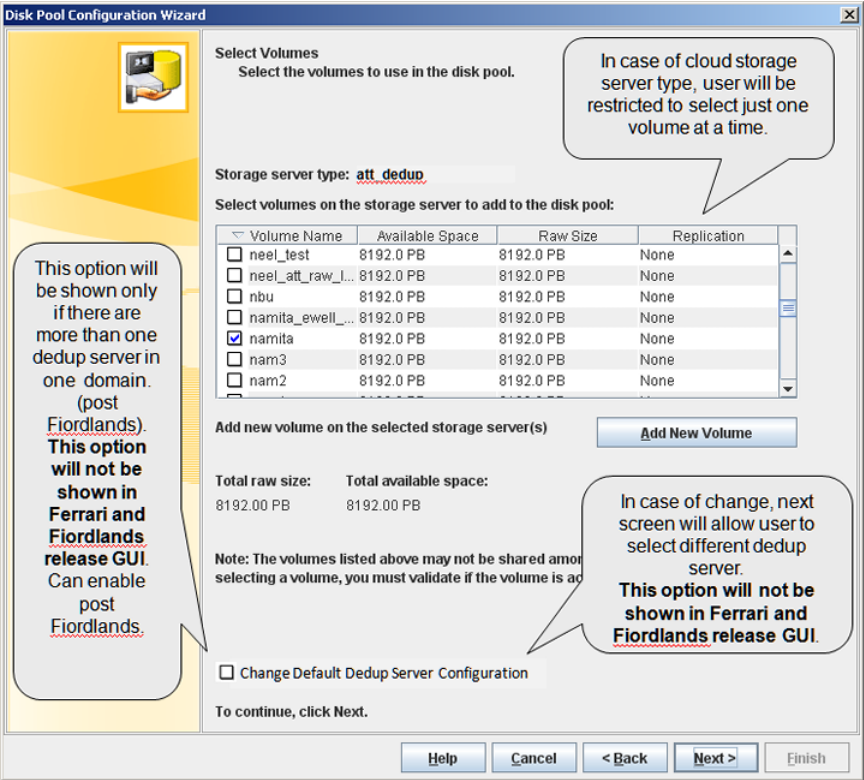
AdvancedDisk

Select the media server or media servers that have a file system mount on the storage. The NetBackup media servers function as both storage servers and data movers.

Cloud Storage	<p>For backups to cloud storage, select the cloud storage vendor's host that functions as the storage server.</p> <p>See “About cloud storage servers” on page 41.</p>
OpenStorage	<p>For backups to disk appliance storage, the disk appliance host is the storage server.</p> <p>See “About cloud storage servers” on page 41.</p>
PureDisk	<p>Select the storage server for the Media Server Deduplication Pool or PureDisk Deduplication Pool storage.</p>
Replication Director	<p>For snapshots that use the NetBackup Replication Director with NetApp, the DFM server is the storage server.</p>
SureScale	<p>The host that you select depends on the storage type, as follows:</p> <p>For a NetBackup 5230 appliance storage, select the NetBackup appliance that hosts the storage.</p> <p>For a NetBackup 5400 appliance, select the virtual host name of the appliance. On the 5400 appliance, the virtual host name is also known as the Media Server Group Director Network Name.</p>

Select Volumes panel

Figure 7-4 [Writer's reference only]



Select the disk volume or disk volumes to include in the disk pool.

NetBackup requires exclusive use of the disk resources. If the volumes are used for purposes other than backups, NetBackup cannot manage disk pool capacity or manage storage lifecycle policies correctly. Therefore, NetBackup must be the only entity that uses the volumes.

See the following for the information that can help you select the disk pool volumes:

AdvancedDisk	<p>The wizard panel displays the volumes available on the storage server. If you selected more than one storage server, volumes that are common to all of them appear.</p> <p>File system requirements or limitations may affect the volumes that you choose for the disk pool.</p>
Cloud Storage	<p>Cloud storage includes SureScale storage on supported cloud storage vendor hosts.</p> <p>The wizard panel displays the volumes that the cloud storage server exposes to NetBackup. The storage server is a vendor's host. You can select only one volume.</p> <p>If you select a volume on a storage destination that requires encryption, a dialog box appears in which you must enter the encryption passphrase.</p> <p>If no volumes are available, click Add New Volume</p> <p>Information about the requirements for volume names is available in the following topics:</p> <p>See “About the Amazon Simple Storage Service (S3) requirements” on page 19.</p> <p>See “About AT&T Synaptic requirements” on page 21.</p> <p>See “About the Nirvanix Cloud Storage Network requirements” on page 22.</p> <p>See “About Rackspace Cloud Files requirements” on page 25.</p>
PureDisk	<p>For a PureDisk type of disk pool, all disk storage is exposed as a single volume. The PureDiskVolume is a virtual name for the entire storage that is dedicated to the deduplicated backups.</p> <p>PureDisk is the type for the following disk pools:</p> <ul style="list-style-type: none">■ A Media Server Deduplication Pool on the disk storage that is attached to a NetBackup deduplication media server.■ A PureDisk Deduplication Pool, which represents a PureDisk storage pool.

See [“About cloud storage disk pools”](#) on page 52.

Create Buckets for Amazon dialog box

The following table describes the **Create Buckets** dialog box options. Be sure to review and follow the restrictions for volume names.

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.

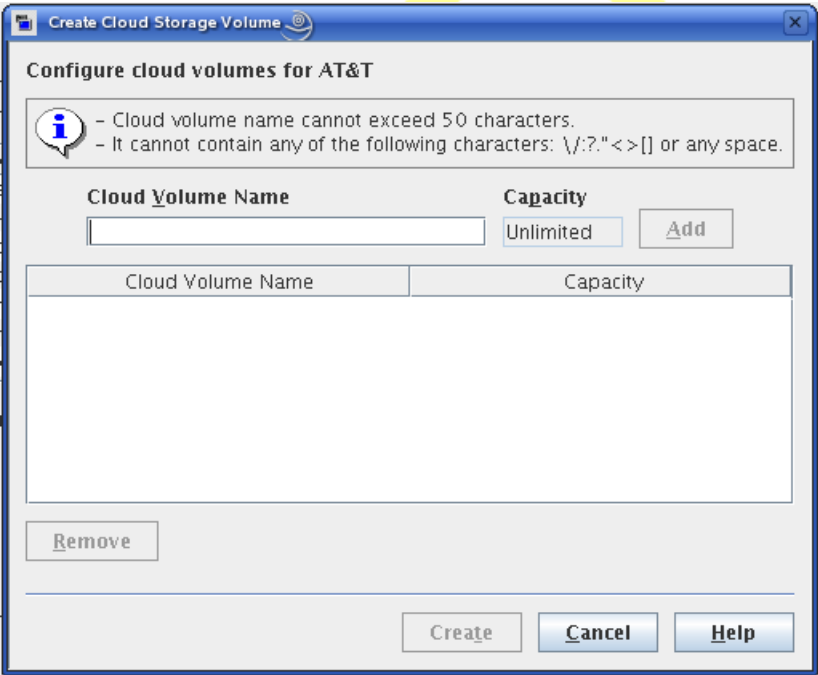
- Bucket Name**
- The name to use for the volume.
- Add**
- Click **Add** to add the volume.
- Remove**
- Select a volume and then click **Remove**

When finished, click **Create** to configure the volume on the storage and return to the **Select Volumes** wizard panel.

See [“Configuring a disk pool for cloud storage”](#) on page 52.

Create Cloud Storage Volume for AT&T dialog box

Figure 7-5 Writer reference only; does not appear in any deliverable



The following table describes the **Create Cloud Storage Volume** dialog box options. Be sure to review and follow the restrictions for volume names.

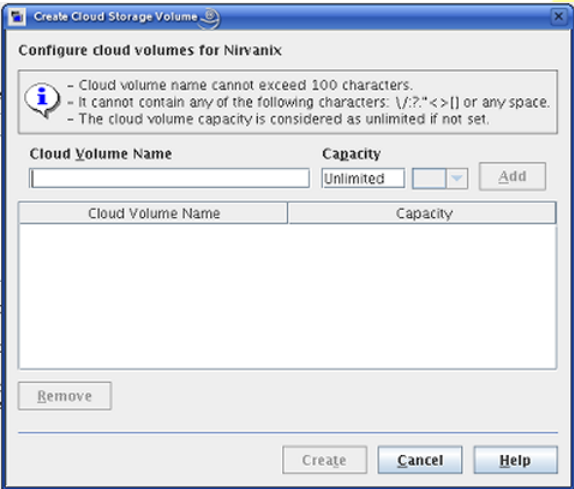
Cloud Volume Name	The name to use for the volume.
Add	Click Add to add the volume.
Remove	Select a volume and then click Remove

When finished, click **Create** to configure the volume on the storage and return to the **Select Volumes** wizard panel.

See [“Configuring a disk pool for cloud storage”](#) on page 52.

Create Cloud Storage Volume for Nirvanix dialog box

Figure 7-6 Writer reference only; does not appear in any deliverable



The following table describes the **Create Cloud Storage Volume** dialog box options. Be sure to review and follow the restrictions for volume names.

Cloud Volume Name	The name to use for the volume. The name you enter becomes a child account to the application name that you entered when you configured the storage server.
Capacity	Enter or change the capacity of the storage and then selected the unit of measure.
Add	Click Add to add the volume.
Remove	Select a volume and then click Remove

When finished, click **Create** to configure the volume on the storage and return to the **Select Volumes** wizard panel.

See [“Configuring a disk pool for cloud storage”](#) on page 52.

Create Cloud Storage Volume for Rackspace dialog box

The following table describes the **Create Cloud Storage Volume** dialog box options. Be sure to review and follow the restrictions for volume names.

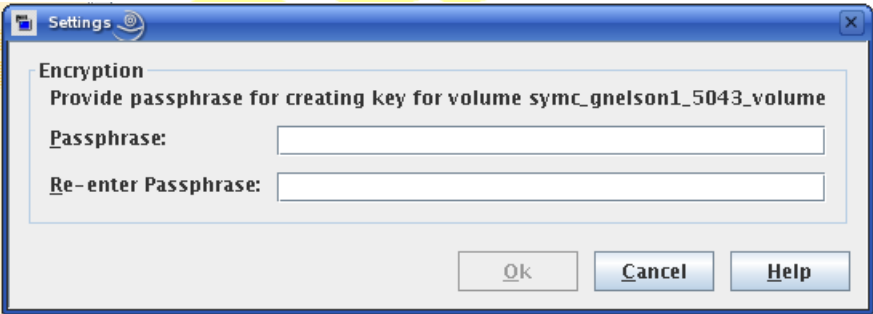
Cloud Storage Volume Name	The name to use for the volume.
Add	Click Add to add the volume.
Remove	Select a volume and then click Remove

When finished, **Create** to configure the volume on the storage and return to the **Select Volumes** wizard panel.

See [“Configuring a disk pool for cloud storage”](#) on page 52.

Settings dialog box

Figure 7-7 Image for review only; it does not appear in the help.



The **Settings dialog box** appears if you selected a disk volume in a storage destination that requires encryption. Encryption is configured in a different wizard.

See [“Specifying Encryption Settings panel”](#) on page 118.

Enter the encryption passphrase for the storage destination, then click **OK** to return to the **Select Volumes** panel.

Disk Pool Properties panel

Figure 7-8 [Writer's reference only]

Disk Pool Properties
Provide additional details and verify the information to create a disk pool

Storage server: daytonvm5
Storage server type: Network_MWS
Disk pool configured for: Snapshot

Disk Pool Size:
Total raw size: 74.42 GB
Total available space: 52.07 GB

Disk Pool name:

Comments:

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

To begin, click Next. For assistance, click Help.

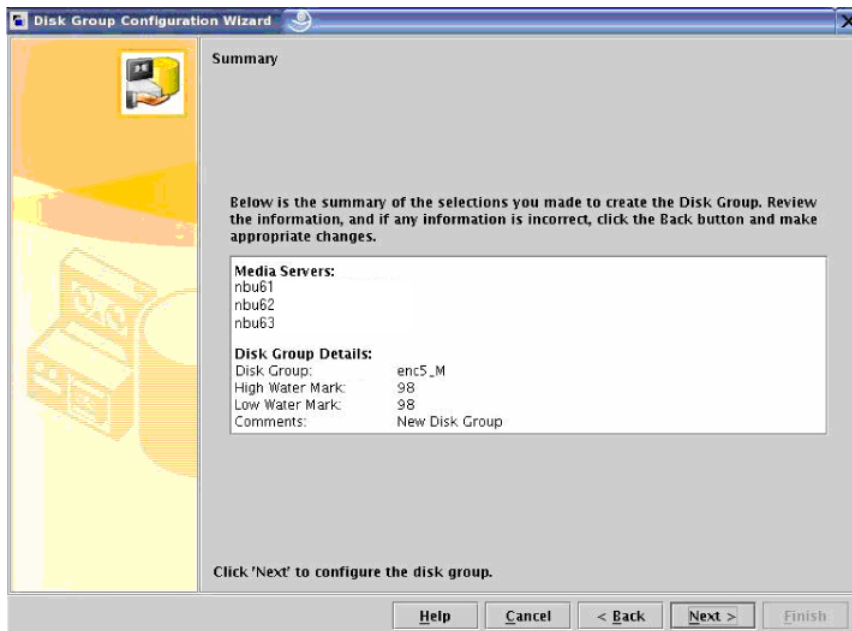
Help Cancel < Back Next > Finish

This wizard panel displays the existing properties for the disk pool. Use this panel to configure the remaining disk pool properties. The properties that you can configure depend on the disk pool type.

See [“Cloud storage disk pool properties”](#) on page 85.

Summary panel

Figure 7-9 [Writer's reference only]



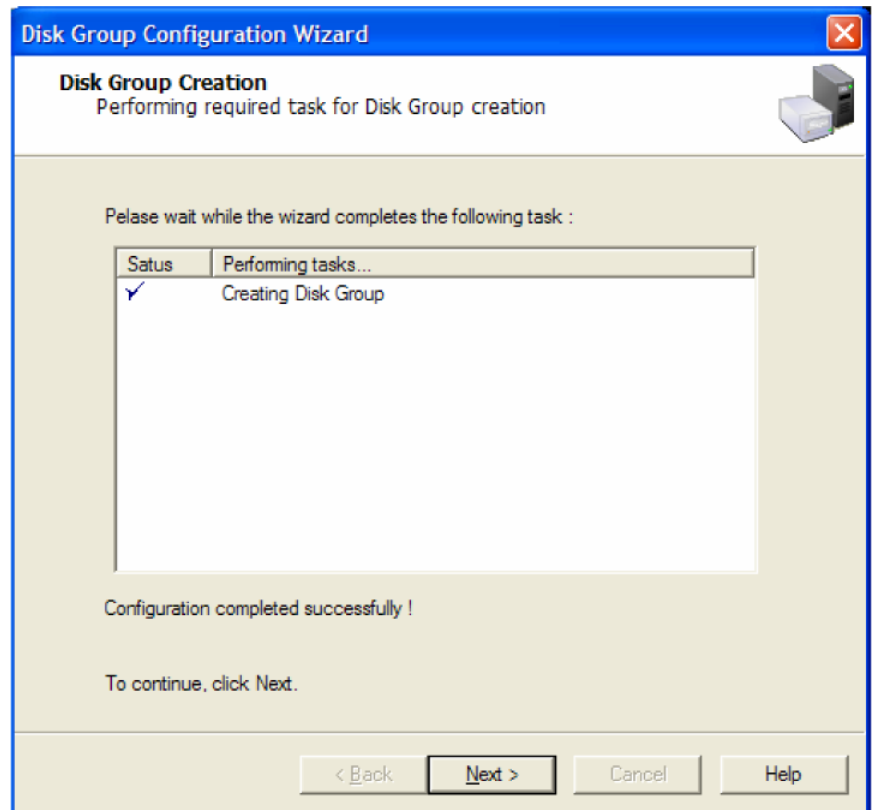
The Summary panel shows your selections to create the NetBackup disk pool.

Click **Back** to return and change the selection.

Click **Next** to create the NetBackup disk pool.

Confirmation panel

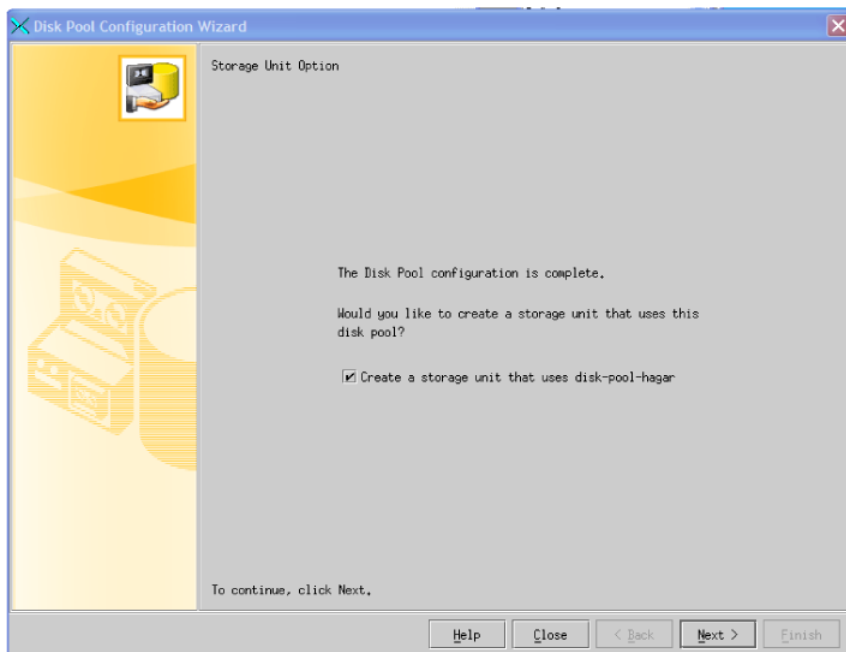
Figure 7-10 [Writer's reference only]



After the wizard creates the disk pool, click **Next** to continue.

Storage Unit Option panel

Figure 7-11 [Writer's reference only]



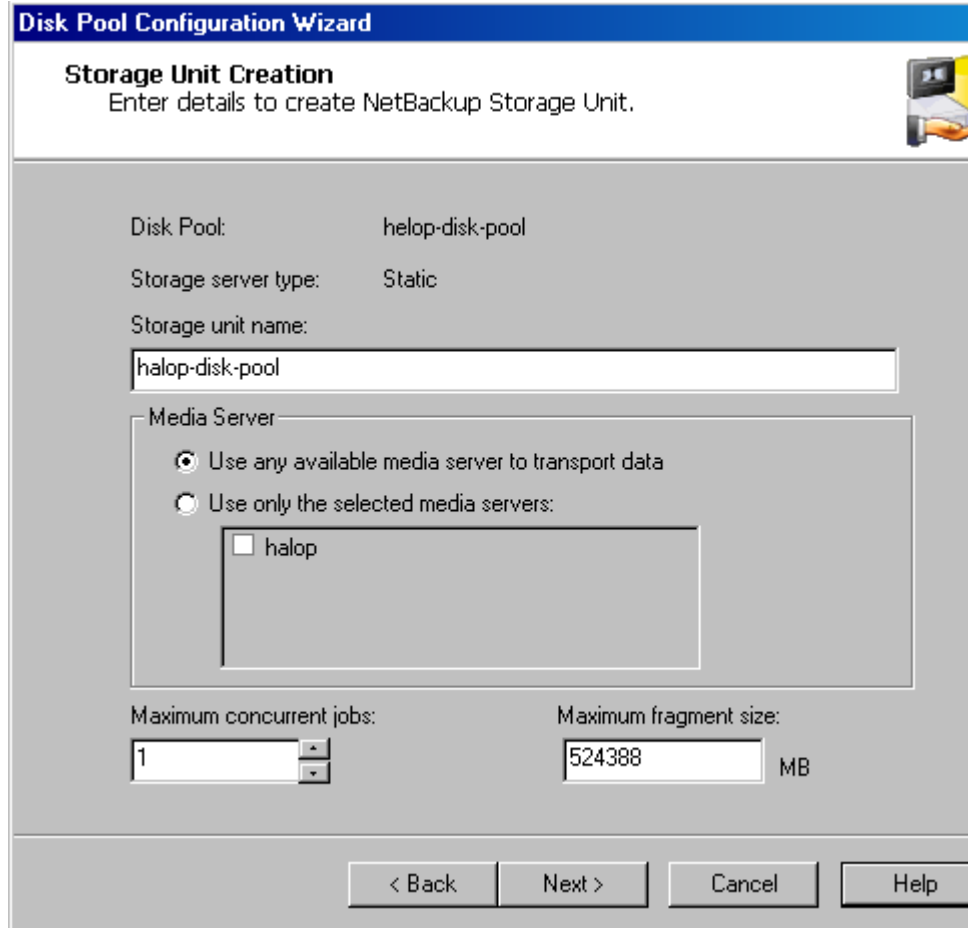
To create a storage unit that uses the disk pool, select **Create a storage unit that uses *diskpoolname***, and then click **Next**.

The wizard creates only one storage unit that uses the disk pool. However, more than one storage unit can use a disk pool. To create other storage units that use the disk pool, use **NetBackup Management > Storage** in the **NetBackup Administration Console**.

To exit the wizard, click **Close**. If you exit, you can create a storage unit later.

Create Storage Unit panel

Figure 7-12 [Writer's reference only]



The screenshot shows the 'Storage Unit Creation' panel of the 'Disk Pool Configuration Wizard'. The panel has a title bar with the wizard's name. Below the title bar, the section is titled 'Storage Unit Creation' with the instruction 'Enter details to create NetBackup Storage Unit.' and a small icon of a server. The main area contains several fields and options: 'Disk Pool' is set to 'helop-disk-pool'; 'Storage server type' is set to 'Static'; 'Storage unit name' is a text box containing 'halop-disk-pool'; 'Media Server' is a section with two radio buttons: 'Use any available media server to transport data' (selected) and 'Use only the selected media servers:' (unselected). Below the second radio button is a list box containing 'halop' with an unchecked checkbox. At the bottom, 'Maximum concurrent jobs' is a spinner box set to '1', and 'Maximum fragment size' is a text box set to '524388' with 'MB' next to it. At the very bottom are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

Disk Pool Configuration Wizard

Storage Unit Creation
Enter details to create NetBackup Storage Unit.

Disk Pool: helop-disk-pool

Storage server type: Static

Storage unit name:
halop-disk-pool

Media Server

☒ Use any available media server to transport data

☐ Use only the selected media servers:

☐ halop

Maximum concurrent jobs: 1

Maximum fragment size: 524388 MB

< Back Next > Cancel Help

Specify the storage unit properties.

See [“Cloud storage unit properties”](#) on page 74.

Finish panel

Click **Finish** to exit the wizard.

DRAFT

Index

C

- cloud
 - storage unit properties 74
- cloud disk pool
 - changing properties 83
- Cloud Settings tab 27
- cloud storage
 - configuring 16
- cloud storage provider
 - Amazon 19
- cloud storage server
 - changing properties 70
 - properties 59
- Configuration
 - Accelerator 78
 - Amazon 112
 - AT&T 113
 - encryption 118
 - Rackspace 115
 - wizard 110
- configuration
 - disk pool configuration wizard 52
 - Nirvanix 114
 - optimized synthetic backups for cloud storage 80
- configuring a deduplication storage unit 73
- configuring cloud storage 16

D

- data classifications
 - use of Any 88
- Deduplication storage unit
 - Only use the following media servers 75
 - Use any available media server 75
- Disk type 75

F

- Features and functionality 11

FlashBackup policy

- Maximum fragment size (storage unit setting) 76

J

- job ID search in unified logs 94

L

- legacy logging 94
 - directories 95
 - locations 94
- logging
 - see legacy logging 94

M

- Maximum concurrent jobs 76
- Maximum fragment size 76
- mklogdir.bat 95
- Monitoring 87

N

- NetBackup Accelerator
 - about 77
- NetBackup CloudStore Service Container
 - about 32
- NetBackup Scalable Storage 29–30

O

- Optimized Synthetic backups
 - about 77

P

- policies
 - changing properties 82
 - creating 82
- Preferences
 - common 60
 - encryption 67
 - Nirvanix specific 68

Preferences (*continued*)

- throttling 63
- properties
 - cloud storage server 59

write buffer size

- about 63

R

- read buffer size
 - about 62
- Reporting 87
- reqlib directory 95
- requirements 18

S

- Scalable Storage host properties 26, 29–30
 - Cloud Settings tab 27
- Scalable Storage, NetBackup 29–30
- server
 - NetBackup debug logs 95
- Status Collection Daemon 95
- Storage provider
 - Nirvanix 22
- storage provider
 - AT&T 21
 - Nirvanix 22
 - Rackspace 25
- storage server
 - about cloud 41
 - changing properties for cloud 70
- storage unit
 - configuring for deduplication 73
 - properties for cloud 74
- Storage unit name 75
- Storage unit type 75

U

- unified logging 91
 - format of files 93
 - location 91

V

- vmscd 95
- vxlogview command 92
 - with job ID option 94

W

- wizards
 - Policy Configuration 82