

Veritas Access Solutions Guide for NetBackup

7.4.2 Linux

Veritas Access Solutions Guide for NetBackup

Last updated: 2020-10-01

Document version: 7.4.2 Rev 5

Legal Notice

Copyright © 2018 Veritas Technologies LLC. All rights reserved.

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

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

<https://www.veritas.com/licensing/process>

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

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

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

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

<http://www.veritas.com>

Technical Support

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

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

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

<https://my.veritas.com>

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

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

Documentation

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

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

Documentation feedback

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

accessdocs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 1	Veritas Access integration with NetBackup	7
	About Veritas Access	7
	About Veritas Access as a NetBackup client	7
	About Veritas Access as backup storage for NetBackup	9
	Use cases for long-term data retention	9
Chapter 2	System requirements	13
	Supported configurations and versions for NetBackup with Veritas Data Deduplication	13
	System requirements for OpenDedup installation	13
	Supported configurations and versions for NetBackup with OpenDedup	14
	Supported configurations and versions for NetBackup with CloudCatalyst	14
Chapter 3	Configuring Veritas Data Deduplication with Veritas Access	16
	About Veritas Data Deduplication	16
	Add-on license for using Veritas Data Deduplication	17
	Benefits of using Veritas Data Deduplication with Veritas Access	18
	Configuring Veritas Data Deduplication using the GUI	19
	Configuring Veritas Data Deduplication using the Veritas Access command-line interface (CLI)	22
	Configuring a Veritas Data Deduplication storage unit on NetBackup	26
	Configuring global deduplication using the Veritas Data Deduplication storage server across the domain	40
Chapter 4	Migrating the NetBackup images from existing storage to Veritas Data Deduplication storage 	42
	Migrating the NetBackup image from OpenDedup/CloudCatalyst/S3 to Veritas Data Deduplication storage	42

Chapter 5	Configuring Veritas Access backup over S3 with OpenDedup and NetBackup	47
	Workflow for OpenDedup	47
	Backing up deduplicated data (OpenDedup and NetBackup) using the S3 protocol to Veritas Access	48
	Backing up data (NetBackup) and deduplicating the data (OpenDedup) on Veritas Access	49
	Creating an S3 bucket on Veritas Access for storing deduplicated backup data from NetBackup	50
	Creating a Media Server Deduplication Pool (MSDP) for primary backup using NetBackup	56
	Creating an OST disk pool and STU in the NetBackup console	64
	Setting up multiple NetBackup media servers in the same domain	72
	Setting up multiple SDFS volumes on a NetBackup media server	73
Chapter 6	Configuring Veritas Access as a cloud storage server with NetBackup CloudCatalyst	77
	Creating an S3 bucket on Veritas Access for storing deduplicated backup data from NetBackup	78
	Configure Veritas Access as a cloud storage server on NetBackup server using CloudCatalyst	80
	Enabling SSL on Veritas Access	97
Chapter 7	Configuring backup and restore using NetBackup policies	101
	Storage Lifecycle Policies	101
	Backup and restore	107
	Running a backup policy manually	114
	Restoring backed up files	120
Chapter 8	Configuring Veritas Access with the NetBackup client	123
	Prerequisites for configuring the NetBackup client	124
	About the NetBackup Snapshot Client	124
	About NetBackup snapshot methods	124
	Enabling or disabling the NetBackup SAN client	125
	Workflow for configuring Veritas Access for NetBackup	125
	Registering a NetBackup master server or adding an optional media server	126

Displaying the excluded files from backup	128
Displaying the included and excluded files for backups	128
Adding or deleting patterns to the list of files in backups	129
Configuring or resetting the virtual IP address used by NetBackup	130
Configuring the virtual name of NetBackup	130
Displaying the status of NetBackup services	131
Configuring backup operations using NetBackup or other third-party backup applications	132
Performing a backup or restore of a Veritas Access file system over a NetBackup SAN client	133
Performing a backup or restore of a snapshot	134
Installing or uninstalling the NetBackup client	134
Configuring Veritas Access for NetBackup cloud storage	138
Chapter 9 Troubleshooting	141
Unmounting the SDFS volume before restarting Veritas Access or the NetBackup media server	141
Upgrading SDFS from earlier versions to 7.4.2	142
Log locations for troubleshooting	143
Changing log levels	144
Additional resources	144
Generating Veritas Access S3 server keys using the helper script	145
OpenDedup tuning recommendations	146
Index	148

Veritas Access integration with NetBackup

This chapter includes the following topics:

- [About Veritas Access](#)
- [About Veritas Access as a NetBackup client](#)
- [About Veritas Access as backup storage for NetBackup](#)
- [Use cases for long-term data retention](#)

About Veritas Access

Veritas Access is a software-defined scale-out network-attached storage (NAS) solution for unstructured data that works on commodity hardware. Veritas Access provides resiliency, multi-protocol access, and data movement to and from the public and private cloud based on policies. You can reduce your storage costs by using low-cost disks and by storing infrequently accessed data in the cloud.

About Veritas Access as a NetBackup client

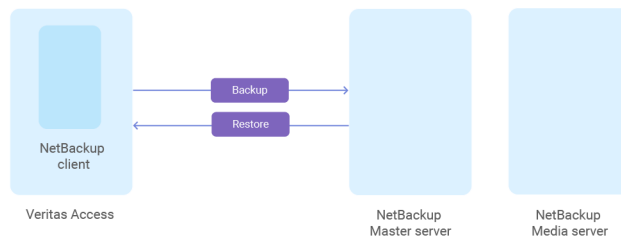
Veritas Access is integrated with Veritas NetBackup so that a NetBackup administrator can back up your Veritas Access file systems to NetBackup master or media servers and retain the data as per your company policy. Once data is backed up, a storage administrator can delete unwanted data from Veritas Access. The NetBackup master and media servers that run on separate computers from Veritas Access are licensed separately from Veritas Access.

You configure NetBackup domain information using any one of the following interfaces:

- Command-line interface (CLI)
The Veritas Access command-line interface has a dedicated `Backup>` menu. From the `Backup>` menu, register the NetBackup client with the NetBackup domain. Information is saved in the `bp.conf` file.
- GUI
Settings > NetBackup Configuration
See the Online Help for how to configure NetBackup using the GUI.
- RESTful APIs
See the *Veritas Access RESTful API Guide*.

Consolidating storage reduces the administrative overhead of backing up and restoring many separate file systems. Critical file data can be backed up and restored through the NetBackup client on Veritas Access.

Figure 1-1 Backing up Veritas Access using NetBackup



If Veritas Access is configured with IPv6 addresses, you have to configure IPv6 support for the NetBackup host as well.

Perform the following steps to configure IPv6 support for the NetBackup host :

- Set the `IP_ADDRESS_FAMILY` option in the NetBackup `bp.conf` file for the host to `AF_UNSPEC`.

```
# bpsetconfig IP_ADDRESS_FAMILY = AF_UNSPEC
```
- You can view the current setting by executing the `bpgetconfig` command.

```
# bpgetconfig  
IP_ADDRESS_FAMILY = AF_UNSPEC
```
- Restart the services after making this change.

About Veritas Access as backup storage for NetBackup

This document describes how Veritas Access fulfills the needs of NetBackup customers looking for a cost-effective solution for moving away from tape backups, yet retain the backed-up data for the long term.

NetBackup is an enterprise-class heterogeneous backup and recovery application. It provides cross-platform backup functionality to a large variety of Windows, UNIX, and Linux operating systems.

Veritas Access is based on the rock-solid and industry-proven Veritas CFS stack. It offers an AWS-compatible S3 protocol as object storage for NetBackup.

Veritas Access is integrated with OpenDedup. OpenDedup is OpenSource software that lets you deduplicate your data to on-premises or cloud storage. OpenDedup installs on top of a NetBackup media server or Veritas Access; it performs data deduplication and stores deduplicated data on Veritas Access over S3.

Use cases for long-term data retention

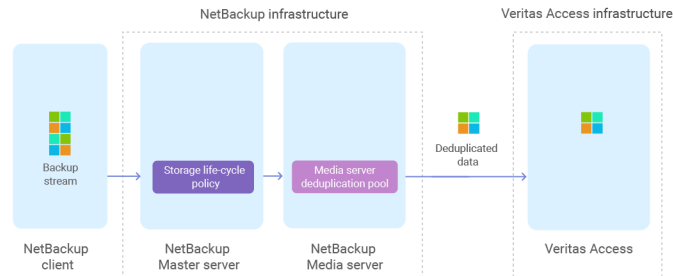
The following are the use cases for long-term data retention (LTR) using Veritas Access:

Use Case: Veritas Access with Veritas Data Deduplication

- Veritas Data Deduplication technology is installed on top of Veritas Access and integrates with NetBackup. It catalogs and organizes incoming deduplicated backup data and stores it on Veritas Access storage.
- Primary backup data is deduplicated by MSDP and stored on the NetBackup server
- The same deduplicated data is sent to Veritas Access for long term retention purpose using SLPs through duplication jobs.

See [“Configuring a Veritas Data Deduplication storage unit on NetBackup”](#) on page 26.

Figure 1-2 Veritas Access with Veritas Data Deduplication

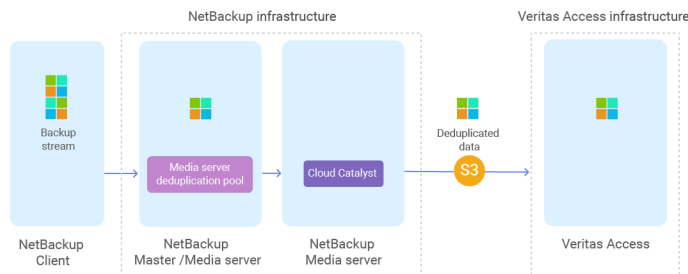


Use Case: Veritas Access with CloudCatalyst

- Primary backup data is deduplicated by MSDP and stored on the NetBackup server.
- The same deduplicated data is moved to Veritas Access through SLP using CloudCatalyst.

See [“Configure Veritas Access as a cloud storage server on NetBackup server using CloudCatalyst”](#) on page 80.

Figure 1-3 Primary backup data deduplicated by MSDP and stored on the NetBackup server



Use Case: Veritas Access as an S3 connector

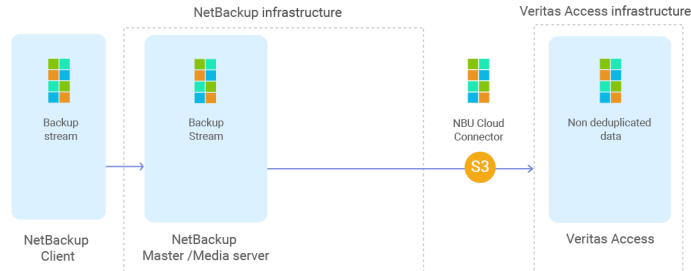
- Backup data is stored in non-deduplicated format on the NetBackup server as primary backup. The same primary backup data is moved to Veritas Access through SLP over the Veritas Access S3 protocol.

Or

- Primary backup data is deduplicated by MSDP and stored on the NetBackup server. The deduplicated data is rehydrated and then moved to Veritas Access through SLP over the Veritas Access S3 protocol.

See [“Creating an S3 bucket on Veritas Access for storing deduplicated backup data from NetBackup”](#) on page 78.

Figure 1-4 Backup data stored in non-deduplicated format on the NetBackup server as primary backup

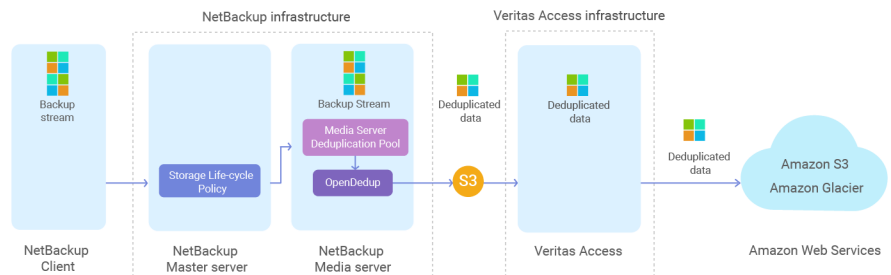


Use Case: OpenStorage Technology (OST) and OpenDedup hosted on a NetBackup master and/or media server

- OST and OpenDedup hosted on a NetBackup master and/or media server sends deduplicated backup data to Veritas Access over the S3 protocol. Veritas Access can move this data to supported public or private clouds, based on the LTR policy configured.

See [“Backing up deduplicated data \(OpenDedup and NetBackup\) using the S3 protocol to Veritas Access”](#) on page 48.

Figure 1-5 OST and OpenDedup hosted on a NetBackup master and/or media server

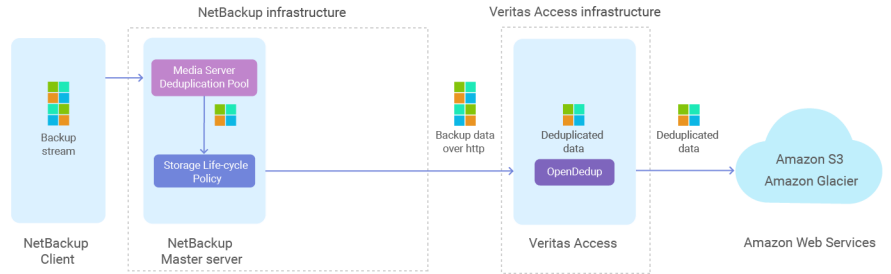


Use Case: OST hosted on a NetBackup master and/or media server

- OST hosted on a NetBackup master and/or media server sends backup data to OpenDedup hosted on Veritas Access, which deduplicates the data and sends this data over the S3 protocol to Veritas Access. Veritas Access moves this deduplicated data to AWS S3 or Glacier.

See “Backing up data (NetBackup) and deduplicating the data (OpenDedup) on Veritas Access” on page 49.

Figure 1-6 OST hosted on a NetBackup master and/or media server



System requirements

This chapter includes the following topics:

- [Supported configurations and versions for NetBackup with Veritas Data Deduplication](#)
- [System requirements for OpenDedup installation](#)
- [Supported configurations and versions for NetBackup with OpenDedup](#)
- [Supported configurations and versions for NetBackup with CloudCatalyst](#)

Supported configurations and versions for NetBackup with Veritas Data Deduplication

Table 2-1 Supported versions

Veritas Access	Veritas NetBackup servers
7.4.2	8.1.1 and later versions (Linux only)

System requirements for OpenDedup installation

The system requirements for OpenDedup installation are:

- 64GB of base memory + 256MB RAM per TB of unique storage
- 200 MB/s local disk speed
- 2K IOPS of disk (local or attached) for the `/opt` directory
- 0.2 % of local disk of logical storage

- 0.2% of local disk storage of unique data
- Expected performance of the system based on the above parameters:
- 120 MB/s per CPU core

Supported configurations and versions for NetBackup with OpenDedup

Table 2-2 Supported versions

OpenDedup	Veritas Access	Veritas NetBackup servers	OST
7.4.2	7.4.2	7.7.3, 8.0, 8.1, 8.1.1 (Linux only)	2.2.9

Download links:

Veritas Access: Veritas Access 7.4.2 DVD

OpenDedup:

https://sort.veritas.com/public/patchcentral/Linux/7.4/access/access-rhel7_x86_64-7.4.2sdfs.tar.gz

OpenStorage Technology (OST):

https://sort.veritas.com/public/patchcentral/Linux/7.4/access/access-rhel7_x86_64-7.4.2ost.tar.gz

Supported configurations and versions for NetBackup with CloudCatalyst

Table 2-3 Supported versions

Veritas Access	Veritas NetBackup servers
7.4.2	8.1, 8.1.1 (Linux only)

Download links:

Veritas Access: Veritas Access 7.4.2 DVD

Cloudprovider.xml version 2.3.1 supports Veritas Access.

https://www.veritas.com/support/en_US/article.000125094

Update the mappings file.

Unix/Linux: <http://www.veritas.com/docs/000025759>

Note: If you want to configure CloudCatalyst, it needs to be recognized by the master server. You have to prepare the CloudCatalyst and media servers with NetBackup certificates. See the *NetBackup documentatio* for more details.

Note: NetBackup 8.1 does not have the Veritas Access S3 cloud provider support. Hence, the Cloud Configuration Package needs to be updated for listing the Veritas Access S3 server in the list of cloud storage providers. The details for updating the Cloud Configuration Package are available at:

https://www.veritas.com/support/en_US/article.000125094

https://www.veritas.com/support/en_US/article.100015983

Configuring Veritas Data Deduplication with Veritas Access

This chapter includes the following topics:

- [About Veritas Data Deduplication](#)
- [Add-on license for using Veritas Data Deduplication](#)
- [Benefits of using Veritas Data Deduplication with Veritas Access](#)
- [Configuring Veritas Data Deduplication using the GUI](#)
- [Configuring Veritas Data Deduplication using the Veritas Access command-line interface \(CLI\)](#)
- [Configuring a Veritas Data Deduplication storage unit on NetBackup](#)
- [Configuring global deduplication using the Veritas Data Deduplication storage server across the domain](#)

About Veritas Data Deduplication

Veritas Access is integrated with a deduplication engine which is based on Media Server Deduplication Pool (MSDP) technology for storing backup data. The storage server component of Veritas Data Deduplication runs on the Veritas Access nodes with high availability in active/passive mode. The deduplication plug-in of the NetBackup media server does segmentation and finger printing of the backup data and sends the deduplicated data to Veritas Access. The Veritas Data Deduplication storage server stores and manages the deduplicated data. The deduplication storage

server provides high availability to protect against storage, node, and network failures. It supports client direct as well as media server deduplication configurations.

All storage that is provisioned for Veritas Data Deduplication is displayed as a single storage pool on NetBackup.

Note: The Veritas Data Deduplication feature is not supported on the Oracle Linux platform.

Note: To use the Veritas Data Deduplication service, you need to get an add-on license. The deduplication functionality is licensed separately and is generated based on your requirement.

See [“Add-on license for using Veritas Data Deduplication”](#) on page 17.

Add-on license for using Veritas Data Deduplication

In addition to the base license, you can also procure an add-on license to use the Veritas Data Deduplication service. The deduplication functionality is licensed separately and is generated based on your requirement. The add-on deduplication license is applied when the base license key is present and is associated with both capacity and time period. The validity of the add-on license may be different from the base license.

The add-on license can also be purchased together with the base Veritas Access license. The new license includes the base license (Per-TB) along with the deduplication license.

If you already have a valid Veritas Access license, and you want to upgrade to Veritas Access 7.4.2, you can procure the add-on deduplication license, or you can purchase the combined license with the Per-TB license along with deduplication.

You can install your license key using the Veritas Access command-line interface or the Veritas Access GUI.

Note: Even if you have installed the add-on deduplication license, the licensing reports display only the base licensing information. All the functionalities are also with respect to the base key only.

If you have installed either the add-on deduplication license or the combined base license with deduplication, you can see the information on the deduplication license

using the following command that displays all the valid licenses installed on your system.

```
/sbin/slic/vxlicrep
```

Benefits of using Veritas Data Deduplication with Veritas Access

- Capability of writing the deduplicated data from the media server to Veritas Access.
- Support global deduplication across media servers within the same domain and across different NetBackup domains.
- The storage server component resides directly on the Veritas Access nodes with high availability in active/passive mode to protect against storage, node, and network failures.

Configuring Veritas Data Deduplication using the GUI

To configure Veritas Data Deduplication

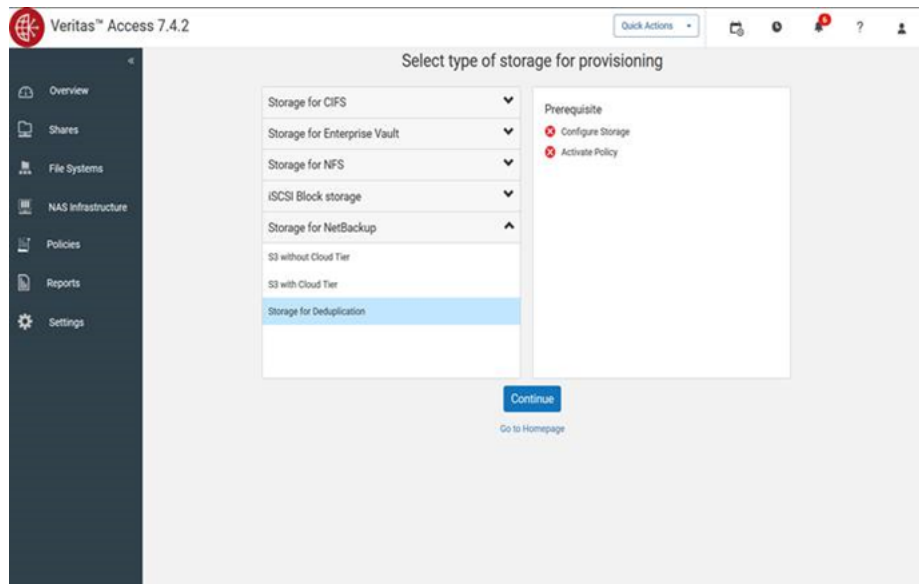
1 Prerequisites:

Configure storage.

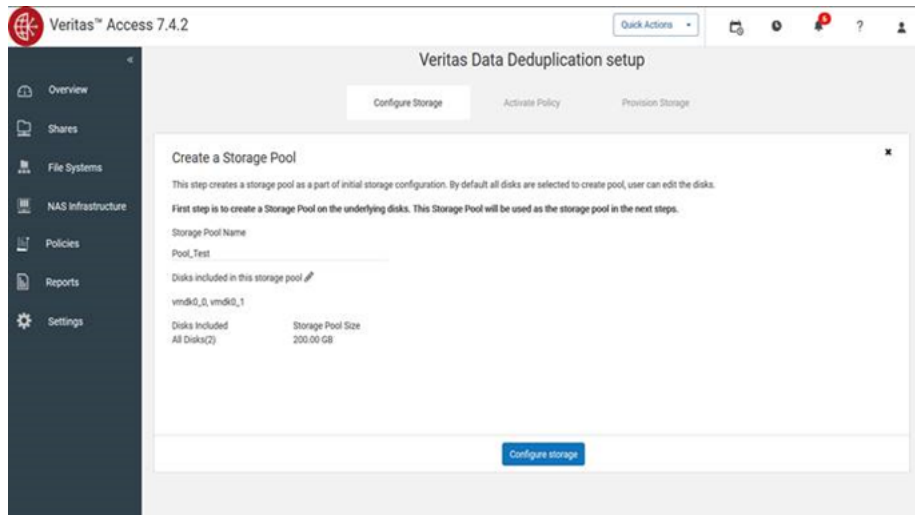
Start the deduplication service.

Activate the Veritas Deduplication policy.

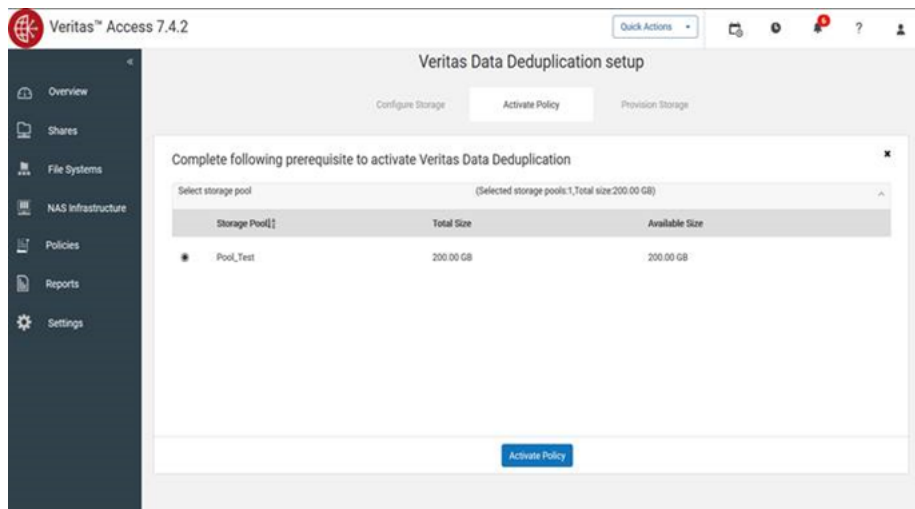
2 Quick Actions: Go to **Provision Storage > Storage for NetBackup > Storage for Deduplication**, and then click **Continue**.



- 3 Click the **Configure Storage** tab and specify the storage options.



- 4 Click the **Activate Policy** tab, select the Veritas Data Deduplication policy, and then click **Activate Policy**.



- 5 Click the **Provision Storage** tab, specify the storage options, enter the user name and password for the service.

You are required to enter the following fields:

- **Size:** Specify the size of the file system.
 Veritas recommends that you grow the deduplication storage pool to a maximum supported size of 960 TiB.
- **Data Protection:** Specify the type of the file system (simple/stripped/mirrored/erasure coded).
- **Virtual IP address:** The virtual IP that you want to use to configure the Veritas Data Deduplication server. This IP should not be the console IP, replication IP, NetBackup client IP, or the loadbalancer IP. If you use any of these IPs to configure deduplication, storage provisioning fails.
 Run the `Network> ipaddress show` command from the Access command-line interface to find an available virtual IP address. Or navigate to **NAS Infrastructure > Nodes** in the Access GUI, and click on the node name to see the virtual IP address.
 If a virtual IP is not available to configure the Veritas Data Deduplication server, you should add at least one virtual IP to the cluster using the Access command-line interface.
- **Username and password:** Credentials with which the Veritas Data Deduplication server gets configured.
 The same credentials are required later to add the Veritas Data Deduplication server to NetBackup.

Click **Provision storage**.

The screenshot shows the Veritas Access 7.4.2 GUI. On the left is a navigation sidebar with options: Overview, Shares, File Systems, NAS Infrastructure, Policies, Reports, and Settings. The main content area is titled 'Veritas Data Deduplication setup' and has three tabs: 'Configure Storage', 'Activate Policy', and 'Provision Storage'. The 'Provision Storage' tab is selected. Inside this tab, there's a form titled 'Veritas Data Deduplication' with the subtitle 'Provision storage for Veritas Data Deduplication'. The form contains the following fields and options:

- Size:** A dropdown menu showing '100' and 'GB'.
- Disk Protection:** A dropdown menu showing 'Simple'.
- VIP (Virtual IP Address):** A text input field containing '10.1.1.1'.
- Define Credentials:**
 - Username:** A text input field containing 'user1'.
 - Password:** A password input field with masked characters.
 - Confirm Password:** A password input field with masked characters.

At the bottom right of the form is a blue button labeled 'Provision storage'. On the right side of the form, there's a 'Define Credentials' sidebar with instructions: 'Enter the user name for the NetBackup Deduplication Engine. The Deduplication components use the credentials when they communicate with NetBackup Deduplication Engine. The credentials are for the engine, not for the host on which it runs.' and 'Confirm Password: To confirm the password, re-enter the password.'

- 6 View the **Recent Activity** panel for the status of the task.
- 7 After storage provisioning is done, click **Finish**.

Configuring Veritas Data Deduplication using the Veritas Access command-line interface (CLI)

This section describes how you can configure Veritas Data Deduplication using the Veritas Access command-line interface.

You can use the `dedupe> config` command to configure the deduplication storage server using the given set of file systems and IP address.

Prerequisites:

- The file system should be already created and the IP should be online before you start deduplication. The file system is used to store the deduplicated data and its metadata. The deduplication storage server uses the specified IP address to receive the backup data from NetBackup.

- Modify the following tunables:

`/sys/kernel/mm/transparent_hugepage/khugepaged/defrag` is set to “0”
`/sys/kernel/mm/transparent_hugepage/defrag` is set to “always madvise [never]”

- Set the following values in the `/etc/sysctl.conf` file:

```
kernel.numa_balancing = 0
vm.overcommit_memory = 2
vm.min_free_kbytes = 2097152
vm.max_map_count = 262144
vm.overcommit_ratio = 90
```

To configure the deduplication storage server

- ◆ To configure the deduplication storage server, enter the following:

```
dedupe> config filesystem1 [, filesystem2,...] IP username
```

Where:

filesystem1,
filesystem2,... Specifies the file system names.

IP Specifies the interface IP.

username Specifies the user name.

You are prompted to enter your password. After you specify your password, Veritas Data Deduplication is configured.

Note: You have to use the same password when you configure the storage server on NetBackup.

Note: If you want to configure deduplication with an IPv6 IP, you are required to have an FQDN entry which resolves to the specific IP. The FQDN should be resolvable on both Veritas Access and NetBackup. You can either have a DNS entry or you can add an entry in the `/etc/hosts` file on all the nodes to resolve the FQDN to a specific IP.

Note: If you have to reconfigure deduplication, you are required to provide the first file system which has the `dedupe` directory inside the `/vx/fcname/` directory using the same user name and password that you used when you initially configured deduplication.

To start the deduplication storage server

- ◆ The storage server is started on the node on which the virtual IP, which you specified in the `dedupe> config` command is online.

To start the deduplication storage server, enter the following:

```
dedupe> start
```

The deduplication storage server should be already configured before you start the deduplication storage server.

To display information the deduplication storage server

- ◆ To display information about the deduplication storage server, enter the following:

```
dedupe> show
```

The information includes the file system(s) being used, the IP, and the cluster node on which the server is running.

To display the deduplication storage server statistics

- ◆ To display the deduplication storage server statistics, enter the following:

```
dedupe> stats
```

The information includes details like total storage size, free storage, and deduplication ratio. The deduplication storage server should be online for this operation.

To show the status of the deduplication storage server

- ◆ To show the status of the deduplication storage server, enter the following:

```
dedupe> status
```

The information includes whether the server is running and the cluster node on which the server is running.

To stop the deduplication storage server

- ◆ To stop the deduplication storage server, enter the following:

```
dedupe> stop
```

The deduplication storage server must be configured and running. If any backup job is running when the server is stopped, the job aborts with an error.

To increase the storage capacity of the deduplication storage server

- ◆ To increase the storage capacity of the deduplication storage server to the given size, enter the following:

```
dedupe> grow size
```

The deduplication storage server should be online for this operation.

To add a new user to the deduplication storage server

- ◆ To add a new user to the deduplication storage server, enter the following:

```
dedupe> adduser username
```

The user name that is mentioned here is the NetBackup media server user name which you use later to configure the storage server on the NetBackup server.

To show the list of users of the deduplication storage server

- ◆ To show the list of users of the deduplication storage server, enter the following:

```
dedupe> listuser
```

To unconfigure the deduplication storage server

- ◆ To unconfigure the deduplication storage server, enter the following:

```
dedupe> unconfig
```

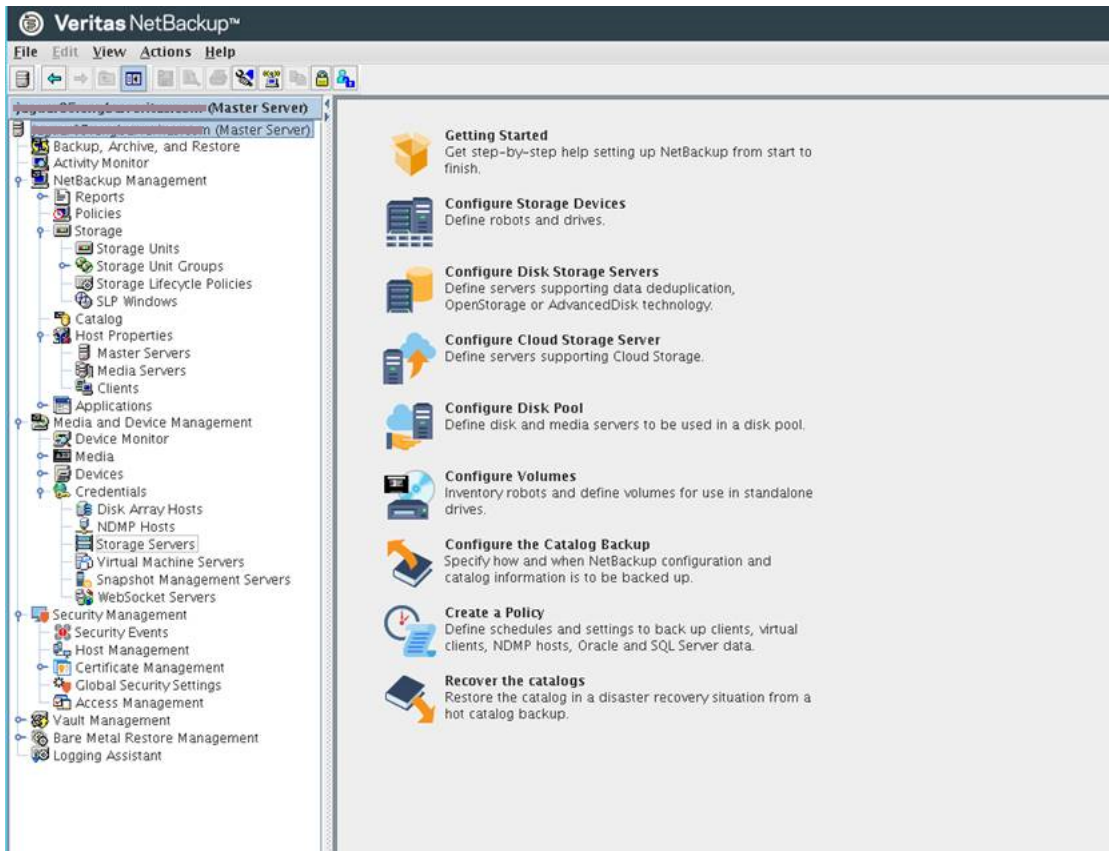
The file system(s) and the deduplicated data stored on it are not destroyed.

See the `dedupe` man page for more information.

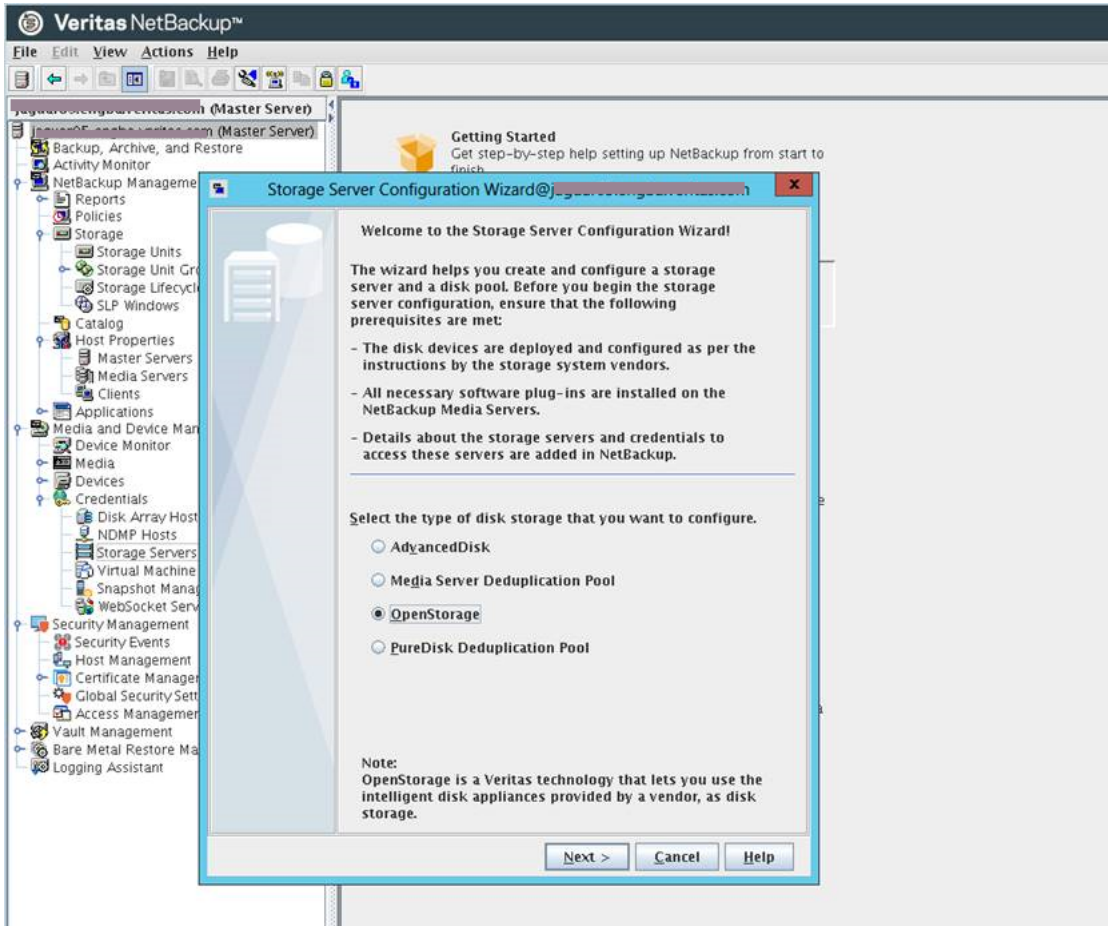
Configuring a Veritas Data Deduplication storage unit on NetBackup

To create a storage server on NetBackup

- 1 Log on to the NetBackup master server from the Java console.
- 2 Select **Configure Disk Storage Servers**.



- 3 The **Welcome to Storage Server Configuration** wizard appears. Select **OpenStorage**. Click **Next**.

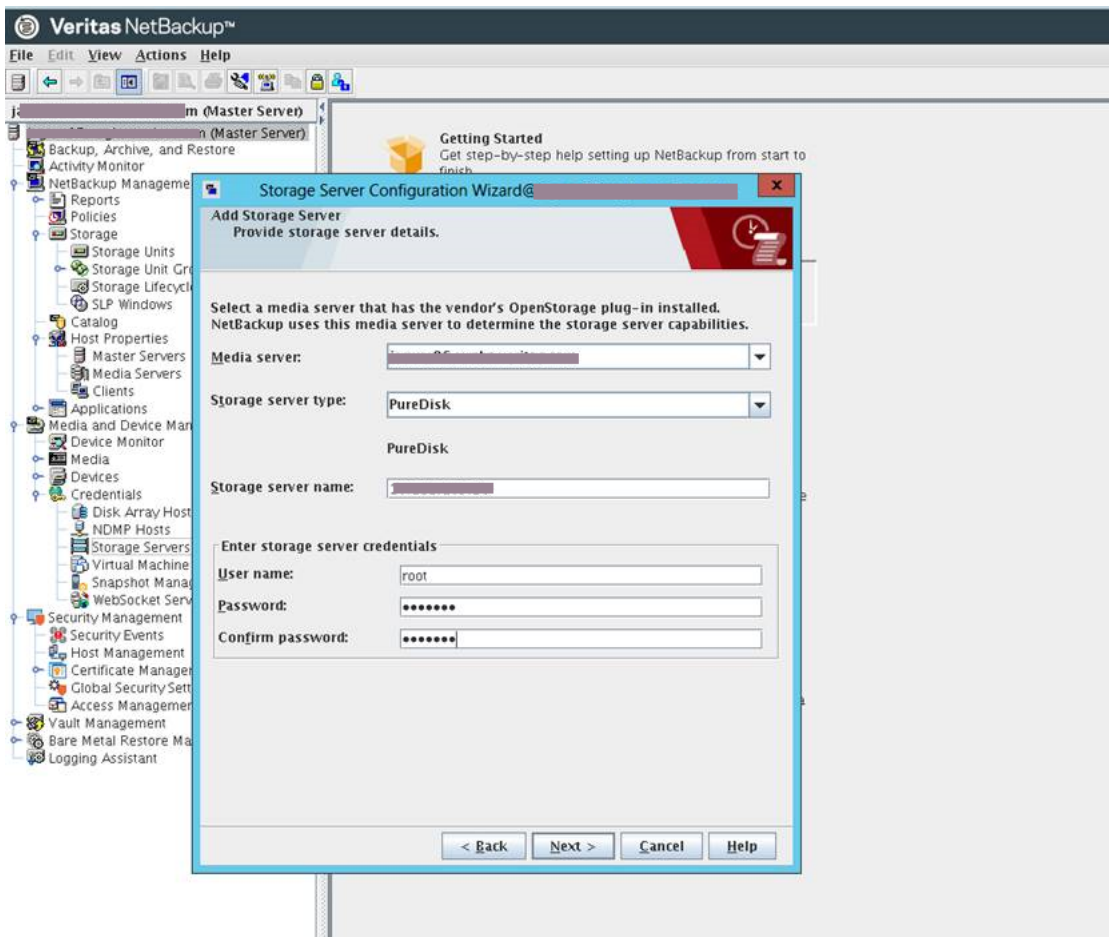


- 4 In the **Add Storage Server** form, enter the required information.
 - Select the media server from the **Media server** drop-down box.
 - Enter the storage server type as **PureDisk**.
 - Enter the IP address of the storage server configured on the Veritas Access cluster.

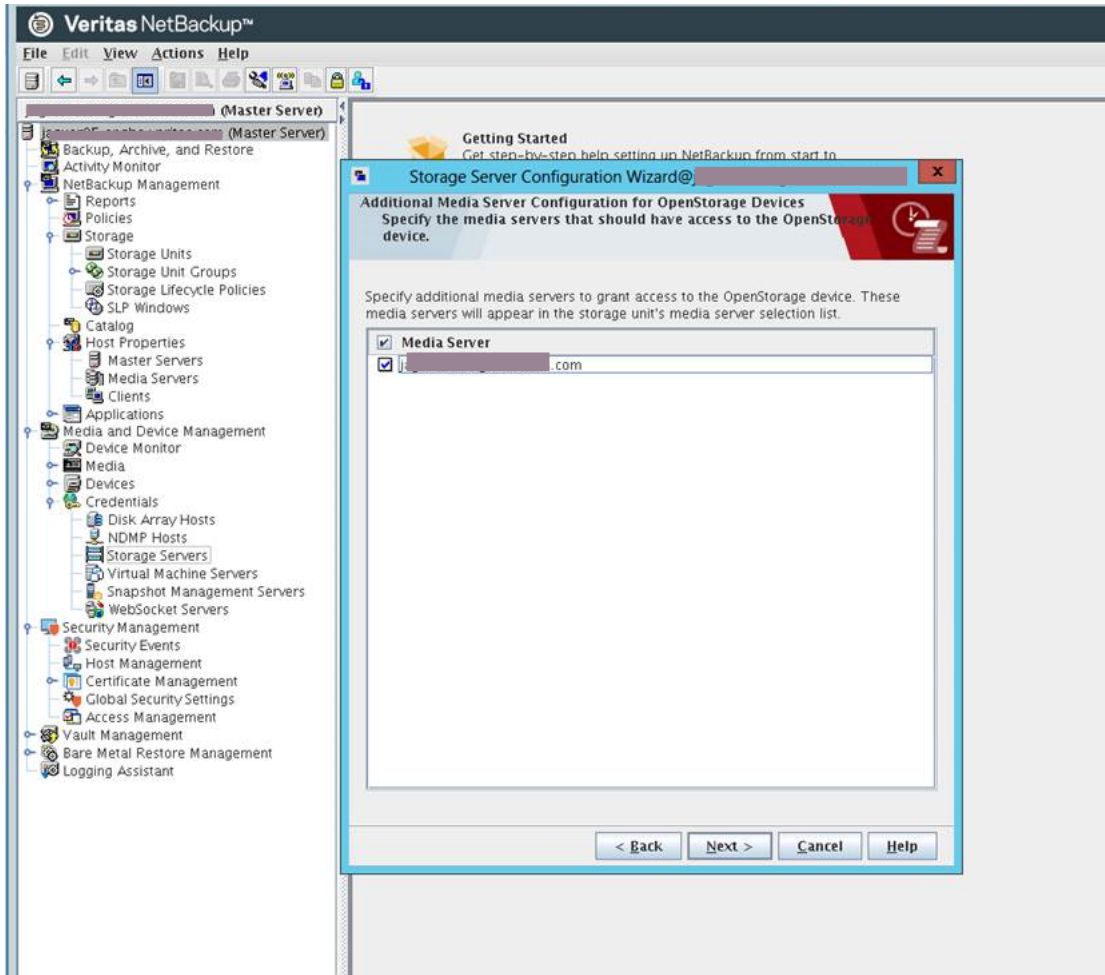
Note: Before you enter the IP address, run the `dedupe> show` command on the Veritas Access command-line interface to get the IP address of the storage server. If you want to use a host name for the storage server instead of an IP address, ensure that it is resolvable to the IP address configured for the deduplication storage server with DNS.

- Enter your credentials that you created when you configured Veritas Data Deduplication.

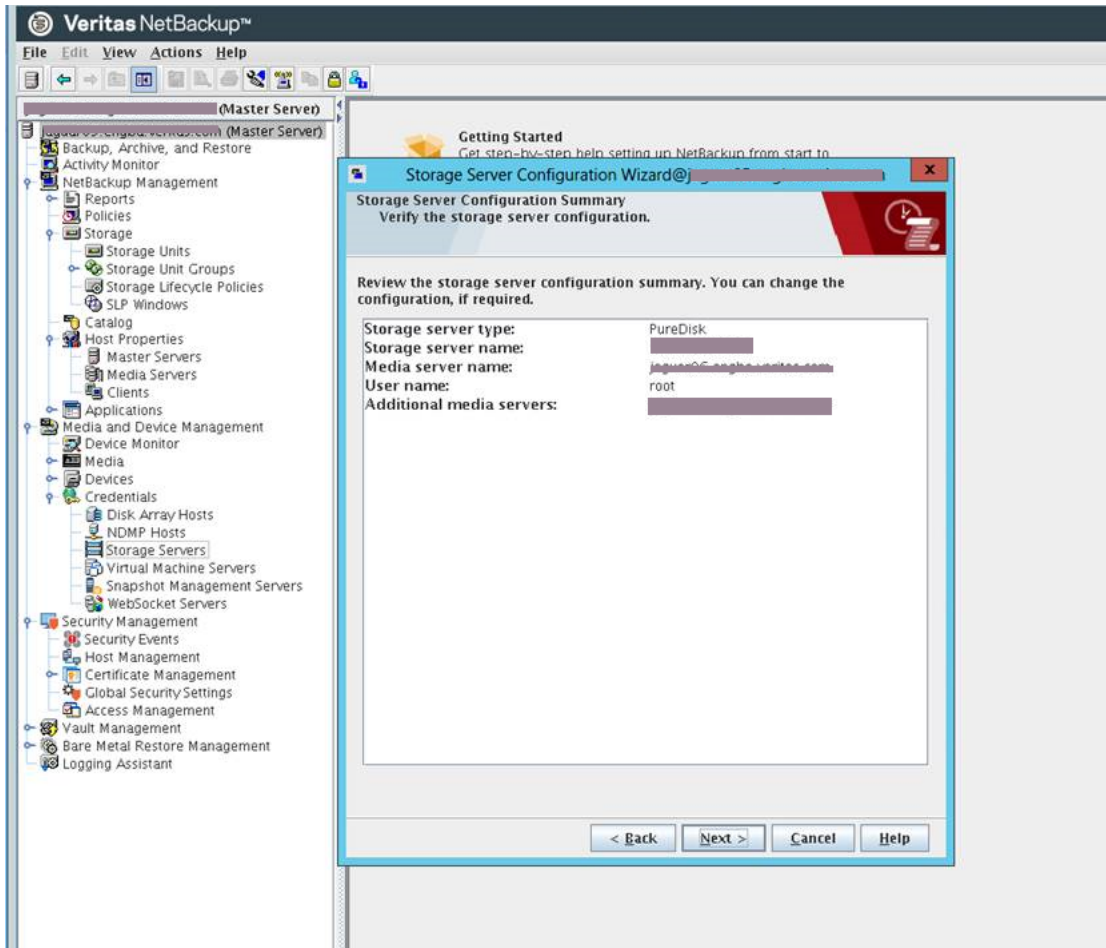
Click **Next**.



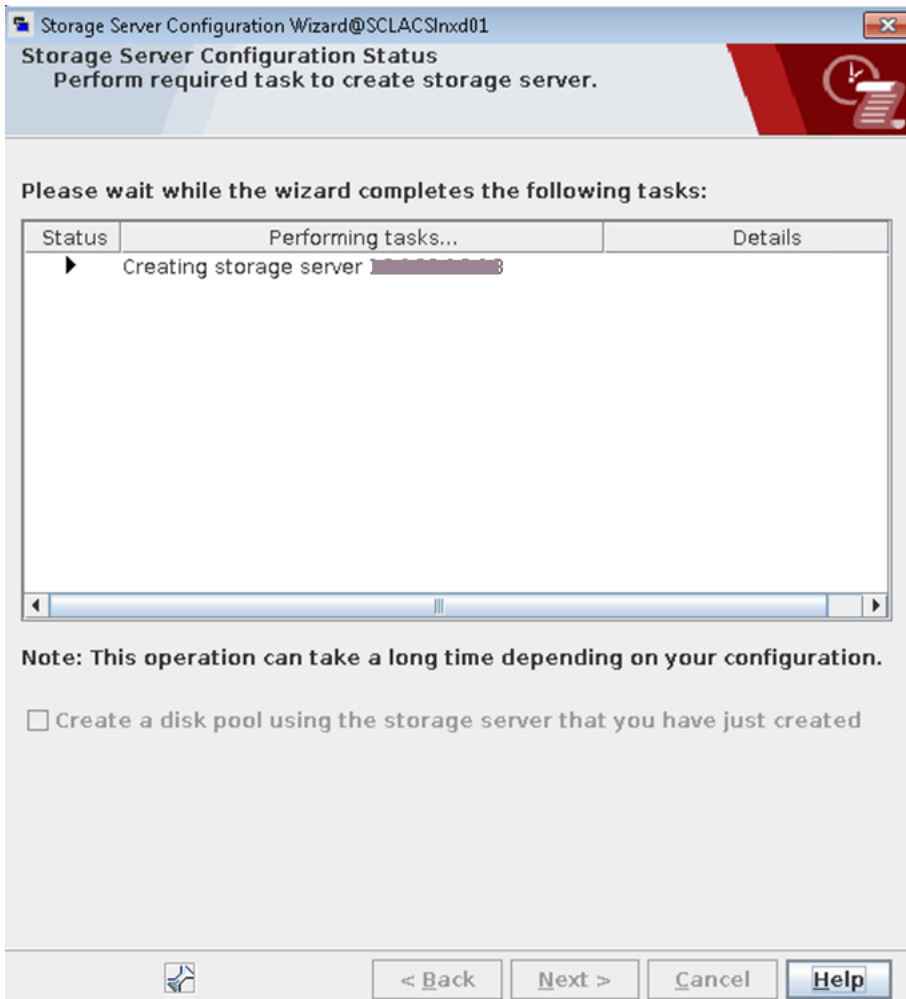
- 5 In the **Additional Media Server Configuration for OpenStorage Devices** form, specify the media servers that should have access to the OpenStorage device. Click **Next**.



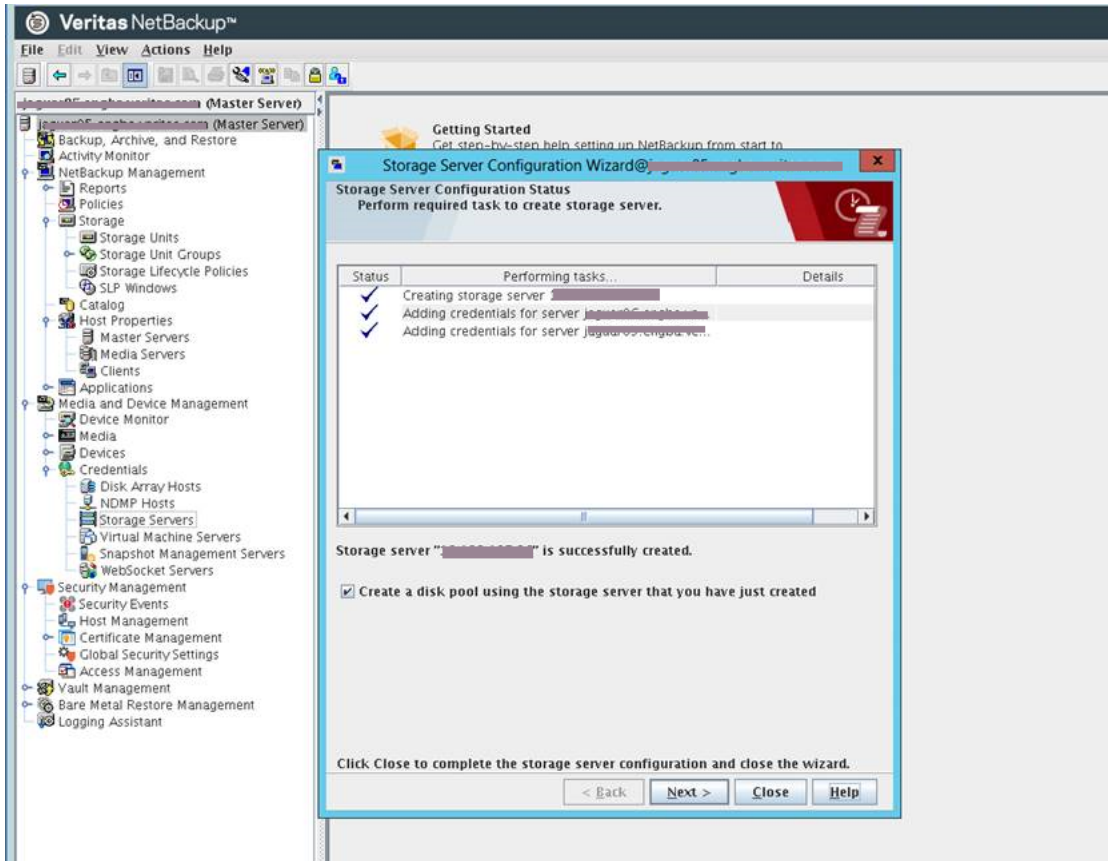
- 6 In the **Storage Server Configuration Summary** form, verify the storage server configuration. Click **Next**.



- 7 Check the status of the tasks in the **Storage Server Configuration Status** form. This operation can take some time depending on your configuration.

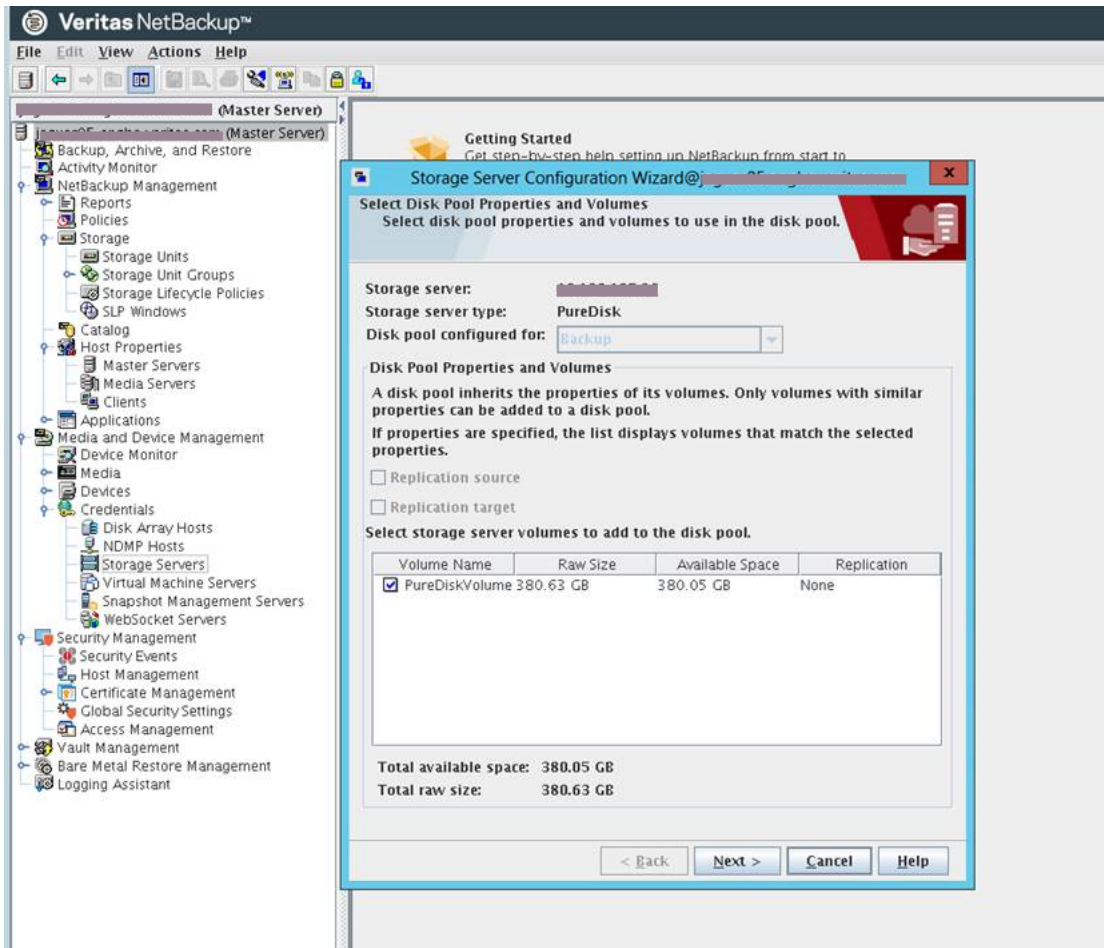


- 8 Verify that the storage server is successfully created and click **Next**.

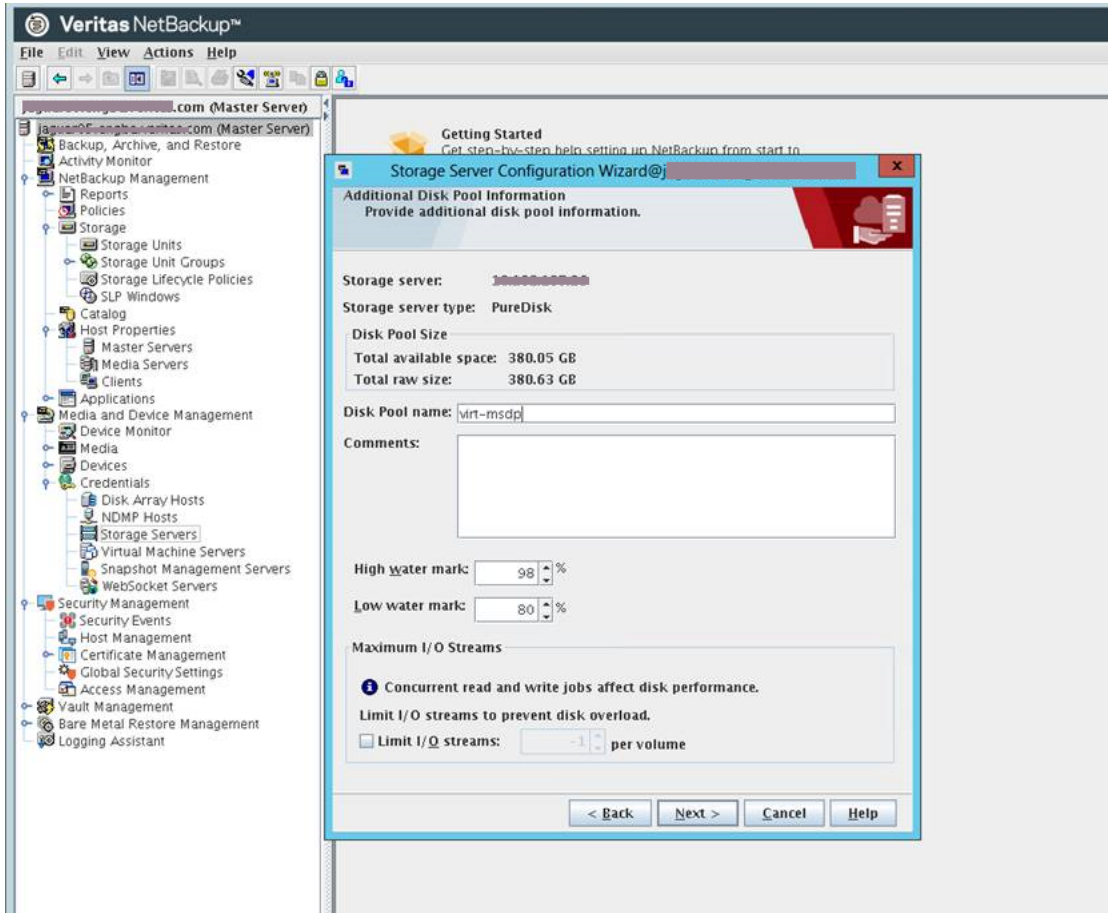


9 The Select Disk Pool Properties and Volumes form lists all the volumes.

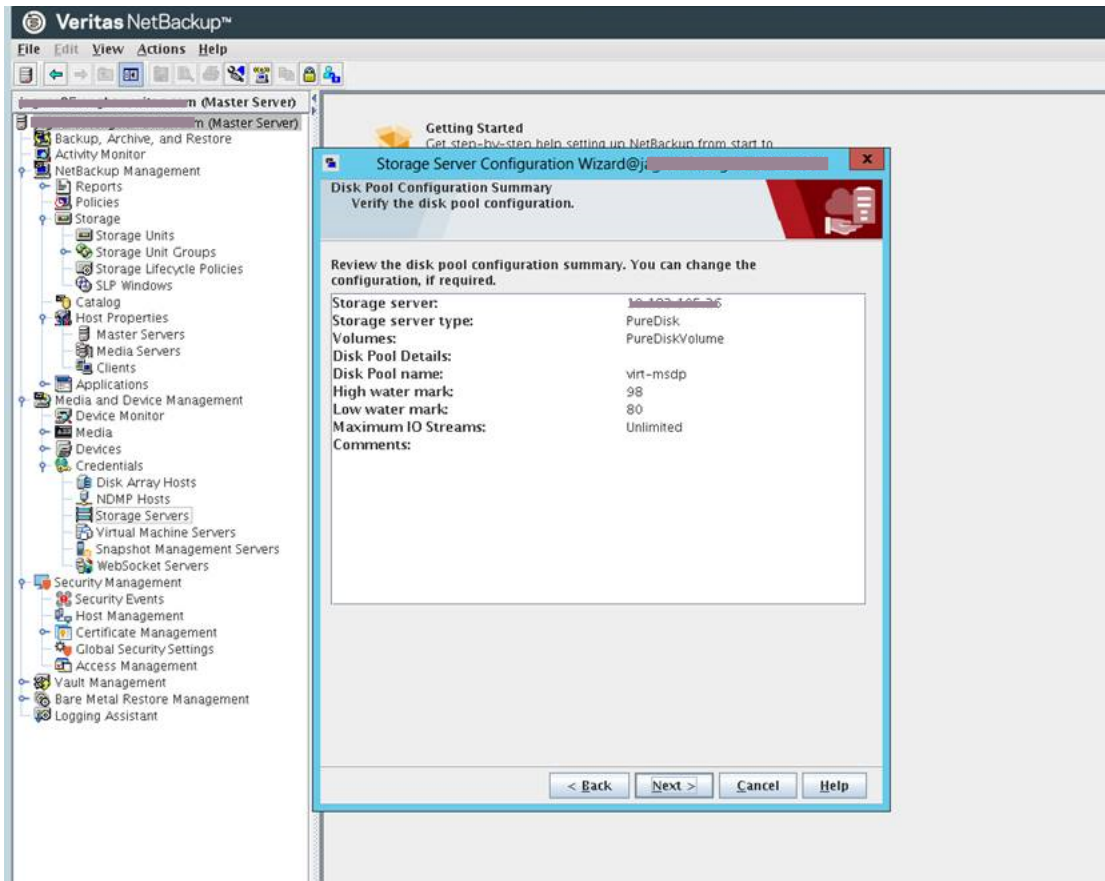
Select the storage server volumes that you want to add to the disk pool and click **Next**.



- 10 In the **Additional Disk Pool Information** form, enter the disk pool name and click **Next**.

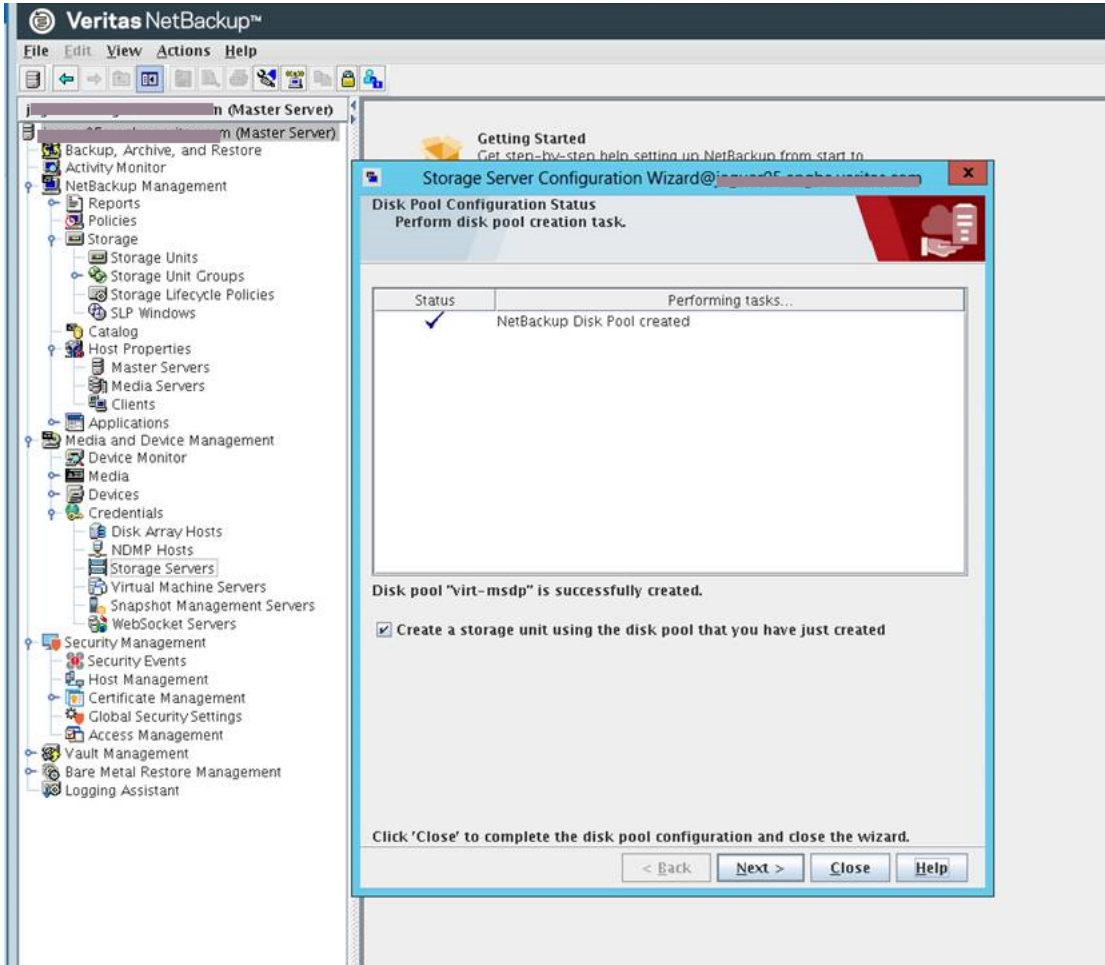


11 Verify the disk pool configuration summary and click **Next**.



12 In the **Disk Pool Configuration Status** form, create a disk pool.

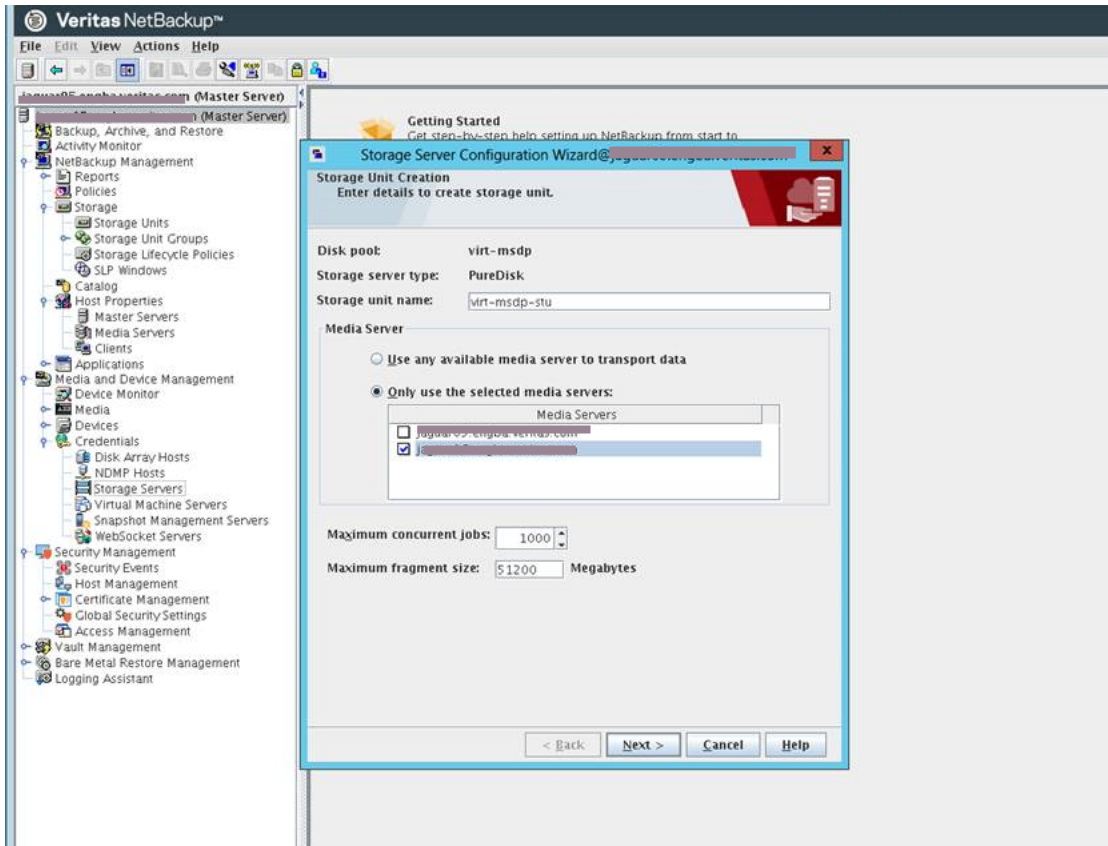
Verify that the disk pool is created successfully. Make sure that the **Create a storage unit using the disk pool that you have just created** check box is selected.



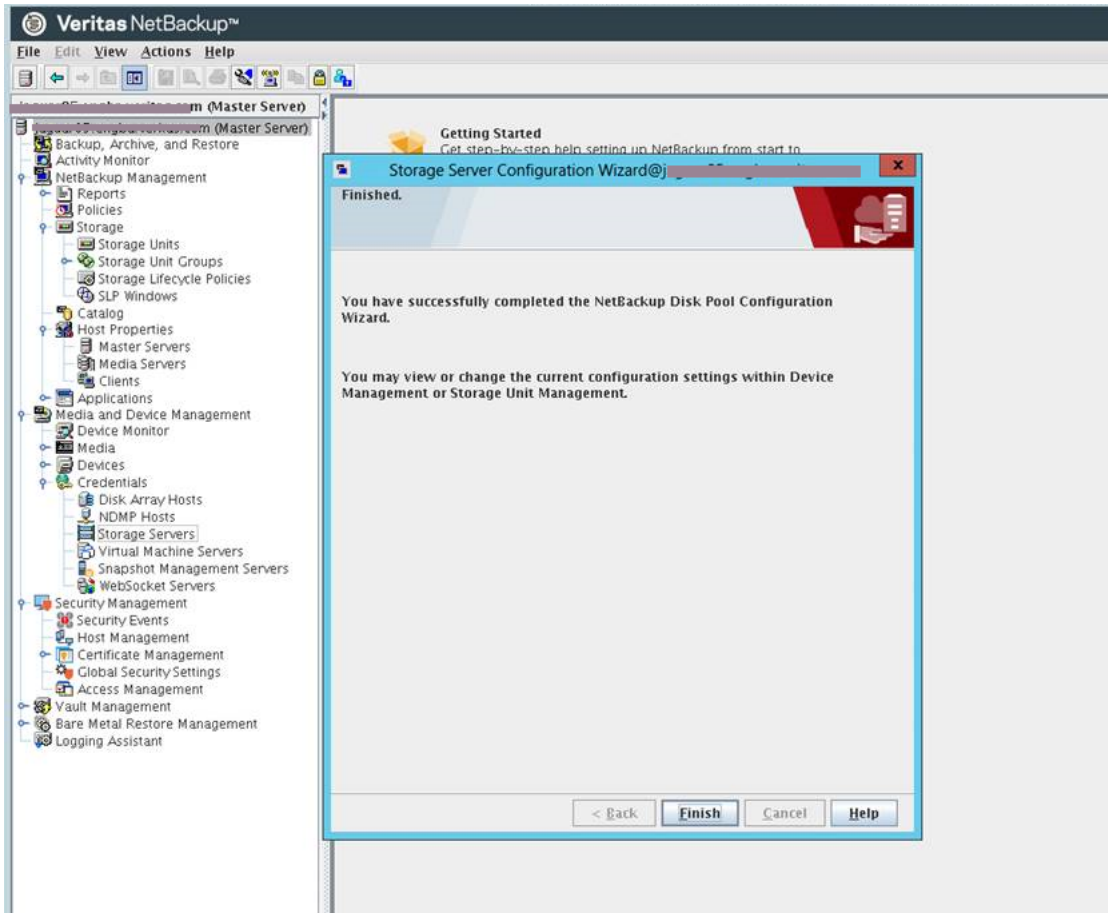
- 13** In the **Storage Unit Creation** wizard, enter the storage unit name. Select **Only use the selected media servers**. Select the media server in the list and update the maximum concurrent jobs field as per the NetBackup recommendations.

Refer to the *Veritas NetBackup* product documentation for more details.

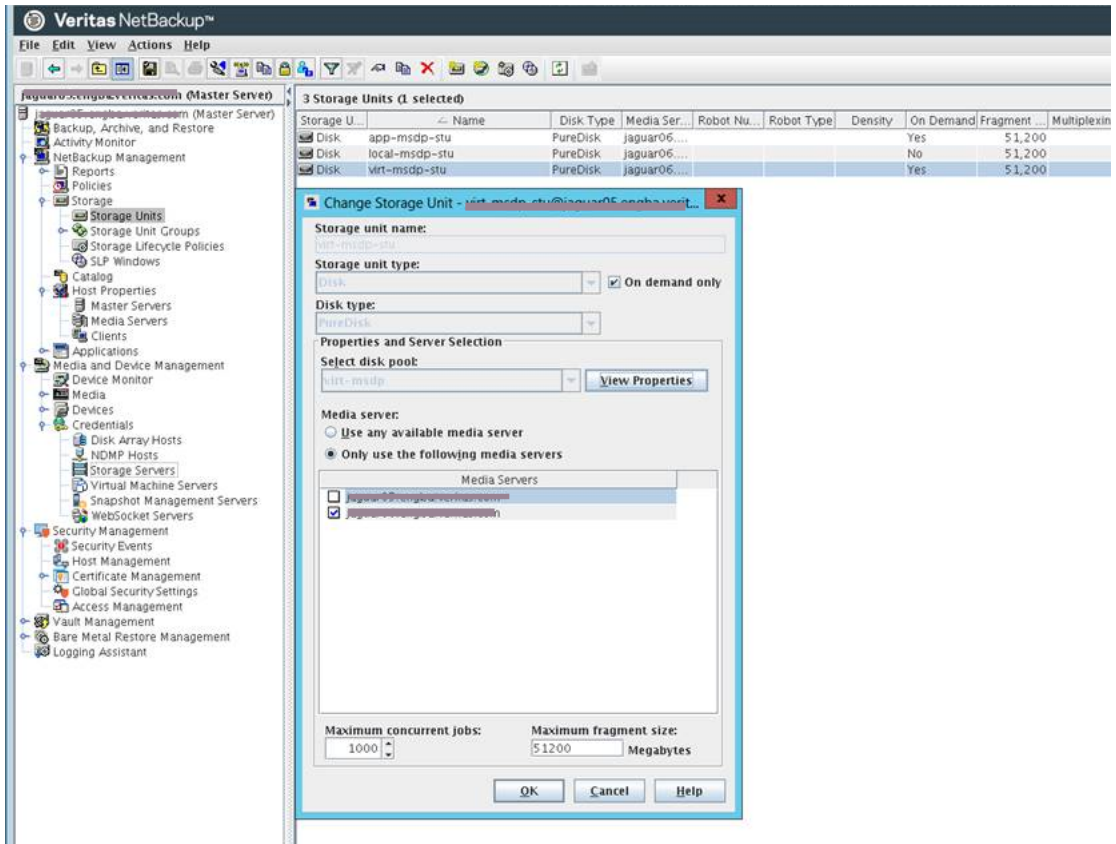
Click **Next**.



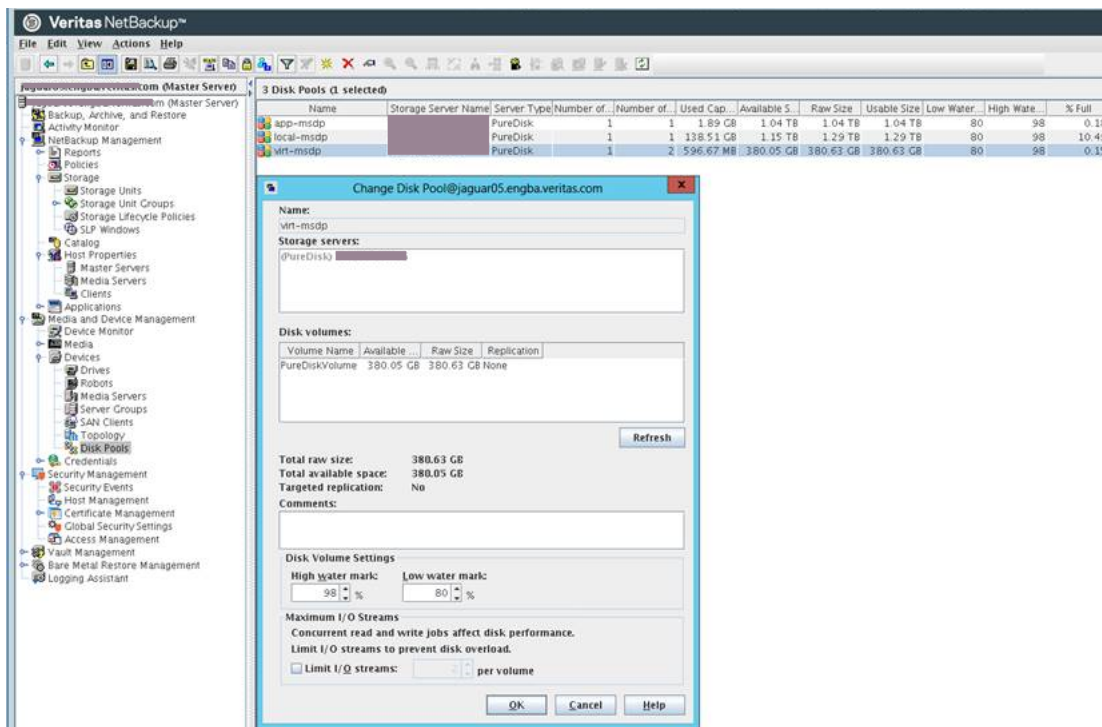
- 14 Verify that the disk pool creation wizard completed successfully. Click **Finish**.



- 15 Go to **NetBackup Management > Storage Units** and verify that the storage server has been added successfully.



- 16 Go to **Media and Device Management > Disk Pools** and verify that the disk pool is created successfully.



Configuring global deduplication using the Veritas Data Deduplication storage server across the domain

Veritas Access supports the configuration of multiple Logical Storage Units (LSU) with Veritas Data Deduplication. Using the global deduplication feature, multiple NetBackup domains can access the Veritas Data Deduplication storage server in Veritas Access. By default, only one NetBackup domain is preconfigured with the Veritas Data Deduplication storage server. To configure multiple domains, you need to create a new user for each domain. Different NetBackup domains require a different Veritas Data Deduplication user. A specific user can access data only from the domain to which the user has been added.

To add a new user to the deduplication storage server, enter the following:

```
dedupe> adduser username
```

Where *username* is the user name of the second domain user.

The command should be run on the Veritas Access cluster.

After a new user name is added to the storage server in Veritas Access, you can use the credentials of the new user to add a STU on NetBackup in the new domain. Any backups taken from the new domain are visible only to the new user. The NetBackup domain can access the catalog and data of the user. When you configure Auto Image Replication and add the storage target, use the Veritas Data Deduplication user name used by the target NetBackup domain.

To show the list of users of the deduplication storage server, enter the following:

```
dedupe> listuser
```

The command should be run on the Veritas Access cluster.

Note: You are required to use the IP address of the Veritas Data Deduplication host that was previously configured with the first domain in the **Add Storage Server** form when you provide the details of the storage server.

Migrating the NetBackup images from existing storage to Veritas Data Deduplication storage

This chapter includes the following topics:

- [Migrating the NetBackup image from OpenDedup/CloudCatalyst/S3 to Veritas Data Deduplication storage](#)

Migrating the NetBackup image from OpenDedup/CloudCatalyst/S3 to Veritas Data Deduplication storage

You can migrate the backup images from the OpenDedup/CloudCatalyst/S3 Storage Unit (STU) to the Veritas Data Deduplication STU.

Note: Veritas recommends using the Veritas Data Deduplication feature rather than using OpenDedup. However, OpenDedup is supported for backward compatibility.

Table 4-1

When OpenDedup is configured as the secondary/LTR storage in the NetBackup SLP	To migrate the NetBackup images from the OpenDedup STU to the Veritas Data Deduplication STU when OpenDedup is configured as secondary storage in the NetBackup SLP
When OpenDedup is configured as the primary storage in the NetBackup policy	To migrate the NetBackup images from the OpenDedup STU to the Veritas Data Deduplication STU when OpenDedup is configured as the primary storage in the NetBackup policy
When CloudCatalyst is configured as the secondary/LTR storage in the NetBackup policy	To migrate the NetBackup images from the CloudCatalyst STU to the Veritas Data Deduplication STU when CloudCatalyst is configured as the secondary storage in the NetBackup SLP
When CloudCatalyst is configured as the primary storage in the NetBackup policy	To migrate the NetBackup images from the CloudCatalyst STU to the Veritas Data Deduplication STU when CloudCatalyst is configured as the primary storage in the NetBackup policy
When S3 is configured as the primary storage in the NetBackup policy	To migrate the NetBackup images from the S3 STU to the Veritas Data Deduplication STU when S3 is configured as the primary storage in the NetBackup policy

To migrate the NetBackup images from the OpenDedup STU to the Veritas Data Deduplication STU when OpenDedup is configured as secondary storage in the NetBackup SLP

- 1 Configure the Veritas Data Deduplication STU.
- 2 Change the SLP to point to the Veritas Data Deduplication STU instead of the OpenDedup STU so that the new images get duplicated on the Veritas Data Deduplication STU.
- 3 Go to the **NetBackup Management > Catalog** and select the **Action** as **Duplicate** from the drop-down menu.
- 4 In the **NetBackup Management > Catalog**, right-click on the image that is stored on the OpenDedup STU and that you want to duplicate on the Veritas Data Deduplication STU. Select **Duplicate**.
- 5 In the pop-up window that appears, select the Veritas Data Deduplication STU and click **OK**.

- 6 In the confirmation screen, click **OK** to start duplication.

You can check the progress of the image duplication in the **NetBackup Activity Monitor**.

- 7 After duplication is complete, expire the backup image stored on the OpenDedup STU.

You can duplicate the images stored on the OpenDedup STU to the Veritas Data Deduplication STU by using the following NetBackup commands:

- Get the list of images stored on the OpenDedup STU.

```
/usr/opensv/netbackup/bin/admincmd/bpimmedia -stype OpenDedupe
| grep ^IMAGE |awk {'print $3'}
```

- Start duplication to the Veritas Data Deduplication STU.

```
/usr/opensv/netbackup/bin/admincmd/bpduplicate -dstunit
<ACCESS MSDP STU NAME> -pt Standard -backupid <backup image id>
```

To migrate the NetBackup images from the OpenDedup STU to the Veritas Data Deduplication STU when OpenDedup is configured as the primary storage in the NetBackup policy

- 1 Configure the Veritas Data Deduplication STU.
- 2 Change the SLP to point to the Veritas Data Deduplication STU instead of the OpenDedup STU so that the new images get created on the Veritas Data Deduplication STU.
- 3 Go to the **NetBackup Management > Catalog** and select the **Action** as **Duplicate** from the drop-down menu.
- 4 In the **NetBackup Management > Catalog**, right-click on the image that is stored on the OpenDedup STU and that you want to duplicate on the Veritas Data Deduplication STU. Select **Duplicate**.
- 5 In the pop-up window that appears, select the Veritas Data Deduplication STU and click **OK**.
- 6 In the confirmation screen, click **OK** to start duplication.

You can check the progress of the image duplication in the **NetBackup Activity Monitor**.
- 7 After duplication is complete, expire the backup image stored on the OpenDedup STU.

To migrate the NetBackup images from the CloudCatalyst STU to the Veritas Data Deduplication STU when CloudCatalyst is configured as the secondary storage in the NetBackup SLP

- 1 Configure the Veritas Data Deduplication STU.
- 2 Change the SLP to point to the Veritas Data Deduplication STU instead of the CloudCatalyst STU so that the new images get duplicated on the Veritas Data Deduplication STU.
- 3 As optimized duplication from CloudCatalyst to Veritas Data Deduplication is not supported, the administrator is required to add the `RESUME_ORIG_DUP_ON_OPT_DUP_FAIL = TRUE` flag in the `/usr/openv/netbackup/bp.conf` file of both the master and media server.
- 4 Go to the **NetBackup Management > Catalog** and select the **Action as Duplicate** from the drop-down menu.
- 5 In the **NetBackup Management > Catalog**, right-click on the image that is stored on the CloudCatalyst STU and that you want to duplicate on the Veritas Data Deduplication STU. Select **Duplicate**.
- 6 In the pop-up window that appears, select the Veritas Data Deduplication STU and click **OK**.
- 7 In the confirmation screen, click **OK** to start duplication.

You can check the progress of the image duplication in the **NetBackup Activity Monitor**.
- 8 After the completion of duplication, the status of the duplication job appears as **The requested operation was partially successful**. In the job detail status, some error messages appear that are expected.
- 9 After duplication is complete, expire the backup image stored on the CloudCatalyst STU.

To migrate the NetBackup images from the CloudCatalyst STU to the Veritas Data Deduplication STU when CloudCatalyst is configured as the primary storage in the NetBackup policy

- 1 Configure the Veritas Data Deduplication STU.
- 2 Change the SLP to point to the Veritas Data Deduplication STU instead of the CloudCatalyst STU so that the new images get created on the Veritas Data Deduplication STU.
- 3 As optimized duplication from CloudCatalyst to Veritas Data Deduplication is not supported, the administrator is required to add the `RESUME_ORIG_DUP_ON_OPT_DUP_FAIL = TRUE` flag in the `/usr/openv/netbackup/bp.conf` file of both the master and media server.

- 4 Go to the **NetBackup Management > Catalog** and select the **Action** as **Duplicate** from the drop-down menu.
- 5 In the **NetBackup Management > Catalog**, right-click on the image that is stored on the CloudCatalyst STU and that you want to duplicate on the Veritas Data Deduplication STU. Select **Duplicate**.
- 6 In the pop-up window that appears, select the Veritas Data Deduplication STU and click **OK**.
- 7 In the confirmation screen, click **OK** to start duplication.
You can check the progress of the image duplication in the **NetBackup Activity Monitor**.
- 8 After the completion of duplication, the status of the duplication job appears as **The requested operation was partially successful**. In the job detail status, some error messages appear that are expected.
- 9 After duplication is complete, expire the backup image stored on the CloudCatalyst STU.

To migrate the NetBackup images from the S3 STU to the Veritas Data Deduplication STU when S3 is configured as the primary storage in the NetBackup policy

- 1 Configure the Veritas Data Deduplication STU.
- 2 Change the SLP to point to the Veritas Data Deduplication STU instead of the S3 STU so that the new images get created on the Veritas Data Deduplication STU.
- 3 Go to the **NetBackup Management > Catalog** and select the **Action** as **Duplicate** from the drop-down menu.
- 4 In the **NetBackup Management > Catalog**, right-click on the image that is stored on the S3 STU and that you want to duplicate on the Veritas Data Deduplication STU. Select **Duplicate**.
- 5 In the pop-up window that appears, select the Veritas Data Deduplication STU and click **OK**.
- 6 In the confirmation screen, click **OK** to start duplication.
You can check the progress of the image duplication in the **NetBackup Activity Monitor**.
- 7 After duplication is complete, expire the backup image stored on the S3 STU.

Configuring Veritas Access backup over S3 with OpenDedup and NetBackup

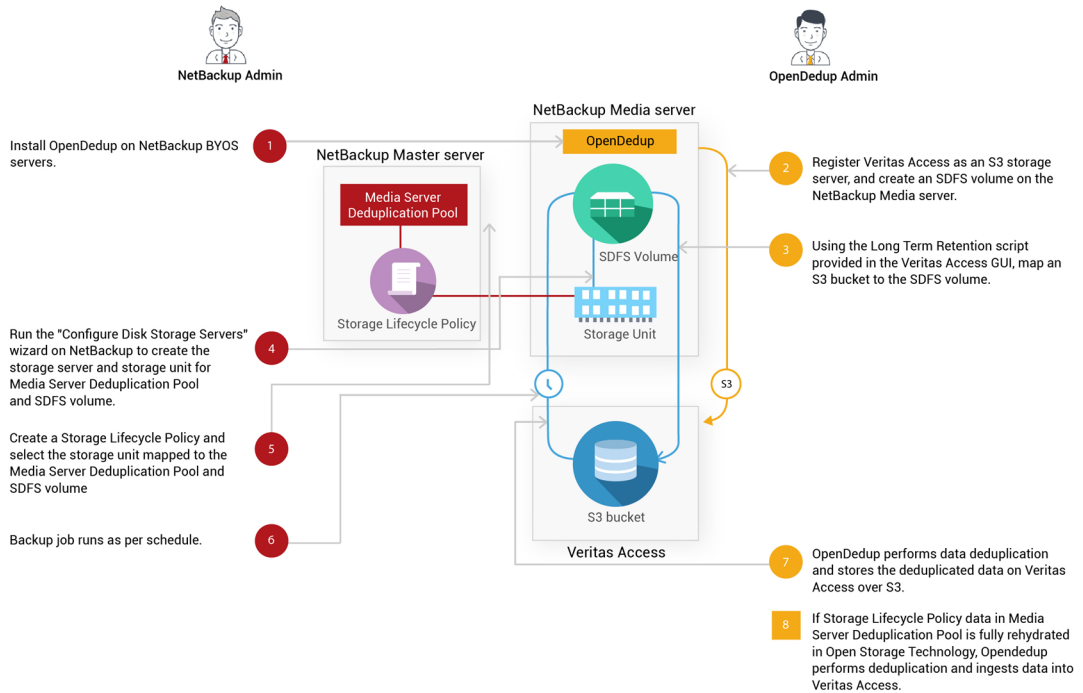
This chapter includes the following topics:

- [Workflow for OpenDedup](#)
- [Backing up deduplicated data \(OpenDedup and NetBackup\) using the S3 protocol to Veritas Access](#)
- [Backing up data \(NetBackup\) and deduplicating the data \(OpenDedup\) on Veritas Access](#)
- [Creating an S3 bucket on Veritas Access for storing deduplicated backup data from NetBackup](#)
- [Creating a Media Server Deduplication Pool \(MSDP\) for primary backup using NetBackup](#)
- [Creating an OST disk pool and STU in the NetBackup console](#)
- [Setting up multiple NetBackup media servers in the same domain](#)
- [Setting up multiple SDFS volumes on a NetBackup media server](#)

Workflow for OpenDedup

[Figure 5-1](#) illustrates the workflow for OpenDedup for Veritas Access.

Figure 5-1 Workflow for OpenDedup



Backing up deduplicated data (OpenDedup and NetBackup) using the S3 protocol to Veritas Access

SDFS is an inline deduplication-based file system.

To download and install the OST and SDFS rpms

- 1 On a standard NetBackup master and/or media server, run the following commands to install sdfs:

```
# wget https://sort.veritas.com/public/patchcentral/Linux/7.4/access/
access-rhel7_x86_64-7.4.2sdfs.tar.gz
# tar -zxvf access-rhel7_x86_64-7.4.2sdfs.tar.gz
# cd rpms/
# rpm -ivh sdfs-7.4.2.0-1.x86_64.rpm
```

- 2 Run the following commands to install OST.

```
# wget https://sort.veritas.com/public/patchcentral/Linux/7.4/access/
access-rhel7_x86_64-7.4.2ost.tar.gz
# tar -zxvf access-rhel7_x86_64-7.4.2ost.tar.gz
# cd rpms/
# tar -zxvf access-rhel-Patch7.4.2.0ost.tar.gz
# cd dist/
# ./media-install.sh
```

- 3 Restart the NetBackup service on the NetBackup media server.

```
# /etc/init.d/netbackup stop
# /etc/init.d/netbackup start
```

Backing up data (NetBackup) and deduplicating the data (OpenDedup) on Veritas Access

SDFS is an inline deduplication-based file system.

To download and install the OST

- ◆ On a standard NetBackup master and/or media server, run the following commands to install the OST:

```
# wget https://sort.veritas.com/public/patchcentral/Linux/7.4/access/
/access-rhel7_x86_64-Patch-7.4.2ost.tar.gz
# tar -zxvf access-rhel7_x86_64-Patch-7.4.2ost.tar.gz
# cd rpms/
# tar -zxvf access-rhel-Patch-7.4.2.0.tar.gz
# cd dist/
# ./media-install.sh
```

Creating an S3 bucket on Veritas Access for storing deduplicated backup data from NetBackup

To create an S3 bucket on Veritas Access for storing deduplicated backup data from NetBackup

- 1 Log on to the Veritas Access GUI as the master user using the following URL:

`https://Veritas Access Management console IP:14161/.`

You can obtain the Veritas Access Management console IP by logging on to the Veritas Access command-line interface using the `su - master` command on the Veritas Access cluster.

- 2 Create a storage pool for the S3 buckets.

Click **NAS Infrastructure** in the GUI navigation on the left.

Select the disks that you want to use for the S3 bucket, and click the **Add to Storage Pool** button to invoke the wizard for storage pool creation.

Follow the steps in the wizard for creating a new storage pool or adding the disks to an existing pool.

- 3 Click **Settings > User Management > Configure Active Directory** to configure AD.

Enter the required information, such as the **DNS Domain**, **DNS Name Servers**, **AD Domain**, **AD Domain Controller**, and the **AD Admin** and **Password**.

- 4 Click **Settings > S3 Management** to configure and enable the S3 server.

Edit the default parameters that are required for the S3 server, such as the storage pool name, underlying S3 bucket layout, and the default size of the bucket.

- 5 Double-click **S3 Server Status** to start the S3 server.

- 6 Log out from the GUI, and log in again as an AD user.

Note: Log in using the `domainname\username` format.

Click on the **Create keys** button to generate the access key and the secret key for the Veritas Access S3 bucket.

Save the access key and secret key in a safe location, as Veritas Access does not allow retrieval of keys after initial creation.

- 7 Log out from the GUI, and log on again as the master user.

- 8 Registration of supported public cloud service is optional, and is only required in case you need to add an AWS cloud as a storage tier. Without this, backups are stored locally in Veritas Access S3 buckets.

Click **Settings > Cloud Storage Registration > Add Cloud Subscription** to register the supported public or private cloud service.

Enter information for the cloud service provider, name of subscription, access key, and secret key.

- 9 Activate the long-term data retention (LTR) policies.

Click **Policies > LTR Policy**.

Click **Activate** for either the **LTR On-Premises + Cloud** policy or the **LTR On-Premises** policy and provide the storage pool when prompted.

- 10 Provision the NetBackup bucket using the policy.

Under **Quick Actions**, click **Provision Storage**. Select **S3 Storage for NetBackup** and click **Next**.

Provide the bucket size, underlying layout of the bucket, the access key, and the secret key of the Veritas Access S3 server generated as the AD user in step 6.

If you selected the **LTR On-Premises + Cloud** policy, add information such as which data should be moved to the AWS cloud tier, AWS region, cloud tier type (S3/Glacier), and when the data movement to the cloud should occur.

- 11 Monitor the progress of the task under **Recent Activity**.

Make a note of the scale-out file system name that was used for the bucket creation.

- 12 Click **File Systems**.

For the scale-out file system that is created, ensure that the **S3 Bucket** column displays **Yes** to indicate that the S3 bucket is enabled.

You may need to wait for some time for this change to be reflected in the GUI.

- 13 Right-click the ellipses (additional options), and click **Configure LTR Script**.

- 14 A pop-up window appears with the following options:

Do you want to Run the LTR script?

Do you want to Download the LTR script?

- Select the **Do you want to Run the LTR script?** option if OpenDedup is hosted on Veritas Access. You will be prompted to enter you access key. Enter the access key and click **Next**. Wait for the task to be completed. The rest of the configuration steps are done automatically.

After the configuration is completed successfully, the output message shows the IP address and the port number on which the OpenDedup volume is mounted on Veritas Access. The IP address and port number are required later during OST configuration.

Note: This operation creates/expands a new file system named `odd_cache_fs` to store the OpenDedup cache data. The default size of this file system is 24 GB. Veritas recommends that you expand the file system to the required size. See the *OpenDedup documentation* for more details.

Note: The `Configure LTR` script randomly chooses a virtual IP from the available Veritas Access virtual IPs. If you are using Veritas Access in mixed mode having both IPv4 and IPv6 addresses, you may need to update virtual IP address used by OpenDedup using the `network> IP addr modify` command from the Veritas Access command-line interface. If your NetBackup server is running on IPv4, make sure that OpenDedup uses the Veritas Access IPv4 virtual IP. If your NetBackup server is running on IPv6, make sure that OpenDedup uses the Veritas Access IPv6 virtual IP.

Go to step 21.

Name	Status	Start Time	End Time
✚ Configuring LTR on Veritas Access cluster.	Success	2017-12-13 11:18:58	2017-12-13 11:21:06
✚ Provision storage for long term retention	Success	2017-12-11 12:08:30	2017-12-11 12:10:25
✚ Provision storage for long term retention	Success	2017-12-11 11:54:00	2017-12-11 11:55:55
✚ Configuring LTR on Veritas Access cluster.	Success	2017-12-08 11:13:19	2017-12-08 11:15:23
✚ Provision storage for long term retention	Success	2017-12-08 11:04:22	2017-12-08 11:06:58
✚ Configuring LTR on Veritas Access cluster.	Success	2017-12-06 18:18:14	2017-12-06 18:20:18
✚ Provision storage for long term retention	Success	2017-12-06 18:10:12	2017-12-06 18:12:07
Run full discovery	Success	2017-12-06 16:03:06	2017-12-06 16:05:00

Output:	ACCESS odd SUCCESS V-493-10-2820 S3fs1512711321 has been created successfully and mounted on 10.209.105.215:6442
Command executed:	NAS_OUTPUT=json /opt/VRTSnas/clish/bin/clish -u master -c "opendedup volume create S3fs1512711321 10GB OGfMzJFhYwQ5N2VkyWJ 4f97ef4c-ee84-4fad-ba2d-cca73828c145s3bucket"

- Select the **Do you want to Download the LTR script?** option if OpenDedup is hosted on the NetBackup master and/or media server. Click **Next**. Wait for the task to be completed.

15 Copy the LTR script to the host where OpenDedup is installed. It can be the host where the NetBackup media server is installed.

- 16 Run the downloaded LTR script. The LTR script requires the Veritas Access S3 keys (access and secret key) as arguments that were generated as the AD user.

The LTR script creates the OpenDedup file system and prompts for the entry in the `/etc/hosts` file for the bucket to IP address mapping.

Output of LTR script execution:

```
[root@host1 ~]# sh LTRscript_<fsname/volname>_<bucketname>.sh
<Access key> <Secret Key>
=====
Insert the below details in /etc/hosts file
10.100.100.1 4f459a2d-736e-4be5-9c5a-f821fbc198fds3bucket.s3.access
=====
Attempting to create SDFS volume ...
Volume [S3fs1497356186] created with a capacity of [10.00GB]
check [/etc/sdfs/S3fs1497356186-volume-cfg.xml] for configuration
details if you need to change anything
```

Note: The volume name highlighted above and its equivalent .xml file are used to mount and update the SDFS volume parameters in later steps.

- 17 Add the IP associated with the virtual hosted-style bucket name (generated from the LTR script) in the `/etc/hosts` file on the media server.

Note: The `Configure LTR` script randomly choose a virtual IP from the available Veritas Access virtual IPs. If you are using Veritas Access in mixed mode having both IPv4 and IPv6 addresses, you may need to update the `/etc/hosts` entries. If your NetBackup server is running on IPv4, make sure that the `/etc/hosts` entry has IPv4 Veritas Access virtual IP. If your NetBackup server is running on IPv6, make sure that the `/etc/hosts` entry has IPv6 Veritas Access virtual IP. Alternatively, you can also modify the virtual IP on a Veritas Access cluster to an IPv4 or IPv6 address using the `network> ip addr modify` command from the Veritas Access command-line interface and add the modified IP to the `/etc/hosts` file.

- 18** Mount the SDFS volume under `/opendedupe/volumes/` on the host where OpenDedup is installed.

```
# mkdir /opendedupe/volumes/filesystem_name

# mount -t sdfs filesystem_name /opendedupe/volumes/filesystem_name
```

The `mount` command mounts a bucket on the Veritas Access cluster or the NetBackup media server.

Note: After mounting the SDFS volume, it starts listening on a specific port, usually starting from 6442.

You can find the port information using the `mount` command.

Example:

```
[root@host1 ~]# mount | grep opendedupe
sdfs:/etc/sdfs/S3fs1497346133-volume-cfg.xml:6443 on
/opendedupe/volumes/S3fs1497346133 type fuse
(rw,nosuid,nodev,allow_other,allow_other)
sdfs:/etc/sdfs/S3fs1497258807-volume-cfg.xml:6442 on
/opendedupe/volumes/pool1 type fuse
(rw,nosuid,nodev,allow_other,allow_other)
```

- 19** Update the `/etc/rc.local` script with the following:

```
/scripts/mount-opendedupe.sh || exit 1
exit 0
```

- 20** Create the `mount-opendedupe.sh` script and `/scripts` directory.

```
cat mount-opendedupe.sh
#!/bin/sh
mount -t sdfs <volume_name> /opendedupe/volumes/<volume_name>
```

21 Execute the following commands:

```
chmod +x /scripts/mount-opendedupe.sh  
chmod +x /etc/rc.d/rc.local
```

22 Update the URL tag in the `/etc/sdfs/ostconfig.xml` present on the NetBackup media server based on the following two cases:

Use case 1: OpenDedup on a NetBackup server

```
<URL>  
http://localhost:6442/  
</URL>
```

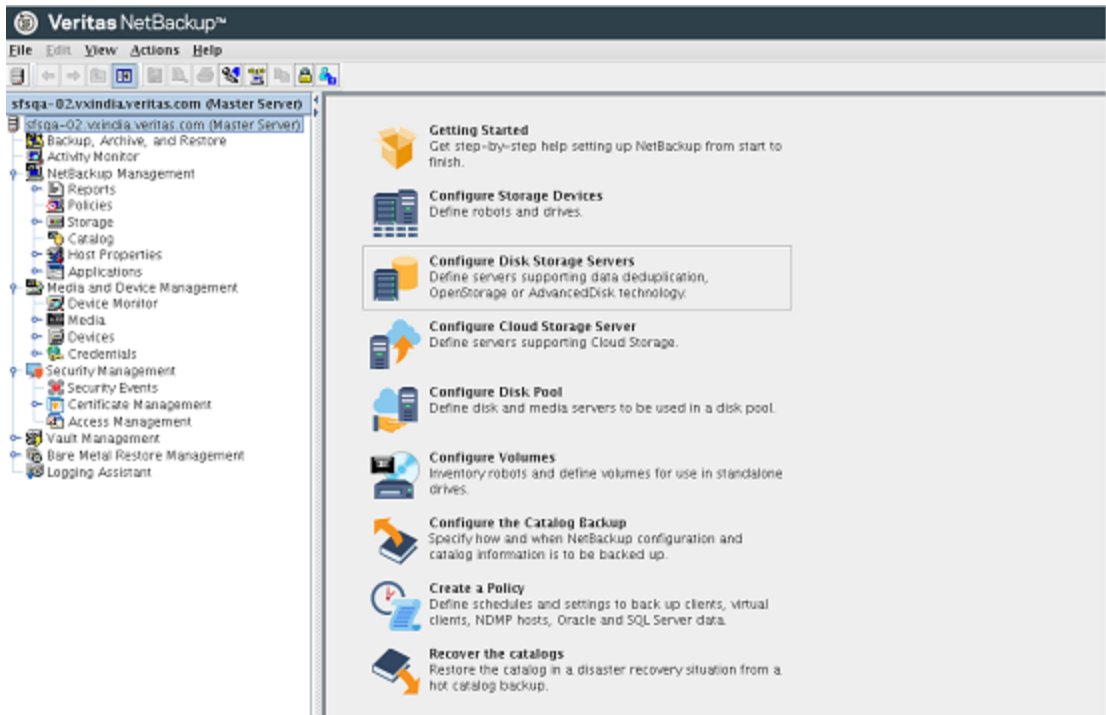
Use case 2: OpenDedup on Veritas Access

```
<URL>  
http://<IP address that was specified in step 14>:<port number that  
was specified in step 14>/  
</URL>
```

Creating a Media Server Deduplication Pool (MSDP) for primary backup using NetBackup

To create an MSDP disk pool and storage unit (STU) in the NetBackup console

- 1 Log on to the NetBackup master server from the Java console.



2 Select Media Server Deduplication Pool.



- 3 Enter the user name, password, and other required details.



The image shows a 'Storage Server Configuration Wizard' window. The title bar reads 'Storage Server Configuration Wizard@sfsqa-02.vxindia.veritas.com'. The main heading is 'Add Storage Server' with the instruction 'Provide storage server details.' Below this, a text block states: 'Select the media server that connects to the storage. The media server runs the core NetBackup Deduplication Engine components and functions as the storage server.' The form contains several fields: 'Media server:' is a dropdown menu showing 'sfsqa-02.vxindia.veritas.com'; 'Storage server type:' is a text field containing 'Media Server Deduplication Pool'; 'Storage server name:' is a text field containing 'sfsqa-02.vxindia.veritas.com'. A section titled 'Define credentials' contains three fields: 'User name:' with 'root', 'Password:' with masked characters '*****', and 'Confirm password:' with masked characters '*****'. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

Storage Server Configuration Wizard@sfsqa-02.vxindia.veritas.com

Add Storage Server
Provide storage server details.

Select the media server that connects to the storage. The media server runs the core NetBackup Deduplication Engine components and functions as the storage server.

Media server: sfsqa-02.vxindia.veritas.com

Storage server type: Media Server Deduplication Pool

Storage server name: sfsqa-02.vxindia.veritas.com

Define credentials

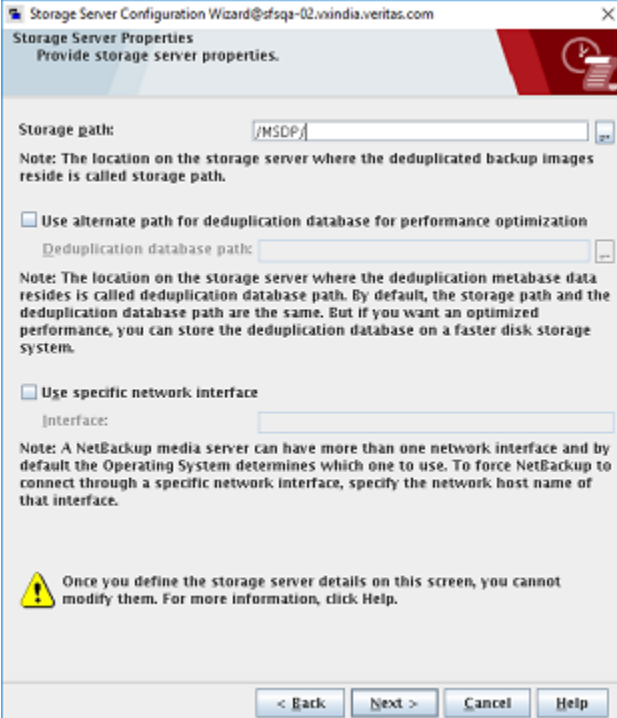
User name: root

Password: *****

Confirm password: *****

< Back Next > Cancel Help

4 Enter the storage path for MSDP.



The image shows a 'Storage Server Configuration Wizard' window with the title bar 'Storage Server Configuration Wizard@dfsqa-02.vxindia.veritas.com'. The main heading is 'Storage Server Properties' with the instruction 'Provide storage server properties.' Below this, there is a 'Storage path:' label followed by a text box containing '/MSDP/' and a browse button. A note states: 'Note: The location on the storage server where the deduplicated backup images reside is called storage path.' There is an unchecked checkbox for 'Use alternate path for deduplication database for performance optimization'. Below it is a 'Deduplication database path:' label with a text box and a browse button. A note explains: 'Note: The location on the storage server where the deduplication metabase data resides is called deduplication database path. By default, the storage path and the deduplication database path are the same. But if you want an optimized performance, you can store the deduplication database on a faster disk storage system.' Another unchecked checkbox is for 'Use specific network interface', followed by an 'Interface:' label and a text box. A note says: 'Note: A NetBackup media server can have more than one network interface and by default the Operating System determines which one to use. To force NetBackup to connect through a specific network interface, specify the network host name of that interface.' At the bottom left is a yellow warning icon and a message: 'Once you define the storage server details on this screen, you cannot modify them. For more information, click Help.' At the bottom right are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

Storage path:

Note: The location on the storage server where the deduplicated backup images reside is called storage path.

☐ Use alternate path for deduplication database for performance optimization

Deduplication database path:

Note: The location on the storage server where the deduplication metabase data resides is called deduplication database path. By default, the storage path and the deduplication database path are the same. But if you want an optimized performance, you can store the deduplication database on a faster disk storage system.

☐ Use specific network interface

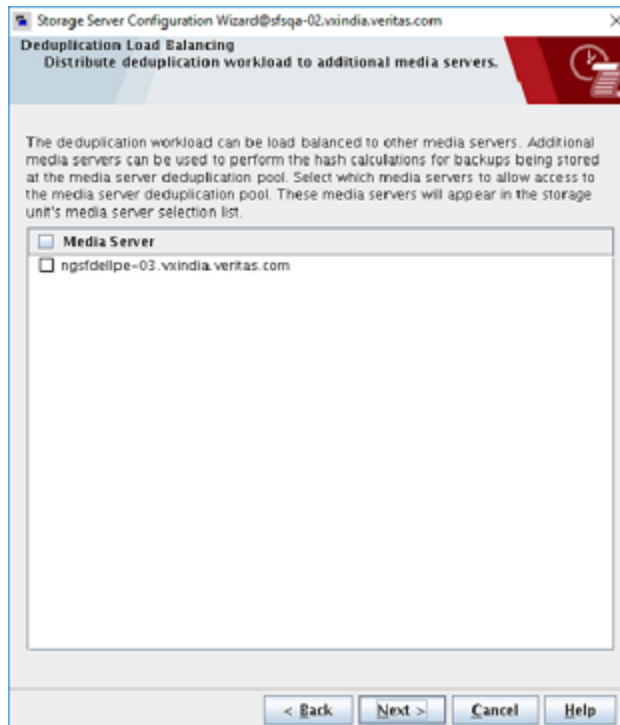
Interface:

Note: A NetBackup media server can have more than one network interface and by default the Operating System determines which one to use. To force NetBackup to connect through a specific network interface, specify the network host name of that interface.

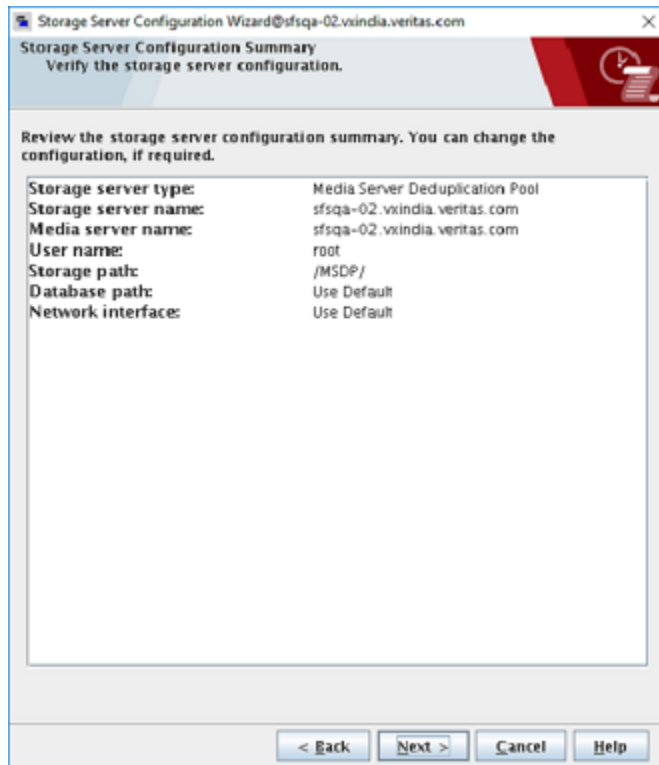
 Once you define the storage server details on this screen, you cannot modify them. For more information, click Help.

< Back Next > Cancel Help

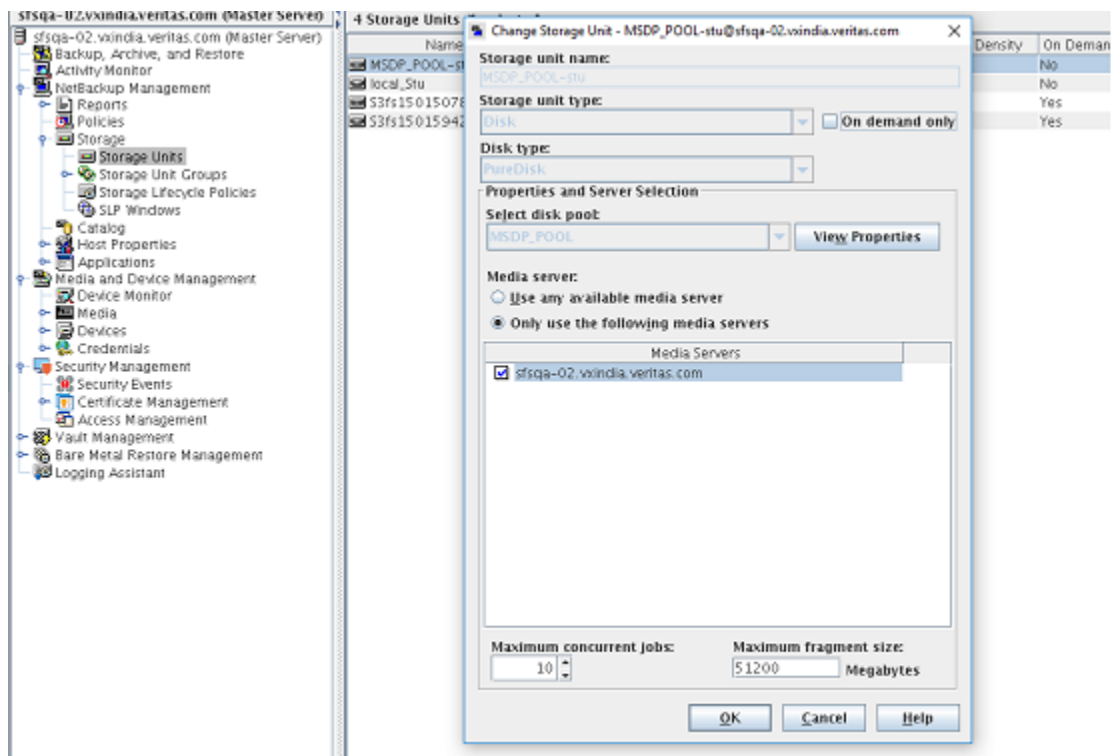
- 5 Enter the load balancing options to distribute the workload.



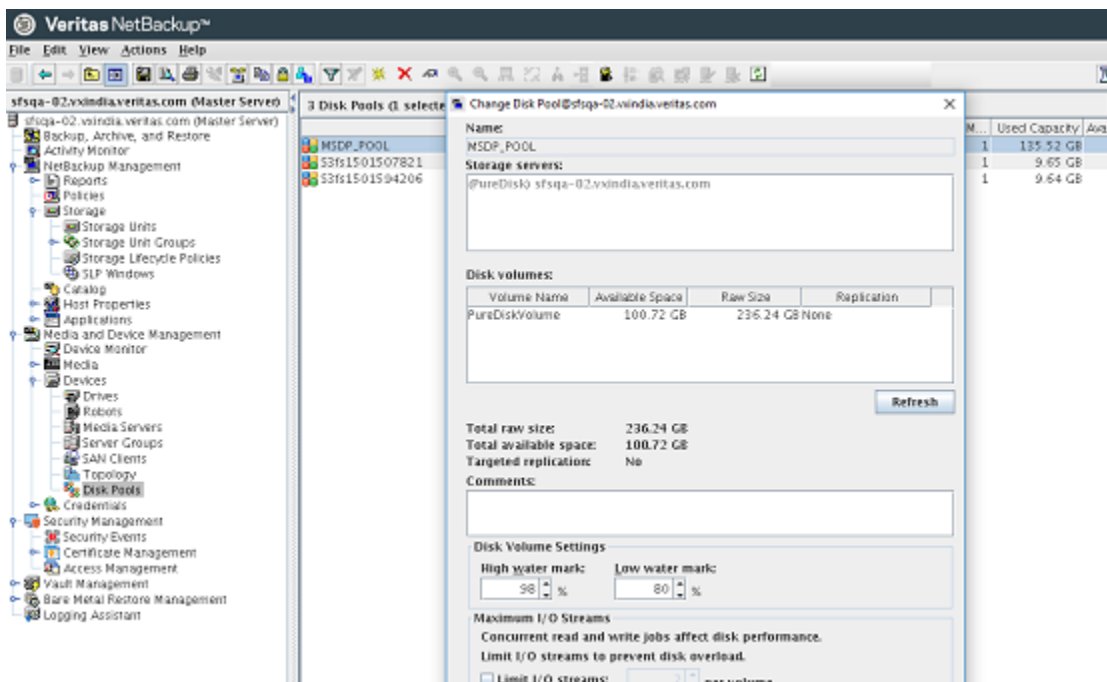
6 Verify the storage server configuration summary.



7 Verify that the storage unit is created for MSDP.



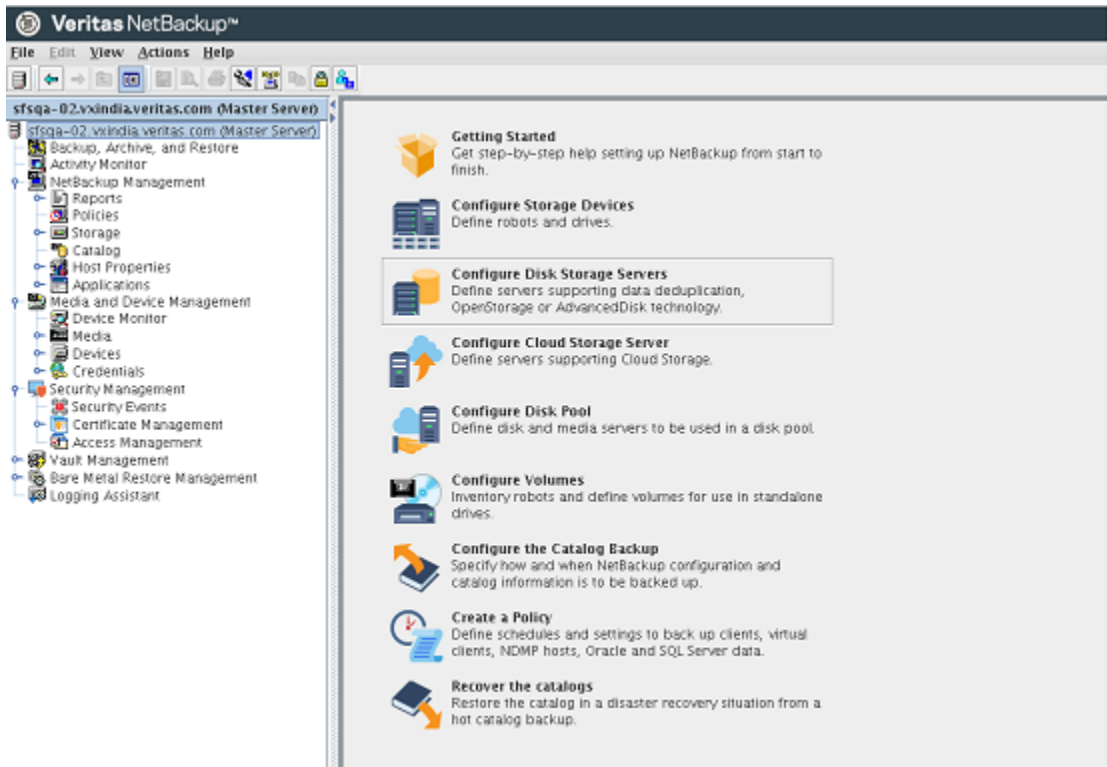
8 Verify that the disk pool is created for MSDP.



Creating an OST disk pool and STU in the NetBackup console

To create an OpenStorage Technology (OST) disk pool and storage unit (STU) in the NetBackup console

- 1 Log on to the NetBackup master server from the Java console.
- 2 Select **Configure Disk Storage Servers**.



- 3 Select the **OpenStorage** option from the **Select the type of disk storage that you want to configure** section of the dialog.



- 4 Add the following options to the **Storage Server Details**:

- **Storage server type:** OpenDedupe

Note: The **Storage server type** field is case-sensitive. **OpenDedupe** has to be entered exactly as shown in the screen shot.

- **Storage Server name:** The name in the <NAME></NAME> tag in the `/etc/sdfs/ostconfig.xml` file. This is `local` by default.

- **Username:** Anything can go in this field. It is not used.
- **Password/Confirm Password:** Anything can go in this field as well.

Storage Server Configuration Wizard@sfsqa-02.vxindia.veritas.com

Add Storage Server
Provide storage server details.

Select a media server that has the vendor's OpenStorage plug-in installed.
NetBackup uses this media server to determine the storage server capabilities.

Media server: sfsqa-02.vxindia.veritas.com

Storage server type: OpenDedupe
OpenDedupe

Storage server name: local2

Enter storage server credentials

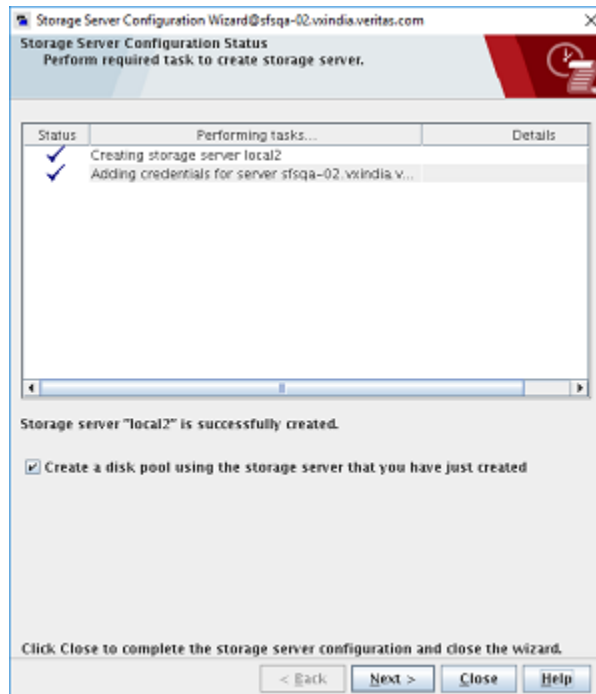
User name: root

Password: *****

Confirm password: *****

< Back Next > Cancel Help

- 5 Finish supplying entries for the storage configuration wizard and make sure **Create a disk pool using the storage server that you just created** is selected.



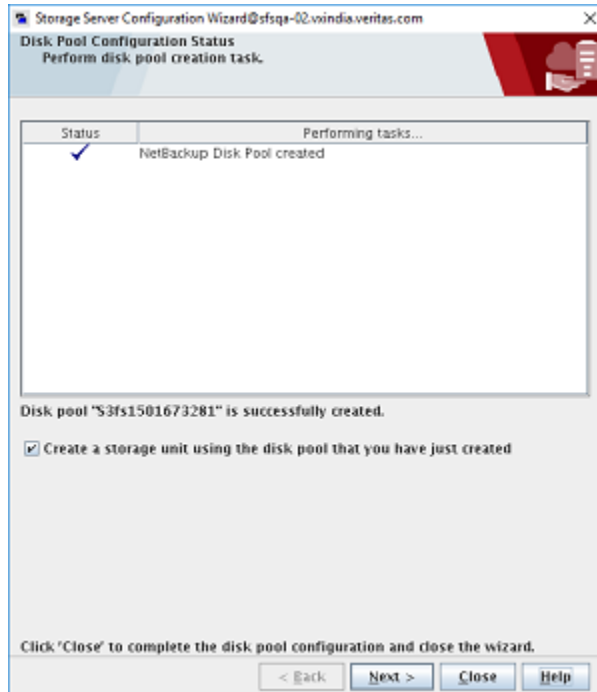
- 6 Select the storage pool that was just created.



- 7 Add a disk pool name.
- 8 Finish the wizard entries and select **Create a storage unit using the disk pool that you just created.**

- 9 In the **Storage Unit Creation** page, select **Only use the selected media servers** and select the media server that the storage was created on. For maximum concurrent jobs, select **8**.

Note: If you plan to run concurrent jobs for this STU, increase the **Maximum concurrent jobs** count to the desired value.



Storage Server Configuration Wizard@sfsqa-02.vxindia.veritas.com

Storage Unit Creation
Enter details to create storage unit.

Disk pool: 53fs1501673281

Storage server type: OpenDedupe

Storage unit name: 53fs1501673281-stu

Media Server

☐ Use any available media server to transport data

☒ Only use the selected media servers:

Media Servers

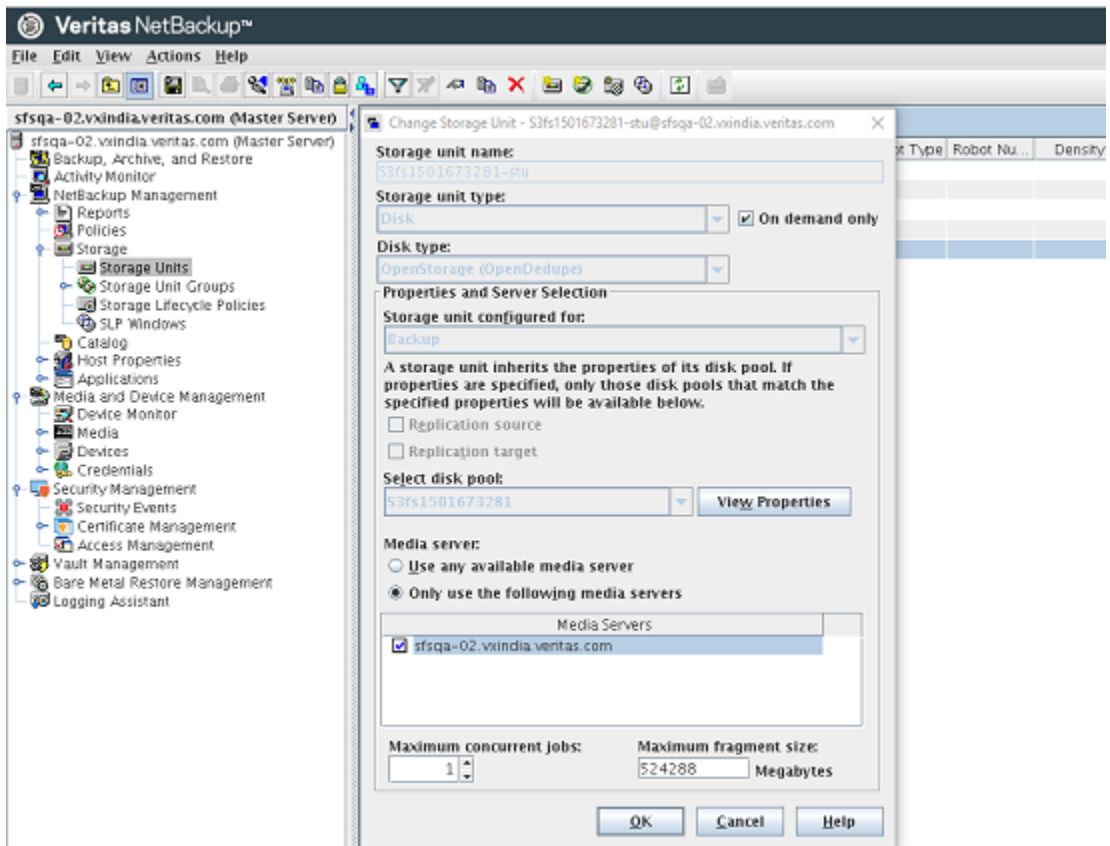
☒ sfsqa-02.vxindia.veritas.com

Maximum concurrent jobs: 1

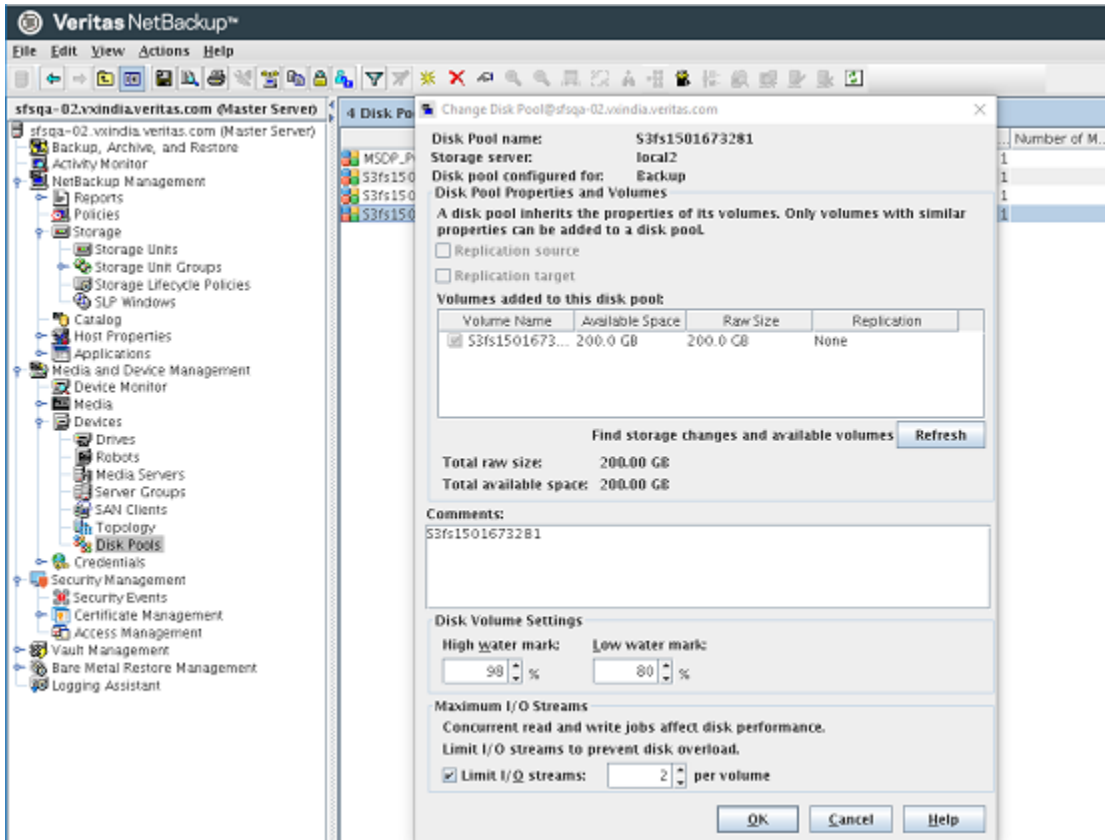
Maximum fragment size: 524288 Megabytes

< Back Next > Cancel Help

10 Verify that the storage unit is added.



11 Verify that the disk pool is added.



Setting up multiple NetBackup media servers in the same domain

To set up the OST connector on multiple NetBackup media servers in the same domain, additional steps must be taken on each NetBackup media server before adding the storage pools in NetBackup.

To set up multiple NetBackup media servers in the same domain

- 1 Follow the instructions for setting up the OST connector on each media server that uses the OST connector.

See [“Backing up deduplicated data \(OpenDedup and NetBackup\) using the S3 protocol to Veritas Access”](#) on page 48.

- 2 Edit `/etc/sdfs/ostconfig.xml` and change the `<name>` tag to something unique in the NetBackup domain, such as the host name with an incremented number, for example:

```
<NAME>hostname-0</NAME>
```

- 3 Follow the instructions in the “Creating an OST disk pool and STU in the NetBackup console” section and use the name in the `<NAME>` tag as the **Storage Server** name.

See [“Creating an OST disk pool and STU in the NetBackup console”](#) on page 64.

See [“Backing up deduplicated data \(OpenDedup and NetBackup\) using the S3 protocol to Veritas Access”](#) on page 48.

Setting up multiple SDFS volumes on a NetBackup media server

The OST connector supports multiple SDFS volumes on the same media server, but additional steps are required to support this configuration.

To set up multiple SDFS volumes on a NetBackup media server

- 1 Follow the instructions for setting up the OST connector on each NetBackup media server that uses the OST connector.

See [“Backing up deduplicated data \(OpenDedup and NetBackup\) using the S3 protocol to Veritas Access”](#) on page 48.

- 2** Edit the `/etc/sdfs/ostconfig.xml` and add a new `<CONNECTION>` tag inside of the `<CONNECTIONS>` tag for the new volume.

Add a name that is unique to the `<NAME>` tag and specify the new volume name in the `<LSU_NAME>` tag (pool1).

In the new `<CONNECTION>` tag, add the port number identified by running the `mount` command to the `<URL>` tag (`http://localhost:6443/`) as shown in the example output.

```
[root@host1 ~]# mount | grep opendedupe
sdfs:/etc/sdfs/S3fs1497346133-volume-cfg.xml:6443 on
/opendedupe/volumes/S3fs1497346133 type fuse
(rw,nosuid,nodev,allow_other,allow_other)
sdfs:/etc/sdfs/S3fs1497258807-volume-cfg.xml:6442 on
/opendedupe/volumes/pool1 type fuse
(rw,nosuid,nodev,allow_other,allow_other)
```

The following is a complete example of an `ostconfig.xml` file with two volumes.

```
<!-- This is the config file for the OST connector for opendedup and Netbackup -->
<CONNECTIONS>
<CONNECTION>
<!--NAME is the local server name that you will reference within Netbackup -->
<NAME>
local
</NAME>
<LSU_NAME>
svol4
</LSU_NAME>
<URL>
http://localhost:6442/
</URL>
<!--PASSWD - The password of the volume if one is required for this sdfs volume -->
<PASSWD>admin</PASSWD>
<!--
<SERVER_SHARE_PATH>
A_SUBDIRECTORY_UNDER_THE_MOUNT_PATH
</SERVER_SHARE_PATH>
-->
</CONNECTION>
<!-- Below is the new volume-->
<CONNECTION>
<!--NAME is the local server name that you will reference within Netbackup -->
<NAME>
```

```
hostname0
</NAME>
<LSU_NAME>
svoll10
</LSU_NAME>
<URL>
http://localhost:6443/
</URL>
<!--PASSWD - The password of the volume if one is required for this sdfs volume -->
<PASSWD>admin</PASSWD>
<!--
<SERVER_SHARE_PATH>
A_SUBDIRECTORY_UNDER_THE_MOUNT_PATH
</SERVER_SHARE_PATH>
-->
</CONNECTION>
</CONNECTIONS>
```


Configuring Veritas Access as a cloud storage server with NetBackup CloudCatalyst

This chapter includes the following topics:

- [Creating an S3 bucket on Veritas Access for storing deduplicated backup data from NetBackup](#)
- [Configure Veritas Access as a cloud storage server on NetBackup server using CloudCatalyst](#)
- [Enabling SSL on Veritas Access](#)

Creating an S3 bucket on Veritas Access for storing deduplicated backup data from NetBackup

To create an S3 bucket on Veritas Access for storing deduplicated backup data from NetBackup

- 1 Log on to the Veritas Access GUI as the master user using the following URL:

`https://Veritas Access Management console IP:14161/.`

You can obtain the Veritas Access Management console IP by logging on to the Veritas Access command-line interface using the `su - master` command on the Veritas Access cluster.

- 2 Create a storage pool for the S3 buckets.

Click **NAS Infrastructure** in the GUI navigation on the left.

Select the disks that you want to use for the S3 bucket, and click the **Add to Storage Pool** button to invoke the wizard for storage pool creation.

Follow the steps in the wizard for creating a new storage pool or adding the disks to an existing pool.

- 3 Click **Settings > User Management > Configure Active Directory** to configure AD.

Enter the required information, such as the **DNS Domain**, **DNS Name Servers**, **AD Domain**, **AD Domain Controller**, and the **AD Admin** and **Password**.

- 4 Click **Settings > S3 Management** to configure and enable the S3 server.

Edit the default parameters that are required for the S3 server, such as the storage pool name, underlying S3 bucket layout, and the default size of the bucket.

If you want to enable SSL, See [“Enabling SSL on Veritas Access”](#) on page 97.

- 5 Click the button in front of **S3 Server Status** to start the S3 server.

- 6 Log out from the GUI, and log in again as an AD user.

Click on the **Create keys** button to generate the access key and the secret key for the Veritas Access S3 bucket.

Save the access key and secret key in a safe location, as Veritas Access does not allow retrieval of keys after initial creation.

Note: Log in using the `domainname\username` format.

- 7 Log out from the GUI, and log in again as the master user.
- 8 Registration of supported public cloud service is optional, and is only required in case you need to add an AWS cloud as a storage tier. Without this, backups are stored locally in Veritas Access S3 buckets.

Click **Settings > Cloud Storage Registration > Add Cloud Subscription** to register the supported public cloud service.

Enter information for the cloud service provider, name of subscription, access key, and secret key.

- 9 Activate the long-term data retention (LTR) policies.

Click **Policies > LTR Policy**.

Click **Activate** for either the **LTR On-Premises + Cloud** policy or the **LTR On-Premises** policy and provide the storage pool when prompted.

- 10 Provision the NetBackup bucket using the policy.

Under **Quick Actions**, click **Provision Storage**. Select **S3 Storage for NetBackup** and click **Next**.

Provide the bucket size, underlying layout of the bucket, the access key, and the secret key of the Veritas Access S3 server generated as the AD user in step 6.

If you selected the **LTR On-Premises + Cloud** policy, add information such as which data should be moved to the AWS cloud tier, AWS region, cloud tier type (S3/Glacier), and when the data movement to the cloud should occur.

- 11 Monitor the progress of the task under **Recent Activity**.

Make a note of the scale-out file system name that was used for the bucket creation.

- 12 Click **File Systems**.

For the scale-out file system that is created, ensure that the **S3 Bucket** column displays **Yes** to indicate that the S3 bucket is enabled.

You may need to wait for some time for this change to be reflected in the GUI.

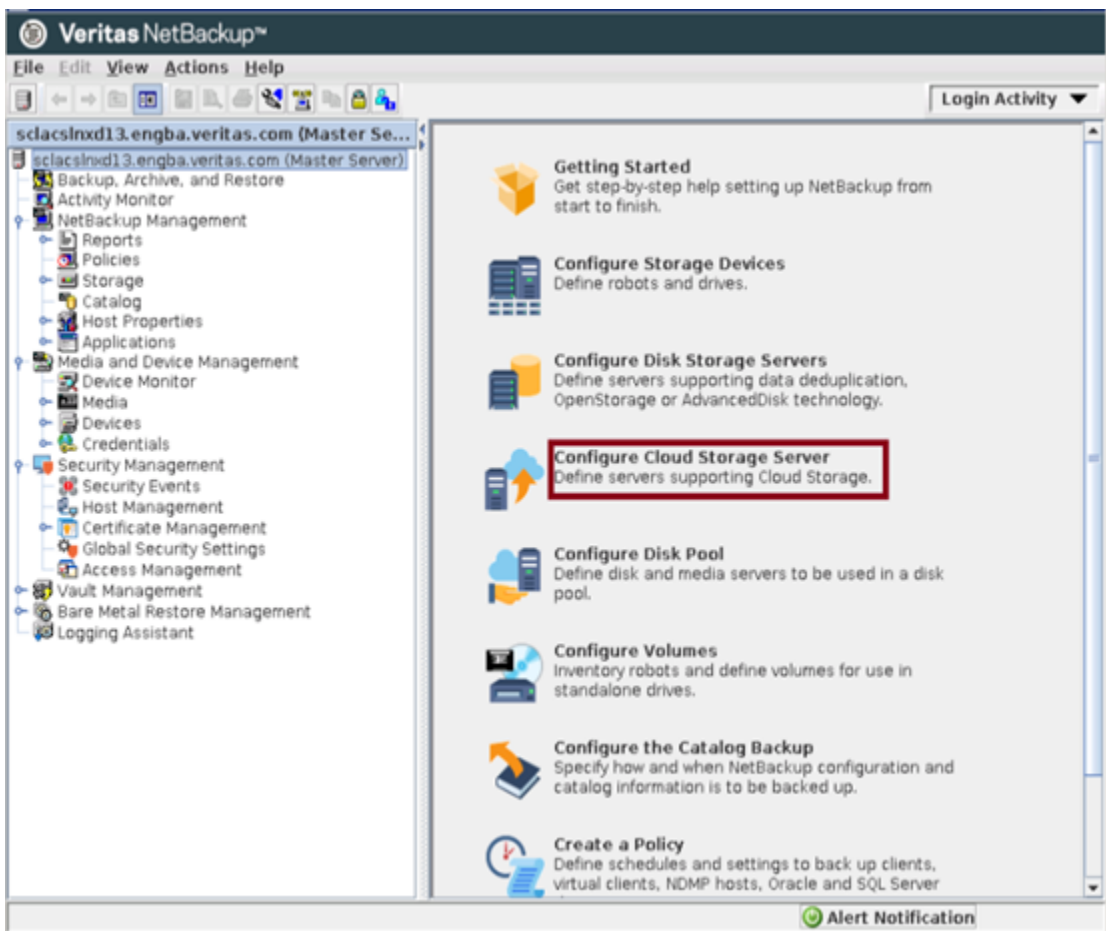
Creating a Media Server Deduplication Pool (MSDP) for primary backup using NetBackup

To create a Media Server Deduplication Pool (MSDP) for primary backup using NetBackup, See [“Creating a Media Server Deduplication Pool \(MSDP\) for primary backup using NetBackup”](#) on page 56.

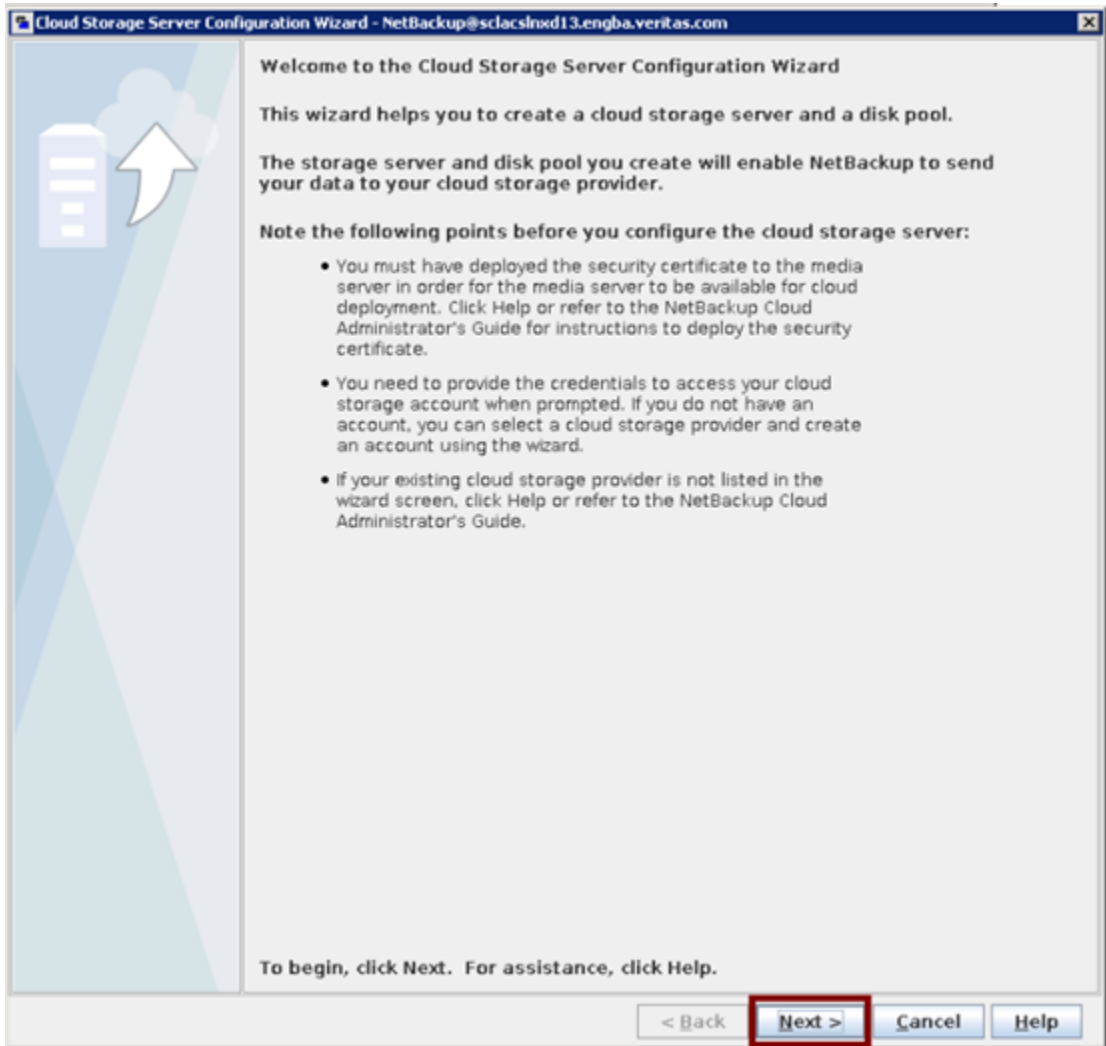
Configure Veritas Access as a cloud storage server on NetBackup server using CloudCatalyst

To configure the Veritas Access cluster as a cloud storage server and create an OpenStorage Technology (OST) disk pool and storage unit (STU) from the NetBackup console

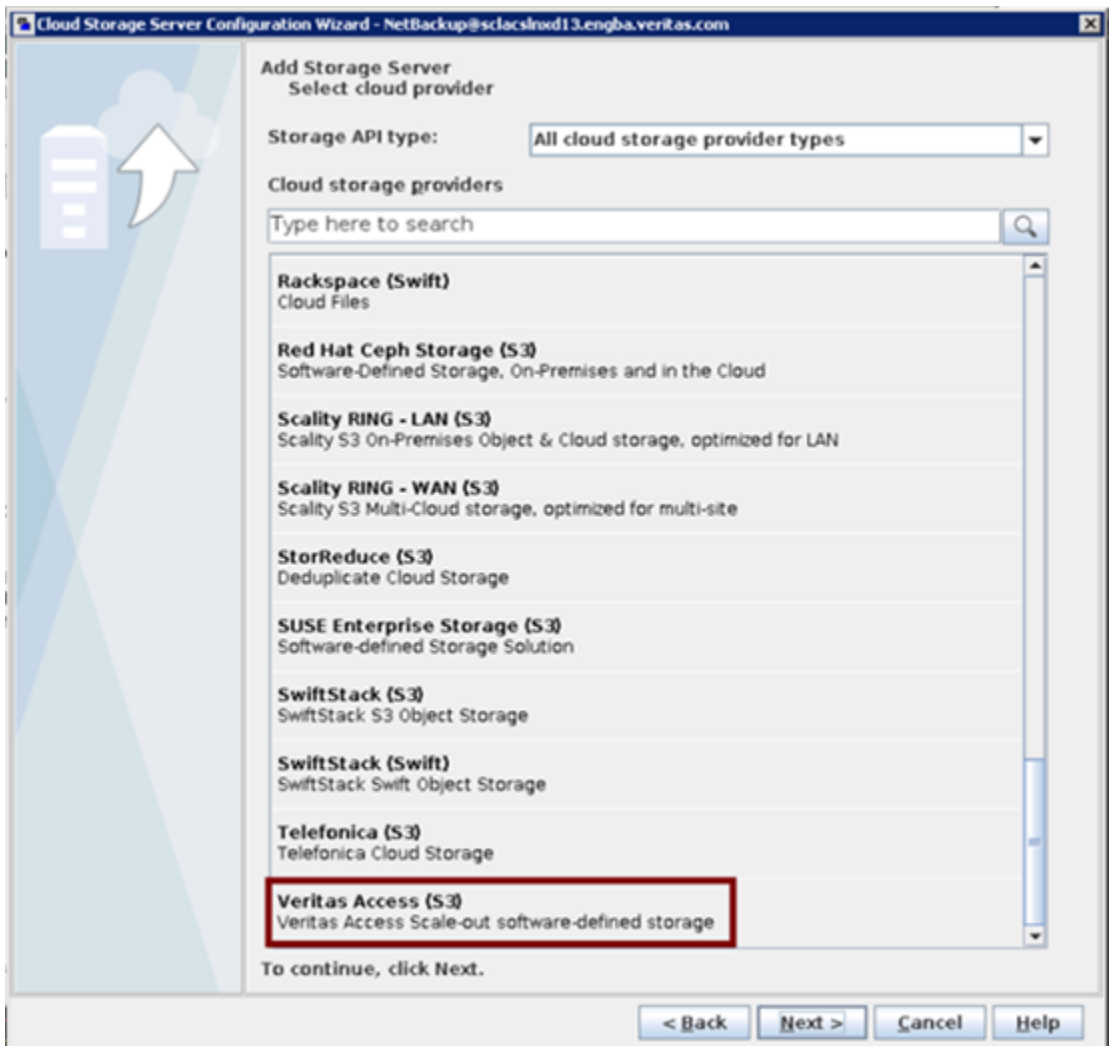
- 1 Log on to the NetBackup master server from the Java console.
- 2 Select **Configure Cloud Storage Servers**.



- 3 The **Welcome to cloud storage server configuration** wizard appears. Click **Next**.



- 4 Select **Veritas Access** in the cloud provider list. Click **Next**.



- 5 On the **Add storage server** form, click on **Add Cloud Storage**.

Cloud Storage Server Configuration Wizard - NetBackup@sciacslnxd13.engba.veritas.com

Add Storage Server
Select a media server and provide cloud storage service credentials. To be listed below in the media server drop-down list a security certificate must be deployed and NetBackup must be running including the NetBackup CloudStore Service Container (nbcss).

Cloud storage provider - Veritas Access

Service host:

Storage server name:

Add Cloud Storage

Media server name:


Deduplication
☐ Enable NetBackup CloudCatalyst

Local cache directory:

Access details for Veritas Access account

Access key ID:

Secret access key:

 If you do not have Veritas Access account [Create an account with Veritas Access.](#)

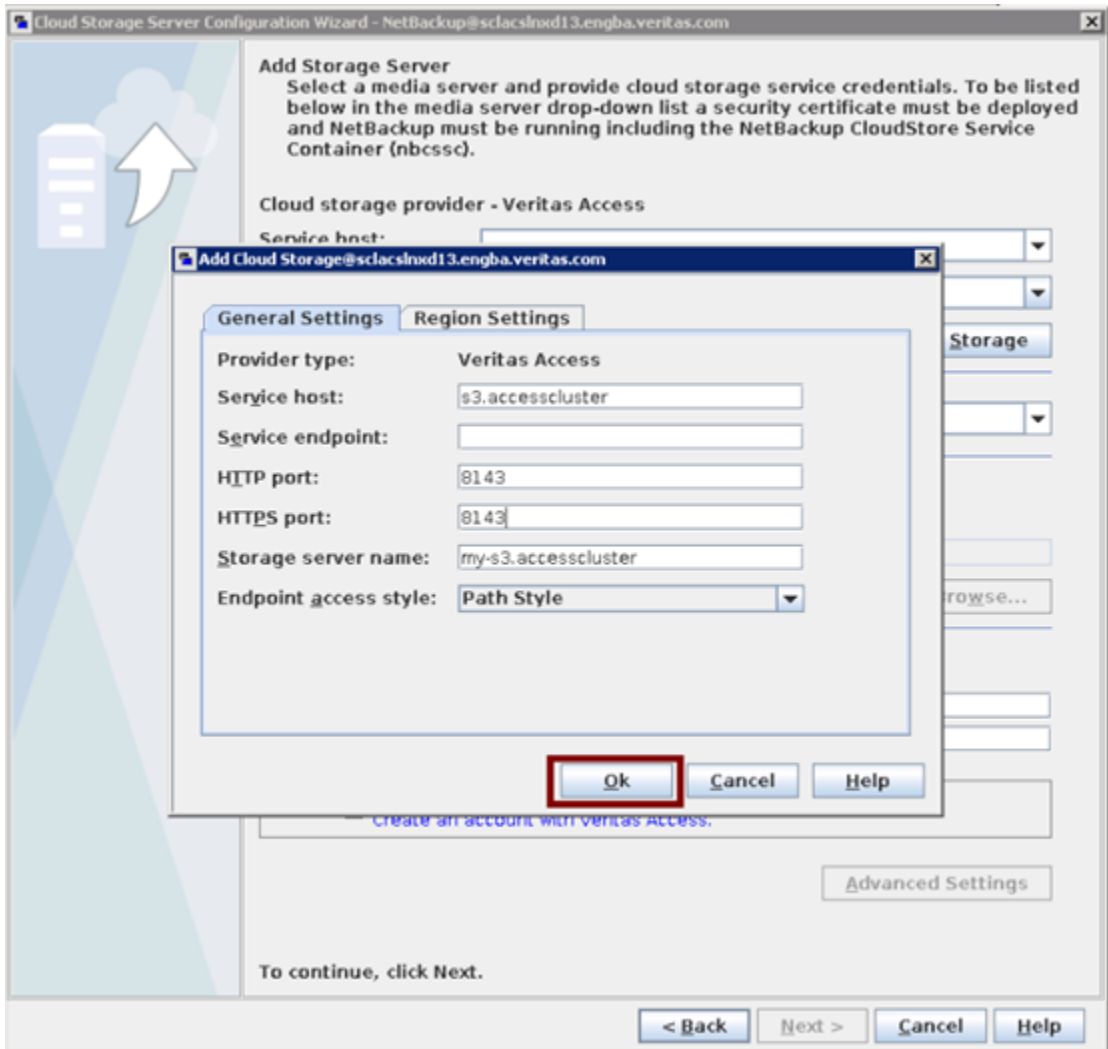
To continue, click Next.

- 6 In the **Add cloud storage** wizard, enter the required information.
- **Service host:** s3.<veritas_access_cluster_name>
 - **HTTP port:** 8143
 - **HTTPS port:** 8143
 - **Storage server Name:** Any string or any auto-generated name.

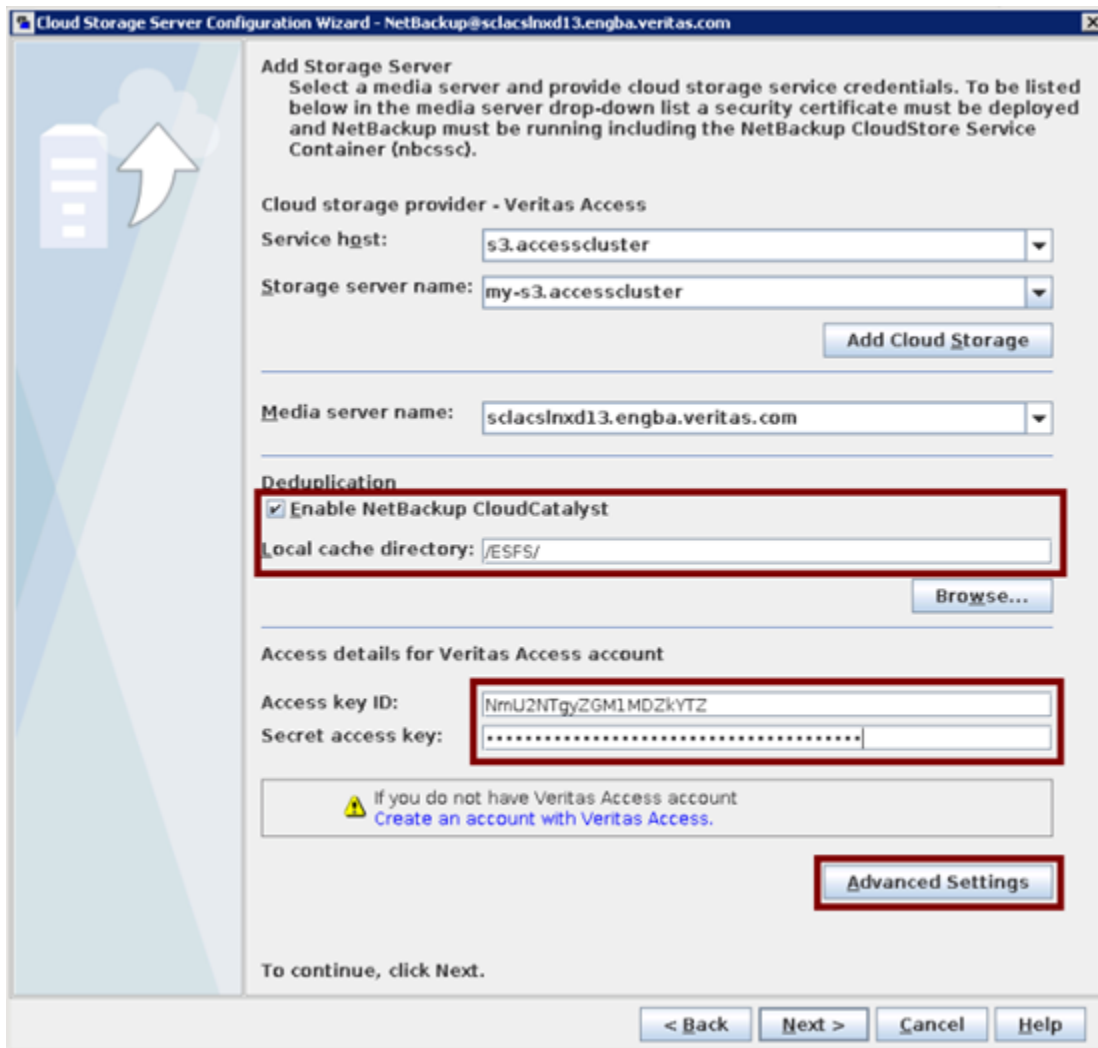
For example, `my-s3.<veritas_access_cluster_name>`

Click **Ok**.

Note: If DNS is not configured, you have to add an entry in the `/etc/hosts` file on the NetBackup master server and the CloudCatalyst media server.



- 7 Select **Media server** from the **Media server name** drop-down box. Select the **Enable NetBackup CloudCatalyst** check box if you want to store the deduplicated MSDP backup data on Veritas Access's ObjectAccess bucket. Specify the path of the local cache directory for CloudCatalyst. Enter the access key and secret key using which you created the bucket is on Veritas Access. For SSL-related settings, click on **Advance Settings**.



Cloud Storage Server Configuration Wizard - NetBackup@sciacslnxd13.engba.veritas.com

Add Storage Server
 Select a media server and provide cloud storage service credentials. To be listed below in the media server drop-down list a security certificate must be deployed and NetBackup must be running including the NetBackup CloudStore Service Container (nbcssc).

Cloud storage provider - Veritas Access

Service host:

Storage server name:

Media server name:

Deduplication


☒ Enable NetBackup CloudCatalyst

Local cache directory:

Access details for Veritas Access account

Access key ID:

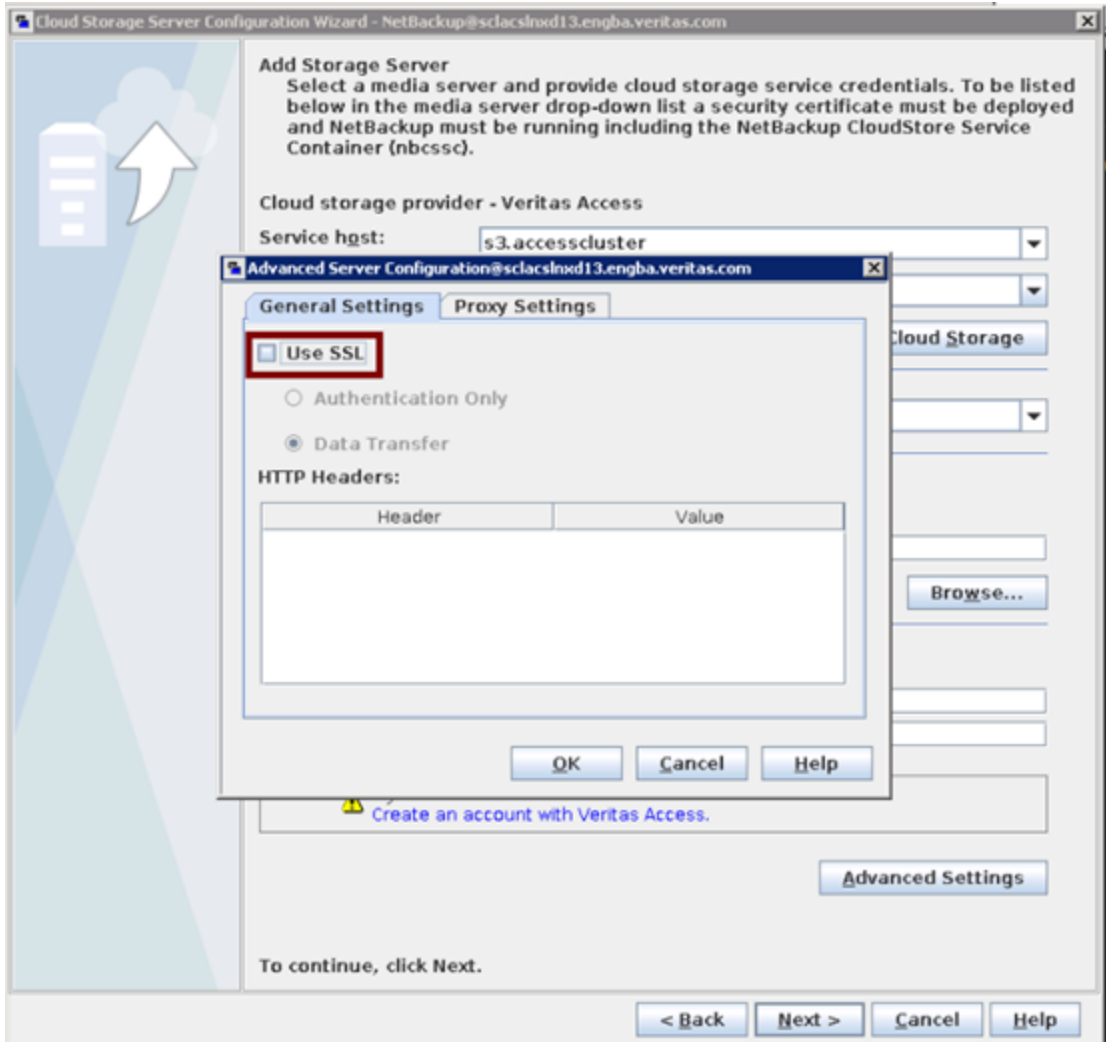
Secret access key:

 If you do not have Veritas Access account [Create an account with Veritas Access.](#)

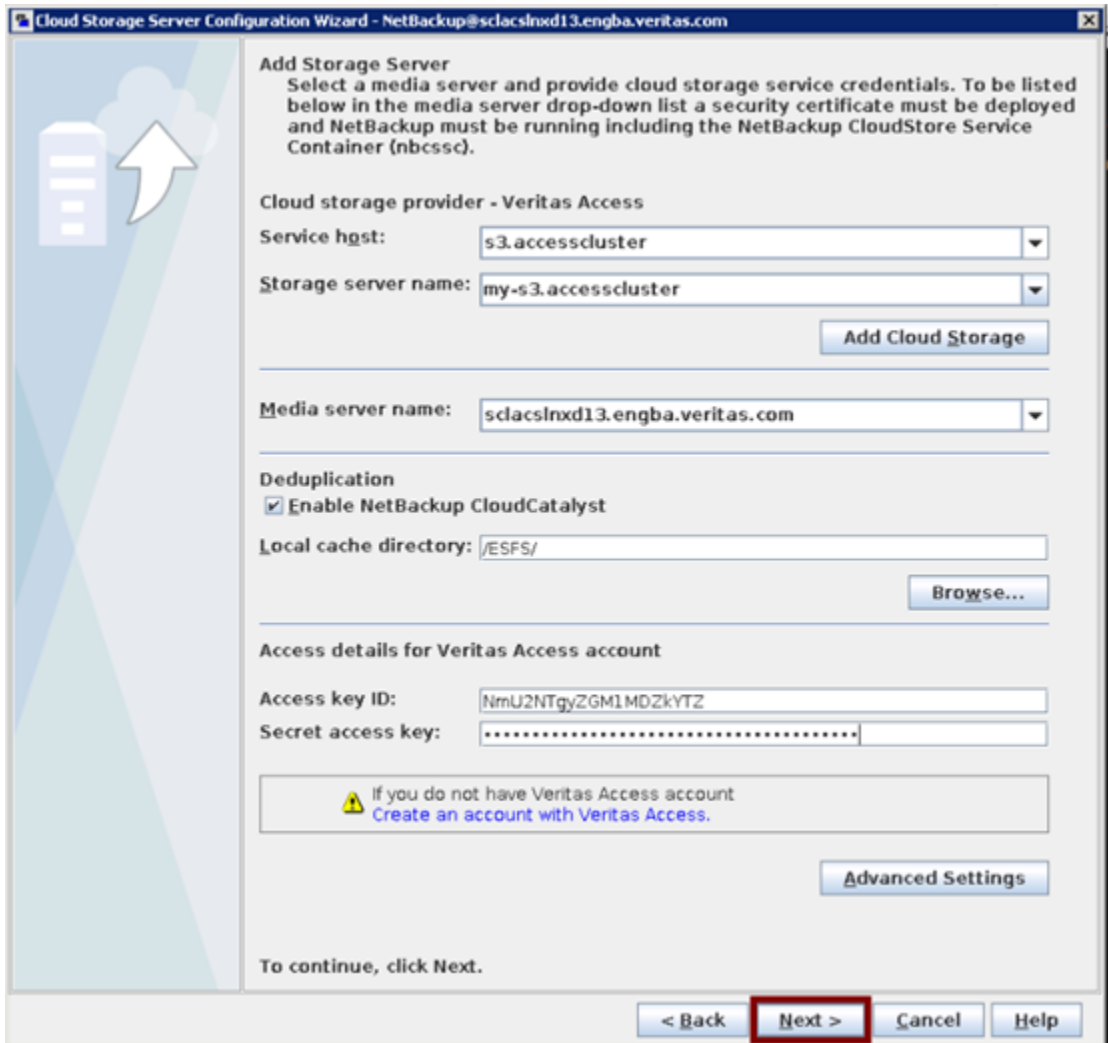
To continue, click Next.

- 8 If the Veritas Access ObjectAccess server is configured with **No SSL**, then clear the **Use SSL** check box and click **Ok**.

To enable SSL, See [“Enabling SSL on Veritas Access”](#) on page 97.



9 Click Next.



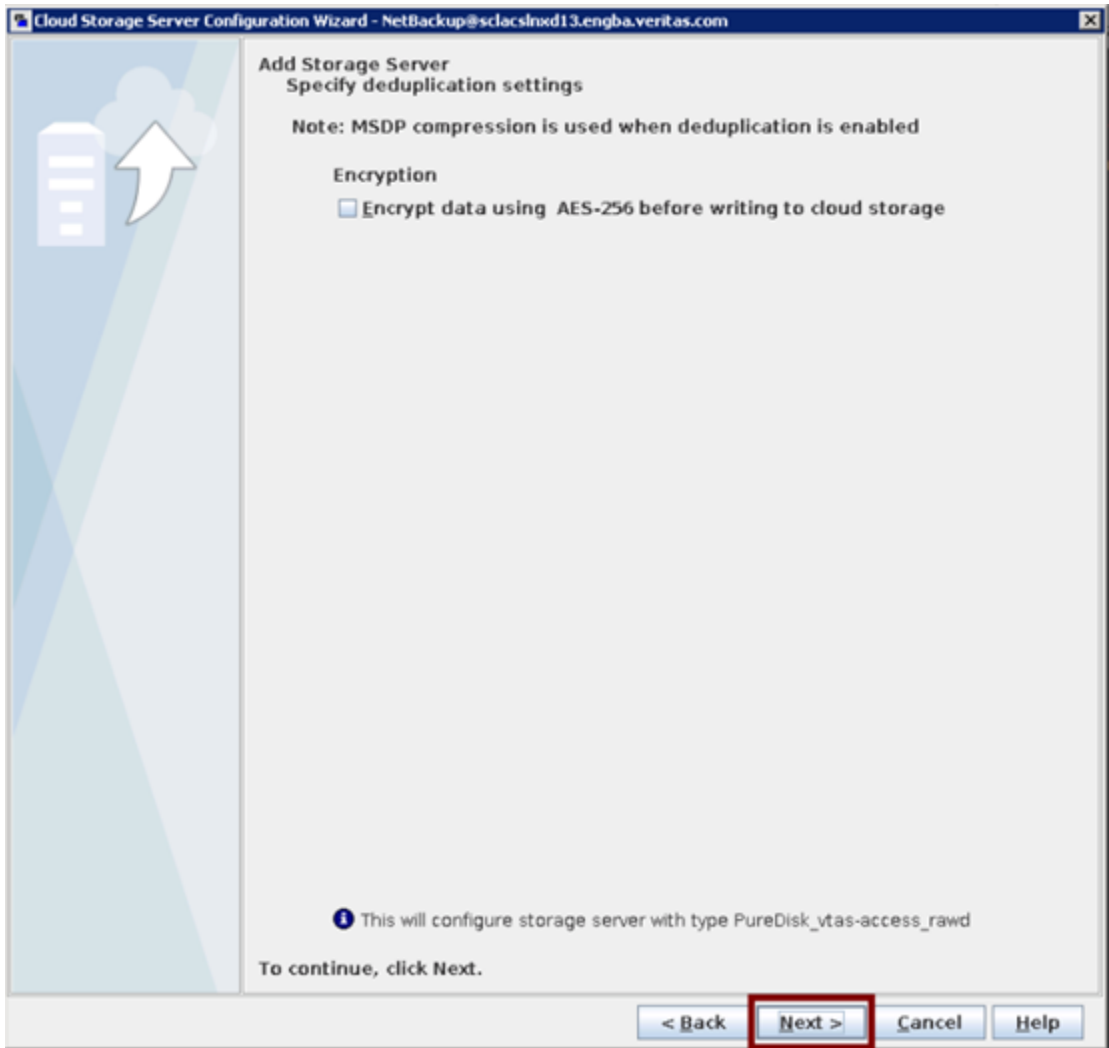
The image shows a 'Cloud Storage Server Configuration Wizard' window. On the left is a decorative graphic with a server icon and an upward arrow. The main area contains the following sections:

- Add Storage Server**
Select a media server and provide cloud storage service credentials. To be listed below in the media server drop-down list a security certificate must be deployed and NetBackup must be running including the NetBackup CloudStore Service Container (nbcssc).
- Cloud storage provider - Veritas Access**
Service host: s3.accesscluster
Storage server name: my-s3.accesscluster
[Add Cloud Storage]
- Media server name:** slacslnxd13.engba.veritas.com
- Deduplication**
☒ Enable NetBackup CloudCatalyst
Local cache directory: /ESFS/ [Browse...]
- Access details for Veritas Access account**
Access key ID: NrmU2NTgyZGM1MDZkYTZ
Secret access key: [masked]
[If you do not have Veritas Access account Create an account with Veritas Access.]
- [Advanced Settings]

To continue, click Next.

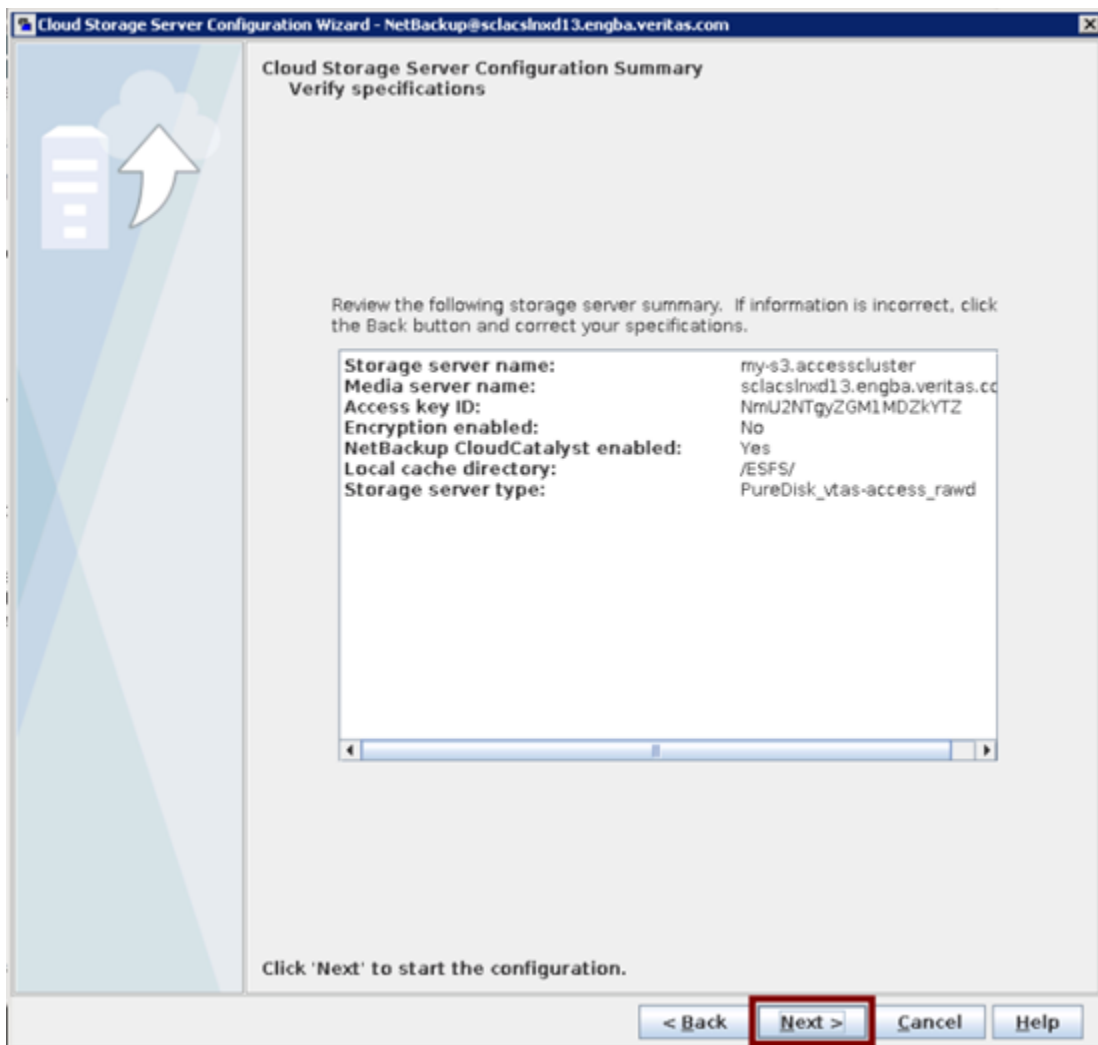
At the bottom are buttons: < Back, Next > (highlighted with a red box), Cancel, and Help.

10 On the **Specify Deduplication setting** form, click **Next**

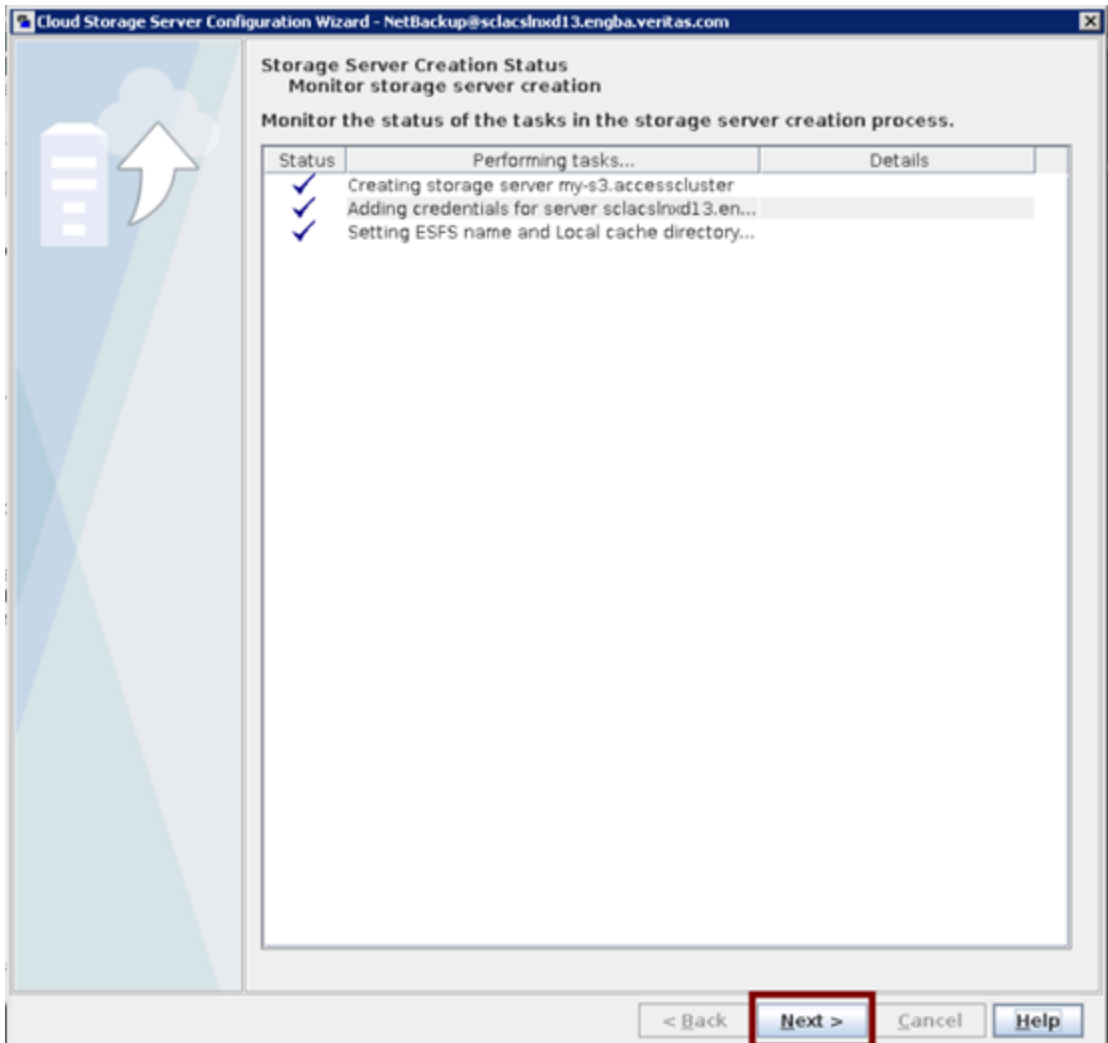


11 Messages related to setting the encryption appear. Click **Yes**.

12 Review the Cloud storage server summary and click **Next**.



- 13 Check the status of the tasks in the storage server creation process. Click **Next**.



- 14 Verify that the storage server is successfully created and click **Next**.

- 15 The **Volume selection to use in disk pool** form lists all the buckets that are created by a user on the Veritas Access cluster as a volume. If the bucket is not created from Veritas Access, then click on **Add volume** and specify the bucket name. After bucket creation, the bucket is listed as a volume. Select a bucket and click **Next**.

Disk Pool Configuration Wizard@sclacslnxd13.engba.veritas.com

Volume Selection
 Select volumes to use in the disk pool.

Storage server type: PureDisk_vtas-access_rawd

Select storage server volumes to add to the disk pool.

Volume Name	Available Space	Raw Size	Replication	Region
<input checked="" type="checkbox"/> testappbkt	---	---	None	Default
<input type="checkbox"/> tests3	---	---	None	Default

Add new volume on the selected storage server(s) **Add New Volume**

Disk Pool Size
 Total available space: ---
 Total raw size: ---

i Before selecting a volume, you must validate if it is shared among the storage servers.

< Back **Next >** Cancel Help

- 16** In the **Additional disk pool information** form, enter the disk pool name and click **Next**.

Disk Pool Configuration Wizard@sciacslnxd13.engba.veritas.com

Additional Disk Pool Information
Provide additional disk pool information.

Storage server type: PureDisk_vtas-access_rawd

Disk Pool Size

Total available space: ---

Total raw size: ---

Disk Pool name: accessbkt_pool

Comments:

High water mark: 98 %

Low water mark: 80 %

i The High water mark and Low water mark values are not applicable for this disk group.

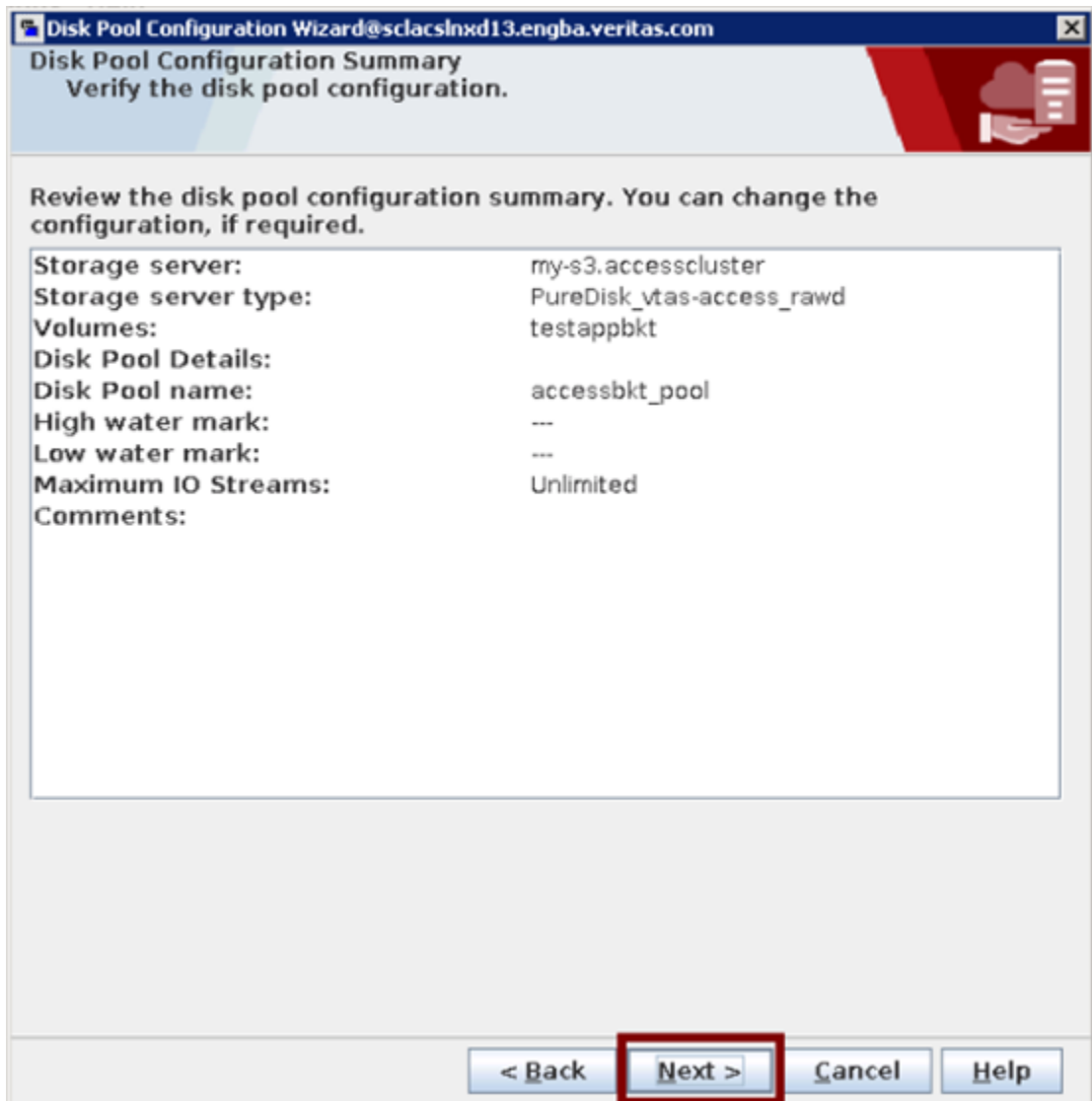
Maximum I/O Streams

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

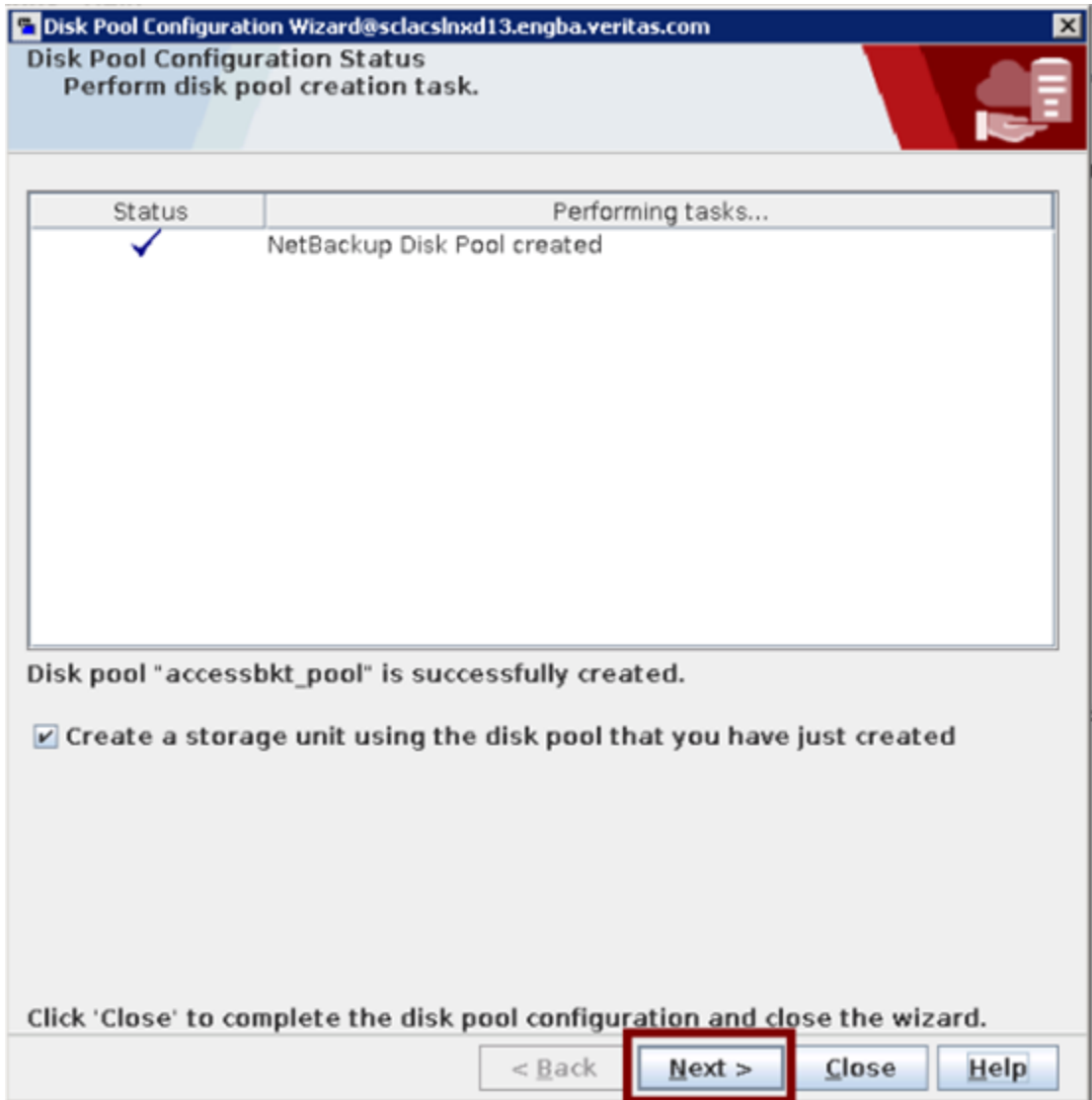
☐ Limit I/O streams: -1 per volume

< Back **Next >** Cancel Help

17 Review the disk pool configuration summary and click **Next**.



- 18 In the **Disk pool creation status** form, verify that the disk pool is created successfully. Make sure that the **Create a storage unit using the disk pool that you have just created** check box is selected.



- 19 In the **Storage unit creation** wizard, enter the storage unit name. Click **Only use the selected media servers**. Select the media server in the list and click **Next**.

Disk Pool Configuration Wizard@sclacslnxd13.engba.veritas.com

Storage Unit Creation
Enter details to create storage unit.

Disk pool: accessbkt_pool

Storage server type: PureDisk_vtas-access_rawd

Storage unit name: accessbkt_pool-stu

Media Server

☐ Use any available media server to transport data

☒ Only use the selected media servers:

Media Servers

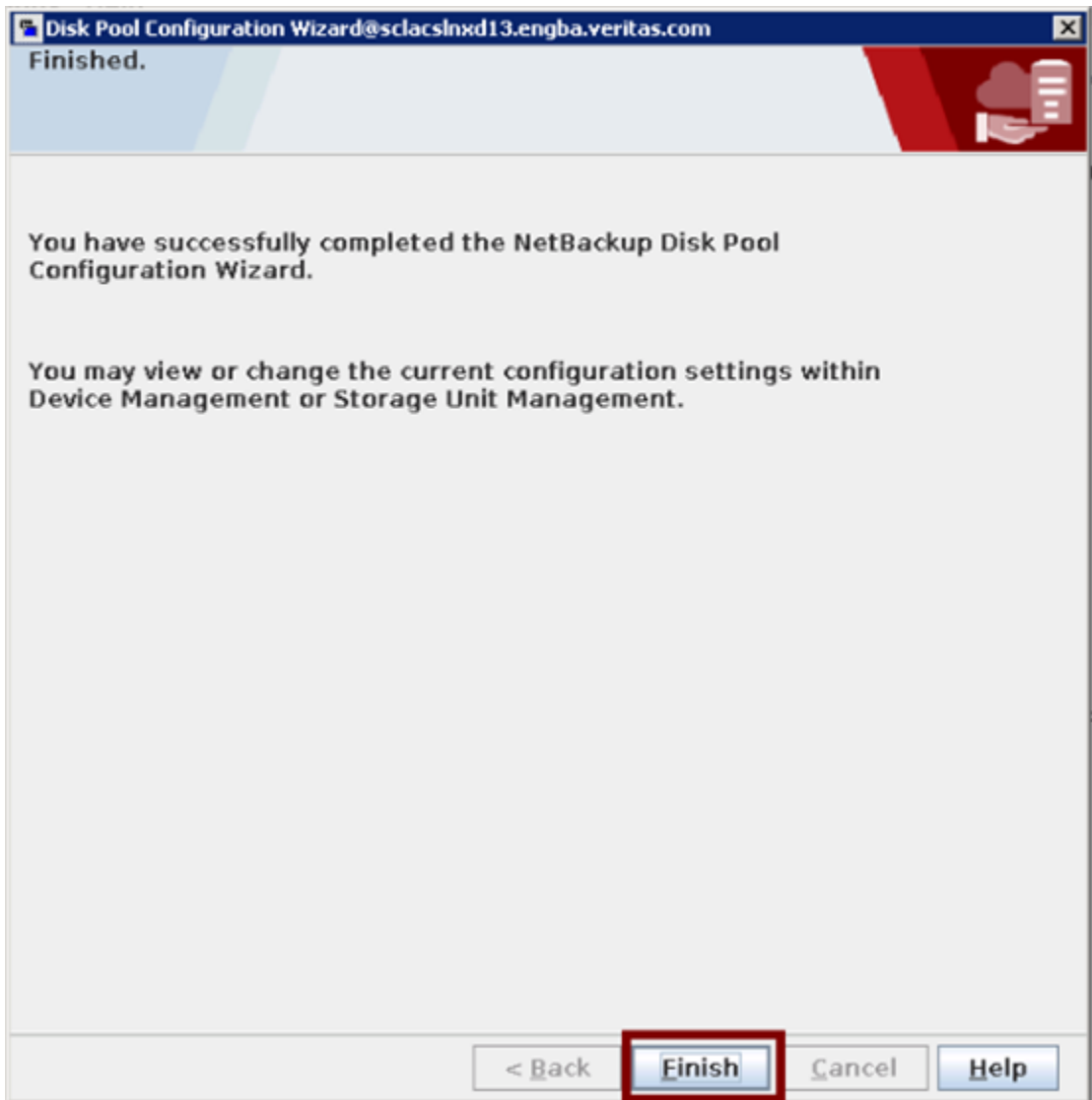
☒ sclacslnxd13.engba.veritas.com

Maximum concurrent jobs: 1

Maximum fragment size: 51200 Megabytes

< Back Next > Cancel Help

- 20 Verify that the disk pool creation wizard completes successfully. Click **Finish**.



Enabling SSL on Veritas Access

To enable SSL on Veritas Access using the Veritas Access GUI

- 1 Log on to the Veritas Access GUI and click on **Settings > S3 Management**.
- 2 Click the **Edit** button at the top.
- 3 Click **Yes** under the **Enable SSL** button. This automatically creates a certificate on Veritas Access in the `/shared/ptgwy/cacert.pem` directory.

To enable SSL on Veritas Access using the Veritas Access command-line interface

- ◆ Enable SSL on Veritas Access.

```
Objectaccess > set ssl_enabled yes
```

```
Objectaccess > server stop
```

```
Objectaccess > server start
```

To copy the certificate to NetBackup

- 1 Go to the bash prompt of the cluster node and copy the following content from the `/shared/ptgwy/cacert.pem` file and append it to the `/usr/openv/netbackup/db/cloud/cacert.pem` on the NetBackup master and media servers.

```
-----BEGIN CERTIFICATE-----
```

```
MIIDjTCCAnWgAwIBAgIJANFjuMEDS0LRMA0GCSqGSIb3DQEBCwUAMF0xCzAJBgNV  
BAYTA1VTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRAwDgYDVQQKDAdWZXJpdGFzMQ8w  
DQYDVQQQLDAZBY2Nlc3MxFjAUBgNVBAMMDXMzM5idTg3M1lhchAwHhcnMTgwMTAz  
MTAwODAxWhcnMjEwMTAyMTAwODAxWjBdMQswCQYDVQQGEwJVUzETMBEGA1UECAwK  
Q2FsaWZvcm5pYTEQM4GA1UECgwHVmVyaXRhczEPMA0GA1UECwwGQWNjZXNzMRYw  
FAYDVQQDDA1zM5YnU4NzItYXBwMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB  
CgKCAQEAl+Xkh9Buzz2KRYsoBbKxOExq2fRDhfTb1lp1leimN/1cryvMkguEFkFk  
kjuTsi3lnuj0Sc5/Fimzfnc1XyvI9uWAB07wdxwjKFB1g0GvxSa/obQ/SMG8fEHL  
qYl/baJKPoz7xvg+QJd/3A1ZJqLvA1i7DEErVuUyNrtjxKnPNIKzzRhBg9M5+HPp  
b4ZOXUnFWU9w4Ci1JBvYTBQ5X2wtGx9cLtHb9ff9XTv2SqWUuRoGDC2DYlgo8j2n  
AsTWzk+mJw12wRcE00FoB1YhOCNJ1Xk14n4VSKbTUdCmkm6Ej5Yf+AIAbLiQNfGv  
Sralc5TFMHjUUg5dgbPizCLTmuQz8QIDAQABolAwTjAdBgNVHQ4EFgQUgBpm7gK1  
q/M/3+Y0st8m2EMzulgwHwYDVR0jBBgwFoAUgBpm7gK1q/M/3+Y0st8m2EMzulgw  
DAYDVR0TBAAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAcw4QIFxIuJMY/6BGBVAA  
dnrRG11+hcZHfbQVeDV9ApijEe/qiIx8QLL9fDx8MqsdIIHcgfuv5mzAQZwa+tH  
7USIqBfxfEytnKBuAYbYyOfXKJDUIAaWFjcM0rOP1z+Dv6zf7B65Mv3aKD1rENFT  
UgPBphLACAU9CzLidJkoE3izOaZbiys/r24yRR8X/Pugsxy7VESN6WSqzYg0jdSf  
iCJkGLEdOYceE85NhW8eaCsffqCkxoskTgulNnf4j01MYP5d+4U8uAEC/uLrndD3Rn
```

n7MB0EeciPgqWZQWNLjyQNNZ/F58wlyTtHv48VMlZXhIJBhjUwFZAEAg43R5n67o

Pw==

-----END CERTIFICATE-----

- 2** Stop and start the services on the master using the following commands in the `/usr/opensv/netbackup/bin` directory.

```
# bp.kill_all -f -v
# bp.start_all
```

- 3** Log into the media server. Stop and start the services on the media server using the following commands:

```
# bp.kill_all -f -v
# bp.start_all
```


Configuring backup and restore using NetBackup policies

This chapter includes the following topics:

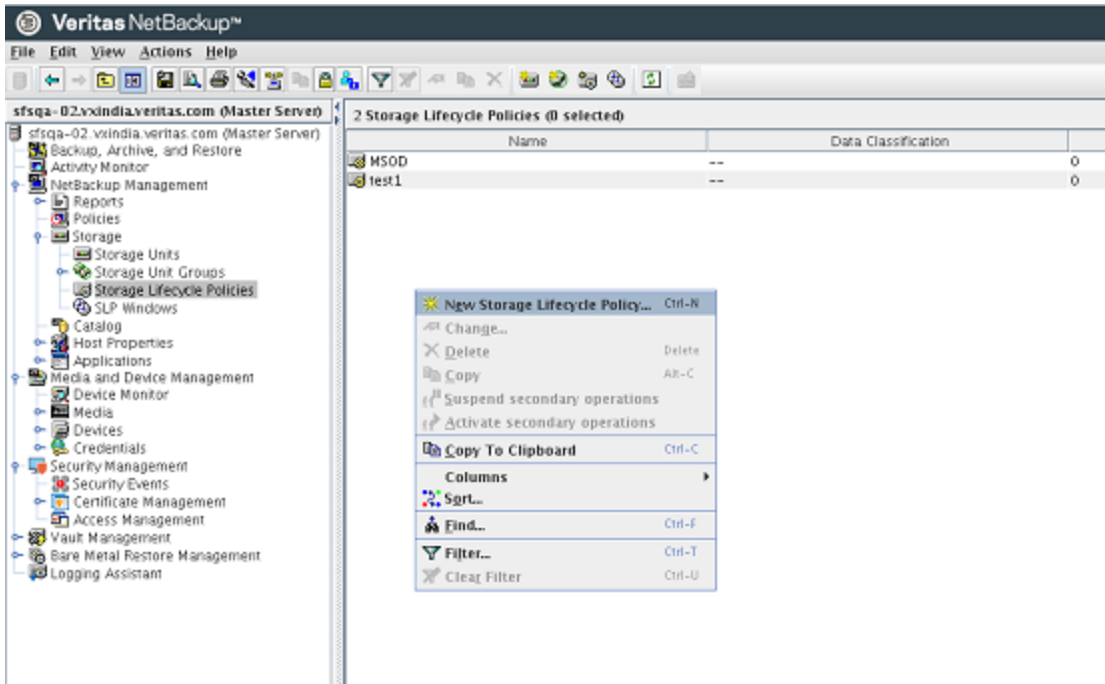
- [Storage Lifecycle Policies](#)
- [Backup and restore](#)
- [Running a backup policy manually](#)
- [Restoring backed up files](#)

Storage Lifecycle Policies

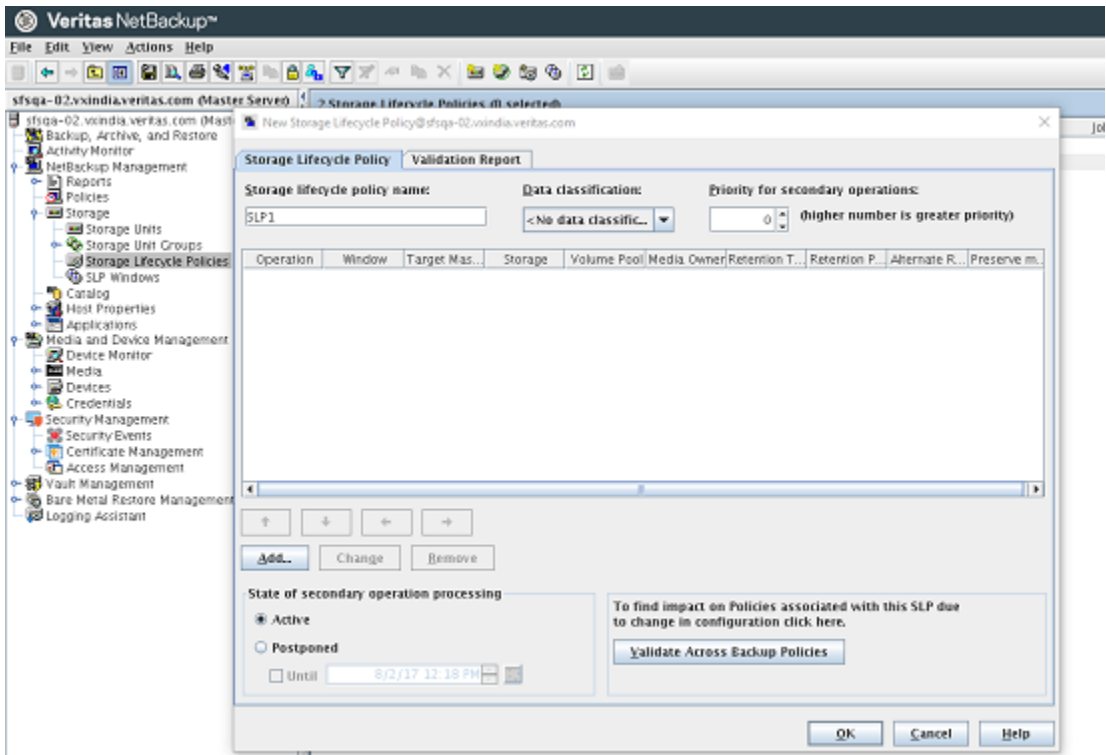
You can create Storage Lifecycle Policies (SLP).

To create Storage Lifecycle Policies

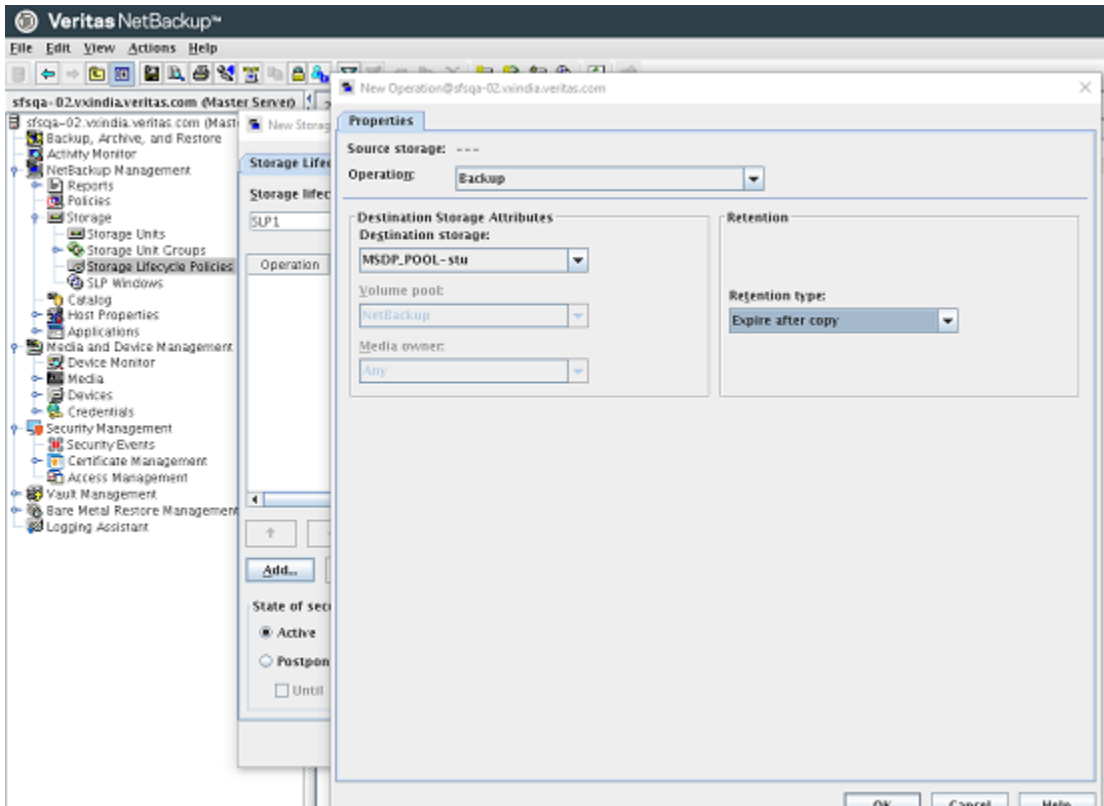
- 1 Click **Storage > Storage Lifecycle Policies** on the NetBackup console. Select **New Storage Lifecycle Policy**.



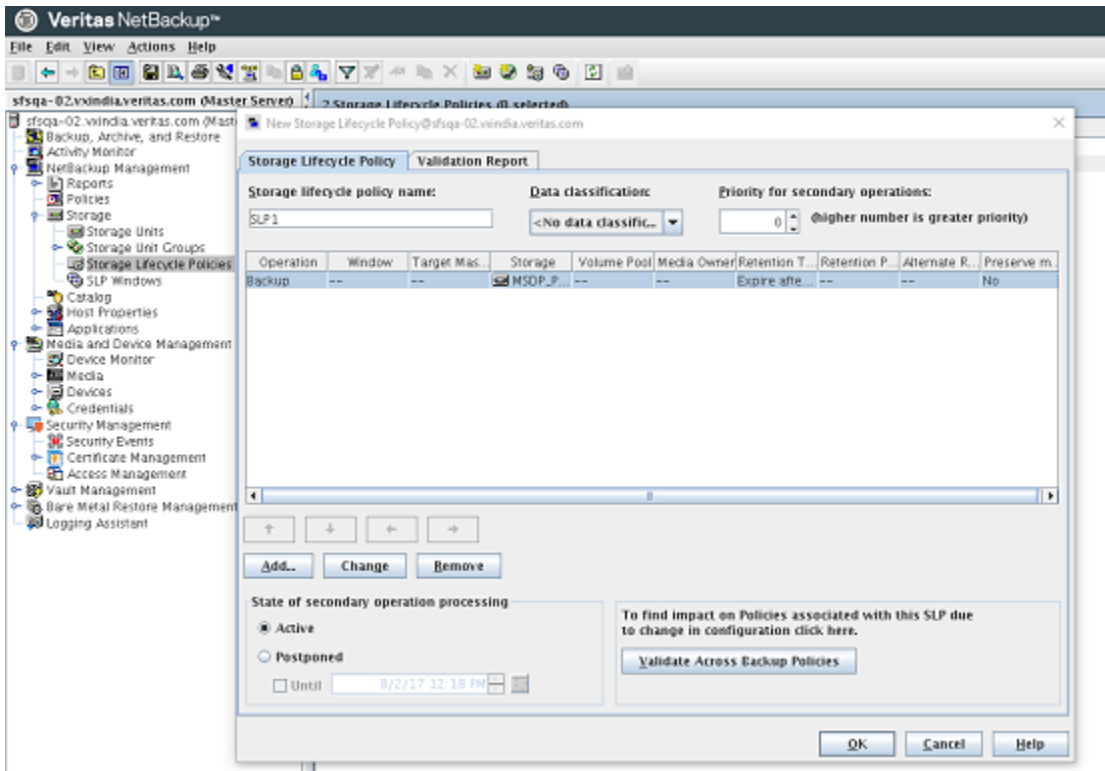
- 2 Enter a unique policy name for the policy. Click on the **Add** button.



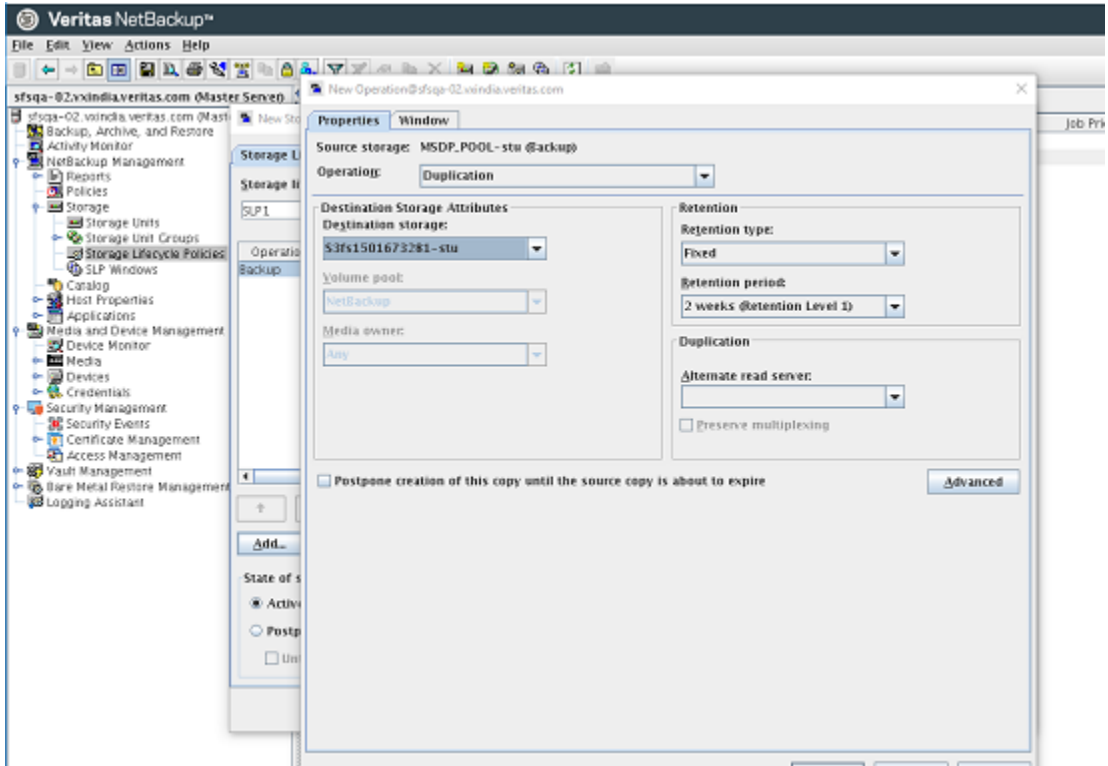
- 3 Select **Operation** as **Backup**, and set the destination pool to the MSDP pool that was created. Choose the **Retention type** based on your requirement.



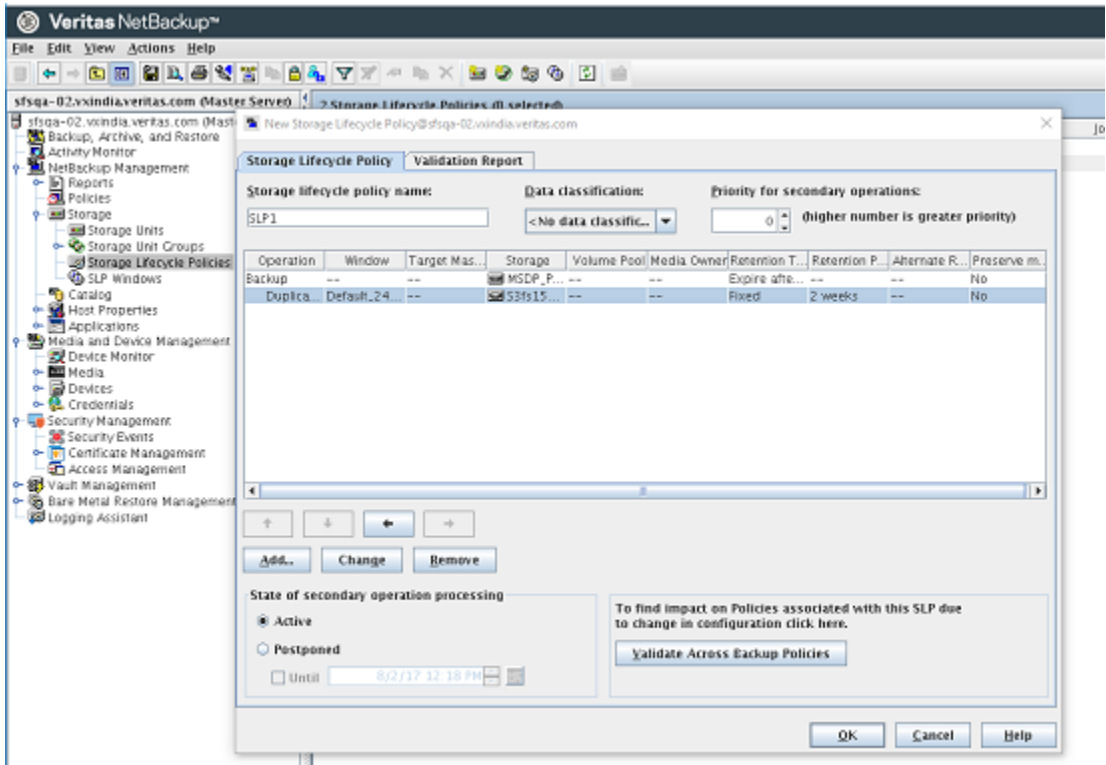
- 4 A new entry for **Backup** gets added. Click on the **Add** button again.



- 5 Select **Operation** as **Deduplication** and set the destination tier to the OST storage unit that was created. Choose the **Retention type** based on your requirement.



- 6 Both entries for SLP appear in the **Storage Lifecycle Policy** tab. The first operation is for **Backup** and the second operation is for **Duplication**.



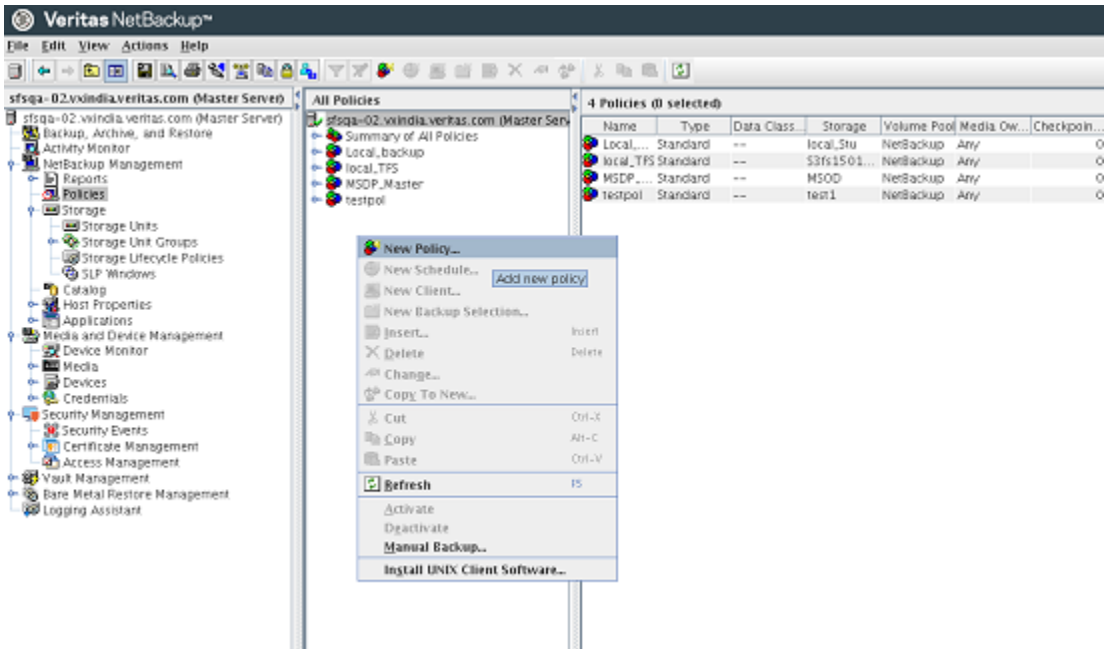
Backup and restore

After you complete the configurations, perform the following steps for backup and restore.

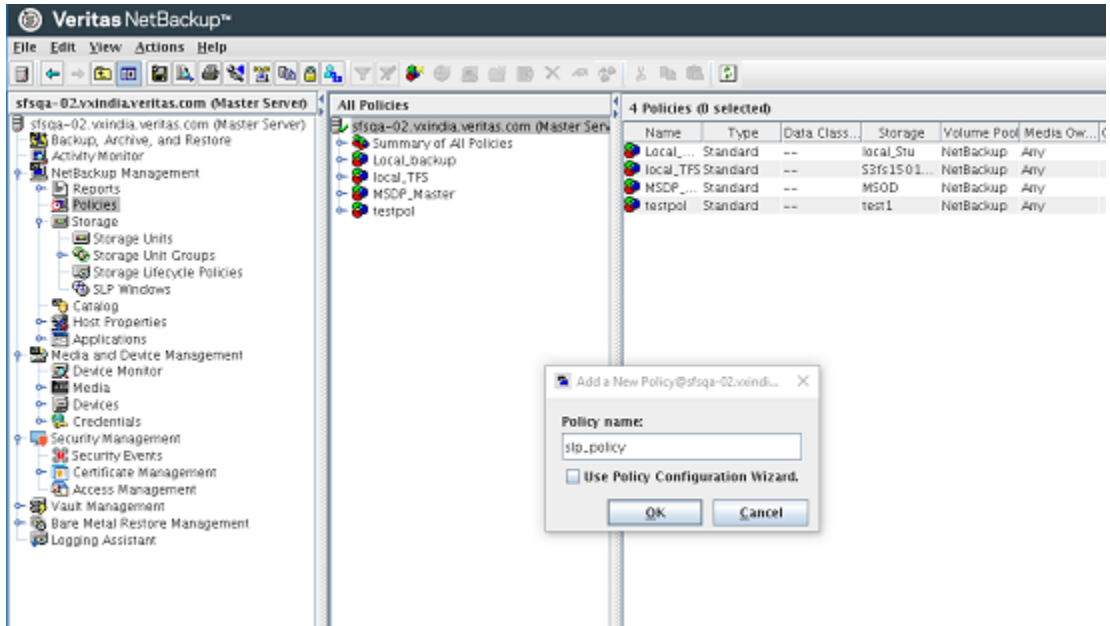
Policy creation

To create policies

- 1 Right-click on **Policies** within the NetBackup console and click on **New Policy**.



- 2 Provide the following information for policy creation.
 - Policy name
 - From the **Attributes** tab, select the appropriate storage unit under **Policy storage**.



- 3 Under **Policy storage**, enter the name of the **Storage Lifecycle Policy** that was created.

See “Storage Lifecycle Policies” on page 101.

Change Policy - stp_policy@sfsqa-02.vxindia.veritas.com

Server: sfsqa-02.vxindia.veritas.com

Attributes Schedules Clients Backup Selections

Policy type: Standard

Destination:

Data classification: <No data classification>

Policy storage: Any_available

Policy volume pool: Any_available

Take checkpoints every:
☐ MSOD_POOL-stu
☐ S3fs1501507821-stu
☐ S3fs1501594206-stu
☐ S3fs1501673281-stu
☐ MSOD (Storage Lifecycle Policy)
☒ SLP1 (Storage Lifecycle Policy)

Limit jobs per policy:
☐ MSOD (Storage Lifecycle Policy)
☒ SLP1 (Storage Lifecycle Policy)

Job priority: 0

Media Owner: Any

Snapshot Client and Replication Director

☐ Perform block level incremental backups

☐ Use Replication Director

☒ Perform snapshot backups Options...

☐ Retain snapshot for Instant Recovery or SLP management

☐ Hyper-V server:

☐ Perform off-host backup

Use:
Machine:

Go into effect at: Aug 2, 2017 12:28:30 PM

☐ Follow NFS

☐ Cross mount points

☐ Compress

☐ Encrypt

Enter recovery information for:

Full Restore

File image restore information

File detection

For synthetic backups and Bare Metal Restore

Multiple data streams

☐ Disable client-side deduplication

☐ Enable granular recovery

☐ Use Accelerator

☐ Enable optimized backup of Windows deduplicated volumes

Keyword phrase (optional):

Microsoft Exchange Server Attributes

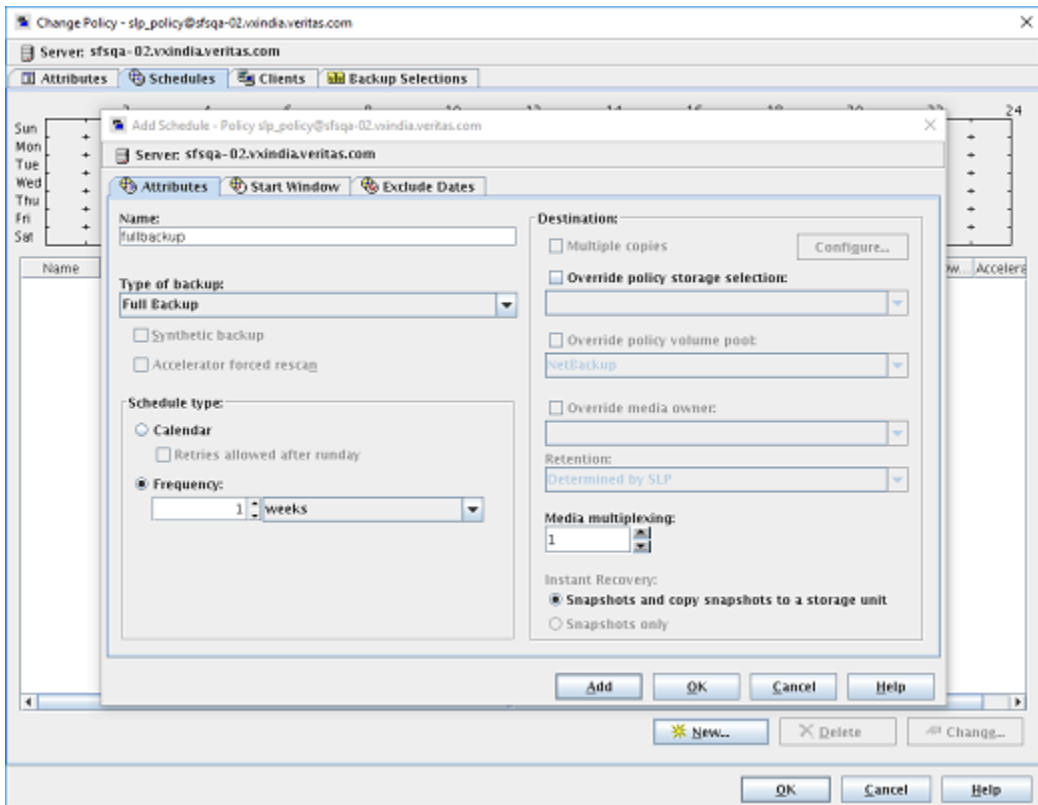
Exchange DAG or Exchange 2007 replication (CCR/CCR)

Database backup source:

Preferred server list... (Exchange DAG only)

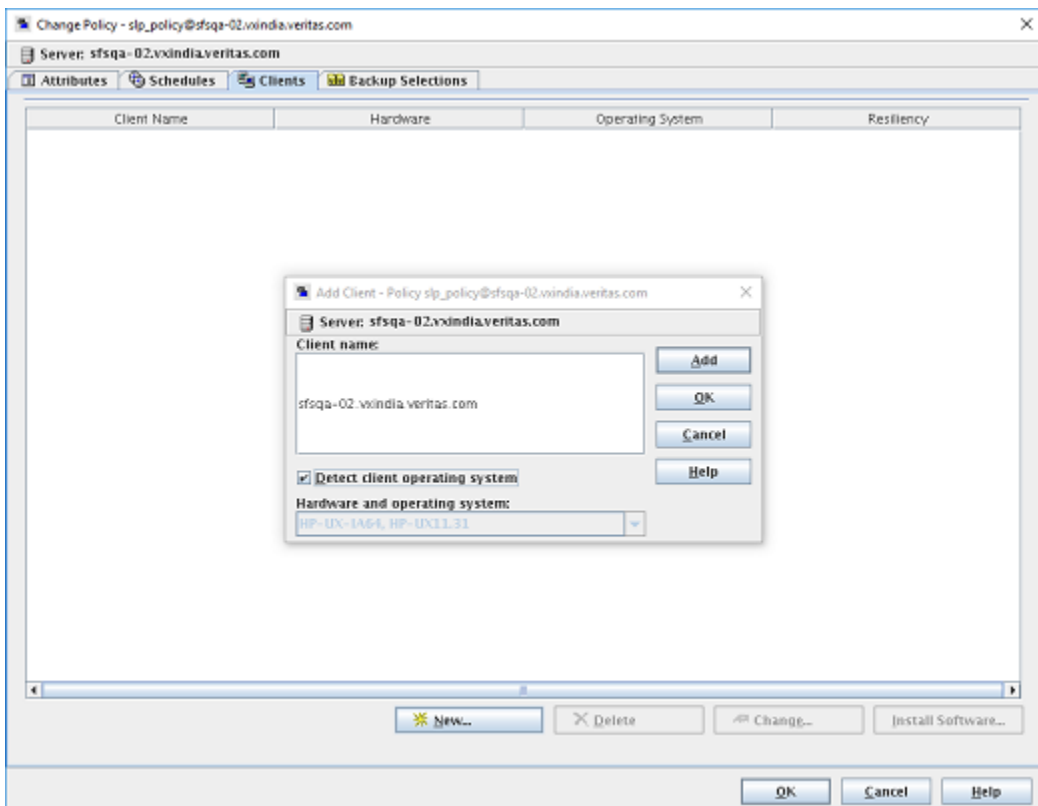
OK Cancel Help

- 4 Enter the attribute information as per your requirement.

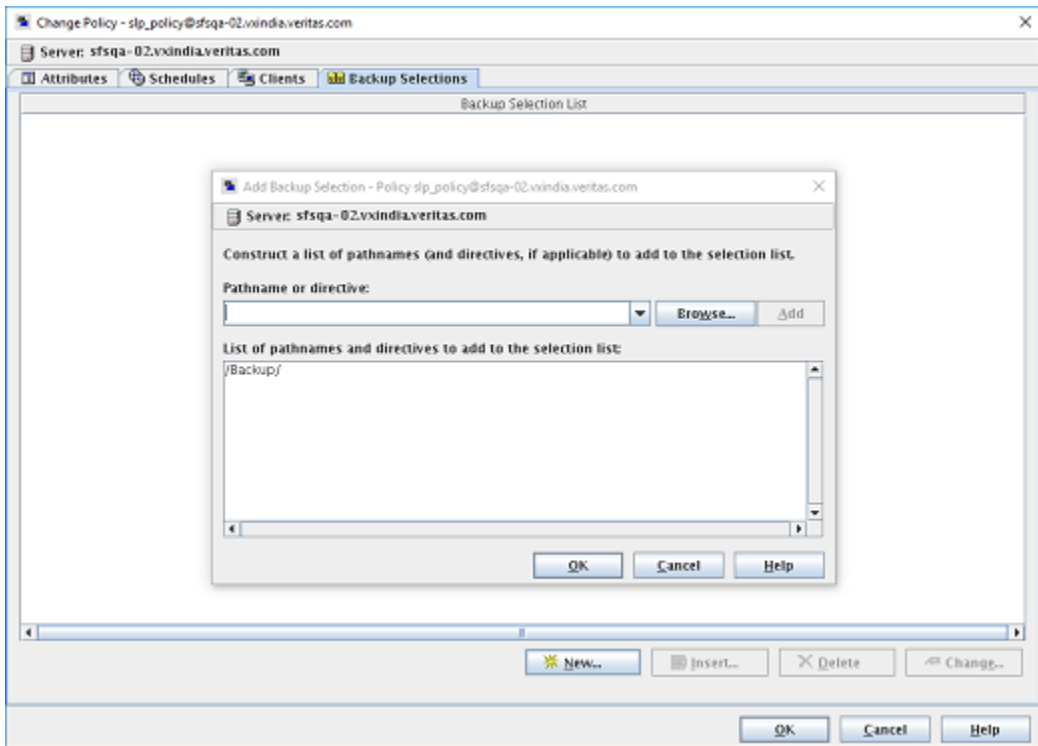


- 5 Under the **Schedule** tab, enter the name of the schedule. For example, **fullbackup**.

6 Enter the client information under the **Clients** tab.



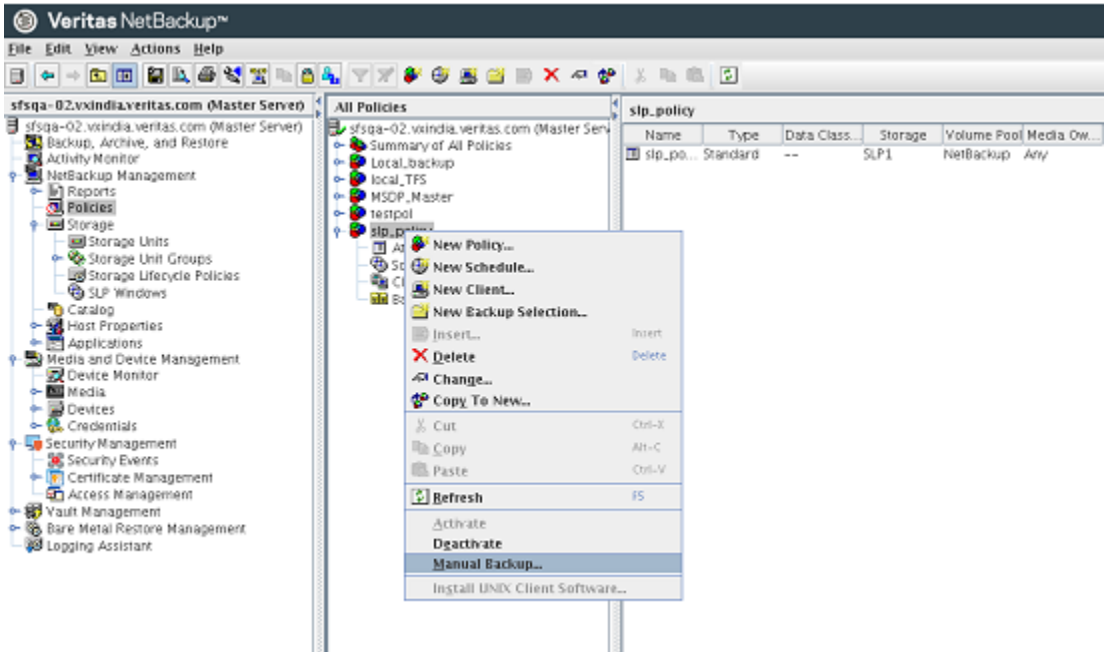
7 Select the folders that need to be backed up under **Backup Selections**.



Running a backup policy manually

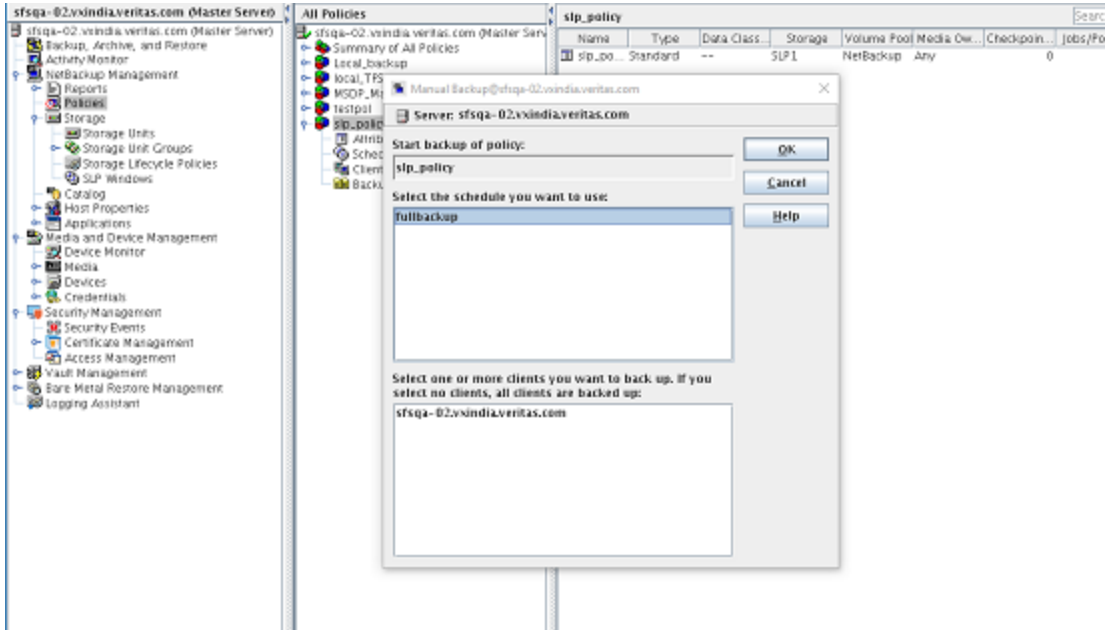
To run a backup policy manually

- 1 Once the policy is created, right-click on the name of the policy that you want to run under **Summary of All Policies**, and click on **Manual Backup**.



- 2 Select the schedule that you want to use and click **OK**.

This starts the manual backup with the policy.



3 To verify the status of the backup, go to **Activity Monitor**.

The screenshot shows the Veritas NetBackup Activity Monitor window. The left sidebar displays a tree view of the NetBackup hierarchy, with 'Activity Monitor' selected. The main pane shows a table of 28 jobs. The table has columns for Job ID, Type, State, State Details, Status, Job Policy, Job Sched., Client, Media Ser., Start Time, Elapsed Ti., and End Time. The jobs are listed in descending order of start time, with the most recent job at the top.

Job ID	Type	State	State Details	Status	Job Policy	Job Sched.	Client	Media Ser.	Start Time	Elapsed Ti.	End Time
28	Backup	Active		0	slp_policy	FullBackup	sfsqa-02...	sfsqa-02...	Aug 2, 20...	00:00:29	
27	Restore	Done		0			sfsqa-02...	sfsqa-02...	Aug 2, 20...	01:52:44	Aug 2, 20...
26	Image Cleanup	Done		1			sfsqa-02...	sfsqa-02...	Aug 2, 20...	00:10:00	Aug 2, 20...
25	Image Cleanup	Done		0			sfsqa-02...	sfsqa-02...	Aug 1, 20...	00:00:02	Aug 1, 20...
24	Image Cleanup	Done		1			sfsqa-02...	sfsqa-02...	Aug 1, 20...	00:30:01	Aug 1, 20...
23	Duplication	Done		0	SUP_Nest1	Default_2...	sfsqa-02...	sfsqa-02...	Aug 1, 20...	01:42:52	Aug 1, 20...
22	Image Cleanup	Done		1			sfsqa-02...	sfsqa-02...	Aug 1, 20...	00:30:01	Aug 1, 20...
21	Backup	Done		0	testpol	Full	sfsqa-02...	sfsqa-02...	Aug 1, 20...	00:13:15	Aug 1, 20...
20	Image Cleanup	Done		1			sfsqa-02...	sfsqa-02...	Aug 1, 20...	00:30:00	Aug 1, 20...
19	Restore	Done		0			sfsqa-02...	sfsqa-02...	Aug 1, 20...	01:53:19	Aug 1, 20...
18	Image Cleanup	Done		0			sfsqa-02...	sfsqa-02...	Jul 31, 20...	00:00:04	Jul 31, 20...
17	Image Cleanup	Done		1			sfsqa-02...	sfsqa-02...	Jul 31, 20...	00:30:00	Jul 31, 20...
16	Duplication	Done		0	SUP_MS00	Default_2...	sfsqa-02...	sfsqa-02...	Jul 31, 20...	01:42:56	Jul 31, 20...
15	Image Cleanup	Done		1			sfsqa-02...	sfsqa-02...	Jul 31, 20...	00:30:01	Jul 31, 20...
14	Backup	Done		0	MSOP_Ma...	Full	sfsqa-02...	sfsqa-02...	Jul 31, 20...	00:13:12	Jul 31, 20...
13	Restore	Done		0			sfsqa-02...	sfsqa-02...	Jul 31, 20...	00:00:08	Jul 31, 20...
12	Restore	Done		0			sfsqa-02...	sfsqa-02...	Jul 31, 20...	00:00:07	Jul 31, 20...
11	Image Cleanup	Done		0			sfsqa-02...	sfsqa-02...	Jul 31, 20...	00:00:01	Jul 31, 20...
10	Duplication	Done		0	SUP_MS00	Default_2...	sfsqa-02...	sfsqa-02...	Jul 31, 20...	00:00:18	Jul 31, 20...
9	Backup	Done		0	MSOP_Ma...	Full	sfsqa-02...	sfsqa-02...	Jul 31, 20...	00:03:07	Jul 31, 20...
8	Image Cleanup	Done		0			sfsqa-02...	sfsqa-02...	Jul 31, 20...	00:00:00	Jul 31, 20...
7	Backup	Done		0	local_TFS	Full_Sch	sfsqa-02...	sfsqa-02...	Jul 31, 20...	00:00:18	Jul 31, 20...
6	Image Cleanup	Done		0			sfsqa-02...	sfsqa-02...	Jul 31, 20...	00:00:02	Jul 31, 20...
5	Image Cleanup	Done		1			sfsqa-02...	sfsqa-02...	Jul 31, 20...	00:00:01	Jul 31, 20...
4	Backup	Done		0	Local_bac...	Full_Sch	ngsf06pe...	ngsf06pe...	Jul 31, 20...	00:00:10	Jul 31, 20...
3	Backup	Done		0	MSOP_Ma...	Full	sfsqa-02...	sfsqa-02...	Jul 31, 20...	00:00:08	Jul 31, 20...
2	Backup	Done		150	MSOP_Ma...	Full	sfsqa-02...	sfsqa-02...	Jul 31, 20...	00:00:13	Jul 31, 20...
1	Image Cleanup	Done		1			sfsqa-02...	sfsqa-02...	Jul 31, 20...	00:00:01	Jul 31, 20...

- 4 Select the appropriate job from the displayed jobs and click on the **Detailed status** tab in the new window to check on the status of the backup.

The screenshot shows the 'Job Details' window for a backup job. The window title is 'Job Details: 28@sfsqa-02.vxindia.veritas.com'. The 'Job ID' is 28 and the 'Job State' is 'Done (Successful)'. The 'Detailed Status' tab is selected, showing a log of the backup process. The log includes timestamps and details about the backup attempt, including the start time, elapsed time, and the completion of the backup operation. The 'Percent Complete' is 100%.

Field	Value
Job ID:	28
Job State:	Done (Successful)
Attempt:	1
Job PID:	31260
Storage Unit:	MSDP_POOL-stu
Media Server:	sfsqa-02.vxindia.veritas.com
Transport Type:	LAN
Attempt Started:	Aug 2, 2017 12:34:14 PM
Attempt Elapsed:	00:13:32
Attempt Ended:	Aug 2, 2017 12:47:46 PM
KB/Sec:	102529

Status:

```

Aug 2, 2017 12:34:15 PM - Info bptm (pid=31279) start
Aug 2, 2017 12:34:15 PM - Info bptm (pid=31279) using 262144 data buffer size
Aug 2, 2017 12:34:15 PM - Info bptm (pid=31279) using 30 data buffers
Aug 2, 2017 12:34:15 PM - Info bptm (pid=31279) start backup
Aug 2, 2017 12:34:18 PM - begin writing
Aug 2, 2017 12:44:43 PM - Info bpbkar (pid=31270) bpbkar waited 519 times for empty buffer, delayed 133777 times
Aug 2, 2017 12:44:43 PM - Info bptm (pid=31279) waited for full buffer 16196 times, delayed 22006 times
Aug 2, 2017 12:44:48 PM - Info bptm (pid=31279) EXTING with status 0 <-----
Aug 2, 2017 12:44:48 PM - Info sfsqa-02.vxindia.veritas.com (pid=31279) StorageServer=PureDisk:sfsqa-02.vxindia.veritas.com; Report=PD00 S
Aug 2, 2017 12:47:44 PM - Info bpbkm (pid=31260) validating image for client sfsqa-02.vxindia.veritas.com
Aug 2, 2017 12:47:44 PM - Info bpbkar (pid=31270) done. status: 0: the requested operation was successfully completed
Aug 2, 2017 12:47:44 PM - end writing; write time: 0:13:26
the requested operation was successfully completed (0)
  
```

Field	Value
Current Kilobytes Written:	63268768
Current Files Written:	25
Current File:	
Estimated Kilobytes:	0
Estimated Files:	0

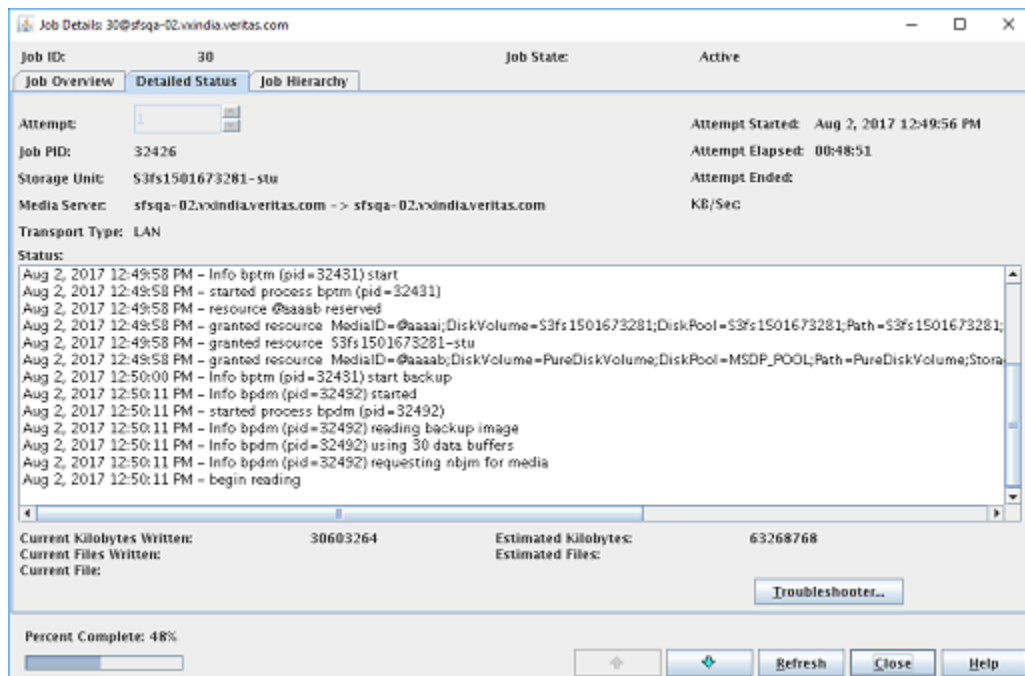
Percent Complete: 100%

Buttons: Troubleshooter..., Refresh, Close, Help

- 5 Once the above backup job is complete, a new duplication job is automatically triggered.

Job ID	Type	State	State Details	Status	Job Policy	Job Sched.	Client	Media Ser...	Start Time	Elapsed TL	End Time	Storage
30	Duplication	Active			SUP_SUP1	Default_2...	sfsga-02...	sfsga-02...	Aug 2, 20...	00:48:01		S3fs1
29	Image Cleanup	Done		1					Aug 2, 20...	00:30:02	Aug 2, 20...	
28	Backup	Done		0	slp_policy	fullbackup	sfsga-02...	sfsga-02...	Aug 2, 20...	00:12:32	Aug 2, 20...	MSDP
27	Restore	Done		0			sfsga-02...	sfsga-02...	Aug 2, 20...	01:52:44	Aug 2, 20...	
26	Image Cleanup	Done		1					Aug 2, 20...	00:30:00	Aug 2, 20...	
25	Image Cleanup	Done		0					Aug 1, 20...	00:00:02	Aug 1, 20...	
24	Image Cleanup	Done		1					Aug 1, 20...	00:30:01	Aug 1, 20...	
23	Duplication	Done		0	SUP_test1	Default_2...	sfsga-02...	sfsga-02...	Aug 1, 20...	01:42:52	Aug 1, 20...	S3fs1
22	Image Cleanup	Done		1					Aug 1, 20...	00:30:01	Aug 1, 20...	
21	Backup	Done		0	testpol	full	sfsga-02...	sfsga-02...	Aug 1, 20...	00:12:15	Aug 1, 20...	MSDP
20	Image Cleanup	Done		1					Aug 1, 20...	00:30:00	Aug 1, 20...	
19	Restore	Done		0			sfsga-02...	sfsga-02...	Aug 1, 20...	01:53:19	Aug 1, 20...	
18	Image Cleanup	Done		0					Jul 31, 20...	00:00:04	Jul 31, 20...	
17	Image Cleanup	Done		1					Jul 31, 20...	00:30:00	Jul 31, 20...	
16	Duplication	Done		0	SUP_MSOD	Default_2...	sfsga-02...	sfsga-02...	Jul 31, 20...	01:42:56	Jul 31, 20...	S3fs1
15	Image Cleanup	Done		1					Jul 31, 20...	00:30:01	Jul 31, 20...	
14	Backup	Done		0	MSDP_Ma...	full	sfsga-02...	sfsga-02...	Jul 31, 20...	00:12:12	Jul 31, 20...	MSDP
13	Restore	Done		0			sfsga-02...	sfsga-02...	Jul 31, 20...	00:00:08	Jul 31, 20...	
12	Restore	Done		0			sfsga-02...	sfsga-02...	Jul 31, 20...	00:00:07	Jul 31, 20...	
11	Image Cleanup	Done		0					Jul 31, 20...	00:00:01	Jul 31, 20...	
10	Duplication	Done		0	SUP_MSOD	Default_2...	sfsga-02...	sfsga-02...	Jul 31, 20...	00:00:18	Jul 31, 20...	S3fs1
9	Backup	Done		0	MSDP_Ma...	full	sfsga-02...	sfsga-02...	Jul 31, 20...	00:02:07	Jul 31, 20...	MSDP
8	Image Cleanup	Done		0					Jul 31, 20...	00:00:00	Jul 31, 20...	
7	Backup	Done		0	local_TPS	full_Sch	sfsga-02...	sfsga-02...	Jul 31, 20...	00:00:18	Jul 31, 20...	S3fs1
6	Image Cleanup	Done		0					Jul 31, 20...	00:00:02	Jul 31, 20...	
5	Image Cleanup	Done		1					Jul 31, 20...	00:00:01	Jul 31, 20...	
4	Backup	Done		0	Local_bac...	full_Sch	ngsfdelipe...	ngsfdelipe...	Jul 31, 20...	00:00:10	Jul 31, 20...	local
3	Backup	Done		0	MSDP_Ma...	full	sfsga-02...	sfsga-02...	Jul 31, 20...	00:00:08	Jul 31, 20...	MSDP
2	Backup	Done		150	MSDP_Ma...	full	sfsga-02...		Jul 31, 20...	00:00:11	Jul 31, 20...	
1	Image Cleanup	Done		1					Jul 31, 20...	00:00:01	Jul 31, 20...	

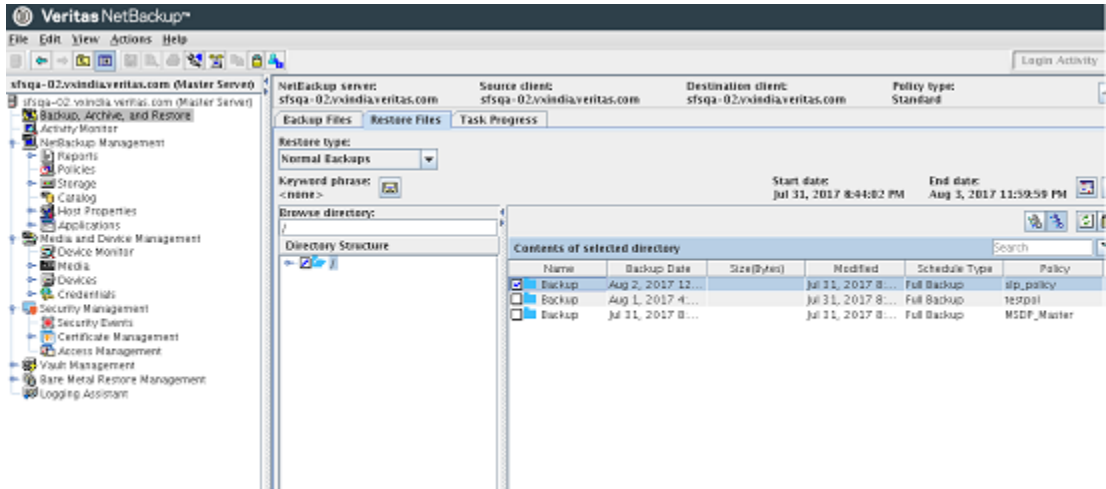
- 6 Click on that job and then select detailed status to check the status of the duplication job.



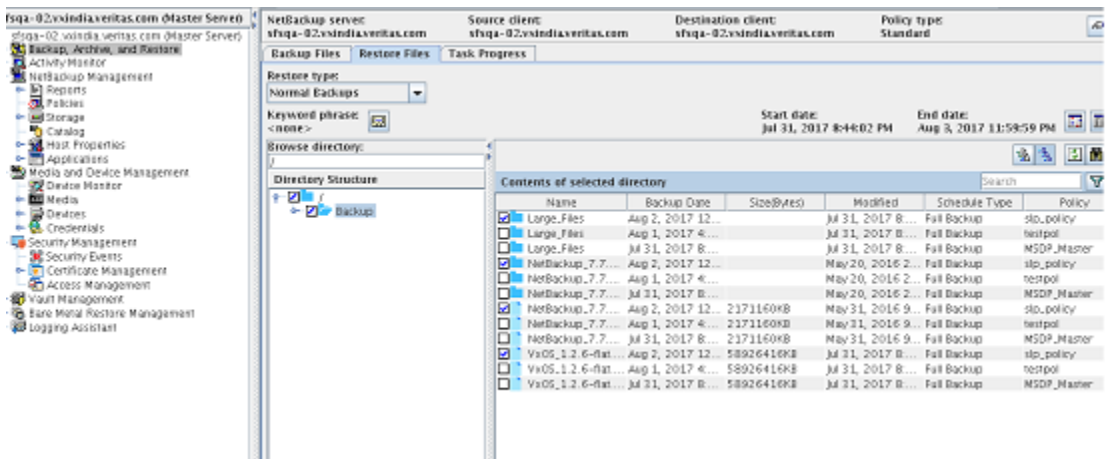
Restoring backed up files

To restore backed up files

- 1 Create a directory where you want to restore the backed-up files.
- 2 Go to the **Restore Files** tab under **Backup, Archive, Restore**.



- 3 Go to the browse directory and select the appropriate files to restore and click **Restore**. The backup to be restored can reside either on NetBackup or on Veritas Access depending on the **Storage Lifecycle Policy** that is set. Hence, the restore location changes accordingly.



- 4 Enter the location where the files should be restored, and click on the **Start Restore** button.

Restore Marked Files@sfsqa-02.vxindia.veritas.com

General

Destination

☐ Restore everything to its original location.

☒ Restore everything to a different location (maintaining existing structure).

Destination:

/Restore/

☐ Restore individual directories and files to different locations.

Source	Destination	Backup Date	Modified
/Backup/		Aug 2, 2017 12:34:14 PM	Jul 31, 2017 8:23:31 PM

Change Selected Destination(s)...

Change All Destinations...

Add Destination...

Remove Selected Destination(s)

☐ Create and restore to a new virtual hard disk file.

Setting

Options

☐ Overwrite existing files

☐ Restore directories without crossing mount points

☐ Restore without access-control attributes (Windows clients only)

☒ Rename hard links

☒ Rename soft links

☐ Force rollback even if it destroys later snapshots

Media Server

Default

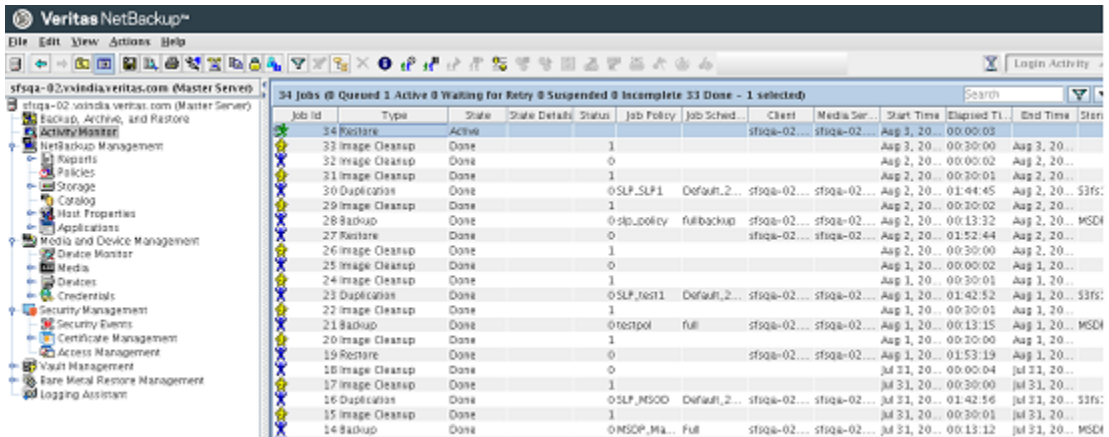
☒ Override default priority

Job Priority: 90000

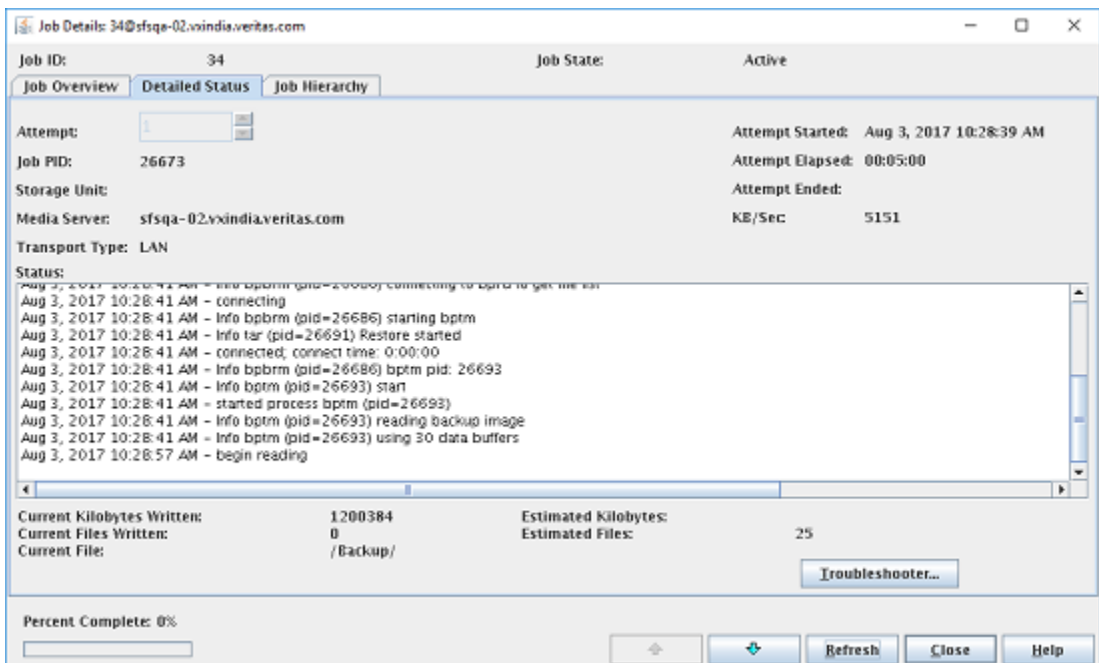
(higher number is greater priority)

Start Restore Cancel

- 5 To view the progress of the restore operation, click **Yes** on the **Restore Initiated** window.



- 6 You can view the progress of the restore operation under the **Detailed Status** tab.



Configuring Veritas Access with the NetBackup client

This chapter includes the following topics:

- [Prerequisites for configuring the NetBackup client](#)
- [About the NetBackup Snapshot Client](#)
- [About NetBackup snapshot methods](#)
- [Enabling or disabling the NetBackup SAN client](#)
- [Workflow for configuring Veritas Access for NetBackup](#)
- [Registering a NetBackup master server or adding an optional media server](#)
- [Displaying the excluded files from backup](#)
- [Displaying the included and excluded files for backups](#)
- [Adding or deleting patterns to the list of files in backups](#)
- [Configuring or resetting the virtual IP address used by NetBackup](#)
- [Configuring the virtual name of NetBackup](#)
- [Displaying the status of NetBackup services](#)
- [Configuring backup operations using NetBackup or other third-party backup applications](#)
- [Performing a backup or restore of a Veritas Access file system over a NetBackup SAN client](#)

- [Performing a backup or restore of a snapshot](#)
- [Installing or uninstalling the NetBackup client](#)
- [Configuring Veritas Access for NetBackup cloud storage](#)

Prerequisites for configuring the NetBackup client

Before configuring the NetBackup client for Veritas Access, you must have completed the following:

- You must have a NetBackup master server external to your Veritas Access cluster. The NetBackup administrator configures the NetBackup master server. See the *Veritas NetBackup* product documentation for more information.
- Add the valid licenses on the NetBackup master server.
- Make sure that host names of the master server and the NetBackup client installed on Veritas Access can be resolved and the reverse lookup is working.

About the NetBackup Snapshot Client

A snapshot is a point-in-time, read-only, disk-based copy of a client volume. After the snapshot is created, NetBackup backs up data from the snapshot, not directly from the client's primary or original volume. Users and client operations can access the primary data without interruption while data on the snapshot volume is backed up. The contents of the snapshot volume are cataloged as if the backup was produced directly from the primary volume. After the backup is complete, the snapshot-based backup image on storage media is indistinguishable from a traditional, non-snapshot backup.

About NetBackup snapshot methods

NetBackup can create different types of snapshots. Each snapshot type that you configure in NetBackup is called a snapshot method. Snapshot methods enable NetBackup to create snapshots within the storage stack (such as the file system) where the data resides. When the data resides in a file system, NetBackup can use a file system method, depending on the client operating system and the file system type.

You select the snapshot method in the backup policy as explained in the *Veritas NetBackup Snapshot Client Administrator's Guide*.

Note: When using Veritas Access with NetBackup, select the `VxFS_Checkpoint` snapshot method. The checkpoint feature is not supported on a scale-out file system.

Enabling or disabling the NetBackup SAN client

You can enable or disable the NetBackup SAN client on Veritas Access. The NetBackup SAN client should only be enabled on Veritas Access if the required licenses are installed on the NetBackup Master Server. If you do not have the required license for the NetBackup SAN client, then you must disable the SAN client on Veritas Access. Otherwise, the Veritas Access backup service fails to start.

To enable or disable the NetBackup SAN client

- ◆ To enable or disable the NetBackup SAN client, enter the following:

```
Backup> netbackup sanclient enable | disable

enable          Enables the NetBackup SAN client.

disable         Disables the NetBackup SAN client.

Backup> netbackup sanclient enable
Success.
```

Workflow for configuring Veritas Access for NetBackup

To back up your data with NetBackup, you must register the installed and configured NetBackup master server with Veritas Access.

To configure NetBackup for Veritas Access, perform the following tasks in the order shown:

Make sure that the prerequisites are met.	See “Prerequisites for configuring the NetBackup client” on page 124.
Register the NetBackup master server.	See “Registering a NetBackup master server or adding an optional media server” on page 126.
Display the current status of the NetBackup client.	See “Displaying the status of NetBackup services” on page 131.

Reset the values for the NetBackup master server.	See “Registering a NetBackup master server or adding an optional media server” on page 126.
Display the current status of the NetBackup client.	See “Displaying the status of NetBackup services” on page 131.
Reset the NetBackup virtual name.	See “Configuring the virtual name of NetBackup” on page 130.
Register the NetBackup master server with the NetBackup client.	See “Registering a NetBackup master server or adding an optional media server” on page 126.
Configure the virtual name that the NetBackup master server uses for the NetBackup client.	See “Configuring the virtual name of NetBackup” on page 130.
Display the current status of the NetBackup client.	See “Displaying the status of NetBackup services” on page 131.
Verify that Veritas Access is configured with the NetBackup client.	See “Displaying the status of NetBackup services” on page 131.
Specify the files to back up or restore.	See “Performing a backup or restore of a Veritas Access file system over a NetBackup SAN client” on page 133.
Specify the snapshot to back up or restore	See “Performing a backup or restore of a snapshot” on page 134.
Uninstalling or installing the NetBackup client.	See “Installing or uninstalling the NetBackup client” on page 134.
Configuring Veritas Access for NetBackup cloud storage	See “Configuring Veritas Access for NetBackup cloud storage” on page 138.

Registering a NetBackup master server or adding an optional media server

You register the NetBackup master server so that it can communicate with Veritas Access. If necessary, you can reset the values of the NetBackup master server to its default configurations. You can optionally add a media server.

The NetBackup master server can be the NetBackup media server, but it is not mandatory that the NetBackup master server be the NetBackup media server. In

production environments, the NetBackup media server is separate from the NetBackup master server.

See the `backup_netbackup(1)` man page for detailed examples.

To register the NetBackup master server with Veritas Access

- ◆ Register the NetBackup master server with Veritas Access.

```
Backup> netbackup master-server set server
```

To reset the value for the NetBackup master server

- ◆ Reset the value for the NetBackup master server.

```
Backup> netbackup master-server reset
```

To add an optional NetBackup media server

- ◆ Add an optional NetBackup media server.

If the NetBackup master server is also acting as a NetBackup media server, then add the NetBackup media server using the NetBackup master server hostname.

For example:

```
Backup> netbackup media-server add FQDN of master server
```

To delete an already configured NetBackup media server

- ◆ Delete an already configured NetBackup media server.

```
Backup> netbackup media-server delete server
```

Displaying the excluded files from backup

To display the entries in the excluded list from backup

- ◆ Display the entries in the excluded list from backup.

```
Backup> netbackup exclude_list show [policy] [schedule]
```

policy Lists the excluded entries by specifying a NetBackup policy.

schedule If a NetBackup policy schedule is specified, then the excluded list entries for the specified NetBackup policy and NetBackup policy schedule are displayed.

```
Backup> netbackup exclude_list show
```

Pattern	Policy	Schedule
-----	-----	-----
hosts	-	-
iscsid.conf	-	-
iscsid.conf	NBU_access12	-
/vx/fs100/as*	policy	-
/vx/fs100/*mp3	policy	-
/vx/fs200/bs*	policy2	sched

The hyphens in the command output indicate that no values have been entered.

Displaying the included and excluded files for backups

You can specify a policy pattern that lets you specify which files to include or exclude from NetBackup backups. For example, you can specify that only `.gif` files are backed up, and `.iso` files are excluded. You can then display those files.

See the `backup_netbackup(1)` man page for detailed examples.

To display files included or excluded for backups

- ◆ Display the files that are included or excluded for backups.

For included files:

```
Backup> netbackup include_list show [policy] [schedule]
```

For excluded files:

```
Backup> netbackup exclude_list show [policy] [schedule]
```

Adding or deleting patterns to the list of files in backups

You can add or delete specified patterns to or from the files that you want to include or exclude from NetBackup backups. For example, you can create a backup policy with different patterns such that only `.gif` files are backed up and `.iso` files are excluded.

See the `backup_netbackup(1)` man page for detailed examples.

To add or delete the given pattern to the list of files included for backup

- ◆ Add the specified pattern to the files that are included for backup.

For adding specified patterns to included files:

```
Backup> netbackup include_list add pattern [policy] [schedule]
```

For deleting specified patterns from included files:

```
Backup> netbackup include_list delete pattern [policy] [schedule]
```

To add or delete a given pattern to the list of files excluded from backup

- ◆ Add a given pattern to the list of files that are excluded from backup.

For adding a given pattern to excluded files:

```
Backup> netbackup exclude_list add pattern [policy] [schedule]
```

For deleting the given pattern from excluded files:

```
Backup> netbackup exclude_list delete pattern [policy] [schedule]
```

Configuring or resetting the virtual IP address used by NetBackup

You can configure or reset the virtual IP address of NetBackup. This address is a highly-available virtual IP address in the cluster.

Note: Configure the virtual IP address using the `Backup> virtual-ip set` command so that it is different from all of the virtual IP addresses, including the console server IP address and the physical IP addresses that are used to install Veritas Access. Use the `Network> ip addr show` command to display the currently assigned virtual IP addresses on Veritas Access.

See the `backup_virtual-ip(1)` man page for detailed examples.

To configure or reset the virtual IP address used by NetBackup

- 1 Configure the virtual IP address of NetBackup on Veritas Access.

```
Backup> virtual-ip set ipaddr [device]
```

- 2 Reset the virtual IP address of NetBackup on Veritas Access.

```
Backup> virtual-ip reset
```

See [“Configuring the virtual name of NetBackup”](#) on page 130.

Configuring the virtual name of NetBackup

You can either configure the virtual name for the NetBackup master server, or you can reset the value to its default or unconfigured state.

See the `backup_virtual-name(1)` man page for detailed examples.

To set or reset the NetBackup virtual name

- ◆ Set or reset the NetBackup virtual name.

For setting the virtual name:

```
Backup> virtual-name set name
```

For resetting the virtual name:

```
Backup> virtual-name reset
```

Make sure that *name* can be resolved through DNS, and its IP address can be resolved back to *name* through the DNS reverse lookup. Also, make sure that *name* resolves to an IP address that is configured by using the `Backup> virtual-ip` command.

See [“Configuring or resetting the virtual IP address used by NetBackup”](#) on page 130.

Displaying the status of NetBackup services

Use the backup commands to display the status of the NetBackup services.

See the following man pages for detailed examples:

- `backup_show(1)`
- `backup_status(1)`
- `backup_start(1)`
- `backup_stop(1)`

To display NetBackup services

- ◆ Display the current NetBackup services.

```
Backup> show
```

If the settings were configured while the backup and the restore services were online, they may not be in use by Veritas Access. To display all of the configured settings, first run the `Backup> stop` command, then run the `Backup> start` command.

To display the status of backup services

- ◆ Display the status of backup services.

```
Backup> status
```

If the NetBackup server is started and online, then `Backup> status` displays any on-going backup or restore jobs.

To start or stop backup services

- 1 Start the backup services.

```
Backup> start [nodename]
```

You can also change the status of a virtual IP address to online after it has been configured using the `Backup> virtual-ip` command. This command applies to any currently active node in the cluster that handles backup and restore jobs.

See [“Configuring or resetting the virtual IP address used by NetBackup”](#) on page 130.

- 2 Stop the backup services.

```
Backup> stop
```

You can also change the status of a virtual IP address to offline after it has been configured using the `Backup> virtual-ip` command.

See [“Configuring or resetting the virtual IP address used by NetBackup”](#) on page 130.

Configuring backup operations using NetBackup or other third-party backup applications

You can backup Veritas Access using NetBackup client capability, or backup applications from other third-party companies that use the standard NFS mount to backup over the network.

For information on NetBackup, refer to the *Veritas NetBackup* product documentation set.

The Backup commands configure the local NetBackup installation of Veritas Access to use an external NetBackup master server or media server. When NetBackup is installed on Veritas Access, it acts as a NetBackup client to perform IP-based backups of Veritas Access file systems.

Note: A new public IP address, not an IP address that is currently used, is required for configuring the NetBackup client. Use the `Backup> virtual-ip` and `Backup> virtual-name` commands to configure the NetBackup client.

Performing a backup or restore of a Veritas Access file system over a NetBackup SAN client

You can perform a backup or restore of a Veritas Access file system over a NetBackup SAN client. A NetBackup SAN client is a NetBackup client for which Fibre Transport services are activated.

Backup and restore operations are done on the NetBackup master server by a NetBackup administrator using the NetBackup Administration Console. If the NetBackup master server can connect to the NetBackup client on Veritas Access, the NetBackup master server starts the backup or restore operations.

Before performing a backup or restoration of a Veritas Access file system over a NetBackup SAN client, do the following:

- Verify that the virtual IP address is online.
- Verify that the NetBackup client state is online.
- Configure the Fibre Transport media server.
 See the *Veritas NetBackup SAN client and Fibre Transport Guide* for more information on configuring the NetBackup Fibre Transport media server.

See the `backup(1)` man page for detailed examples.

To perform a backup of a file system over a NetBackup SAN client

- 1 Check the status of the NetBackup client.

```
Backup> status
```

- 2 Enable the SAN client from the CLI.

```
Backup> netbackup sanclient enable
```

- 3 Verify if the SAN client has been enabled or not from the CLI.

```
Backup> status
```

- 4 Using the NetBackup Administration Console, start a backup operation.

To perform a restore of a file system over a NetBackup SAN client

- 1 Check the status of the NetBackup client.

```
Backup> status
```

- 2 Using the NetBackup Administration Console, start a restore operation.
- 3 Check the status of the NetBackup client.

```
Backup> status
```

Performing a backup or restore of a snapshot

Using the NetBackup Administration Console, a NetBackup administrator can perform a backup or restore of a snapshot.

Veritas Access as a NetBackup client supports the VxFS_Checkpoint snapshot method. See the *Veritas NetBackup Snapshot Client Administrator's Guide* for more information on configuring snapshot policies.

To perform a backup of a snapshot

- ◆ Using the NetBackup Administration Console, start a snapshot backup.
The snapshot triggered by the NetBackup job can be seen from the CLI.

```
Storage> snapshot list
```

To perform a restore of a snapshot

- 1 Using the NetBackup Administration Console, navigate to **Backup, Archive, and Restore**.
- 2 Click the **Restore Files** tab.
- 3 Click the **Restore** option.
- 4 Specify the directory location for performing the restore operation.

```
/vx/name_of_file_system/Restores
```

Installing or uninstalling the NetBackup client

The NetBackup master server version should be higher or equal to the NetBackup client version. To upgrade the NetBackup client, uninstall the currently installed version of the NetBackup client and then install the specified version of the

NetBackup client. The uninstall command runs on all the nodes of the Veritas Access cluster.

Veritas Access supports two major versions of the NetBackup client, version 7.7 and 8.0. By default, Veritas Access comes with the 8.0 version of the NetBackup client.

See the `backup (1)` man page for detailed examples.

To install the NetBackup client

- 1 Display the currently installed version of the NetBackup client.

```
Backup> show
```

- 2 Install the specified NetBackup client.

```
Backup> install version [URL]
```

You must specify the version of the NetBackup client that you want to install. If you do not specify a URL, the `Backup> install` command has the information on the file system for the location it needs. Specify the major release version (8.0 or 7.7) as the second parameter. You can specify the NetBackup package minor release or patches (7.7.1 for a 7.7 major release) as the third parameter to install.

If the base NetBackup client version is 7.7.

```
Backup> install 7.7 scp://support@192.168.2.10:/home/NetBackup_7.7_
CLIENTS2.tar.gz
```

If the base NetBackup client version is 8.0.

```
Backup> install 8.0 scp://support@192.168.2.10:/home/NetBackup_8.0_
CLIENTS2.tar.gz
```

If there are minor releases or patches from the NetBackup client.

```
Backup> install 7.7 scp://support@192.168.2.10:/home/NetBackup_7.7.1_
CLIENTS2.tar.gz
```

```
Backup> install 7.7 scp://support@192.168.2.10:/home/NetBackup_7.7.2_
CLIENTS2.tar.gz
```

For example, consider that the NetBackup client binaries are placed on the following host:

```
192.168.2.10
```

```
Backup> install 7.7 scp://support@192.168.2.10:/home/NetBackup_7.7.3_
CLIENTS2.tar.gz
```

Where 192.168.2.10 is the host IP address on which the NetBackup client packages are placed.

```
NetBackup_7.7.3_CLIENTS2.tar.gz
```

This is the NetBackup client package.

- 3 Double check if the Red Hat compatible NetBackup client is available in this package.

```
support:  
system user and specify password when prompted.
```

- 4 Verify that the specified NetBackup client is installed.

```
Backup> show
```

To uninstall the NetBackup client

- 1 Display the currently installed version of the NetBackup client.

```
Backup> show
```

- 2 Uninstall the existing version of the NetBackup client.

```
Backup> uninstall
```

- 3 Display the current running version of the NetBackup client.

```
Backup> show
```

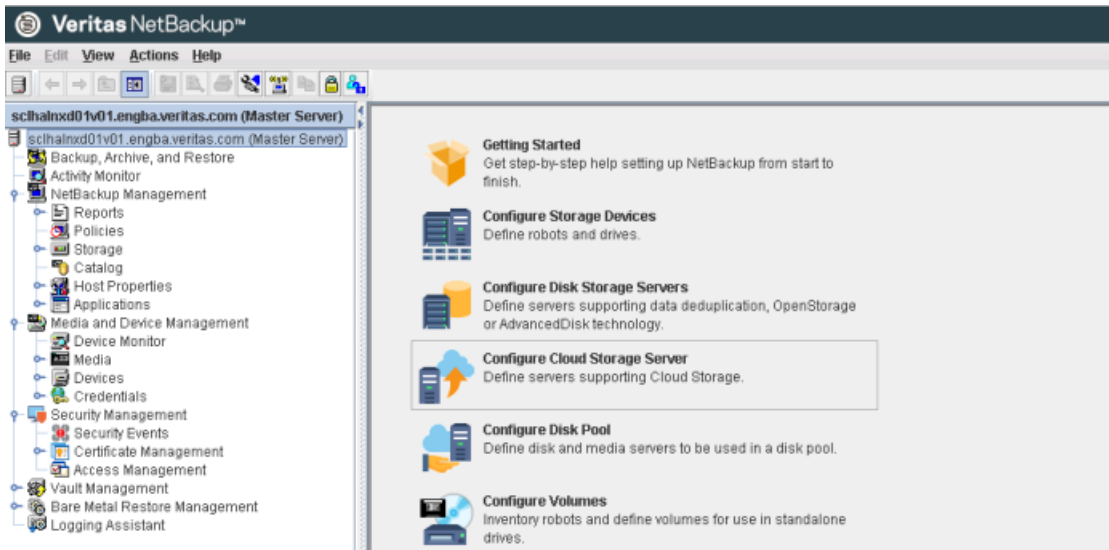
- 4 Verify that the NetBackup client is not installed.

```
Backup> show
```

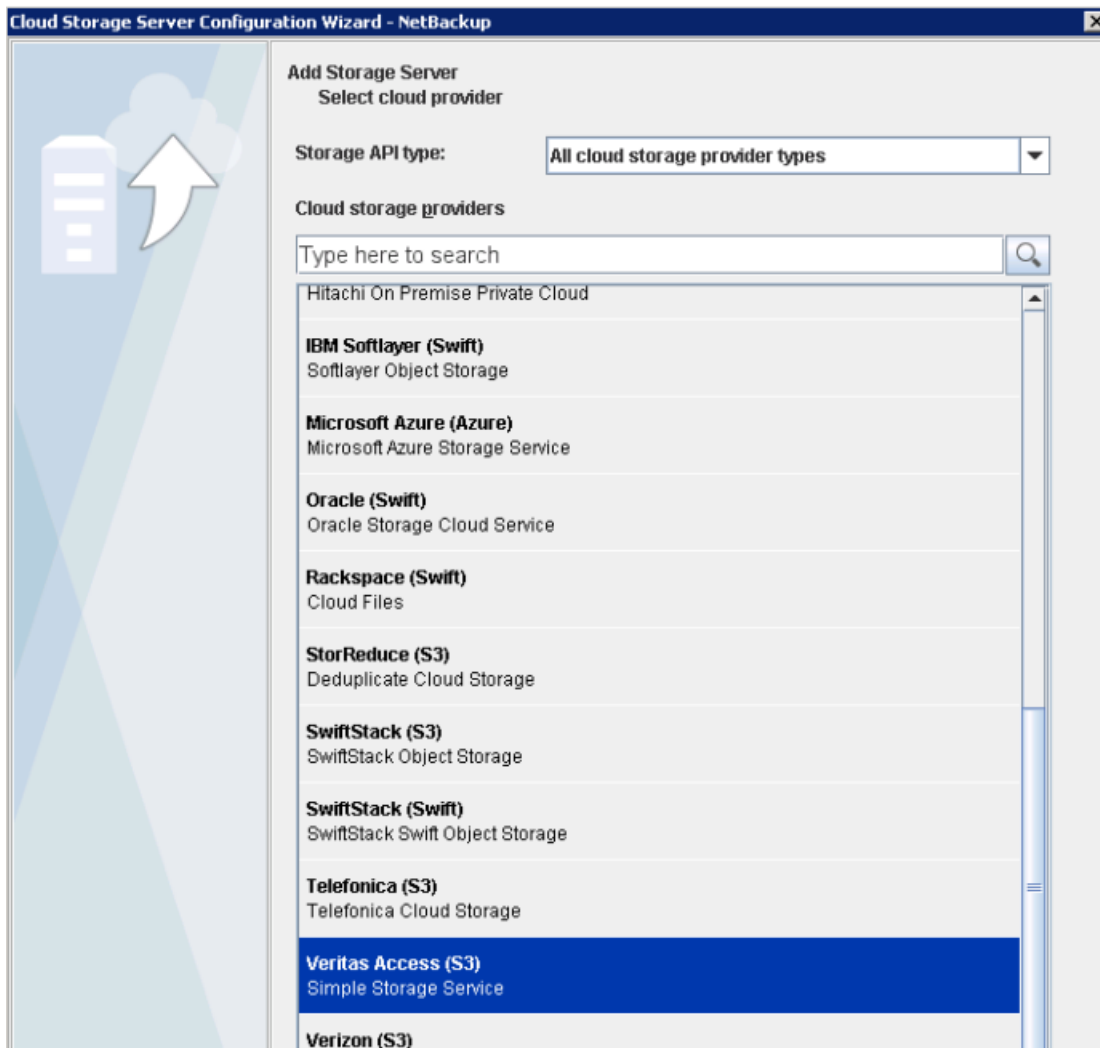
Configuring Veritas Access for NetBackup cloud storage

To configure Veritas Access for NetBackup cloud storage

- 1 Log on to the NetBackup Console and select **Configure Cloud Storage Server**.



- 2 From the **Cloud Storage Server Configuration** wizard, select **Veritas Access (S3)**.



- 3 Add the required information such as **Service host**, **Service endpoint**, **HTTP/HTTPS port**, **Access key ID**, **Secret access key**, and follow the rest of the wizard prompts.

Cloud Storage Server Configuration Wizard - NetBackup

Add Storage Server
 Select a media server and provide cloud storage service credentials. To be listed below in the media server drop-down list a security certificate must be deployed and NetBackup must be running including the NetBackup CloudStore Service Container (nbcssc).

Cloud storage provider: Veritas Access

Service host: s3.nbappclust

Storage server name:

Add Cloud Storage

Media server name: schahed01v01.nbgba.veritas.com

Deduplication
☐ Deduplicate data using MSDP before writing to cloud storage

Local cache directory:

Access details for Veritas Access account

Access key ID:

Secret access key:

Add Cloud Storage

General Settings | Region Settings

Provider type: Veritas Access

Service host:

Service endpoint:

HTTP port: 80

HTTPS port: 443

Storage server name:

Endpoint access style: Path Style

OK **Cancel** **Help**

Cloud Storage Server Configuration Wizard - NetBackup

Add Storage Server
 Select a media server and provide cloud storage service credentials. To be listed below in the media server drop-down list a security certificate must be deployed and NetBackup must be running including the NetBackup CloudStore Service Container (nbcssc).

Cloud storage provider: Veritas Access

Service host: s3.nbappclust

Storage server name:

Add Cloud Storage

Media server name: schahed01v01.nbgba.veritas.com

Deduplication
☐ Deduplicate data using MSDP before writing to cloud storage

Local cache directory:

Access details for Veritas Access account

Access key ID:

Secret access key:

Add Cloud Storage

General Settings | Region Settings

Provider type: Veritas Access

Service host:

Service endpoint:

HTTP port: 80

HTTPS port: 443

Storage server name:

Endpoint access style: Path Style

OK **Cancel** **Help**

Troubleshooting

This chapter includes the following topics:

- [Unmounting the SDFS volume before restarting Veritas Access or the NetBackup media server](#)
- [Upgrading SDFS from earlier versions to 7.4.2](#)
- [Log locations for troubleshooting](#)
- [Changing log levels](#)
- [Additional resources](#)
- [Generating Veritas Access S3 server keys using the helper script](#)
- [OpenDedup tuning recommendations](#)

Unmounting the SDFS volume before restarting Veritas Access or the NetBackup media server

Before restarting Veritas Access or the NetBackup media server, create a backup copy of the SDFS volume and unmount the SDFS volume.

To perform a clean unmount of the SDFS volume

- 1 Create a backup copy of the SDFS volume .xml file in the `/etc/sdfs` directory.
- 2 Unmount the SDFS volume and wait for the `jsvc` process to exit before restarting Veritas Access.
- 3 In case of OpenDedup on Veritas Access, use the following command to offline the OpenDedup volume:

```
# openedup volume offline <vol_name>
```

Where `vol_name` is the OpenDepdup volume.

Upgrading SDFS from earlier versions to 7.4.2

- If you are an existing customer and have taken backup with an SDFS version earlier than 7.3.1.2 , you have to set the `dist-layout` parameter to `false` in the extended config `volume.xml` file before mounting the SDFS volume.
- If you are an existing customer and have taken backup with SDFS 7.3.1.2 and later versions without setting the `dist-layout` parameter to `false`, and if there is a problem with restore, you have to unmount the SDFS volume, set the `retry-layout` parameter to `true` in the `volume.xml` file and remount the SDFS volume before you start restore.

Note: The default value of the `dist-layout` parameter is `true`.

- If you are a new customer, no modification is required.

Sample from the `volume.log` file:

```
<extended-config allow-sync="false"
block-size="30 MB"
data-appendix=".data"
delete-unclaimed="true"
disabledDNSBucket="false"
dist-layout="true"
retry-layout="true"
glacier-archive-days="0"
io-threads="16"
local-cache-size="10 GB"
map-cache-size="200"
read-speed="0"
refresh-blobs="false"
```

```
retry-layout="true"
simple-metadata="true"
simple-s3="true"
sync-check-schedule="4 59 23 * * ?"
sync-files="true"
upload-thread-sleep-time="10000"
use-basic-signer="true"
write-speed="0">
```

Log locations for troubleshooting

OpenDedup logs

- /opt/VRTSnas/log/odd.log
- /opt/VRTSnas/log/odd-vcs.log

Veritas Access S3 logs

- /opt/VRTSnas/log/portald.log
- /opt/VRTSnas/log/portald_access.log

SDFS logs

SDFS creates its logs under

/var/logs/sdfs/<volume-name>-volume-cfg.xml.log. Errors can be identified in this log file.

OST plug-in logs

The OpenDedup OST plug-in log can be found in /tmp/logs/opendedup.log.

NetBackup logs

Pertinent OST-related errors and logging are trapped in the `bptm` log. NetBackup logging for `bptm` can be enabled by creating the `bptm` logging directory:

```
mkdir /usr/openv/netbackup/logs/bptm
```

Veritas Access support debug information upload command

```
CLISH> support debuginfo upload path
```

Changing log levels

The logging framework for SDFS is updated to log4j2. For SDFS 7.4.1 and later releases, changing the log levels using the `volume.xml` is not effective. You have to update the `/etc/sdfs/log4j2.xml` file.

To change the log level:

- Edit the `/etc/sdfs/log4j2.xml` file.
- Go to the `Loggers` section.
- Search for `Logger name="sdfs"`
- Set the level to an appropriate parameter.

For example:

```
<Loggers>
<Logger name="sdfs" additivity="false" level="debug">
<appender-ref ref="sdfsLog" />
```

The following log levels are available:

- `trace`
- `debug`
- `info`
- `warn`
- `error`
- `fatal`

You can find more details about the `log4j2.xml` parameters at <https://logging.apache.org/log4j/log4j-2.2/manual/configuration.html>.

Additional resources

See the following documentation for more information on Veritas Access, OpenDedup, and Veritas NetBackup:

- *Veritas Access Installation Guide* for the supported NetBackup clients and the OpenDedup ports.
- *Veritas Access Troubleshooting Guide* for setting the NetBackup client log levels and debugging options.
- *Veritas NetBackup* product documentation on the [SORT](#) website.

- *OpenDedup* product documentation on the [OpenDedup website](#).

Generating Veritas Access S3 server keys using the helper script

Create the access and the secret keys using the Veritas Access helper script in case you do not want to use the Active directory Domain user to create and own the buckets. This is an alternative way to get the Veritas Access S3 server credential keys.

- Location of the helper script:
`/opt/VRTSnas/scripts/utils/objectaccess/objectaccess_client.py`
- The Veritas Access helper script can be used from any client system that has Python installed.
- To run the script, your S3 client needs to have the `argparse` and `requests` Python modules.
If these modules are missing, install both these modules using `pip` or `easy_install`.
- Add the `ADMIN_URL` name in your `/etc/hosts` file.
where the `ADMIN_URL` is `admin.<cluster_name>` and the port is 8144. This url should point to the Veritas Access management console IP address.
- Create the access and the secret key using the Veritas Access helper script by providing the user name, password, and `ADMIN_URL` (check the online Help of the Veritas Access helper script for all of the provided operations like `list key` and `delete key`).

Create a secret key:

```
clus_01:~ # ./objectaccess_client.py --create_key
--server admin.clus:8144 --username localuser1 --password root123
--insecure
UserName                : localuser1
AccessKeyId              : Y2FkODU2NTU2MjVhYzV
Status                   : Active
SecretAccessKey          : ODk0YzQxMDhkMmRjM2M5OTUzNjI5OWIzMdgyNzY
```

The `<localuser1>` is the local user created on both the Veritas Access cluster nodes with same unique ID.

List a secret key for the specified user:

```
clus_01:~ # ./objectaccess_client.py --list_key --server
admin.clus:8144 --username localuser2 --password root123 --insecure
```

Delete a secret key for the specified user:

```
clus_01:~ # ./objectaccess_client.py --delete_key
ZTkyNDdjZTViM2EyMWZ --server admin.clus:8144 --username localuser2
--password root123 --insecure
```

- If the object server is enabled without the `SSL` option, you need to add the `--insecure` option.

```
clus_01 ~# ./objectaccess_client.py --server
admin.clus:8144 --username <uname> --create_key --insecure
```

OpenDedup tuning recommendations

OpenDedup has a flexible design that works for small users as well as large data enterprises. You can tune OpenDedup as per your requirements to serve your use case. Veritas recommends that you perform the following tuning before you start using the LTR solution.

Table 9-1 XML tags

XML parameter	Value
max-open-files	200
write-threads	32
io-threads	64 (within extended config)
map-cache-size	1024
local-cache-size	500 GB (as per your local cache)
sync-on-write	false
refresh-blobs	true (only to be set when Glacier cloud tier is used)
glacier-archive-days	30 (only to be set when Glacier cloud tier is being used)
sync-files	true (within extended config)
chunk-size	40960
hash-type	VARIABLE_MD5

Table 9-1 XML tags (*continued*)

XML parameter	Value
max-file-writebuffers	80

On the media server for the ODD-on-Media_Server use case:

```
# echo "* hard nofile 65535" >> /etc/security/limits.conf
# echo "* soft nofile 65535" >> /etc/security/limits.conf
# exit
```

Based on the system workload, ensure that the number of portal threads are increased (on Veritas Access):

```
/opt/VRTSnas/conf/portald.conf >> cf_max_s3_threads
```

Index

A

- about
 - backup storage for NetBackup 9
 - Veritas Access 7
 - Veritas Data Deduplication 16
- adding
 - external NetBackup master server to work with Veritas Access 126
 - NetBackup media server 126
- adding or deleting patterns
 - included in the list of files for backups 129
- additional resources
 - documentation 144

B

- back up
 - Veritas Access file system over a SAN client 133
- backing up deduplicated data
 - using S3 protocol 48
- backing up NetBackup data
 - deduplicating data on Veritas Access 49
- backup
 - displaying excluded files 128
- backup and restore 107
- backup or restore
 - NetBackup snapshot 134
- backup services
 - displaying the status of 131
 - starting 131
 - stopping 131
- backup storage for NetBackup 9

C

- changing
 - log levels 144
- configuring
 - backups using NetBackup or other third-party backup applications 132
 - NetBackup virtual IP address 130
 - NetBackup virtual name 130

- configuring *(continued)*
 - Veritas Data Deduplication 19, 22
- configuring NetBackup
 - prerequisites 124
- configuring using GUI
 - Veritas Data Deduplication 26
- configuring Veritas Access
 - NetBackup cloud storage 138
 - using CloudCatalyst 80
- configuring Veritas Access as a cloud storage server 80
- Configuring Veritas Access for NetBackup workflow 125
- creating
 - Storage Lifecycle Policies 101
- Creating a Media Server Deduplication Pool
 - primary backup using NetBackup 56
- creating a MSDP
 - primary backup using NetBackup 56
- creating a storage unit
 - NetBackup console 64
- creating an OST disk pool
 - NetBackup console 64
- creating S3 bucket
 - storing deduplicated backup data 50, 78

D

- deleting
 - configured NetBackup media server 126
- disabling
 - NetBackup SAN client 125
- displaying
 - excluded files from backup 128
 - included files for backups 128
 - NetBackup configurations 131
 - status of backup services 131

E

- enabling
 - NetBackup SAN client 125

- enabling SSL
 - copy the certificate to NetBackup 97
- excluded files
 - displaying 128

G

- generating Veritas Access S3 server keys
 - using the helper script 145
- global deduplication
 - Veritas Data Deduplication 40

I

- included files
 - for backups 128
- installing
 - NetBackup client 134
- integration with Veritas Access
 - NetBackup 7

L

- log locations
 - troubleshooting 143

M

- migrating
 - Veritas Data Deduplication 42

N

- NetBackup
 - configuring 132
 - configuring NetBackup virtual IP address 130
 - configuring virtual name 130
 - displaying configurations 131
 - integration with Veritas Access 7
 - Snapshot Client 124
 - snapshot methods 124
- NetBackup master server
 - configuring to work with Veritas Access 126
- NetBackup media server
 - adding 126
 - deleting 126
 - setting up multiple SDFS volumes 73
- NetBackup SAN client
 - disabling 125
 - enabling 125
- NetBackup snapshot
 - backup or restore 134

O

- OpenDedup
 - workflow 47
- OpenDedup installation
 - system requirements 13
- OpenDedup tuning
 - recommendations 146

P

- patterns
 - adding or deleting from the list of files included
 - in backups 129
- policy creation 107
- prerequisites
 - configuring NetBackup 124

R

- registering
 - NetBackup master server 126
- resetting
 - NetBackup master server 126
 - virtual IP address of NetBackup 130
- restoring backup files 120
- running a backup policy
 - manually 114

S

- SAN client
 - back up 133
- SDFS volume
 - unmounting before rebooting Veritas Access 141
- setting up multiple NetBackup media servers 72
- setting up multiple SDFS volumes
 - NetBackup media server 73
- snapshot methods
 - NetBackup 124
- starting
 - backup services 131
- stopping
 - backup services 131
- Storage Lifecycle Policies
 - creating 101
- supported configurations and versions
 - NetBackup with CloudCatalyst 14
 - NetBackup with OpenDedup 14
 - NetBackup with Veritas Data Deduplication 13
- system requirements
 - OpenDedup installation 13

system requirements *(continued)*

- supported configurations and versions for
NetBackup with CloudCatalyst 14
- supported configurations and versions for
NetBackup with OpenDedup 14
- supported configurations and versions for
NetBackup with Veritas Data Deduplication 13

T

- troubleshooting
 - log locations 143

U

- uninstalling
 - NetBackup client 134
- unmounting
 - SDFS volume before rebooting Veritas
Access 141
- upgrade
 - SDFS 142
- use case
 - backing up deduplicated data 48
 - backing up NetBackup data 49
 - long-term data retention 9
- using the helper script
 - generating Veritas Access S3 server keys 145
- using Veritas Data Deduplication
 - benefits 18

V

- Veritas Data Deduplication
 - about 16
 - configuring 22
 - configuring using GUI 19, 26
 - global deduplication 40
 - migration 42
- virtual IP address
 - configuring or changing for NetBackup 130
- virtual name
 - configuring for NetBackup 130

W

- Workflow
 - configuring Veritas Access for NetBackup 125