

Veritas Access NetBackup Solutions Guide

Linux

7.4

Veritas Access NetBackup Solutions Guide

Last updated: 2018-08-13

Document version: 7.4 Rev 2

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:

doc.feedback@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	6
	About Veritas Access	6
	About Veritas Access as a NetBackup client	6
	About Veritas Access as backup storage for NetBackup	8
	Use cases for long-term data retention	8
	Benefits of using Veritas Access with NetBackup and OpenDedup/CloudCatalyst	10
Chapter 2	System requirements	11
	System requirements for OpenDedup installation	11
	Supported configurations and versions for NetBackup with OpenDedup	12
	Supported configurations and versions for NetBackup with CloudCatalyst	12
Chapter 3	Configuring Veritas Access backup over S3 with OpenDedup and NetBackup	14
	Workflow for OpenDedup	14
	Use case 1: Backing up deduplicated data (OpenDedup and NetBackup) using the S3 protocol to Veritas Access	15
	Use case 2: Backing up data (NetBackup) and deduplicating the data (OpenDedup) on Veritas Access	16
	Creating an S3 bucket on Veritas Access for storing deduplicated backup data from NetBackup	17
	Creating a Media Server Deduplication Pool (MSDP) for primary backup using NetBackup	23
	Creating an OST disk pool and STU in the NetBackup console	31
	Setting up multiple NetBackup media servers in the same domain	39
	Setting up multiple SDFS volumes on a NetBackup media server	40

Chapter 4	Configuring Veritas Access as a cloud storage server with NetBackup CloudCatalyst	44
	Creating an S3 bucket on Veritas Access for storing deduplicated backup data from NetBackup	45
	Configure Veritas Access as a cloud storage server on NetBackup server	47
Chapter 5	Configuring backup and restore using NetBackup policies	64
	Storage Lifecycle Policies	64
	Backup and restore	70
	Running a backup policy manually	77
	Restoring backed up files	83
Chapter 6	Troubleshooting	86
	Unmounting the SDFS volume before restarting Veritas Access or the NetBackup media server	86
	Log locations for troubleshooting	87
	Additional resources	87
	Generating Veritas Access S3 server keys using the helper script	88
Index	90

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](#)
- [Benefits of using Veritas Access with NetBackup and OpenDedup/CloudCatalyst](#)

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

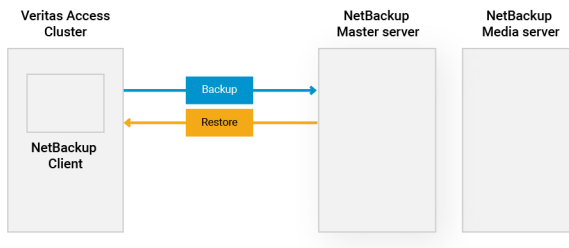
Veritas Access is integrated with Veritas NetBackup so that a NetBackup administrator can back up your Veritas Access file systems to NetBackup master or media servers and retain the data as per your company policy. Once data is backed up, a storage administrator can delete unwanted data from Veritas 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 Veritas Access interfaces:

- **CLISH**
The Veritas Access CLISH 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 on Veritas Access.
- **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

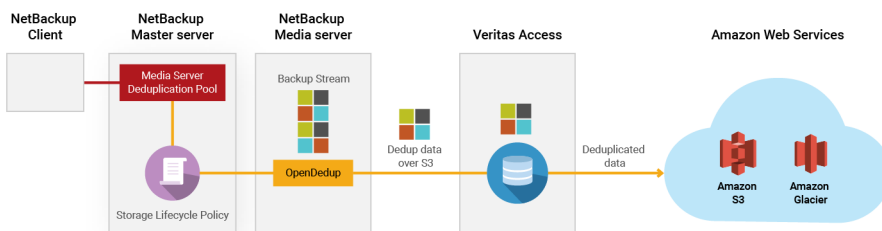
The following are the use cases for long-term data retention (LTR) with OpenDedup:

Use Case 1: 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 [“Use case 1: Backing up deduplicated data \(OpenDedup and NetBackup\) using the S3 protocol to Veritas Access”](#) on page 15.

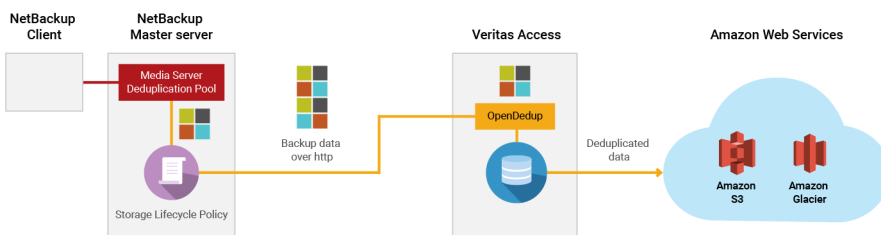
Figure 1-2 OST and OpenDedup hosted on a NetBackup master and/or media server



Use Case 2: 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 [“Use case 2: Backing up data \(NetBackup\) and deduplicating the data \(OpenDedup\) on Veritas Access”](#) on page 16.

Figure 1-3 OST hosted on a NetBackup master and/or media server

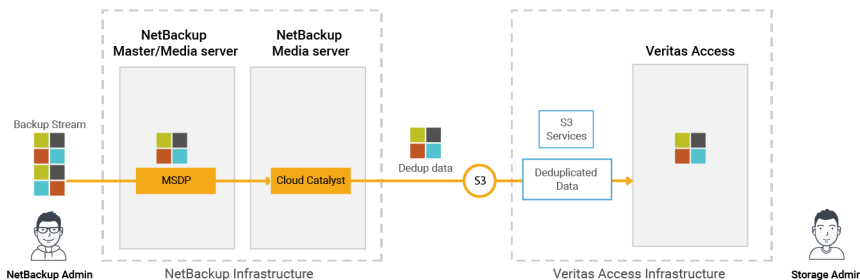


Use Case 3: Veritas Access with CloudCatalyst

- 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 [“Creating an S3 bucket on Veritas Access for storing deduplicated backup data from NetBackup”](#) on page 45.

Figure 1-4 Primary backup data deduplicated by MSDP and stored on the NetBackup server



Use Case 4: Veritas Access as an S3 connector

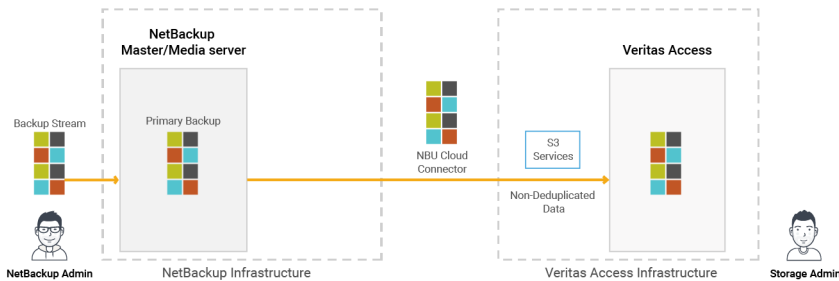
- Backup data is stored in non-deduplicated format on the NetBackup server as primary backup. The same primary backup data is moved to Veritas Access through SLP over the Veritas Access S3 protocol.

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 [“Configure Veritas Access as a cloud storage server on NetBackup server”](#) on page 47.

Figure 1-5 Backup data stored in non-deduplicated format on the NetBackup server as primary backup



Benefits of using Veritas Access with NetBackup and OpenDedup/CloudCatalyst

- Low-cost, flexible alternative for long-term data retention.
- Eliminate the need for cumbersome, time-consuming tape management.
- Cost-effective and resilient solution that is scale-out (linear performance) and elastic (grow/shrink on demand).

System requirements

This chapter includes the following topics:

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

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 2-1 Supported versions

OpenDedup	Veritas Access	Veritas NetBackup servers	OST
7.4	7.4	7.7.3 8.0 8.1 8.1.1 (Linux only)	2.2.9

Download links:

Veritas Access: Veritas Access 7.4 DVD

OpenDedup:

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

OpenStorage Technology (OST):

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

Supported configurations and versions for NetBackup with CloudCatalyst

Table 2-2 Supported versions

Veritas Access	Veritas NetBackup servers
7.4	8.1 8.1.1 (Linux only)

Download links:

Veritas Access: Veritas Access 7.4 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: 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 present at"

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

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

Configuring Veritas Access backup over S3 with OpenDedup and NetBackup

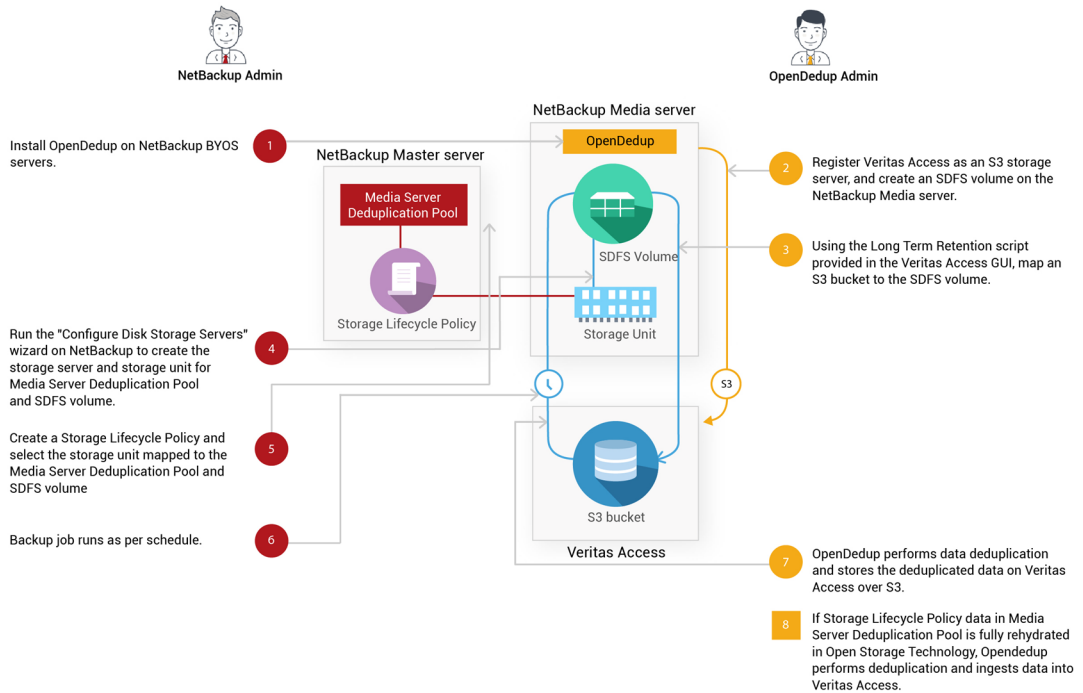
This chapter includes the following topics:

- [Workflow for OpenDedup](#)
- [Use case 1: Backing up deduplicated data \(OpenDedup and NetBackup\) using the S3 protocol to Veritas Access](#)
- [Use case 2: 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 3-1](#) illustrates the workflow for OpenDedup for Veritas Access.

Figure 3-1 Workflow for OpenDedup



Use case 1: 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 OST:

```
# wget https://sort.veritas.com/public/patchcentral/Linux/7.4/access/  
access-rhel7_x86_64-7.4ost.tar.gz  
# tar -xzvf access-rhel7-7.4ost.tar.gz  
# cd rpms/  
# tar -xzvf access-ost-7.4.tar.gz  
# cd dist/  
# ./media-install.sh
```

- 2 Run the following commands to replace the SDFS rpms with the latest rpms.

```
# rpm -e sdfs  
# wget https://sort.veritas.com/public/patchcentral/Linux/7.4/access/  
access-rhel7_x86_64-7.4sdfs.tar.gz  
# tar -xvf access-rhel7_x86_64-7.4sdfs.tar.gz  
# cd rpms/  
# rpm -ivh sdfs-7.4.0.0-1.x86_64.rpm
```

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

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

Use case 2: 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-7.4ost.tar.gz
# tar -zxvf access-rhel7_x86_64-Patch-7.4ost.tar.gz
# cd rpms/
# tar -zxvf access-ost-7.4.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 CLISH 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.

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.

- 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 will start listening on a specific port, usually starting from 6442.

Port information can be found using the `mount` command.

Example:

```
[root@host1 ~]# mount | grep opendedupe
sdfs:/etc/sdfs/S3fsl497346133-volume-cfg.xml:6443 on
/opendedupe/volumes/S3fsl497346133 type fuse
(rw,nosuid,nodev,allow_other,allow_other)
sdfs:/etc/sdfs/S3fsl497258807-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>
```

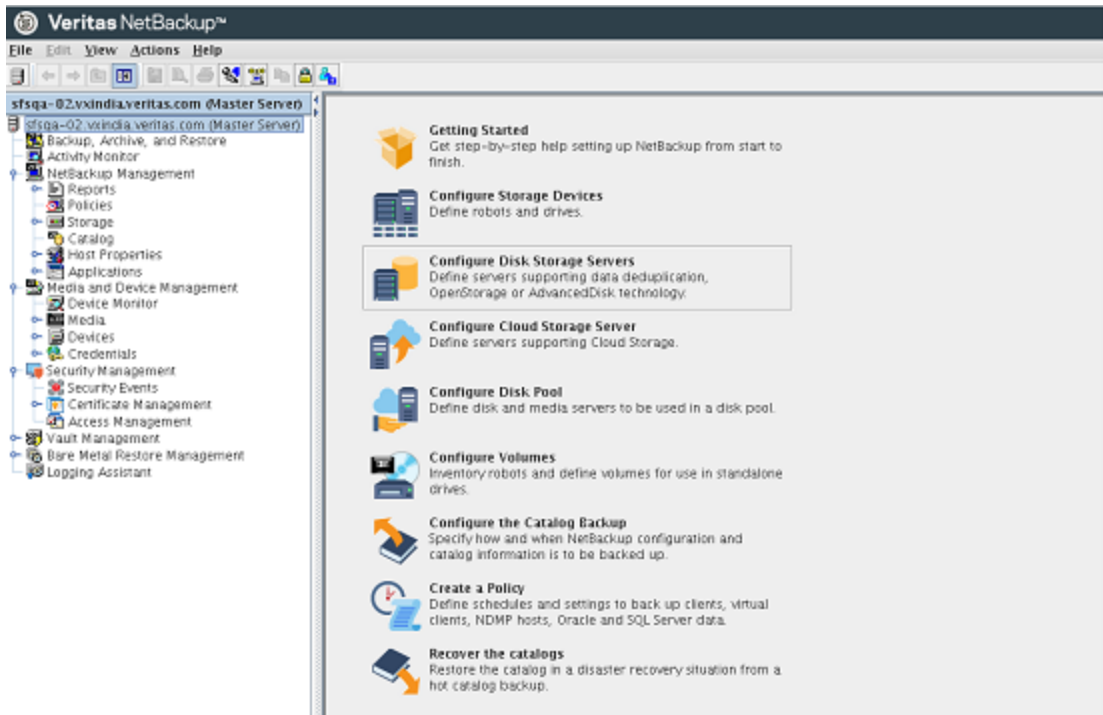
Use case 2: OpenDedup on Veritas Access

```
<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 the following fields: 'Media server:' with a dropdown menu showing 'sfsqa-02.vxindia.veritas.com'; 'Storage server type:' with a text box containing 'Media Server Deduplication Pool'; 'Storage server name:' with a text box containing 'sfsqa-02.vxindia.veritas.com'; and a 'Define credentials' section with 'User name:' (text box with 'root'), 'Password:' (text box with masked characters), and 'Confirm password:' (text box with masked characters). At the bottom 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 reads: '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 Server Configuration Wizard@dfsqa-02.vxindia.veritas.com

Storage Server Properties
Provide storage server properties.

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

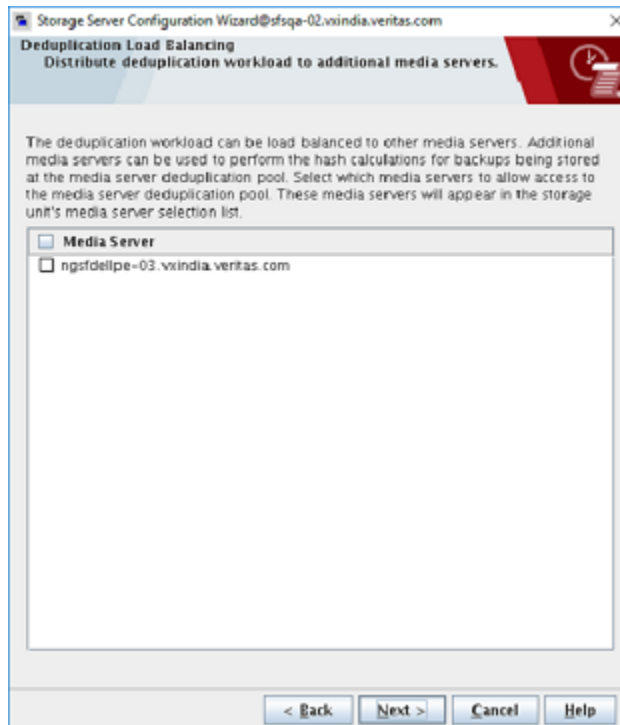
Interface:

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.

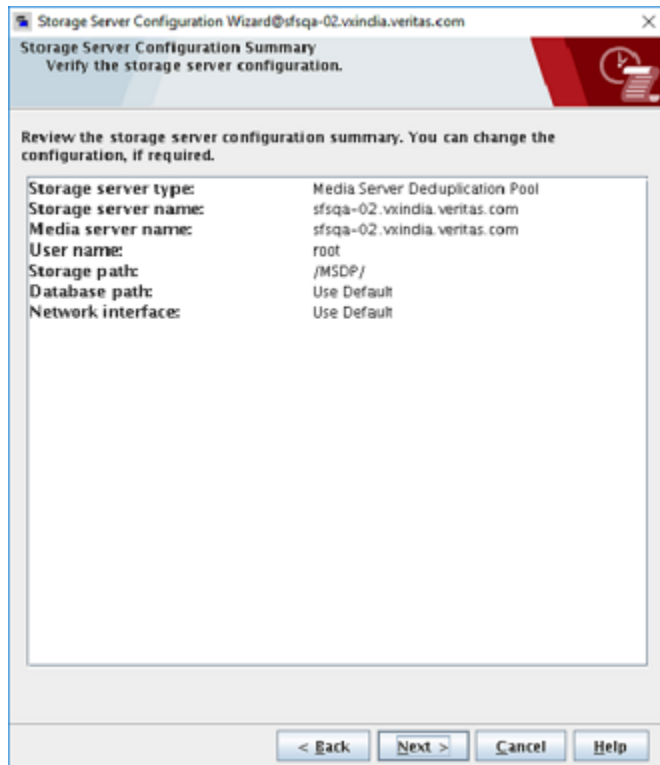
 Once you define the storage server details on this screen, you cannot modify them. For more information, click Help.

< Back Next > Cancel Help

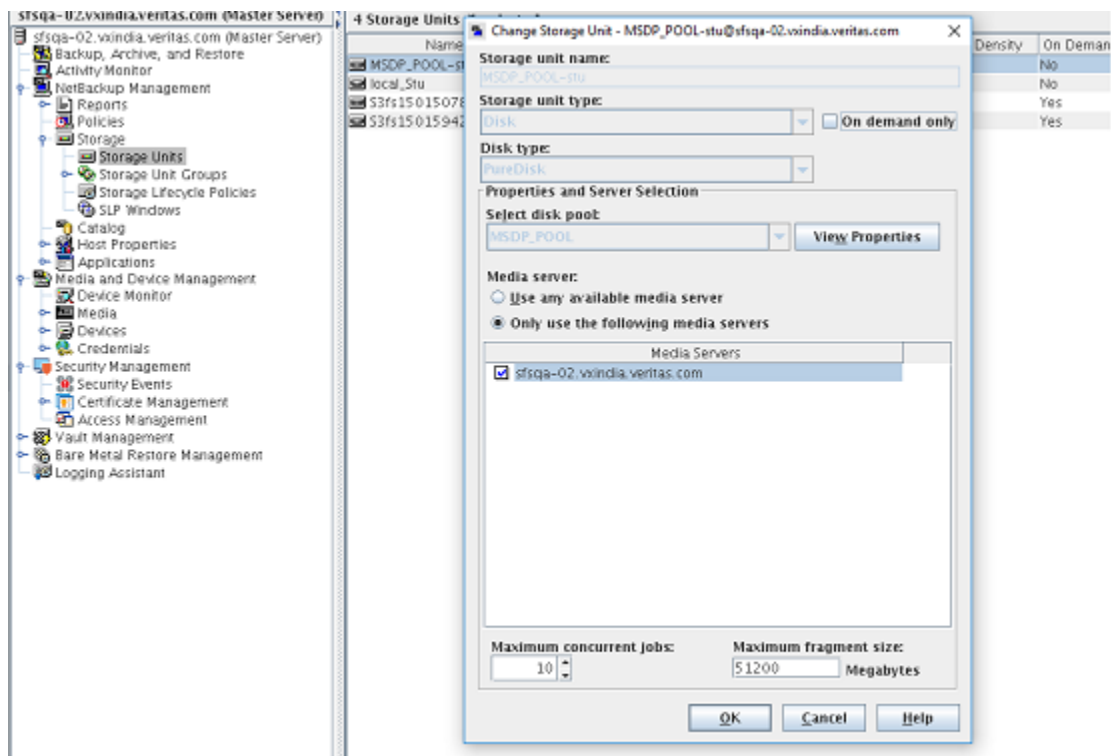
- 5 Enter the load balancing options to distribute the workload.



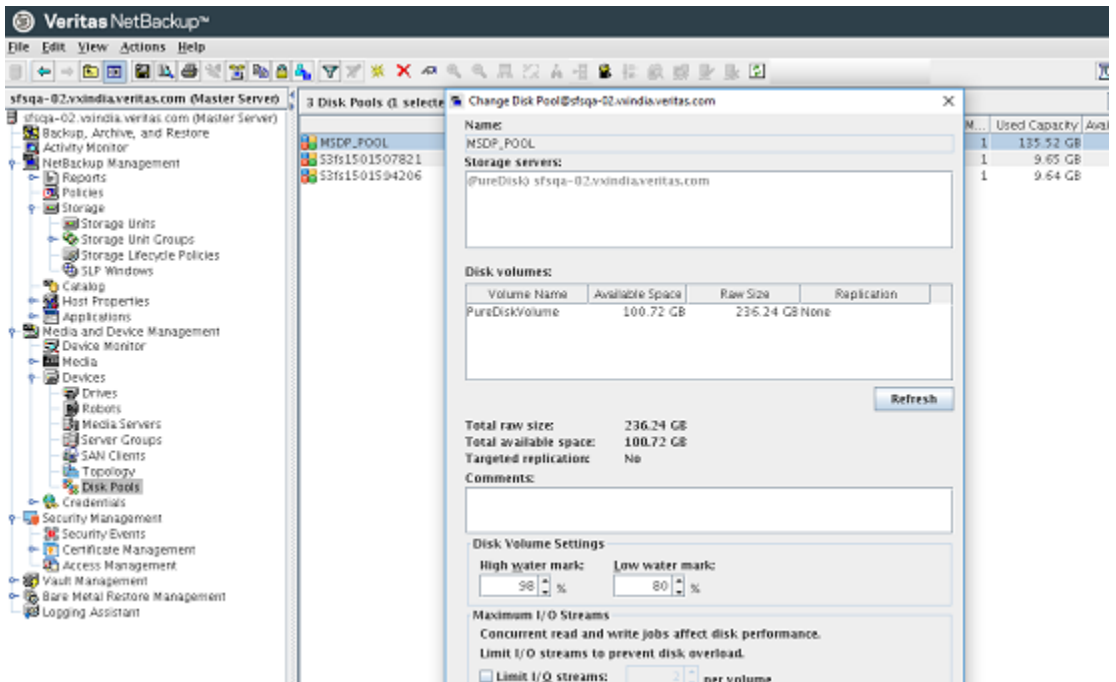
6 Verify the storage server configuration summary.



7 Verify that the storage unit is created for MSDP.



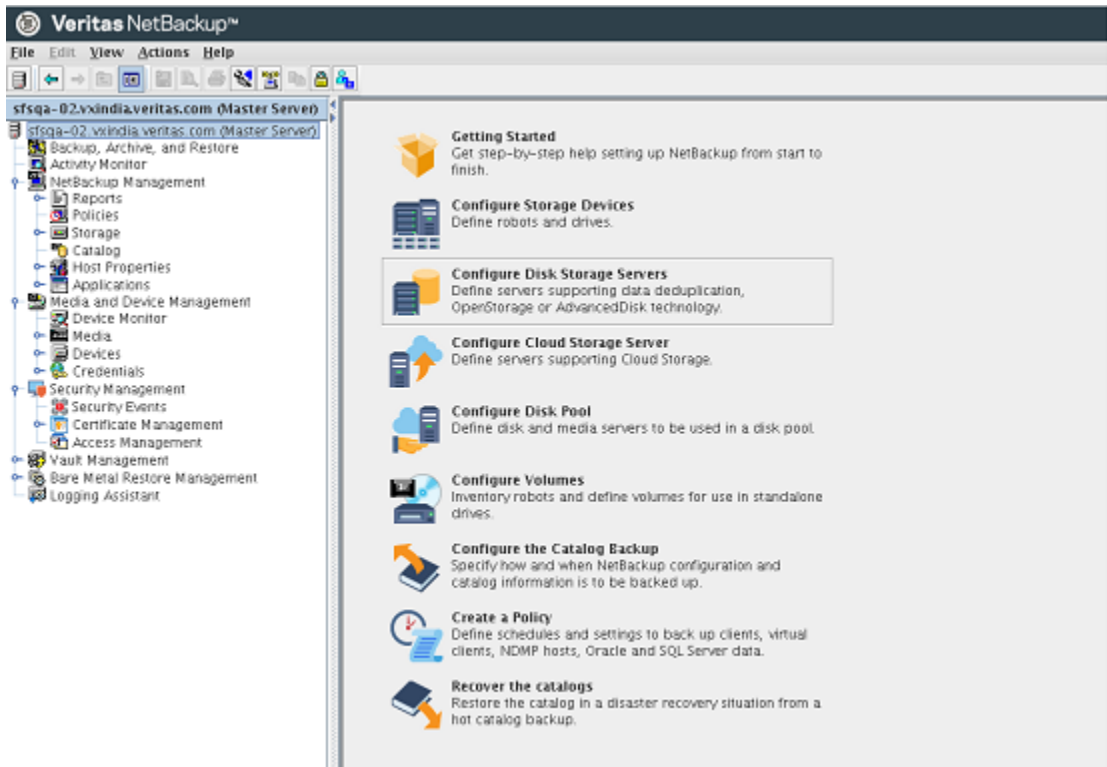
8 Verify that the disk pool is create for MSDP.



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

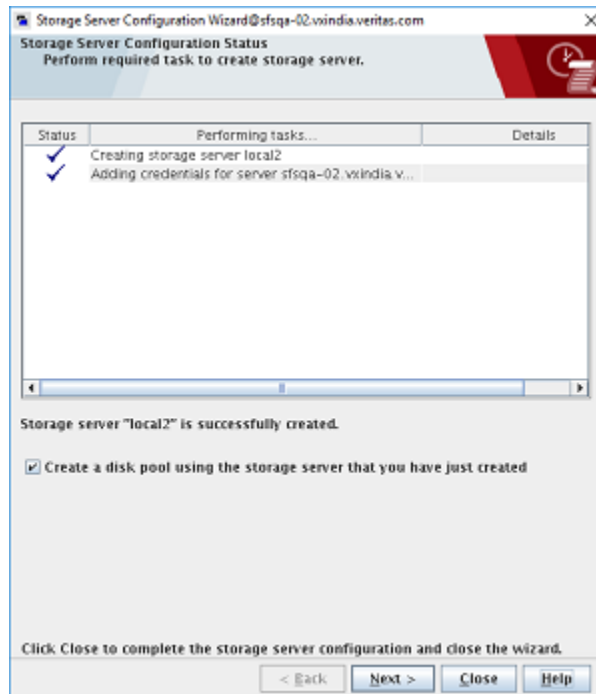
User name: root

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.

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

Select Disk Pool Properties and Volumes
 Select disk pool properties and volumes to use in the disk pool.

Storage server: local2
 Storage server type: OpenDedup
 Disk pool configured for: Backup

Disk Pool Properties and Volumes
 A disk pool inherits the properties of its volumes. Only volumes with similar properties can be added to a disk pool.
 If properties are specified, the list displays volumes that match the selected properties.

☐ Replication source
☐ Replication target

Select storage server volumes to add to the disk pool.

Volume Name	Available Space	Raw Size	Replication
<input checked="" type="checkbox"/> S3fs15016732B1	200.0 GB	200.0 GB	None

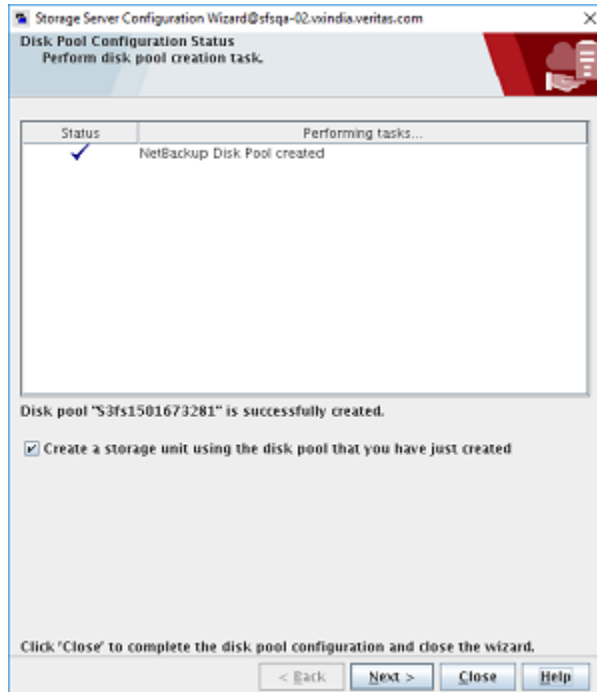
Total available space: 200.00 GB
 Total raw size: 200.00 GB

< Back Next > Cancel Help

- 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

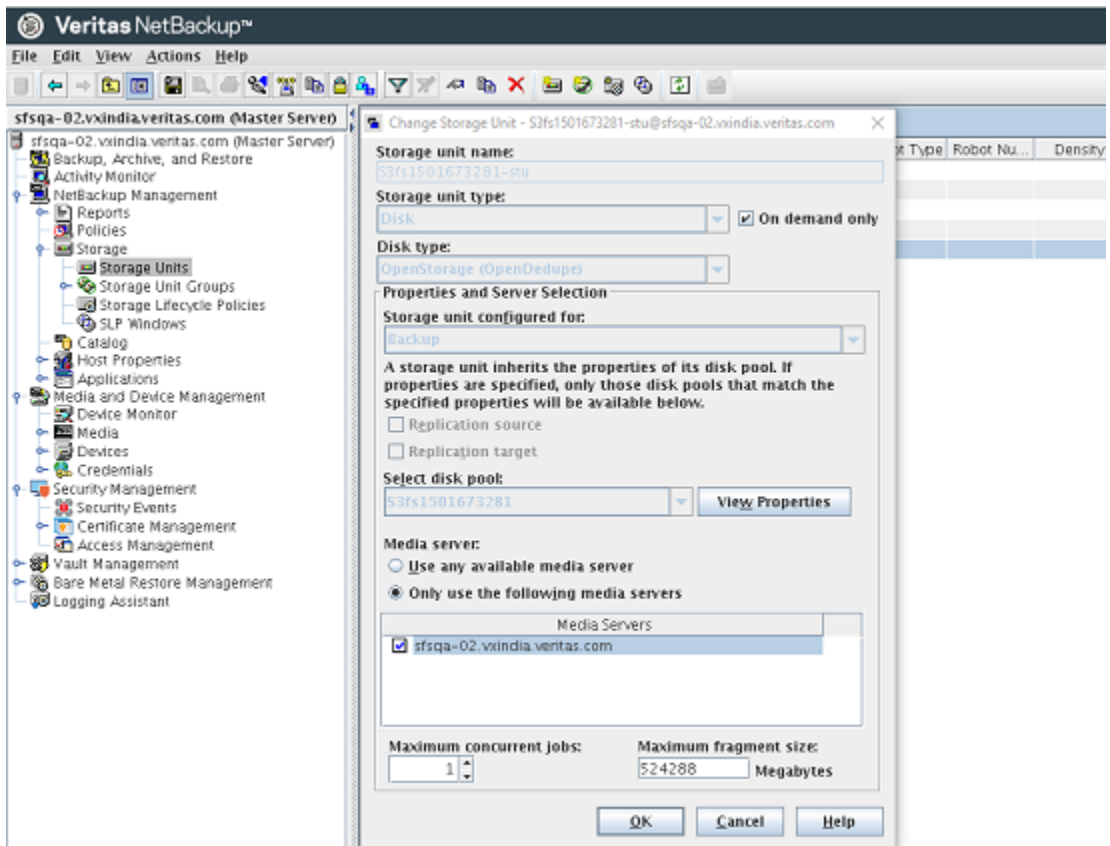
☒ sfsqa-02.vxindia.veritas.com

Maximum concurrent jobs: 1

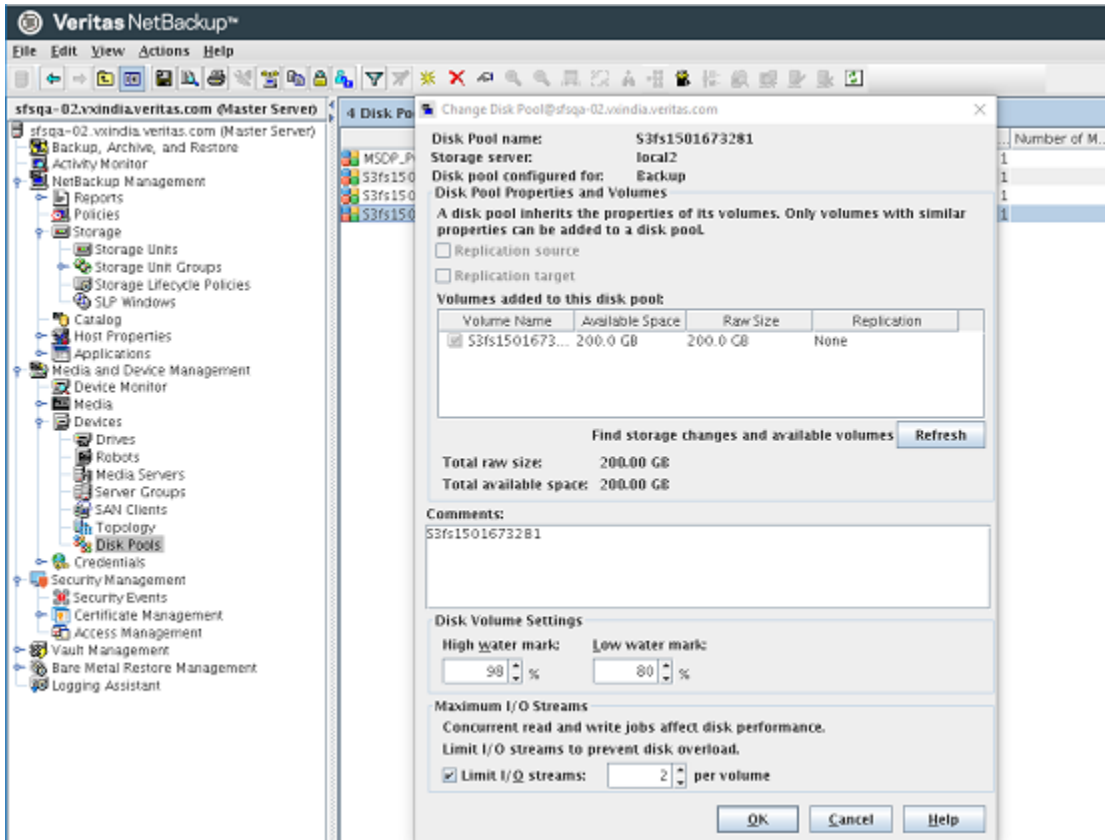
Maximum fragment size: 524288 Megabytes

< 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 [“Use case 1: Backing up deduplicated data \(OpenDedup and NetBackup\) using the S3 protocol to Veritas Access”](#) on page 15.

- 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 31.

See [“Use case 1: Backing up deduplicated data \(OpenDedup and NetBackup\) using the S3 protocol to Veritas Access”](#) on page 15.

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 [“Use case 1: Backing up deduplicated data \(OpenDedup and NetBackup\) using the S3 protocol to Veritas Access”](#) on page 15.

- 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](#)

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 CLISH 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 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.

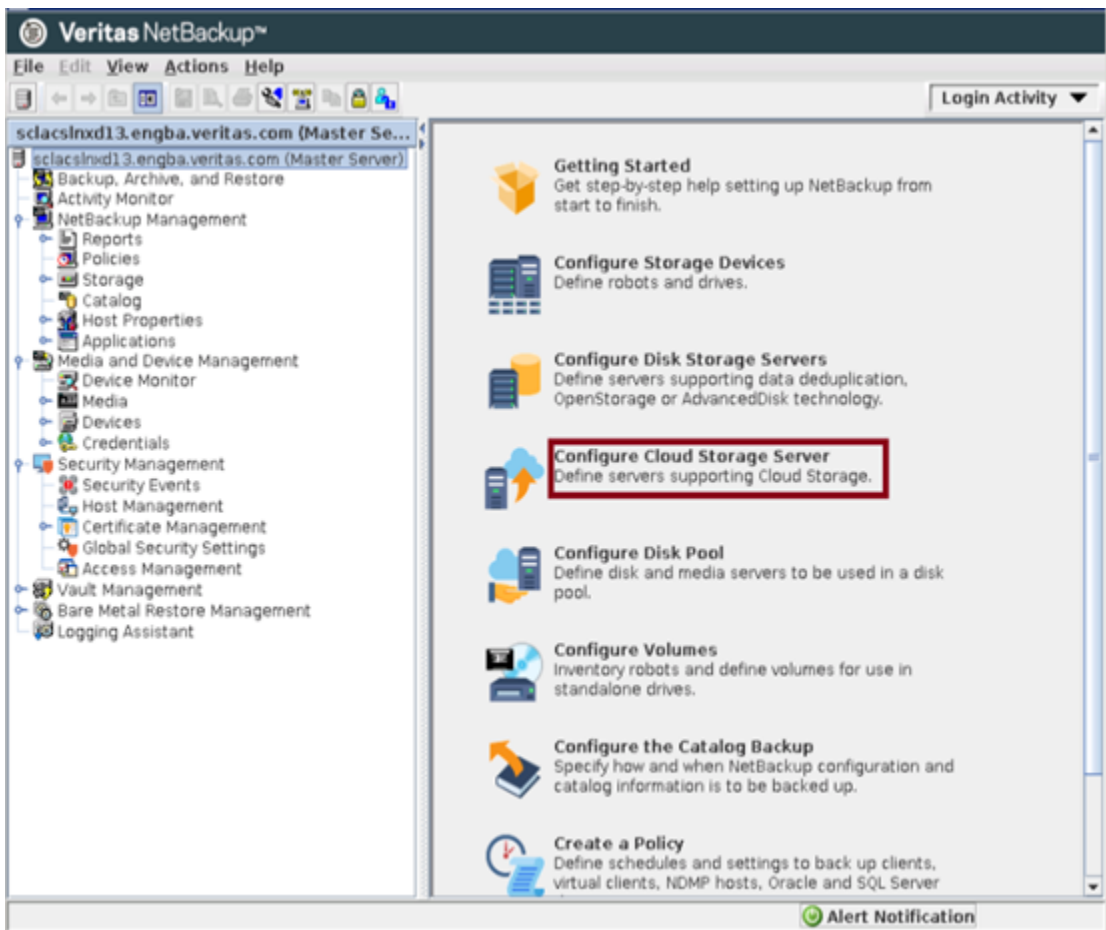
Creating a Media Server Deduplication Pool (MSDP) for primary backup using NetBackup

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 23.

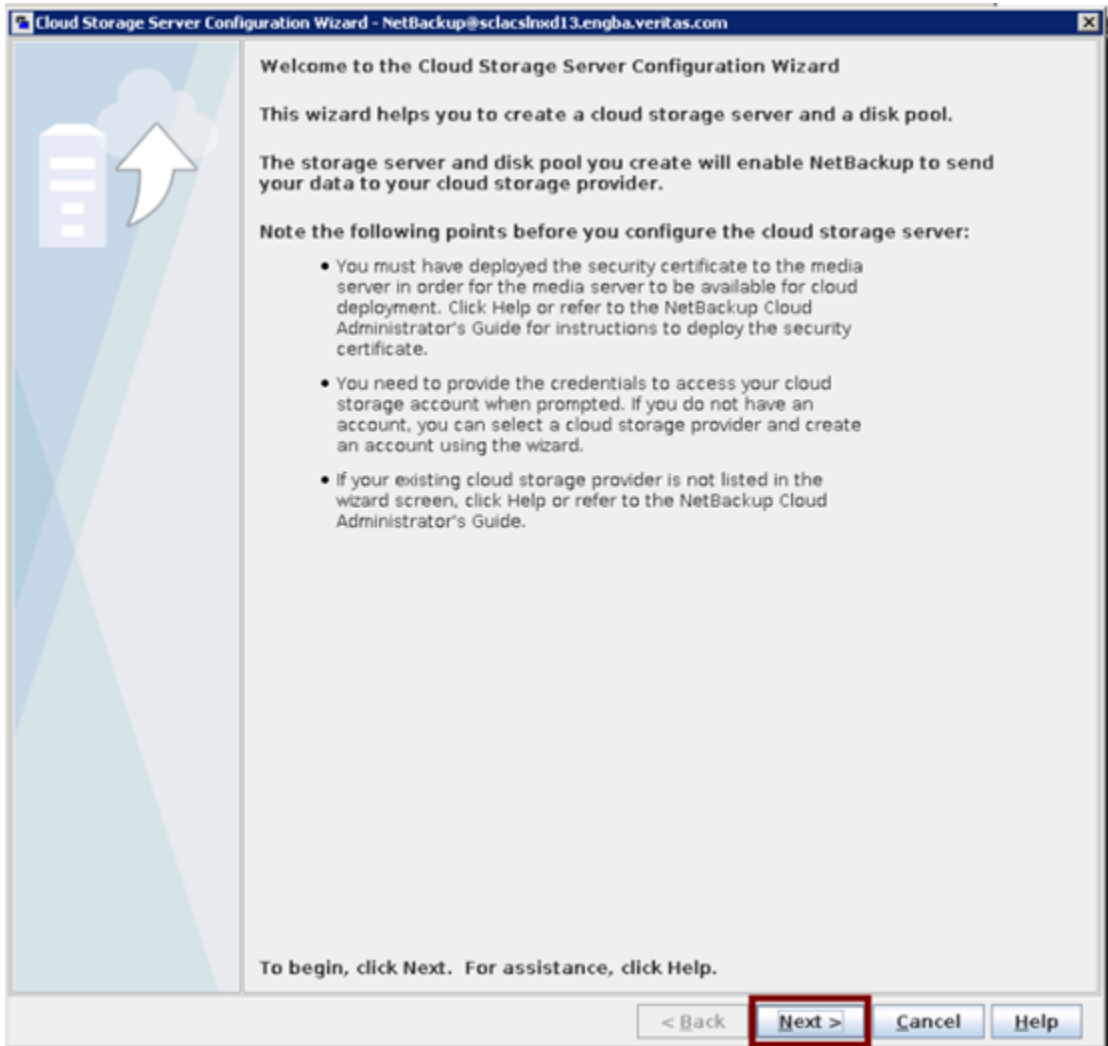
Configure Veritas Access as a cloud storage server on NetBackup server

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

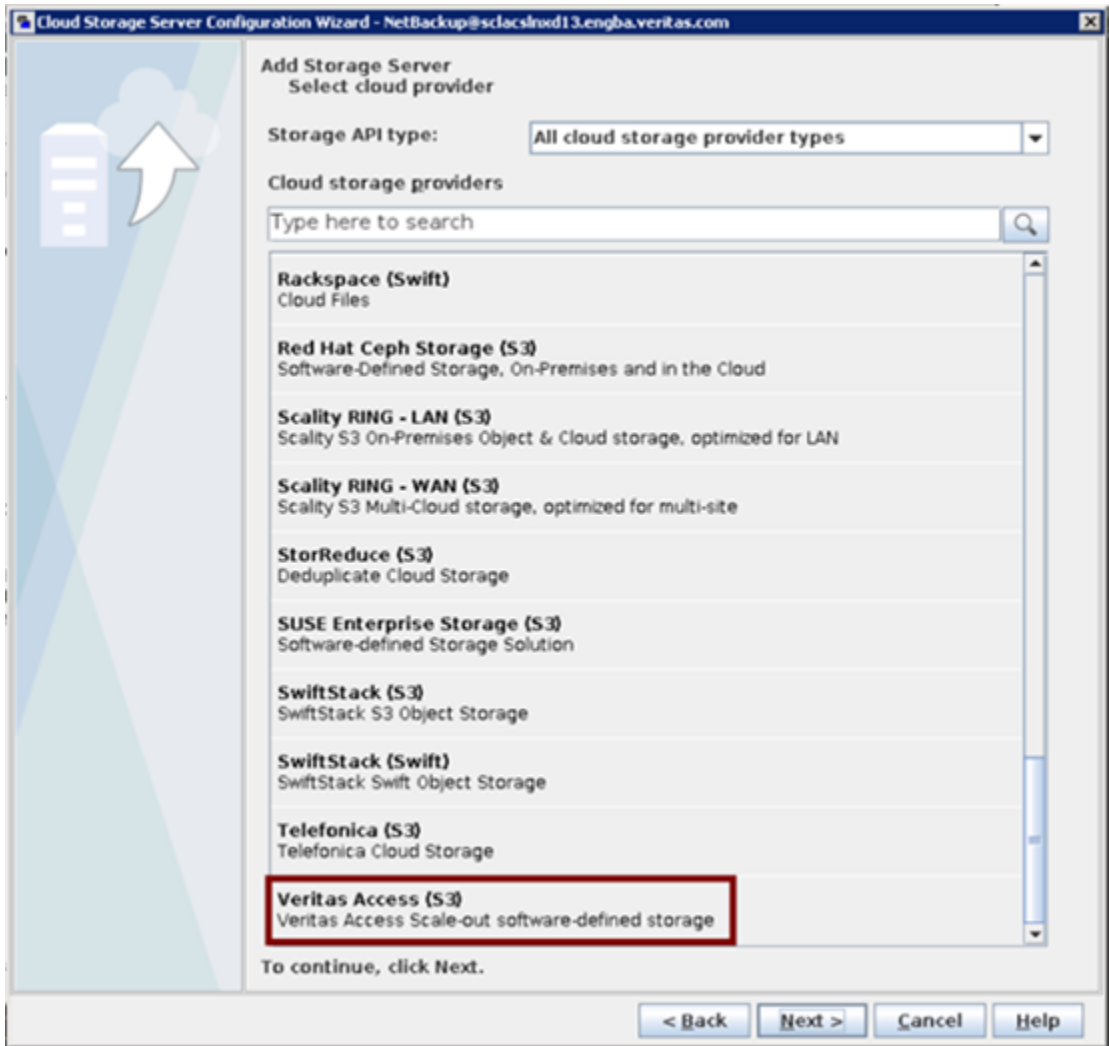
- 1 Log on to the NetBackup master server from the Java console.
- 2 Select **Configure Cloud Storage Servers**.



- 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**.

The screenshot shows the 'Cloud Storage Server Configuration Wizard - NetBackup@slclacslinx13.engba.veritas.com' window. The main window has a title bar and a sidebar with a cloud icon and an upward arrow. The main content area is titled 'Add Storage Server' and contains instructions: '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).' Below this, it says 'Cloud storage provider - Veritas Access' and 'Service host:'. A dialog box titled 'Add Cloud Storage@slclacslinx13.engba.veritas.com' is open in the foreground. It has two tabs: 'General Settings' and 'Region Settings'. The 'General Settings' tab is active and contains the following fields: 'Provider type: Veritas Access', 'Service host: s3.accesscluster', 'Service endpoint:', 'HTTP port: 8143', 'HTTPS port: 8143', 'Storage server name: my-s3.accesscluster', and 'Endpoint access style: Path Style'. The 'Ok' button is highlighted with a red rectangle. Below the dialog box, there is a link 'Create an account with Veritas Access.' and an 'Advanced Settings' button. At the bottom of the main window, there is a message 'To continue, click Next.' and a set of navigation buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

Cloud Storage Server Configuration Wizard - NetBackup@slclacslinx13.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:

Add Cloud Storage@slclacslinx13.engba.veritas.com

General Settings Region Settings

Provider type: Veritas Access
Service host: s3.accesscluster
Service endpoint:
HTTP port: 8143
HTTPS port: 8143
Storage server name: my-s3.accesscluster
Endpoint access style: Path Style

Ok Cancel Help

Create an account with Veritas Access.

Advanced Settings

To continue, click Next.

< Back Next > Cancel Help

- 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 local cache directory for CloudCatalyst. Enter the access key and secret key using which the bucket is created on Veritas Access. For SSL-related settings, click on **Advance Setting**.

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: s3.accesscluster

Storage server name: my-s3.accesscluster

Add Cloud Storage

Media server name: sciacslnxd13.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:

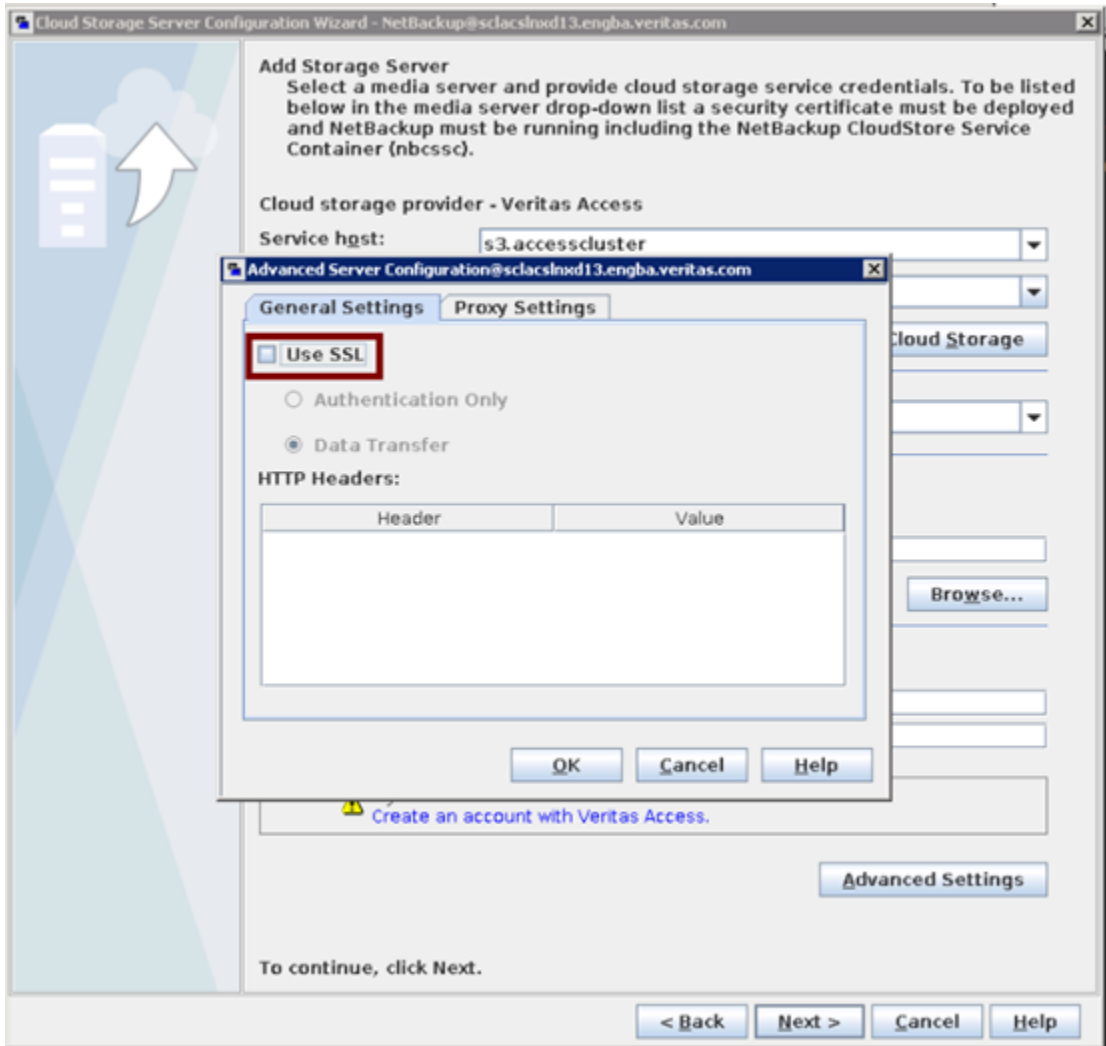
If you do not have Veritas Access account [Create an account with Veritas Access.](#)

Advanced Settings

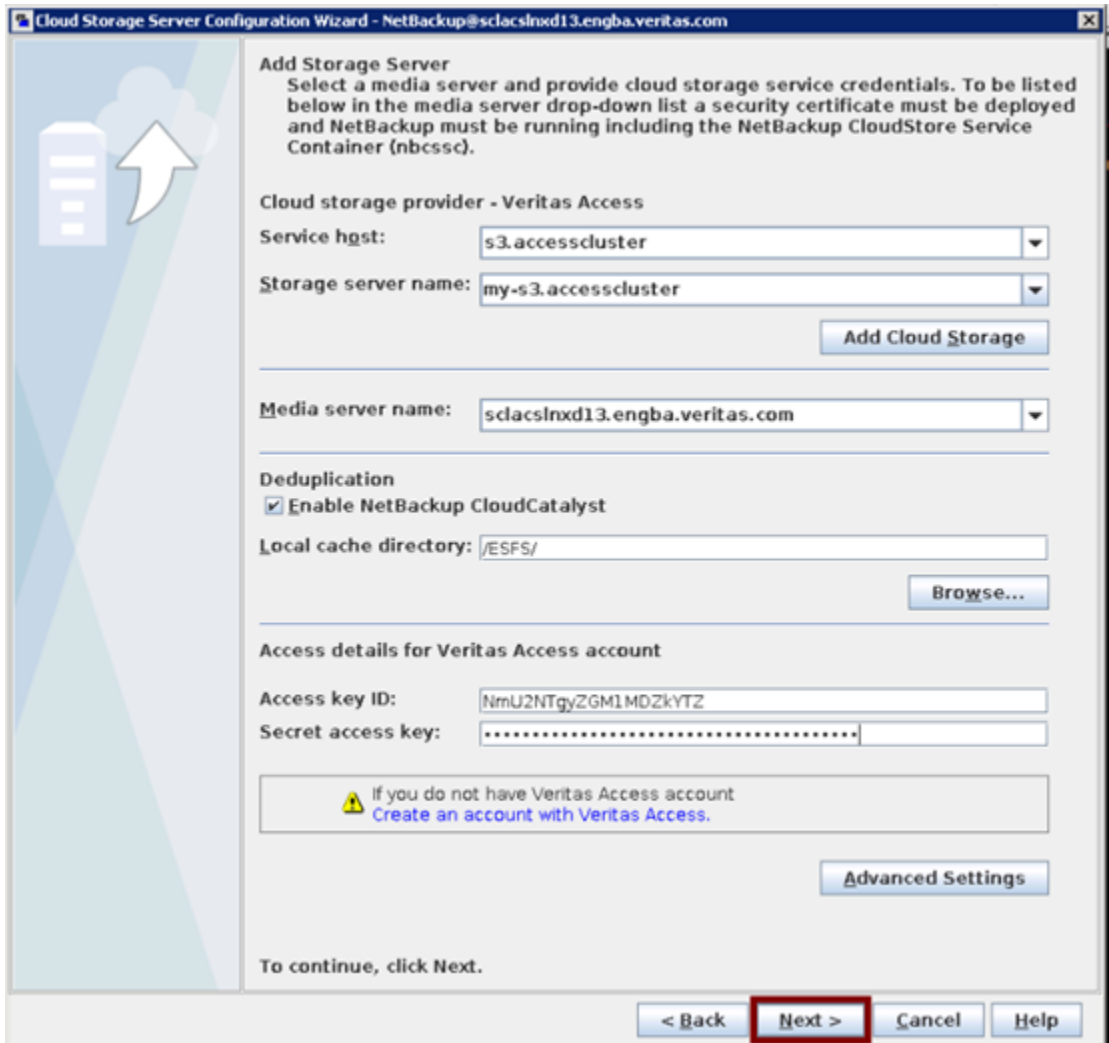
To continue, click Next.

< Back Next > Cancel Help

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




9 Click Next



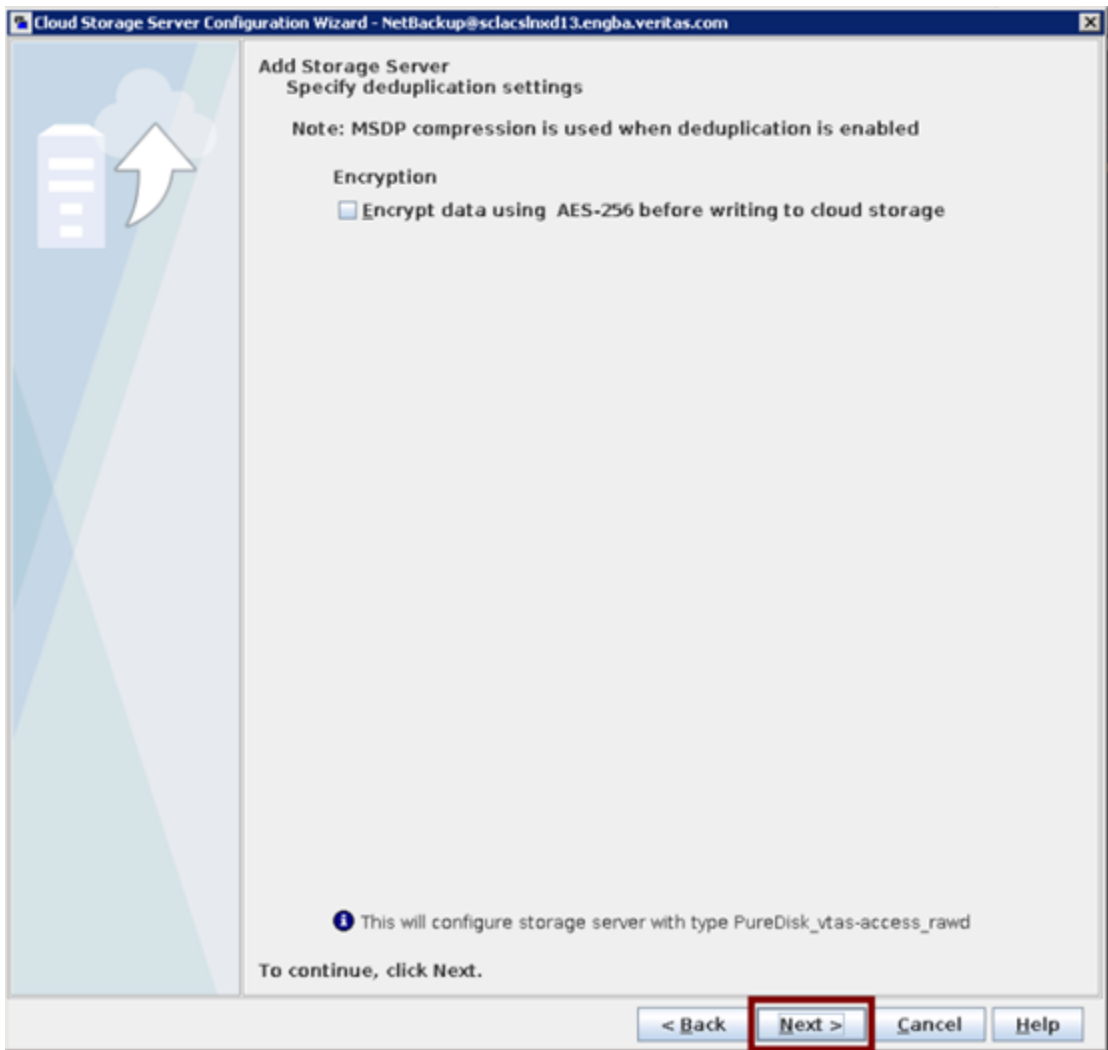
The image shows a 'Cloud Storage Server Configuration Wizard' window. On the left is a decorative graphic with a server icon and an upward arrow. The main area contains the following sections:

- 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:
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.**

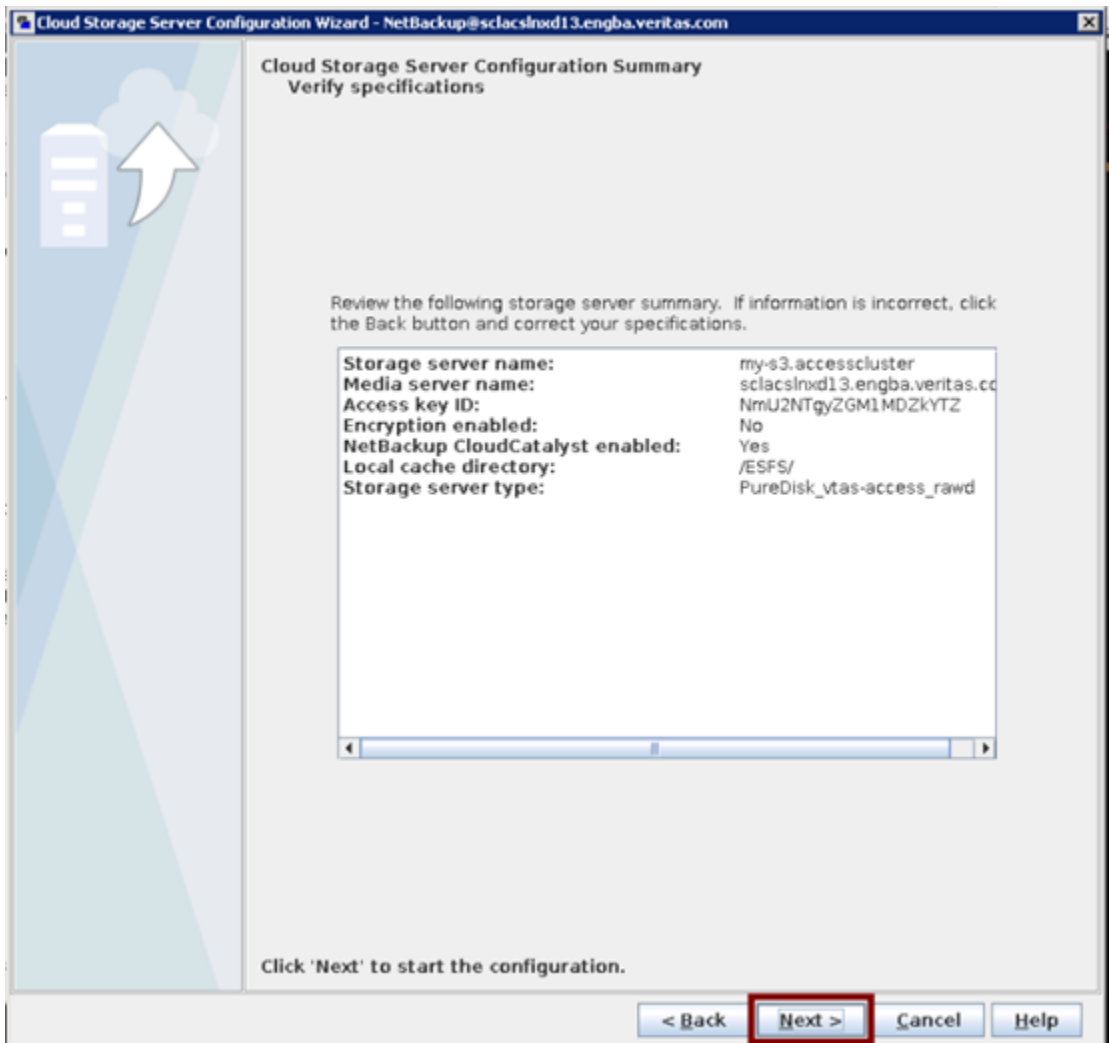
At the bottom are four buttons: '< Back', 'Next >' (highlighted with a red rectangle), 'Cancel', and 'Help'.

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

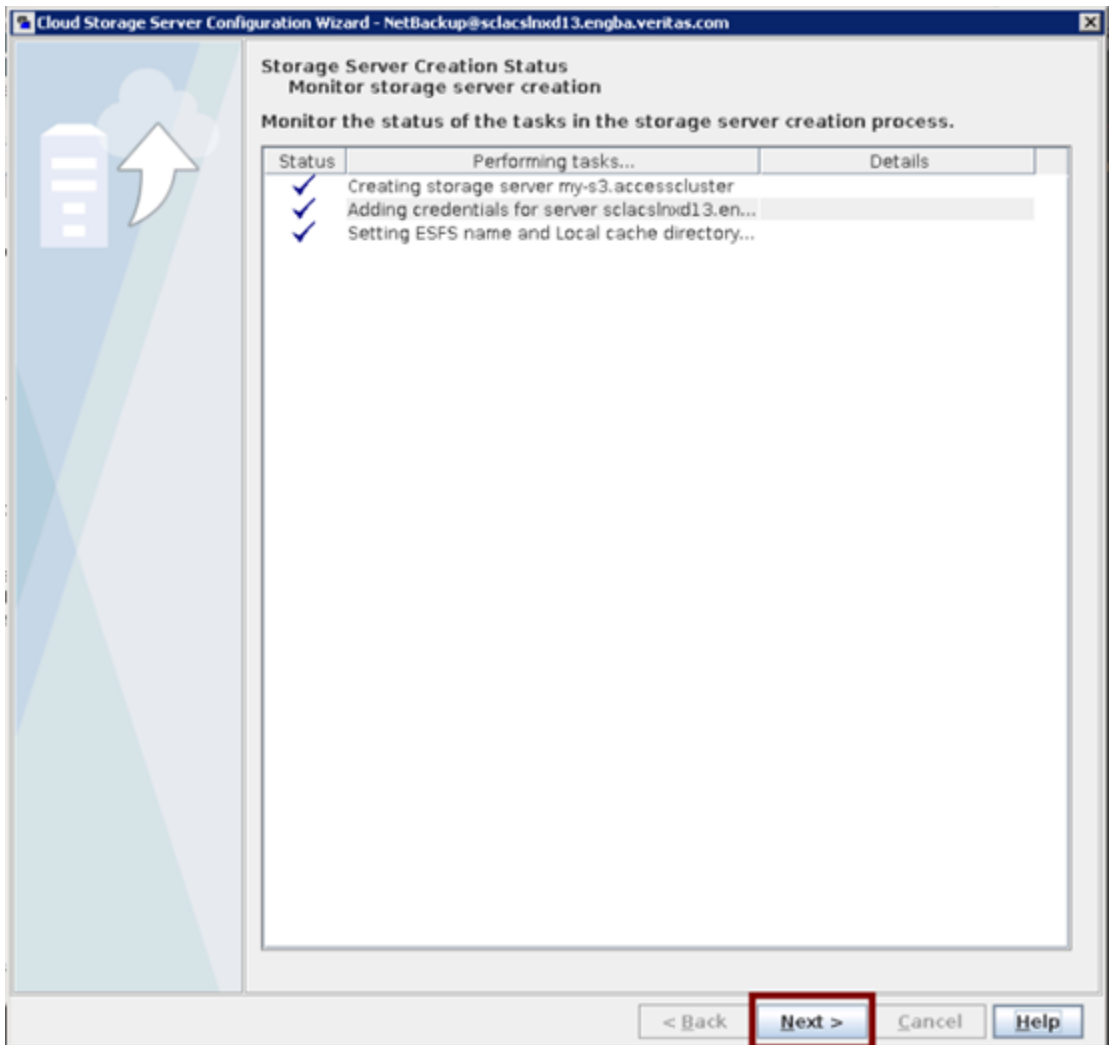


11 Messages related to setting the encryption appear. Click **Yes**.

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

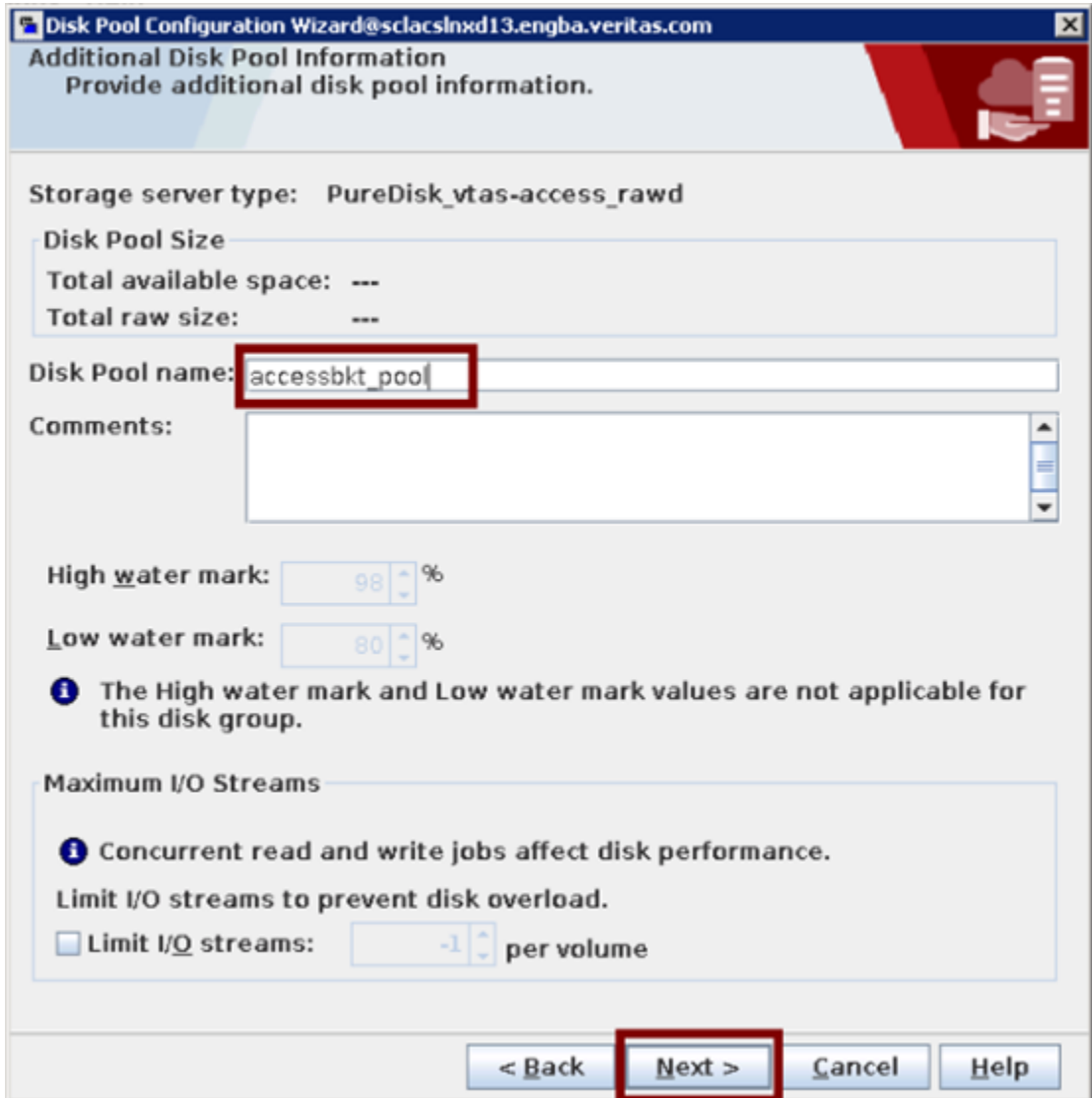
Add new volume on the selected storage server(s) **Add New Volume**

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

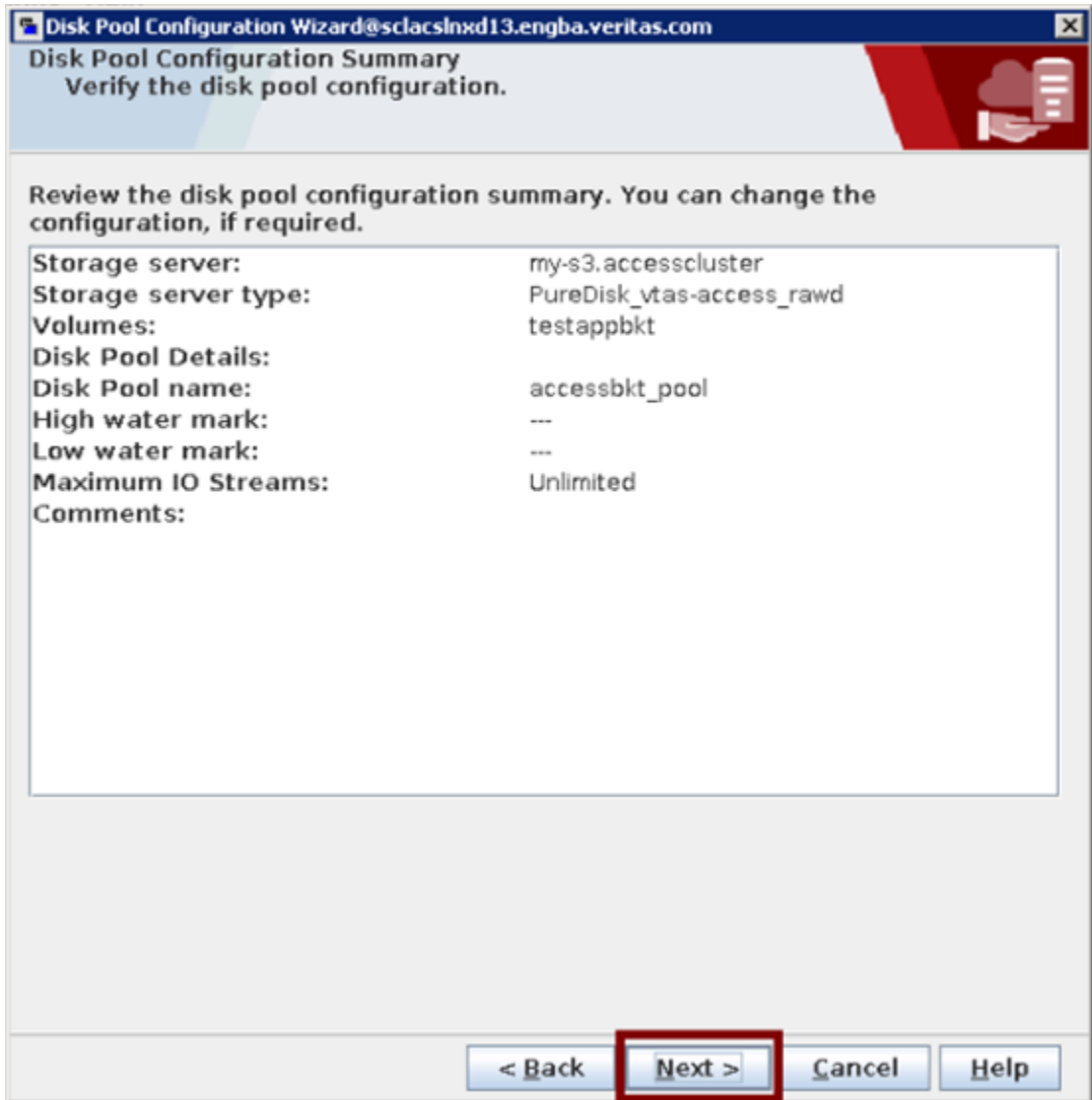
i Concurrent read and write jobs affect disk performance.

Limit I/O streams to prevent disk overload.

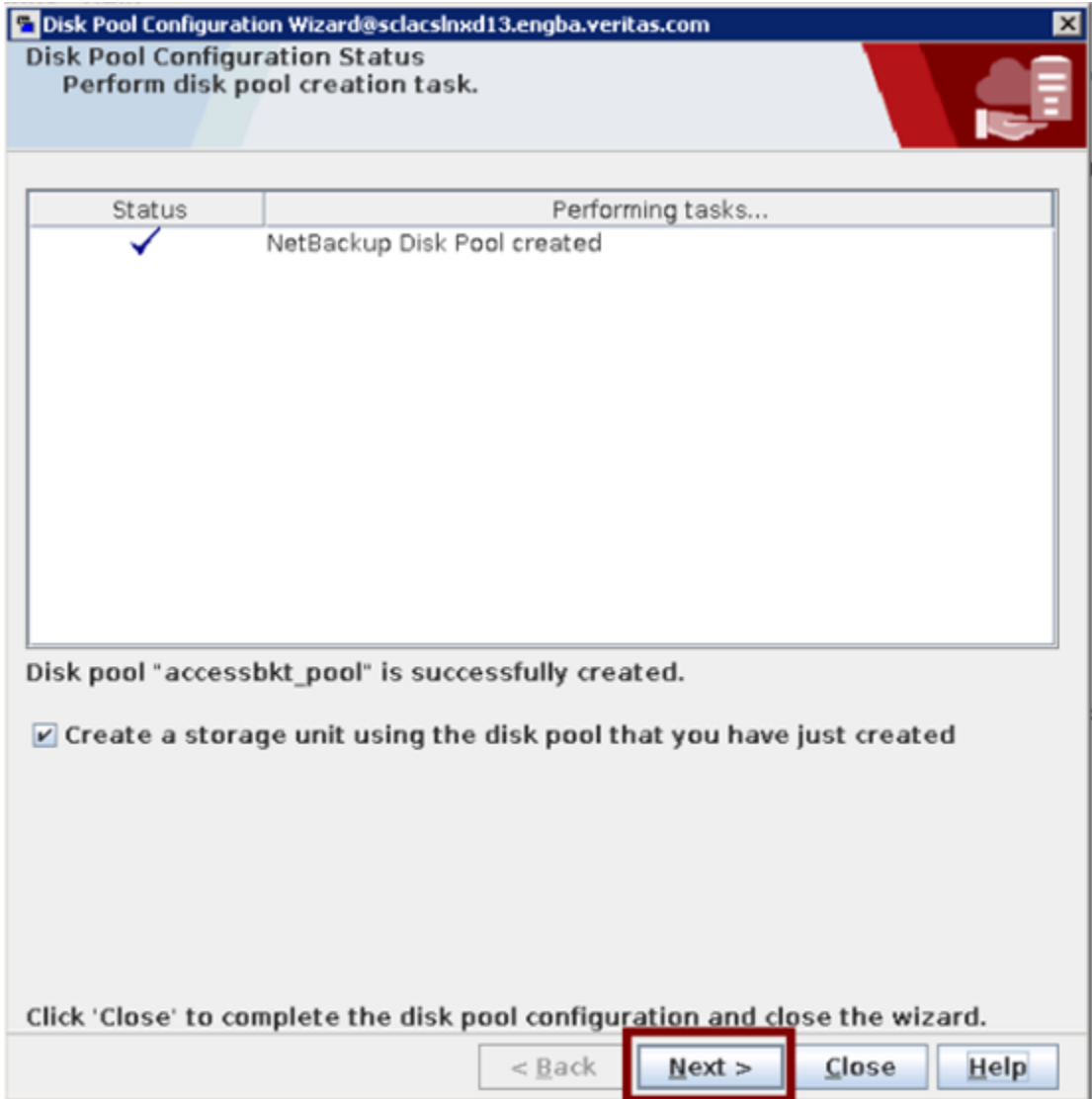
☐ Limit I/O streams: -1 per volume

< 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 storage unit using disk pool which you have just created** check box is selected.



The screenshot shows the 'Disk Pool Configuration Wizard' window. The title bar reads 'Disk Pool Configuration Wizard@sclacslnxd13.engba.veritas.com'. The main heading is 'Disk Pool Configuration Status' with the instruction 'Perform disk pool creation task.' Below this is a table with two columns: 'Status' and 'Performing tasks...'. The table contains one row with a blue checkmark in the 'Status' column and the text 'NetBackup Disk Pool created' in the 'Performing tasks...' column. Below the table, a message states 'Disk pool "accessbkt_pool" is successfully created.' A checkbox labeled 'Create a storage unit using the disk pool that you have just created' is checked. At the bottom, a message says 'Click 'Close' to complete the disk pool configuration and close the wizard.' The 'Next >' button is highlighted with a red rectangle.

Status	Performing tasks...
✓	NetBackup Disk Pool created

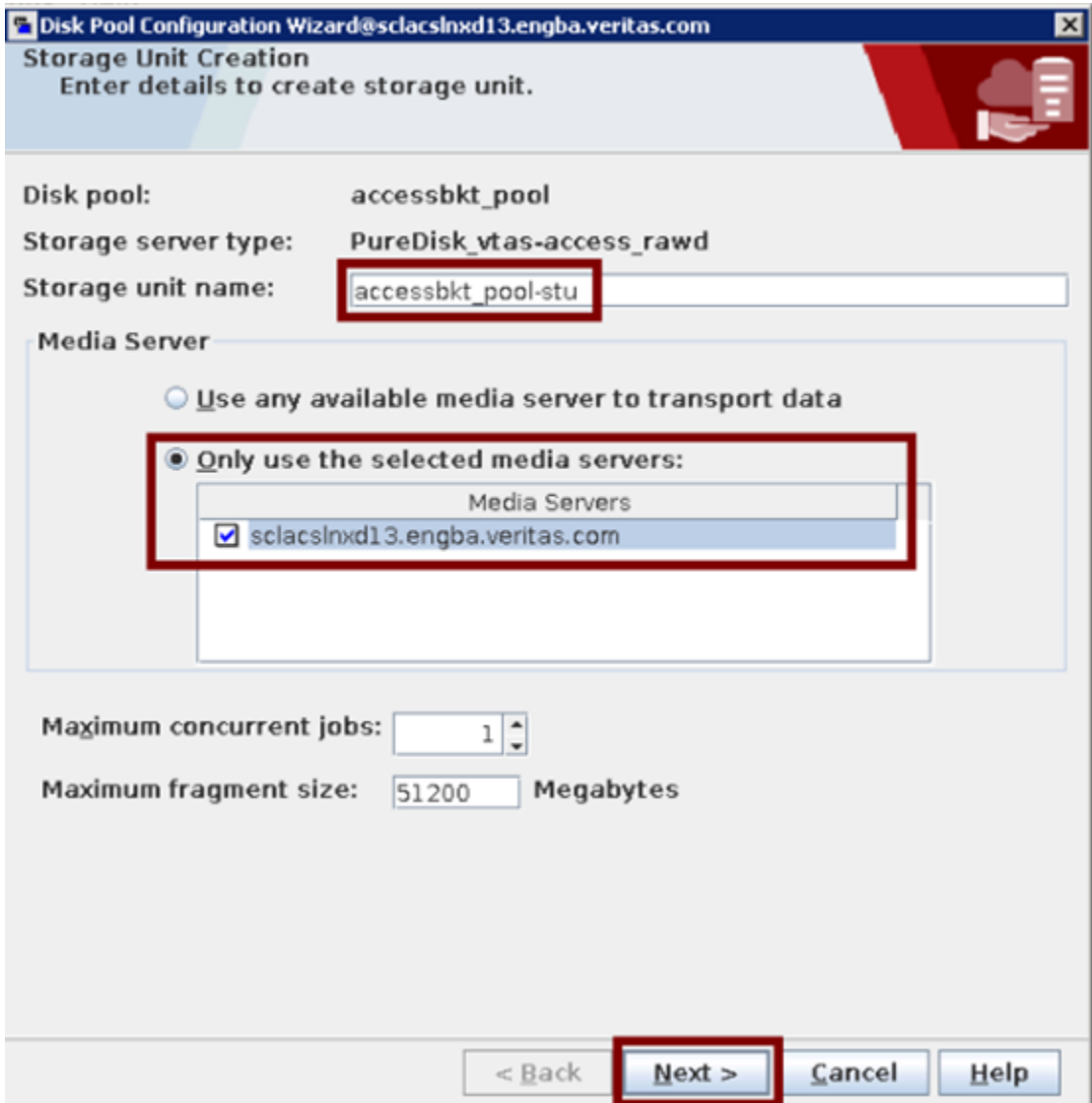
Disk pool "accessbkt_pool" is successfully created.

☒ Create a storage unit using the disk pool that you have just created

Click 'Close' to complete the disk pool configuration and close the wizard.

< Back **Next >** Close Help

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



The screenshot shows the 'Disk Pool Configuration Wizard' window for 'Storage Unit Creation'. The title bar reads 'Disk Pool Configuration Wizard@sclacslnxd13.engba.veritas.com'. The main heading is 'Storage Unit Creation' with the instruction 'Enter details to create storage unit.'.

The configuration details are as follows:

- Disk pool:** accessbkt_pool
- Storage server type:** PureDisk_vtas-access_rawd
- Storage unit name:** accessbkt_pool-stu

The **Media Server** section contains two radio button options:

- ☐ Use any available media server to transport data
- ☒ Only use the selected media servers:

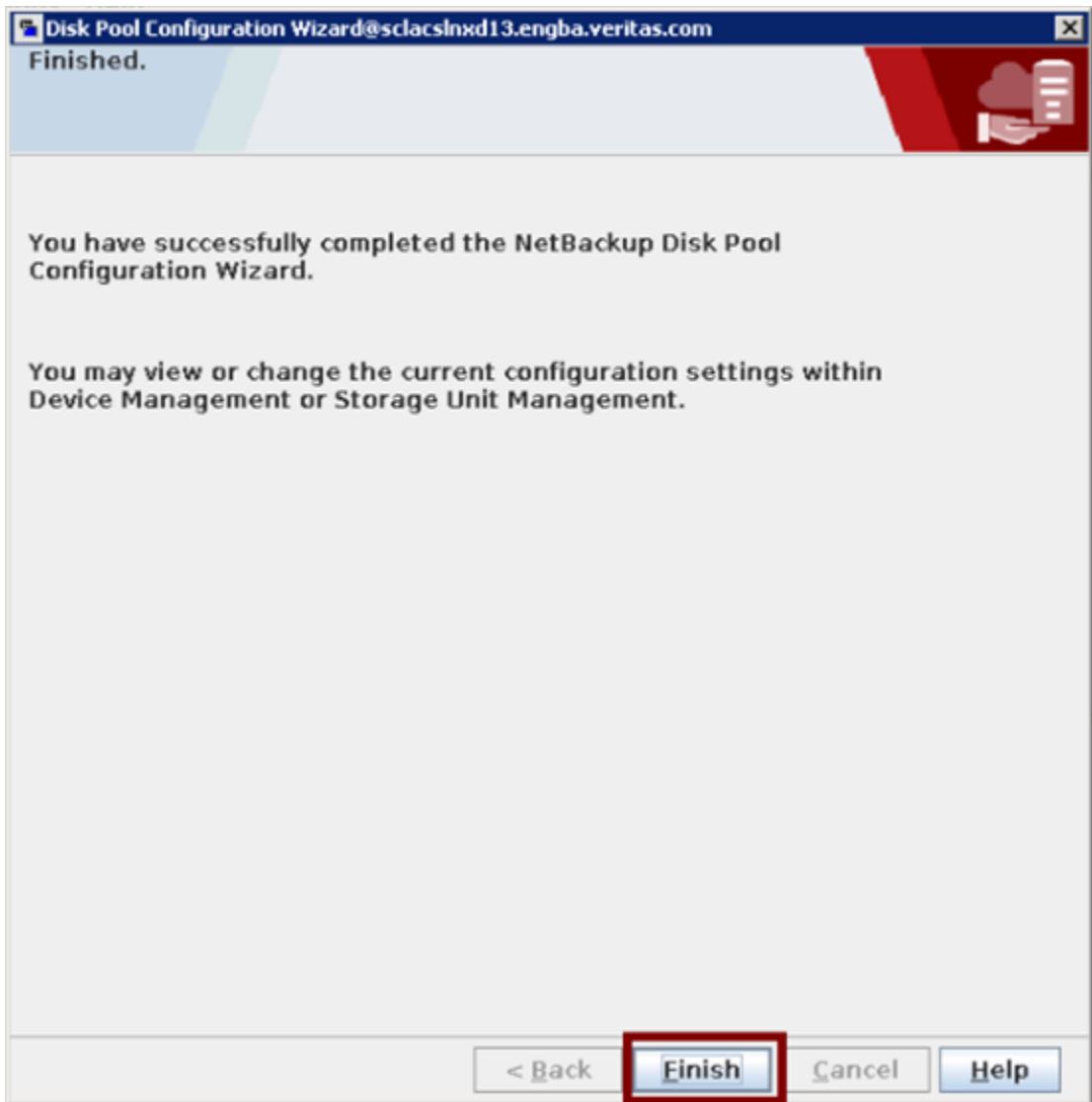
Below the selected option is a list box titled 'Media Servers' containing one entry: 'sclacslnxd13.engba.veritas.com', which is checked with a blue square.

At the bottom, there are two more fields:

- Maximum concurrent jobs:** 1
- Maximum fragment size:** 51200 Megabytes

The bottom navigation bar includes four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a red box.

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



Configuring backup and restore using NetBackup policies

This chapter includes the following topics:

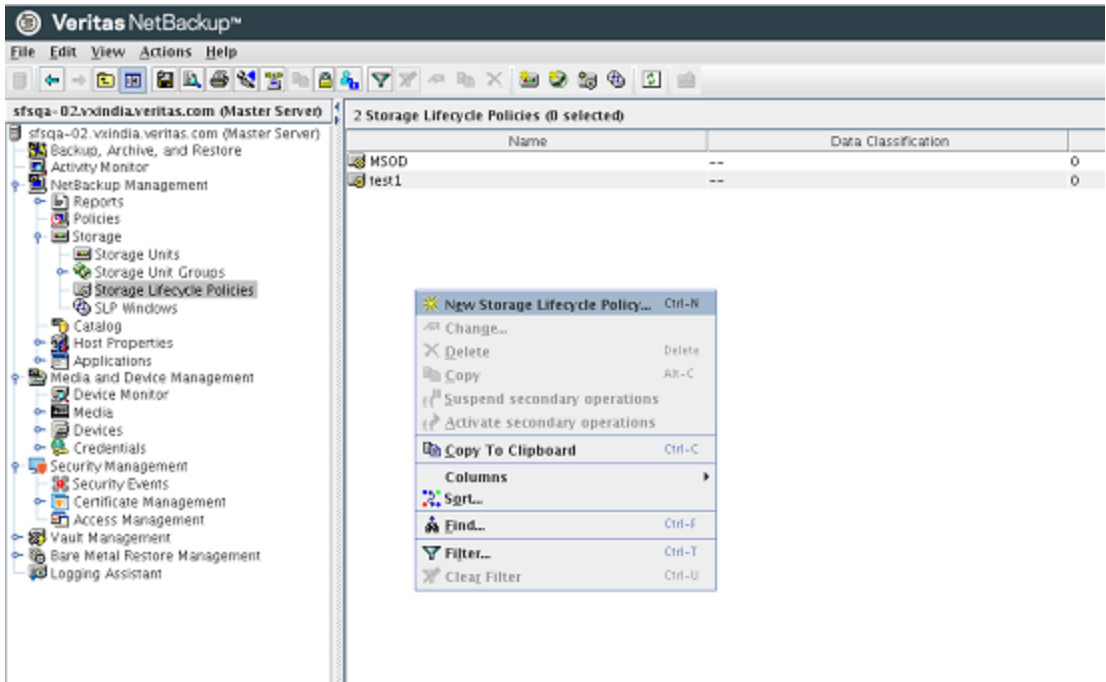
- [Storage Lifecycle Policies](#)
- [Backup and restore](#)
- [Running a backup policy manually](#)
- [Restoring backed up files](#)

Storage Lifecycle Policies

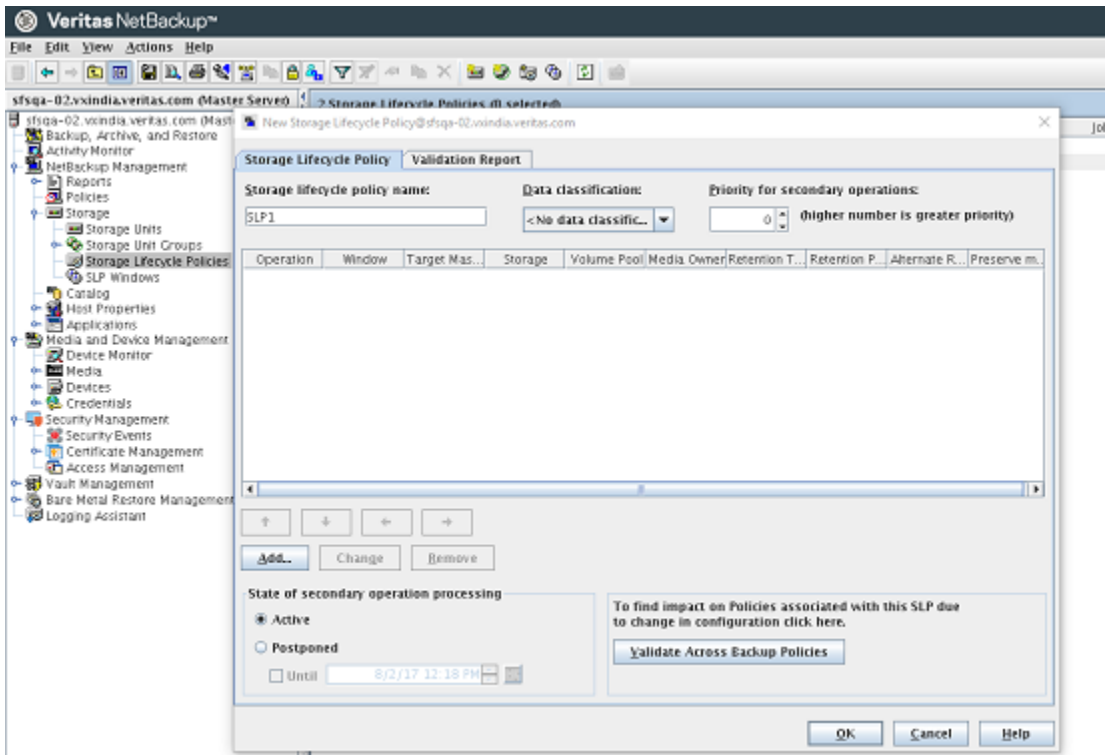
You can create Storage Lifecycle Policies (SLP).

To create Storage Lifecycle Policies

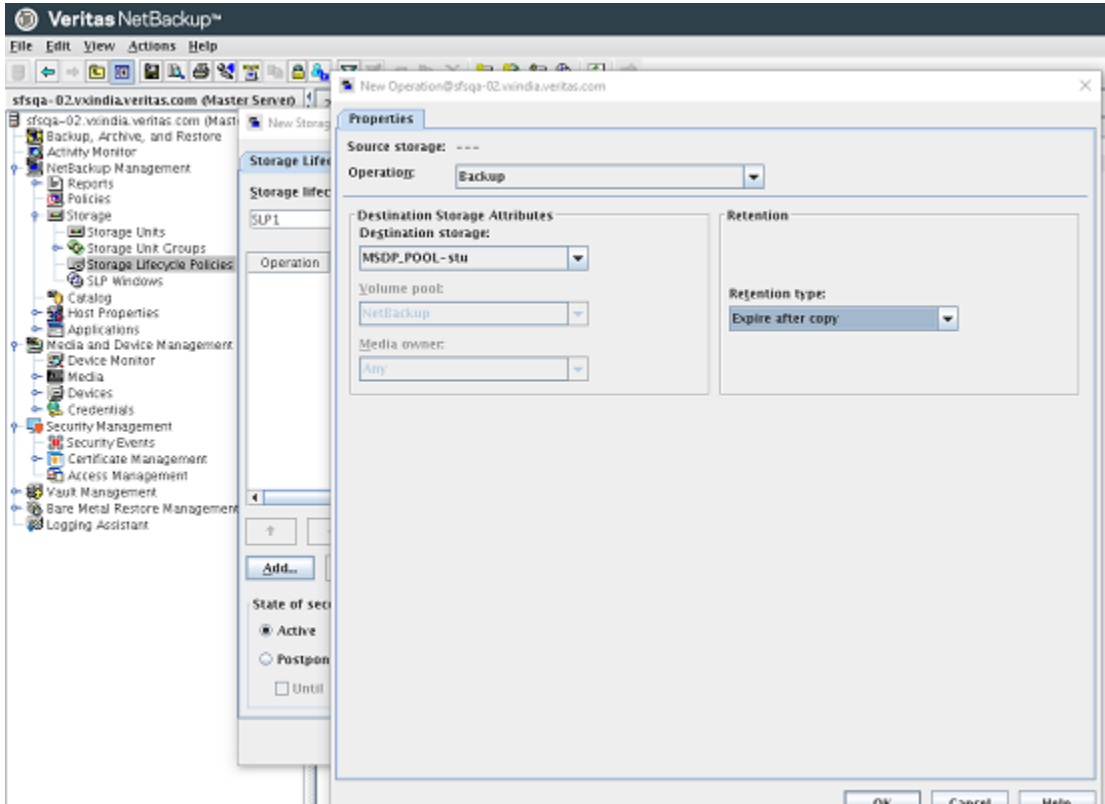
- 1 Click **Storage** -> **Storage Lifecycle Policies** on the NetBackup console. Select **New Storage Lifecycle Policy**.



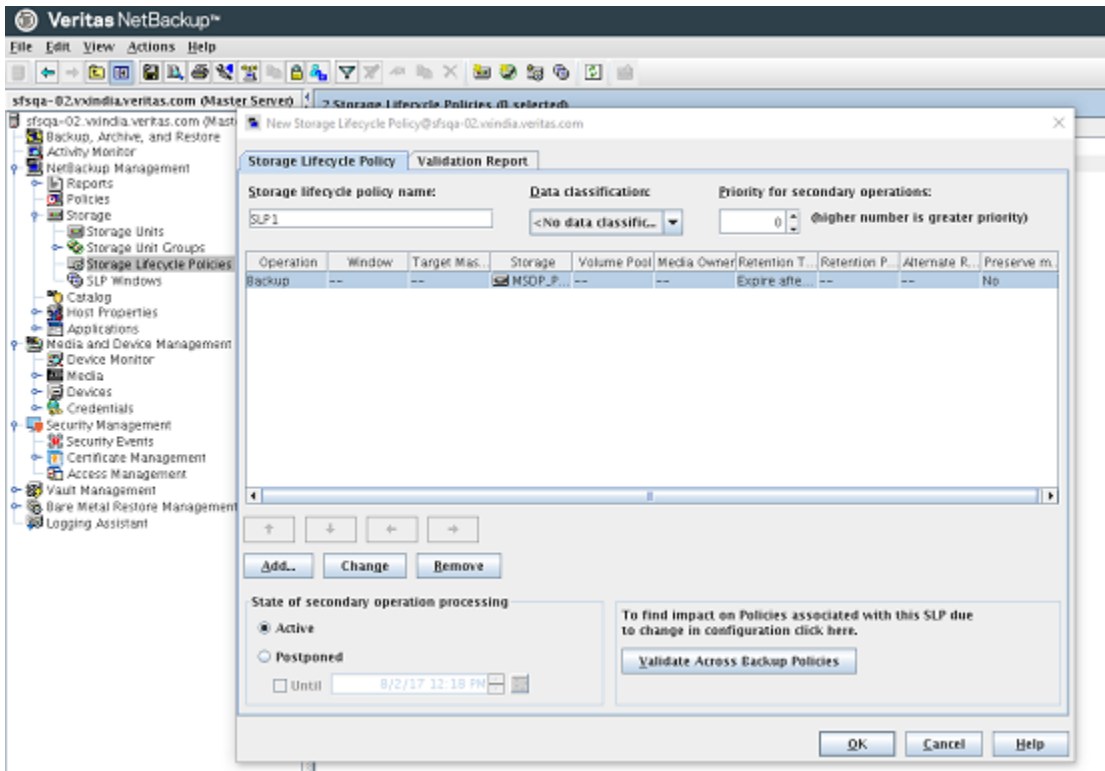
- 2 Enter a unique policy name for the policy. Click on the **Add** button.



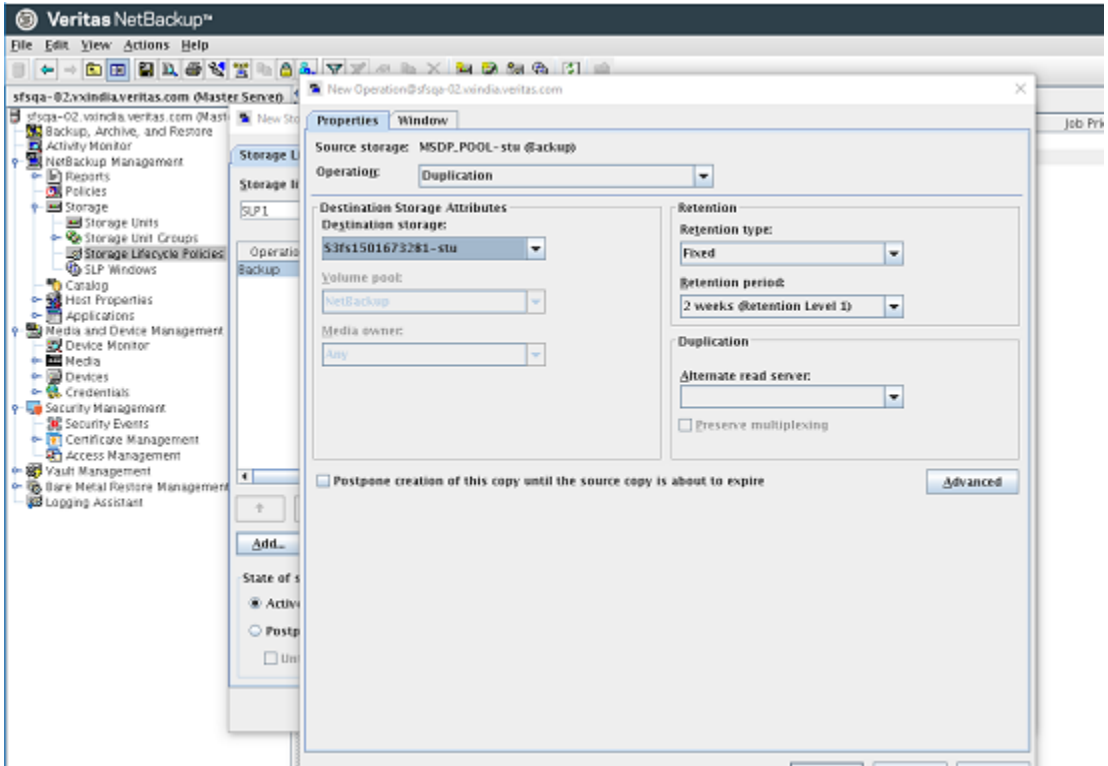
- 3 Select **Operation** as **Backup**, and set the destination pool to the MSDP pool that was created. Choose the **Retention type** based on your requirement.



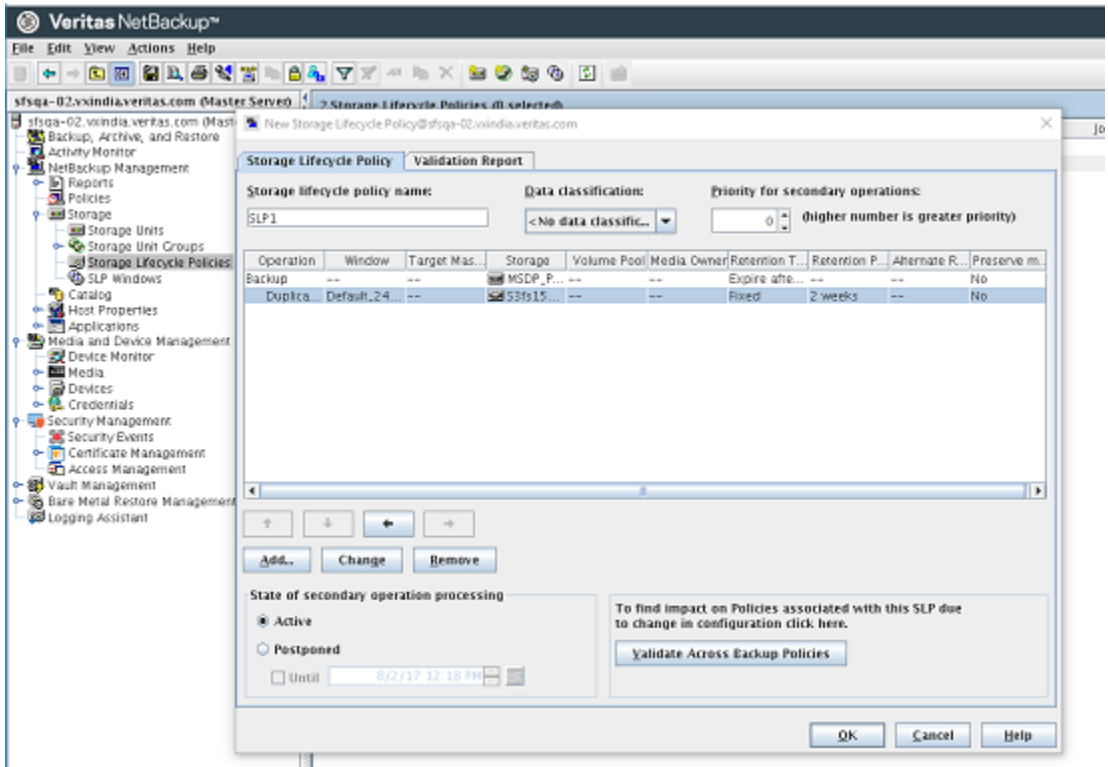
- 4 A new entry for Backup gets added. Click on the **Add** button again.



- 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.



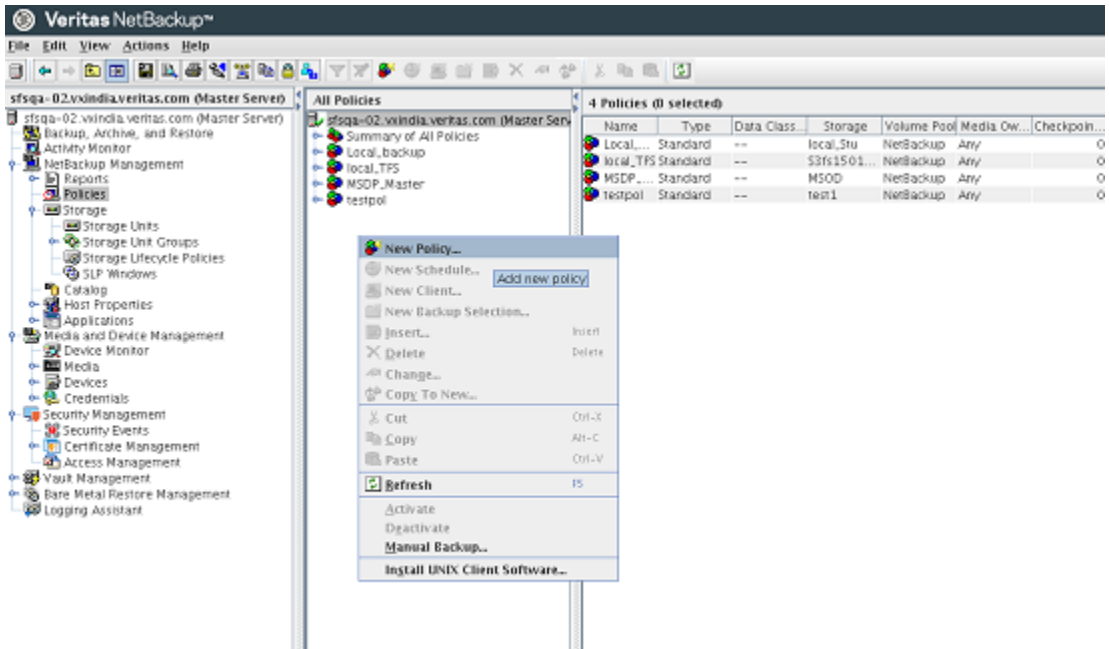
Backup and restore

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

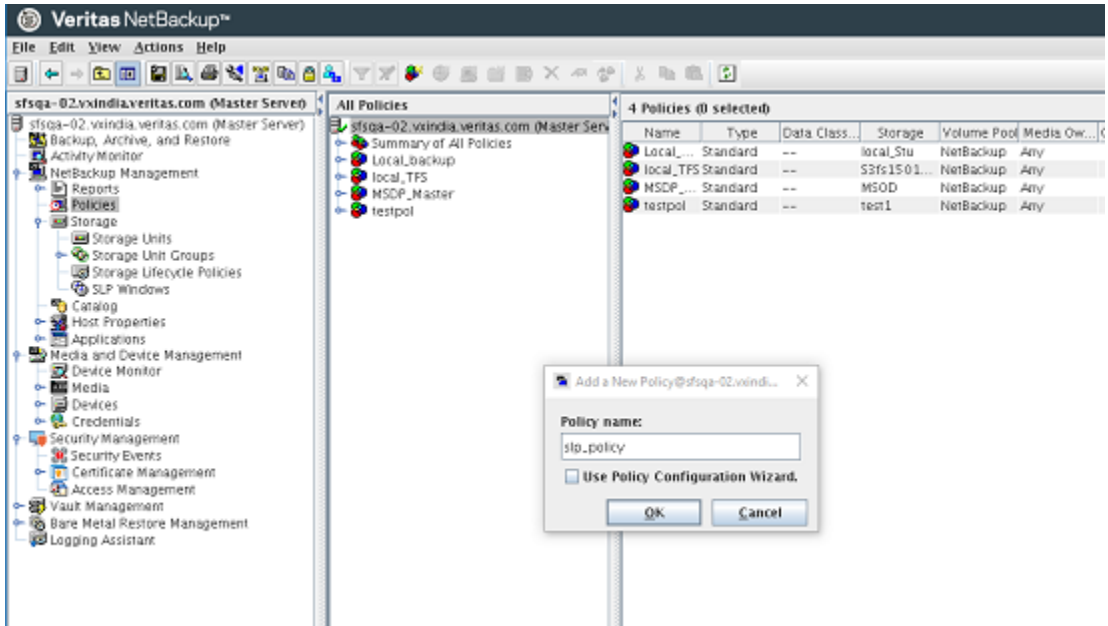
Policy creation

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 64.

Change Policy - slp_policy@dfsqa-02.vxindia.veritas.com

Server: dfsqa-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: MSDP_POOL-stu S3fs1501507821-stu S3fs1501594206-stu S3fs1501673281-stu

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: Metal Restore Image restore information Image 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

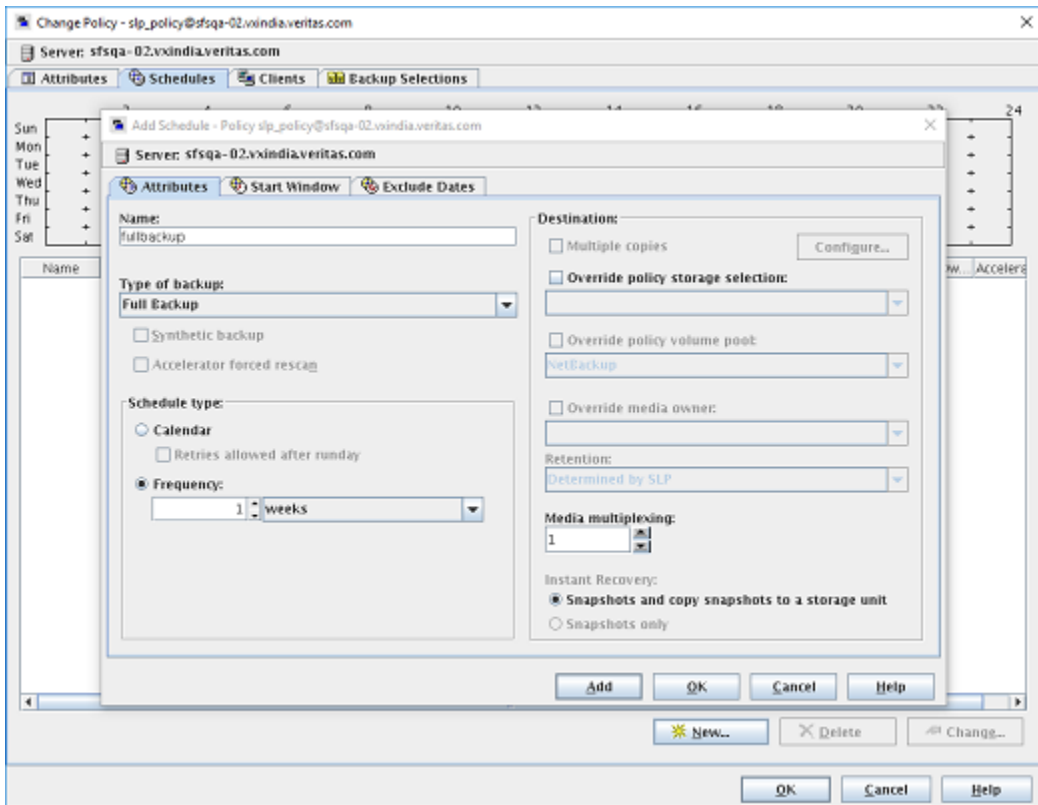
Exchange DAG or Exchange 2007 replication (LCR/CCR)

Database backup source:

Preferred server list... (Exchange DAG only)

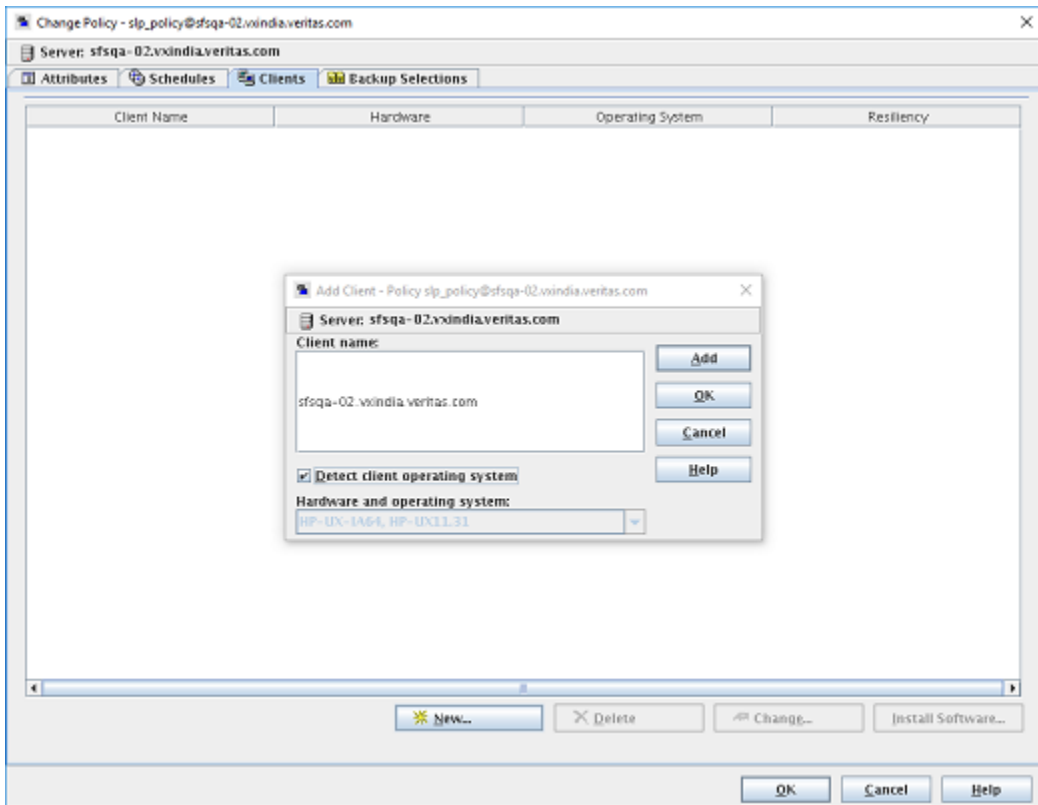
OK Cancel Help

- 4 Enter the attribute information as per your requirement.

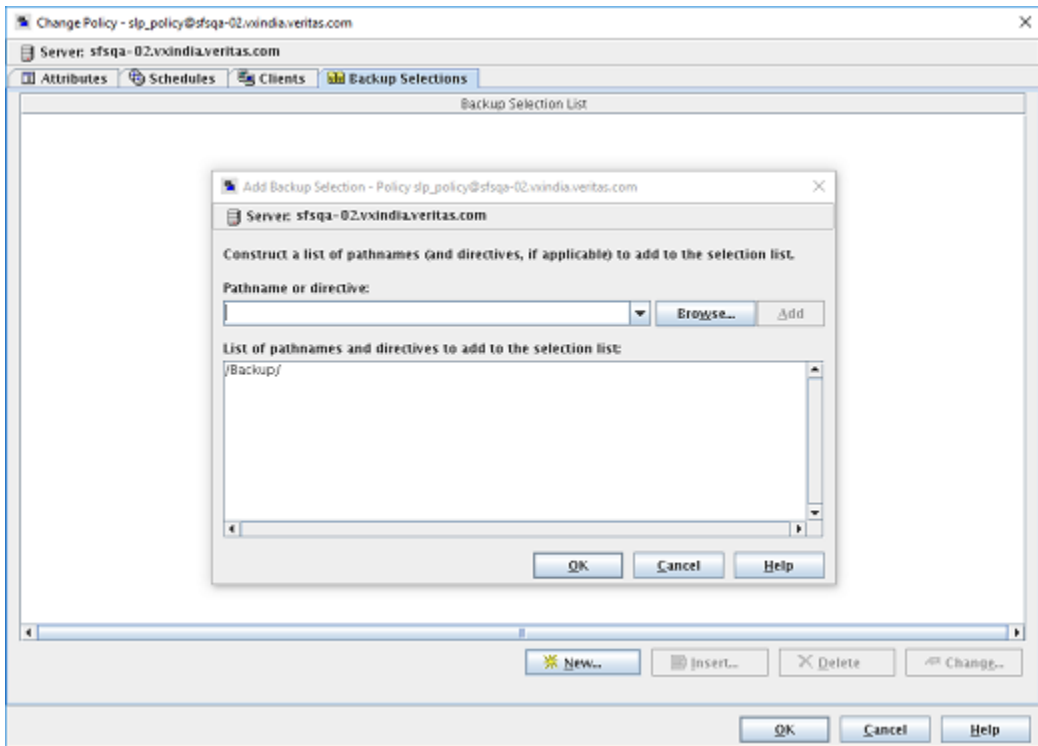


- 5 Under the **Schedule** tab, enter the name of the schedule. For example, **fullbackup**.

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



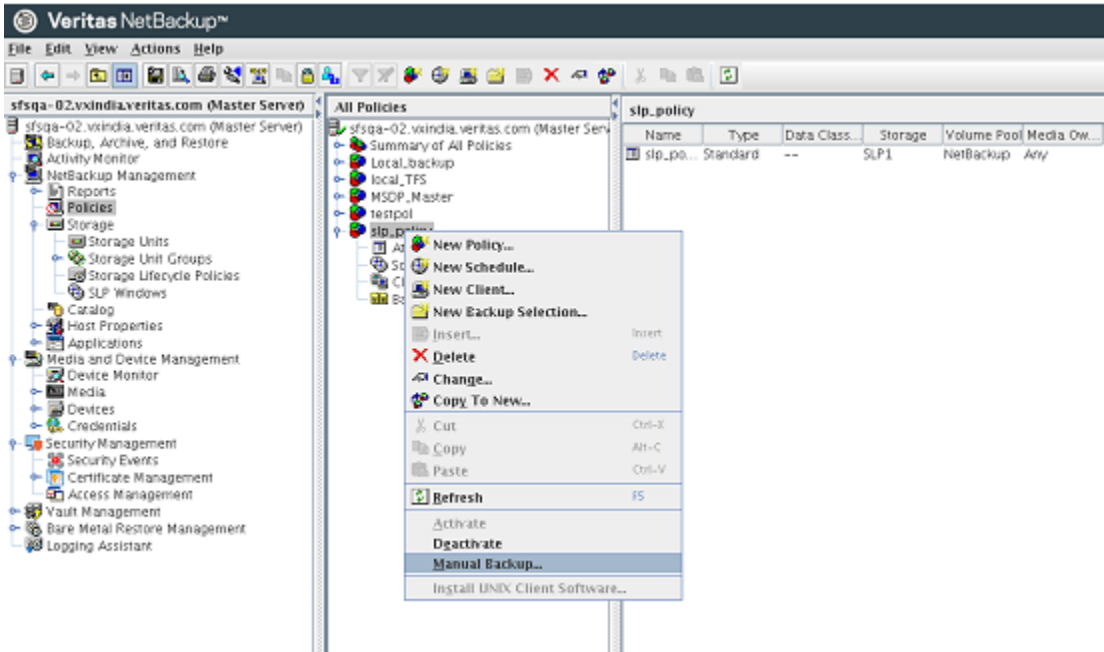
7 Select the folders that need to be backed up under **Backup Selections**.



Running a backup policy manually

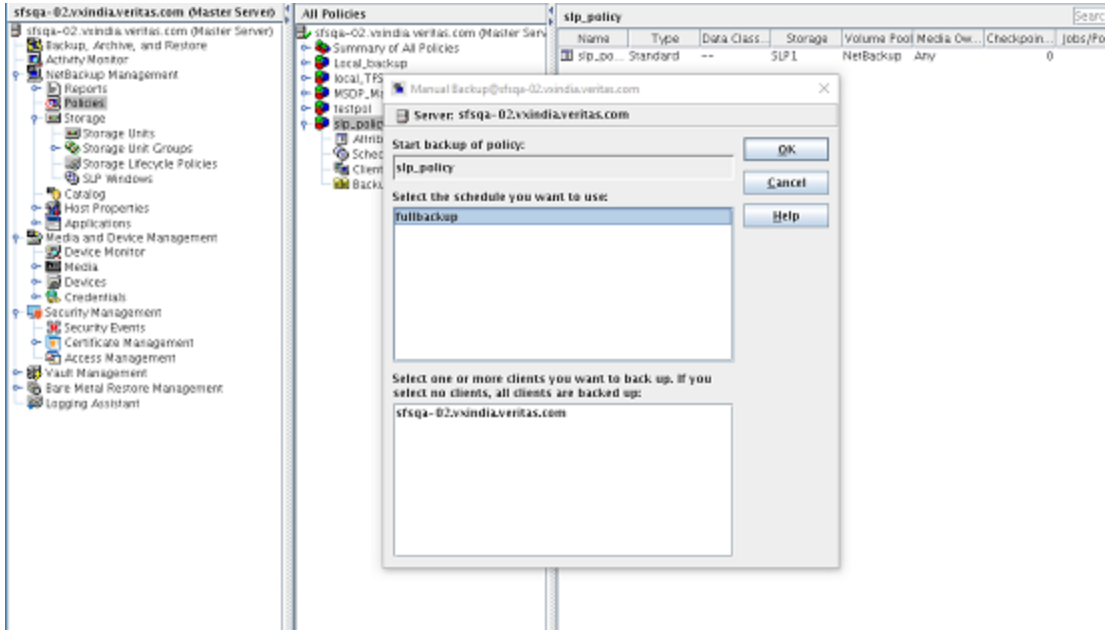
To run a backup policy manually

- 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.

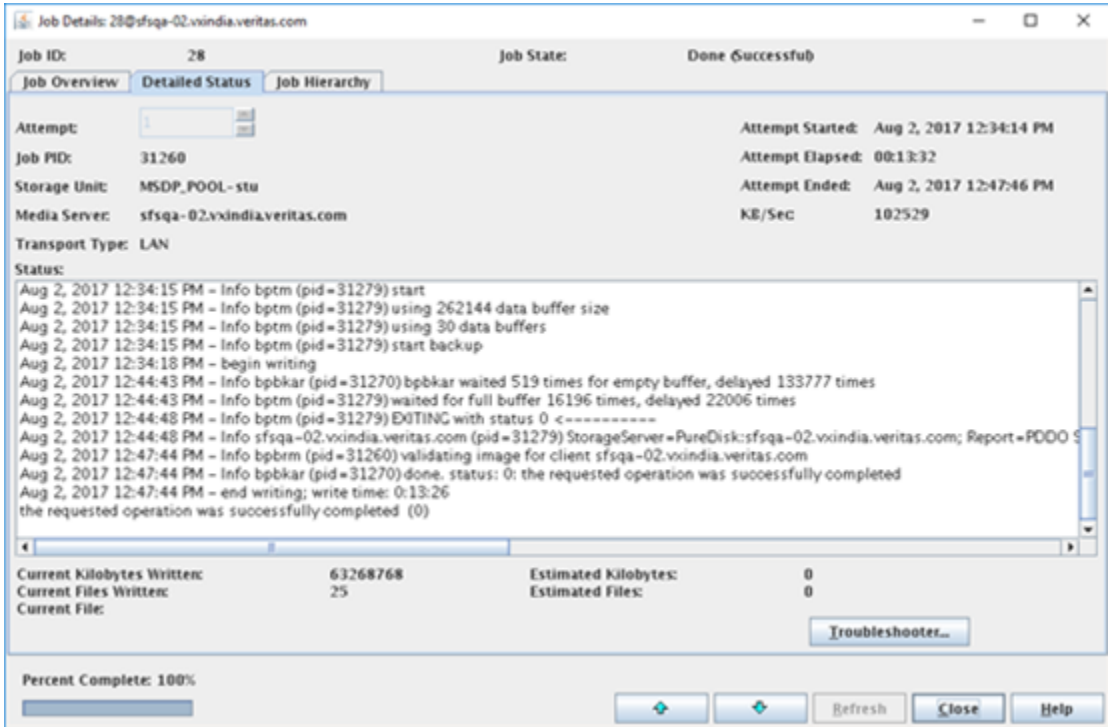


3 To verify the status of the backup, go to **Activity Monitor**.

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	Aug 2, 20...
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.



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

Veritas NetBackup™

File Edit View Actions Help

sfsga-02.vindia.veritas.com (Master Server)

30 Jobs: 0 Queued 1 Active 0 Waiting for Retry 0 Suspended 0 Incomplete 29 Done - 1 selected

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	ngsfdelip...	ngsfdelip...	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.

The screenshot shows the 'Job Details' window for job ID 30. The window has tabs for 'Job Overview', 'Detailed Status', and 'Job Hierarchy'. The 'Detailed Status' tab is selected. The job state is 'Active'. The job ID is 30, and the job PID is 32426. The storage unit is 'S3fs1501673281-stu' and the media server is 'sfsqa-02.vxindia.veritas.com'. The transport type is 'LAN'. The status section shows a log of events from August 2, 2017, 12:49:58 PM to 12:50:11 PM, including the start of the backup process, resource allocation, and the start of the backup image reading. The progress bar shows 48% completion. The current kilobytes written is 30603264, and the estimated kilobytes is 63268768. The current files written is 63268768, and the estimated files is 63268768. A 'Troubleshooter...' button is visible. The bottom of the window shows a 'Percent Complete: 48%' bar and buttons for 'Refresh', 'Close', and 'Help'.

Job Details: 30@sfsqa-02.vxindia.veritas.com

Job ID: 30 Job State: Active

Job Overview Detailed Status Job Hierarchy

Attempt: 1 Attempt Started: Aug 2, 2017 12:49:56 PM
Job PID: 32426 Attempt Elapsed: 00:48:51
Storage Unit: S3fs1501673281-stu Attempt Ended:
Media Server: sfsqa-02.vxindia.veritas.com -> sfsqa-02.vxindia.veritas.com KB/Sec
Transport Type: LAN

Status:

Aug 2, 2017 12:49:58 PM - Info bptm (pid=32431) start
Aug 2, 2017 12:49:58 PM - started process bptm (pid=32431)
Aug 2, 2017 12:49:58 PM - resource @aaaab reserved
Aug 2, 2017 12:49:58 PM - granted resource MediaID=@aaaab;DiskVolume=S3fs1501673281;DiskPool=S3fs1501673281;Path=S3fs1501673281;
Aug 2, 2017 12:49:58 PM - granted resource S3fs1501673281-stu
Aug 2, 2017 12:49:58 PM - granted resource MediaID=@aaaab;DiskVolume=PureDiskVolume;DiskPool=MSDP_POOL;Path=PureDiskVolume;Stora
Aug 2, 2017 12:50:00 PM - Info bptm (pid=32431) start backup
Aug 2, 2017 12:50:11 PM - Info bptm (pid=32431) started
Aug 2, 2017 12:50:11 PM - started process bptm (pid=32492)
Aug 2, 2017 12:50:11 PM - Info bptm (pid=32492) reading backup image
Aug 2, 2017 12:50:11 PM - Info bptm (pid=32492) using 30 data buffers
Aug 2, 2017 12:50:11 PM - Info bptm (pid=32492) requesting nbjm for media
Aug 2, 2017 12:50:11 PM - begin reading

Current Kilobytes Written: 30603264 Estimated Kilobytes: 63268768
Current Files Written: Estimated Files:
Current File:

Troubleshooter...

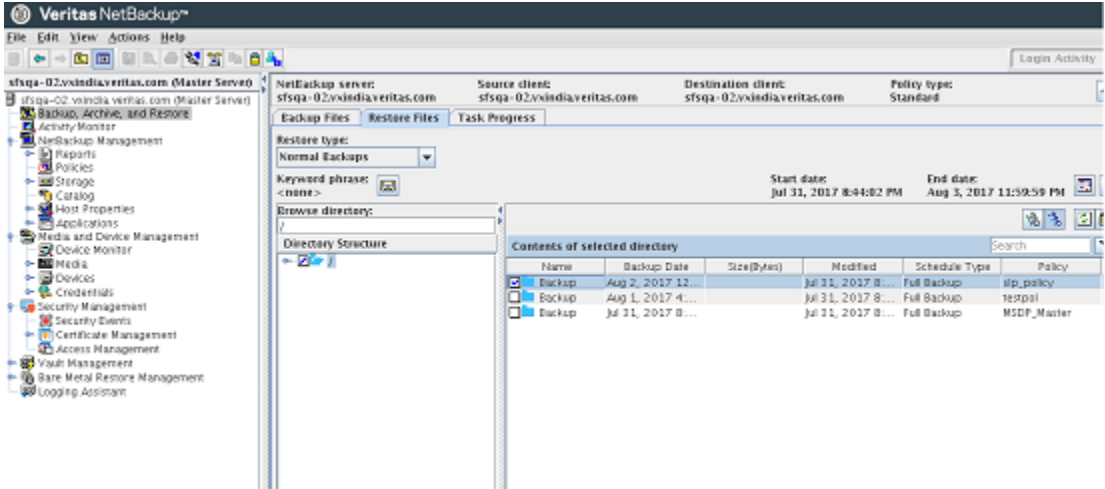
Percent Complete: 48%

Refresh Close Help

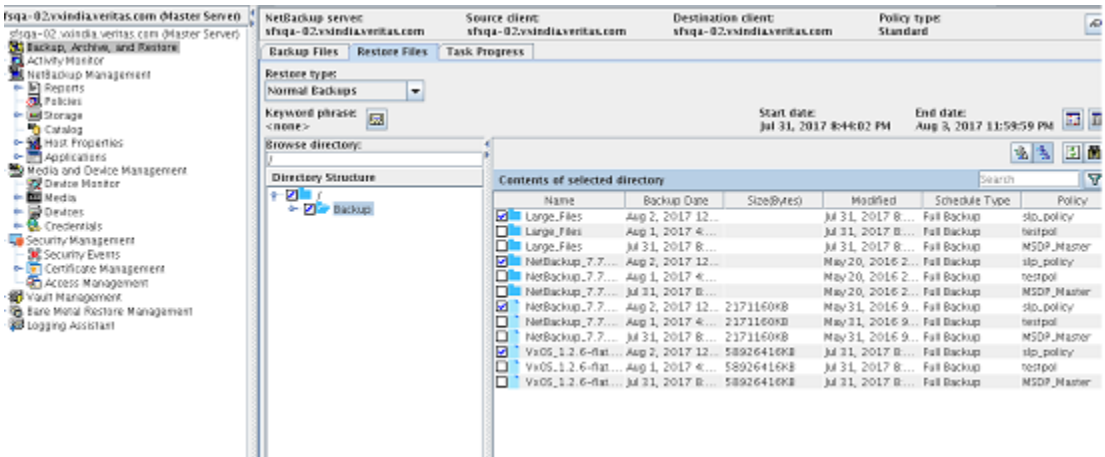
Restoring backed up files

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@sfsga-02.vxindia.veritas.com

General

Destination

☐ Restore everything to its original location.

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

Destination:

☐ 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

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

Options

☐ Overwrite existing files

☐ Restore directories without crossing mount points

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

☒ Rename hard links

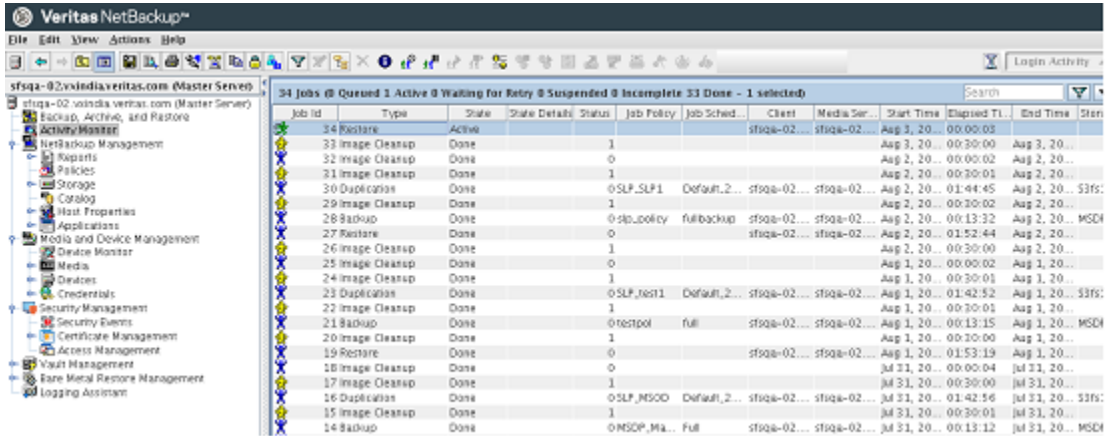
☒ Rename soft links

☐ Force rollback even if it destroys later snapshots

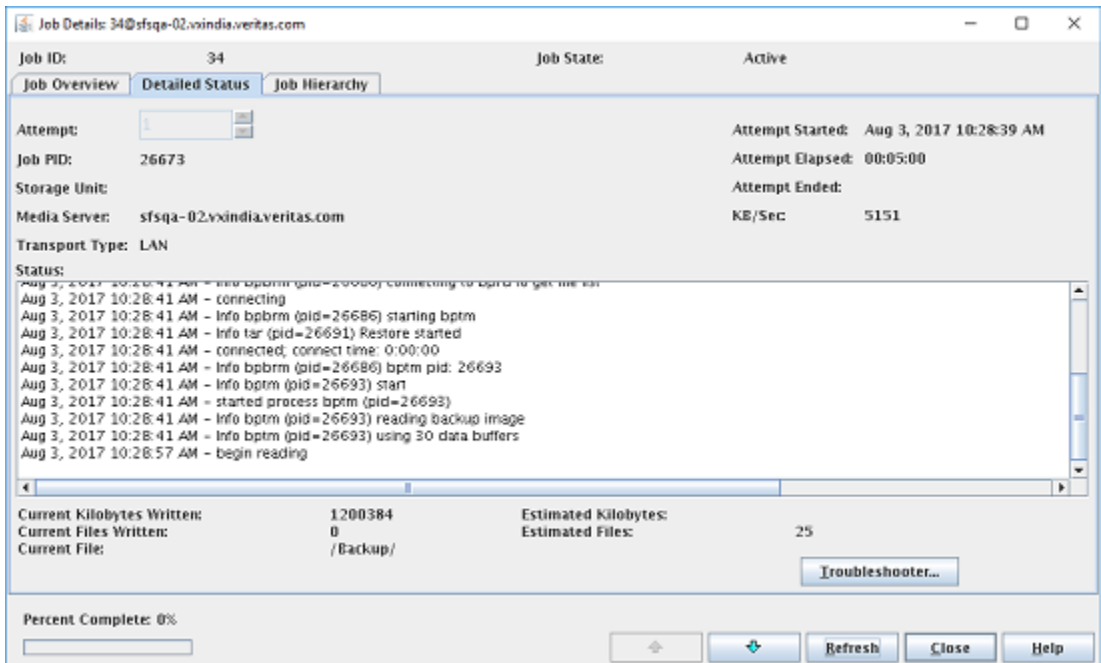
Media Server

☐ Override default priority
 Job Priority
 (higher number is greater priority)

- 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.



Troubleshooting

This chapter includes the following topics:

- [Unmounting the SDFS volume before restarting Veritas Access or the NetBackup media server](#)
- [Log locations for troubleshooting](#)
- [Additional resources](#)
- [Generating Veritas Access S3 server keys using the helper script](#)

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.

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
```

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
```

Index

A

- about
 - backup storage for NetBackup 8
 - Veritas Access 6
- additional resources
 - documentation 87

B

- backing up deduplicated data
 - using S3 protocol 15
- backing up NetBackup data
 - deduplicating data on Veritas Access 16
- backup and restore 70
- backup storage for NetBackup 8

C

- configuring Veritas Access as a cloud storage server 47
- creating
 - Storage Lifecycle Policies 64
- Creating a Media Server Deduplication Pool
 - primary backup using NetBackup 23
- creating a MSDP
 - primary backup using NetBackup 23
- creating a storage unit
 - NetBackup console 31
- creating an OST disk pool
 - NetBackup console 31
- creating S3 bucket
 - storing deduplicated backup data 17, 45

G

- generating Veritas Access S3 server keys
 - using the helper script 88

I

- integration with Veritas Access
 - NetBackup 6

L

- log locations
 - troubleshooting 87

N

- NetBackup
 - integration with Veritas Access 6
- NetBackup media server
 - setting up multiple SDFS volumes 40

O

- OpenDedup
 - workflow 14
- OpenDedup installation
 - system requirements 11

P

- policy creation 70

R

- restoring backup files 83
- running a backup policy
 - manually 77

S

- SDFS volume
 - unmounting before rebooting Veritas Access 86
- setting up multiple NetBackup media servers 39
- setting up multiple SDFS volumes
 - NetBackup media server 40
- Storage Lifecycle Policies
 - creating 64
- supported configurations and versions
 - NetBackup with CloudCatalyst 12
 - NetBackup with OpenDedup 12
- system requirements
 - OpenDedup installation 11
 - supported configurations and versions for
 - NetBackup with CloudCatalyst 12

- system requirements *(continued)*
 - supported configurations and versions for NetBackup with OpenDedup 12

T

- troubleshooting
 - log locations 87

U

- unmounting
 - SDFS volume before rebooting Veritas Access 86
- use case
 - backing up deduplicated data 15
 - backing up NetBackup data 16
 - long-term data retention 8
- using the helper script
 - generating Veritas Access S3 server keys 88
- using Veritas Access with CloudCatalyst
 - benefits 10
- using Veritas Access with NetBackup and OpenDedup
 - benefits 10