Veritas Access NetBackup Solutions Guide

Linux 7.3.2

(Use with the Veritas Access 3340 Appliance documentation)

August 2018

VERITAS™

Veritas Access NetBackup Solutions Guide

Last updated: 2018-08-10

Document version: 7.3.2 Rev 0

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 7
Use cases for long-term data retention 8

Chapter 2 System requirements 11

Supported configurations and versions for NetBackup with CloudCatalyst 11

Chapter 3 Configuring Veritas Access as a cloud storage server with NetBackup CloudCatalyst 12

Benefits of using Veritas Access with NetBackup and CloudCatalyst 12
Creating an S3 bucket on Veritas Access for storing deduplicated backup data from NetBackup 13
Creating a Media Server Deduplication Pool (MSDP) for primary backup using NetBackup 15
Configuring Veritas Access as a cloud storage server on NetBackup server 23
Configuring Veritas Access SSL with NetBackup 40

Chapter 4 Configuring backup and restore using NetBackup policies 43

Storage Lifecycle Policies 43
Backup and restore 49
Running a backup policy manually 56
Restoring backed up files 62

Chapter 5 Troubleshooting 65

Unmounting the SDFS volume before restarting Veritas Access or the NetBackup media server 65
Log locations for troubleshooting 66

Additional resources 66
Generating Veritas Access S3 server keys using the helper script 67

Index 69

Chapter 1

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 3340 Appliance is a software-defined, network-attached storage (NAS) solution for unstructured data.

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

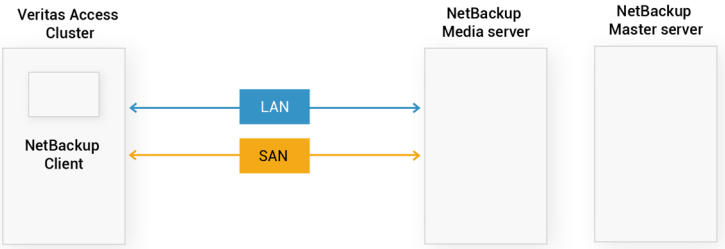
Veritas Access is integrated with Veritas NetBackup so that a NetBackup administrator can back up your Veritas Access file systems to NetBackup master or media servers and retain the data as per your company policy. Once data is backed up, a storage administrator can delete unwanted data from Veritas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



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.

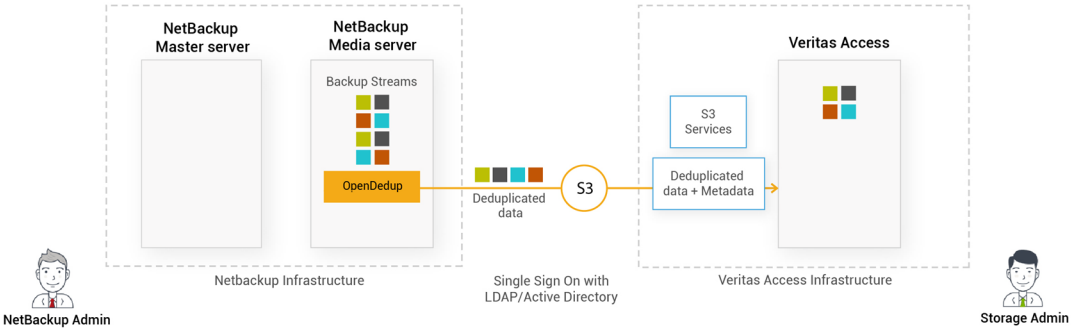
NetBackup is an enterprise-class heterogeneous backup and recovery application. It provides cross-platform backup functionality to a large variety of Windows, UNIX, and Linux operating systems.

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.

Figure 1-2 shows how Veritas Access integrates with OpenDedup over S3 to store NetBackup backup streams as deduplicated data.

Figure 1-2



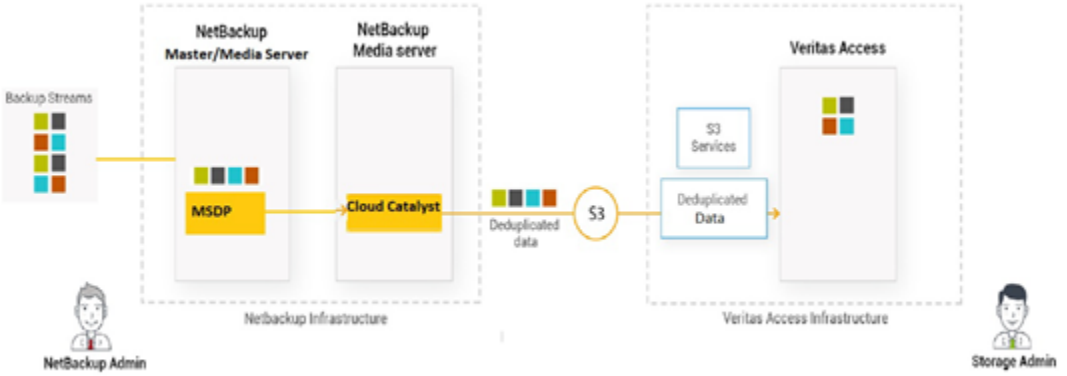
Use cases for long-term data retention

The following are the use cases for long-term data retention (LTR) with Veritas Access 3340 Appliance.

Use Case 1: Veritas Access with CloudCatalyst

- Primary backup data is deduplicated by MSDP and stored on the NetBackup server.
- The same deduplicated data is moved to the Veritas Access 3340 Appliance through SLP using CloudCatalyst.

Figure 1-3



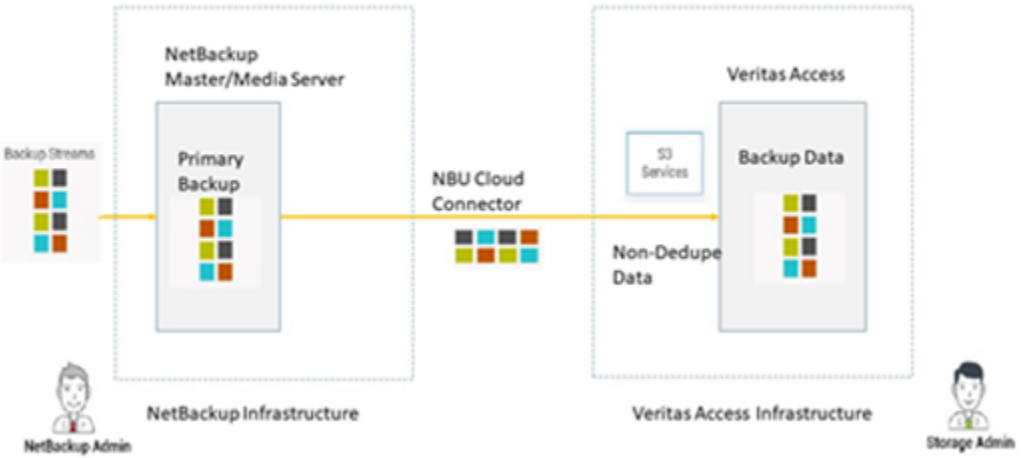
Use Case 2: Veritas Access as an S3 connector

- 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 3340 Appliance 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 the Veritas Access 3340 Appliance through SLP over the Veritas Access S3 protocol.

Figure 1-4


NetBackup
Master/Media Server
Backup Streams
Primary
Backup
NBU Cloud
Connector
Veritas Access
S3
Services
Backup Data
Non-Dedupe
Data
NetBackup Admin
NetBackup Infrastructure
Veritas Access Infrastructure
Storage Admin

Chapter 2

System requirements

This chapter includes the following topics:

- Supported configurations and versions for NetBackup with CloudCatalyst

Supported configurations and versions for NetBackup with CloudCatalyst

Table 2-1 Supported versions

Veritas Access	Veritas NetBackup servers
7.3.2	8.1 and later (Linux only)

Download links:

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

Chapter 3

Configuring Veritas Access as a cloud storage server with NetBackup CloudCatalyst

This chapter includes the following topics:

- Benefits of using Veritas Access with NetBackup and CloudCatalyst
- 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
- Configuring Veritas Access as a cloud storage server on NetBackup server
- Configuring Veritas Access SSL with NetBackup

Benefits of using Veritas Access with NetBackup and 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).

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/.`

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.

Note: Data movement policy to the public cloud is not supported for the Appliance 1.0 release as the default policy needs to be manually updated.

---

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**.

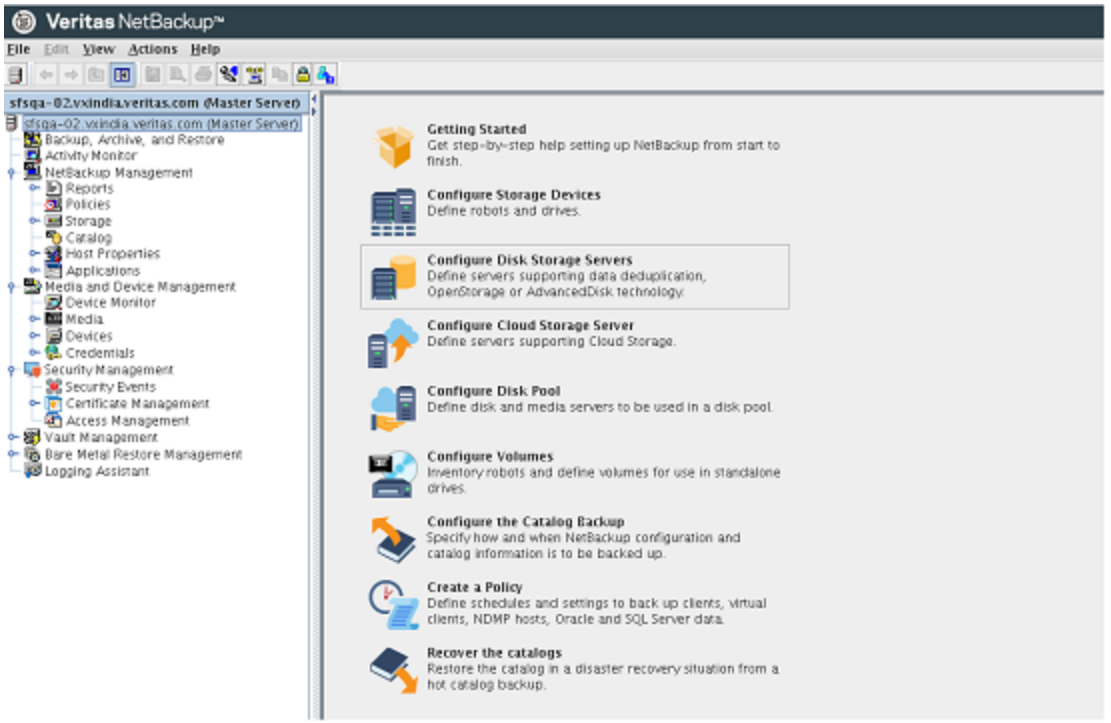
For the scale-out file system that is created, ensure that the **S3 Bucket** column displays **Yes** to indicate that the S3 bucket is enabled.

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

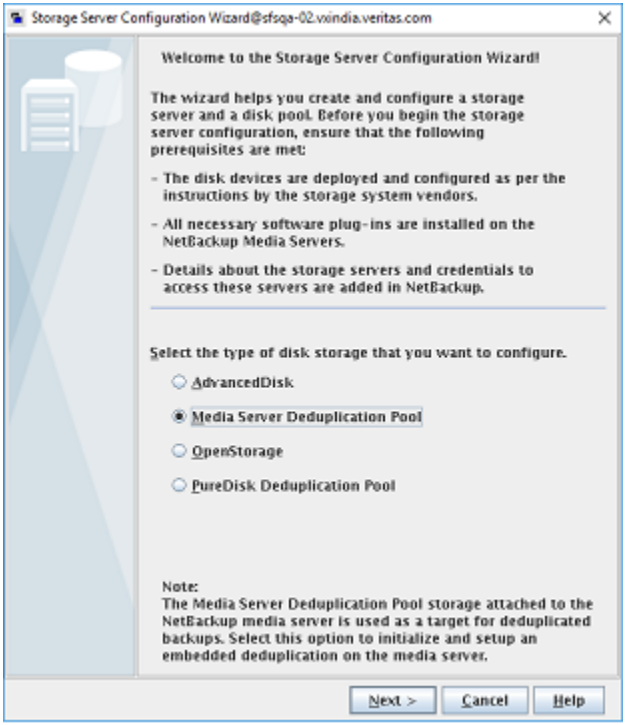
Creating a Media Server Deduplication Pool (MSDP) for primary backup using NetBackup

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

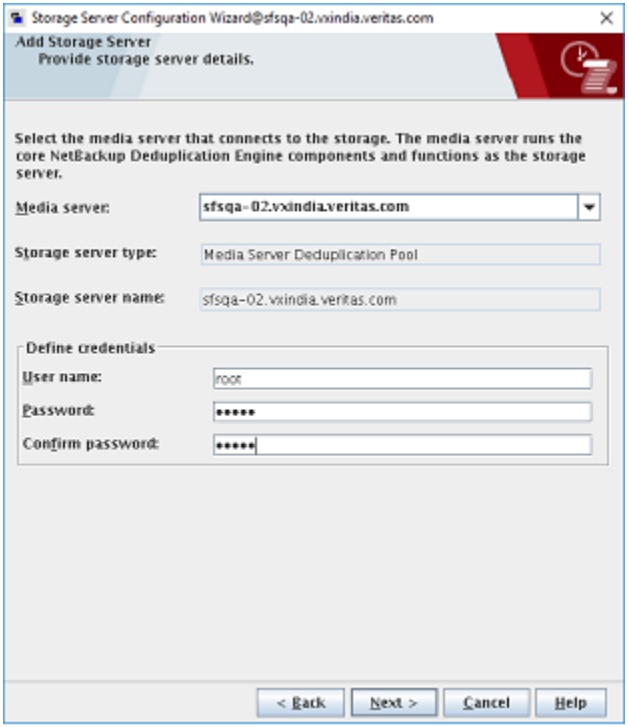
1 Log on to the NetBackup master server from the Java console.



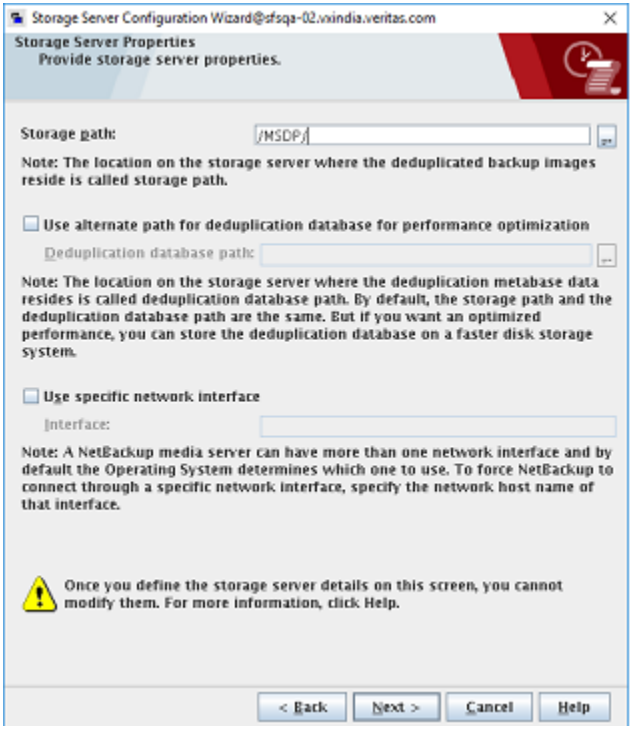
2 Select **Media Server Deduplication Pool**.



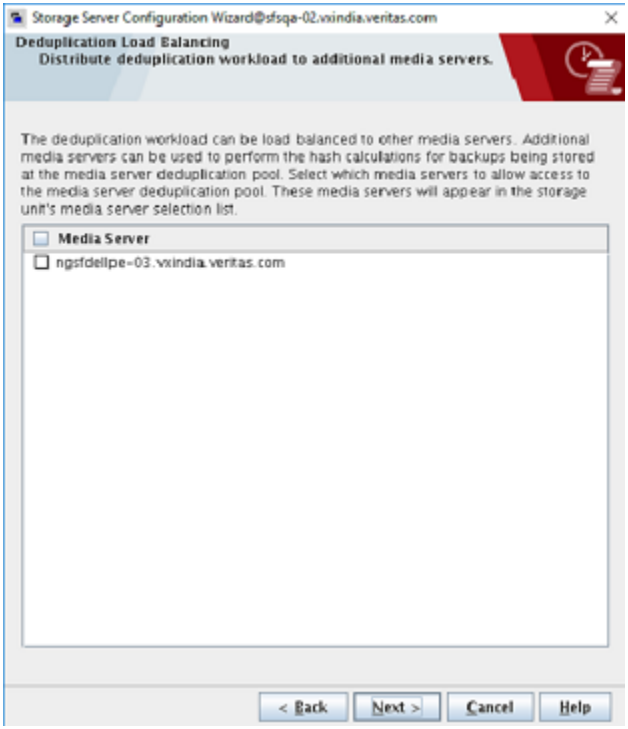
3 Enter the user name, password, and other required details.



4 Enter the storage path for MSDP.

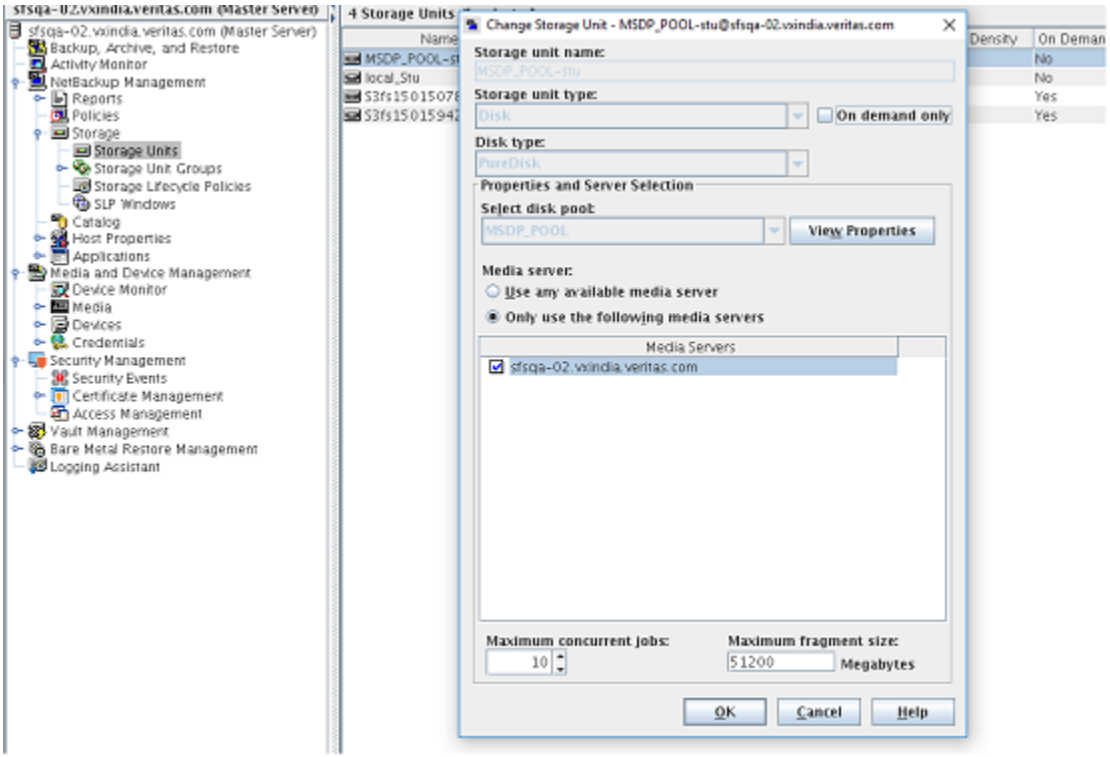


5 Enter the load balancing options to distribute the workload.

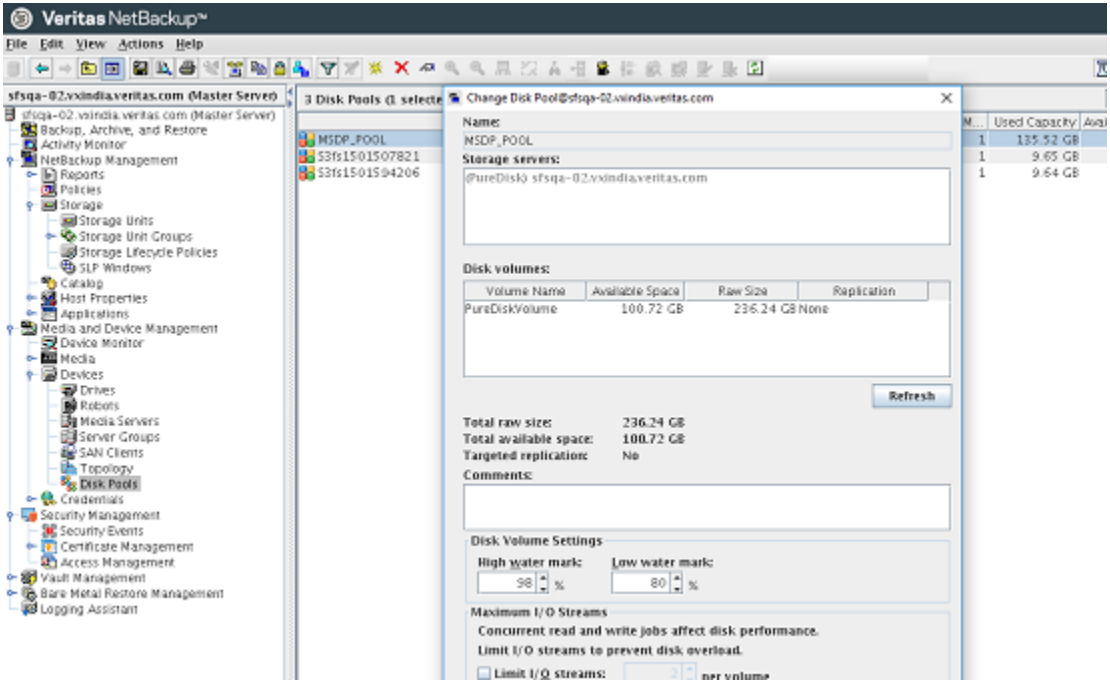


6 Verify the storage server configuration summary.

7 Verify that the storage unit is created for MSDP.



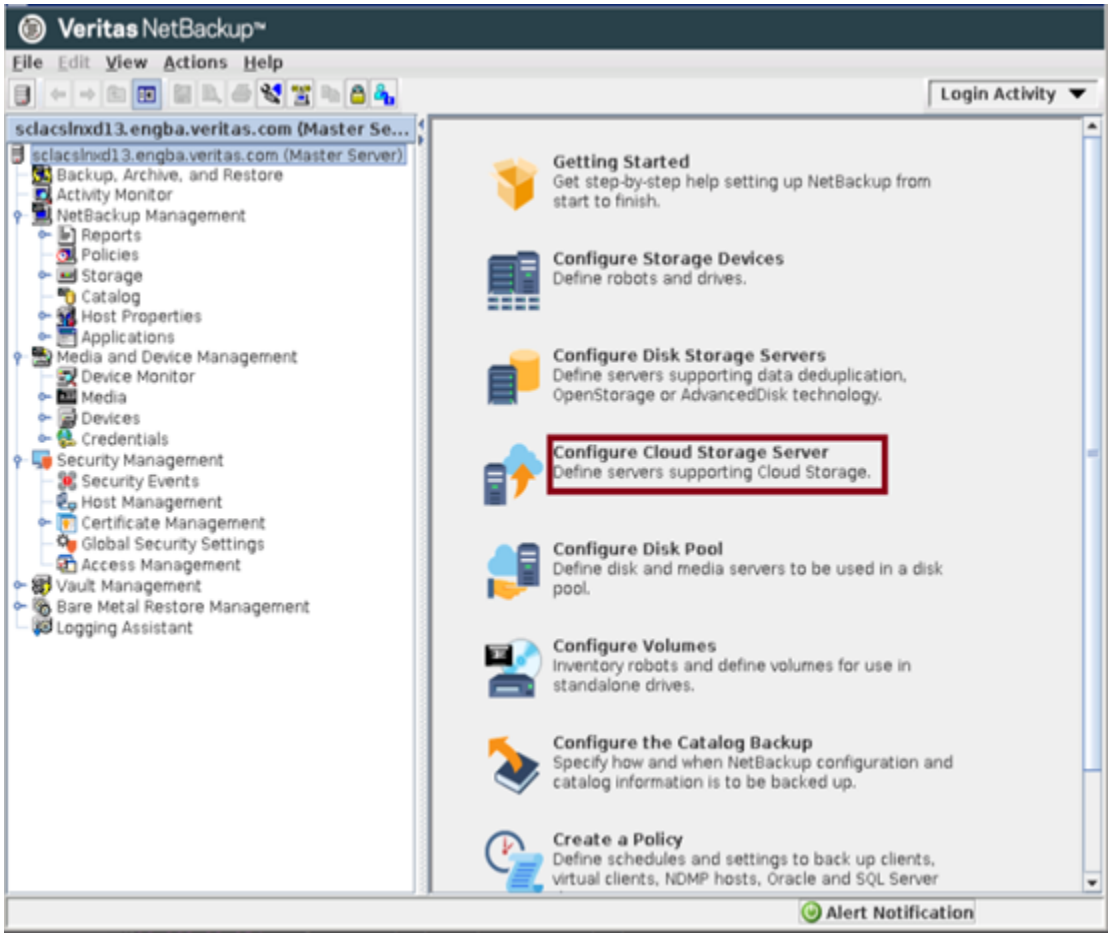
8 Verify that the disk pool is create for MSDP.



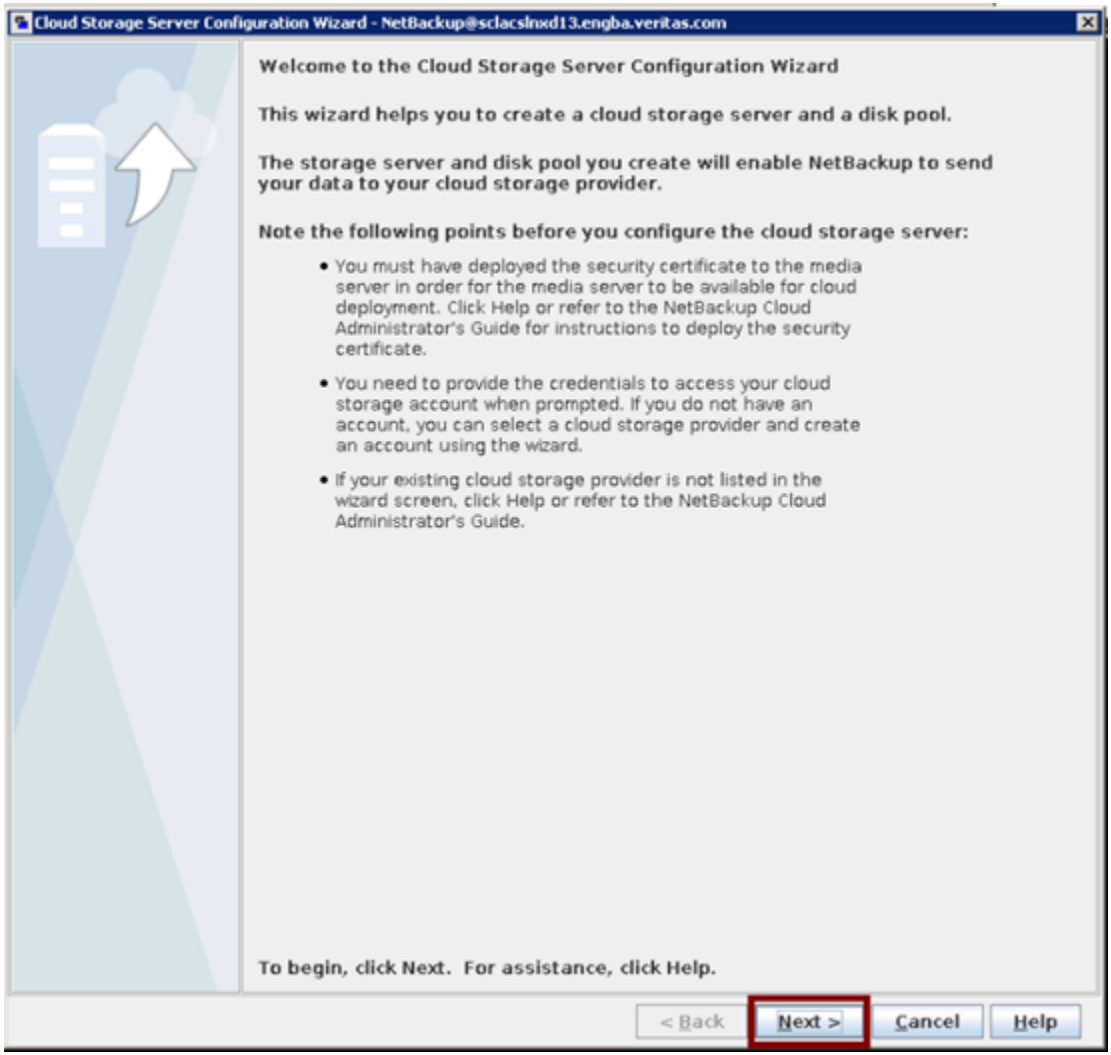
Configuring Veritas Access as a cloud storage server on NetBackup server

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

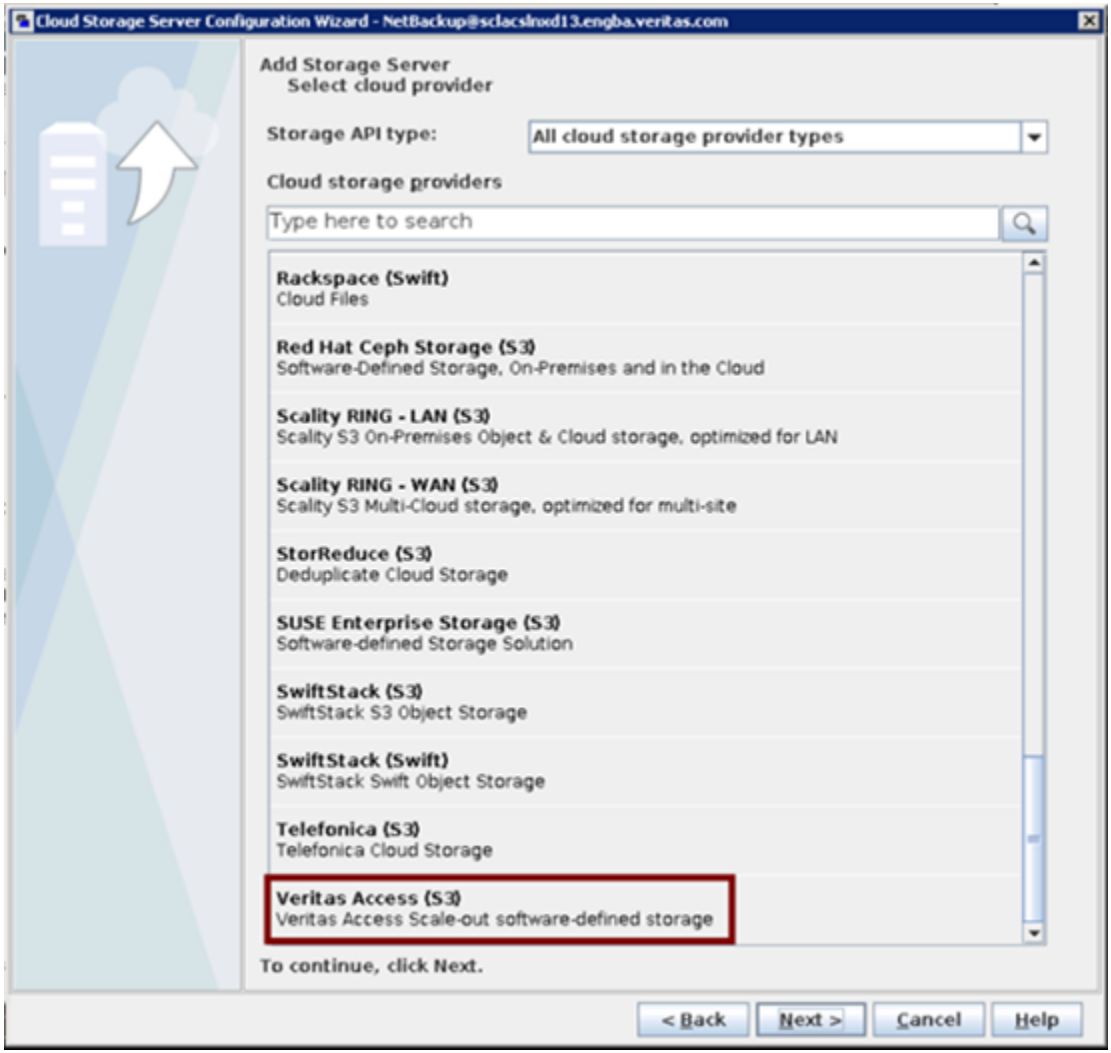
1. Log on to the NetBackup master server from the Java console.
2. Select **Configure Cloud Storage Servers**.



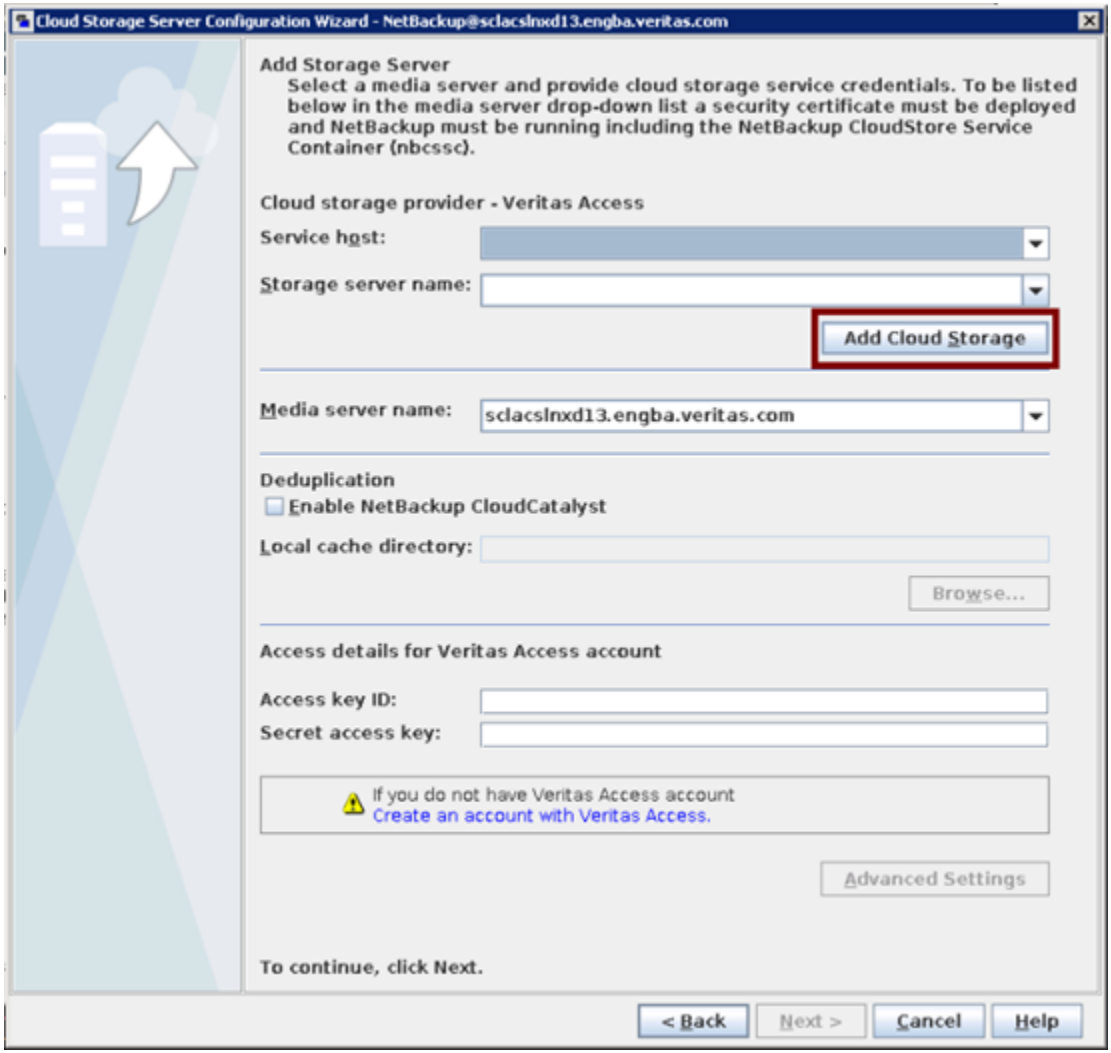
3 The **Welcome to cloud storage server configuration** wizard appears. Click **Next**.



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



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

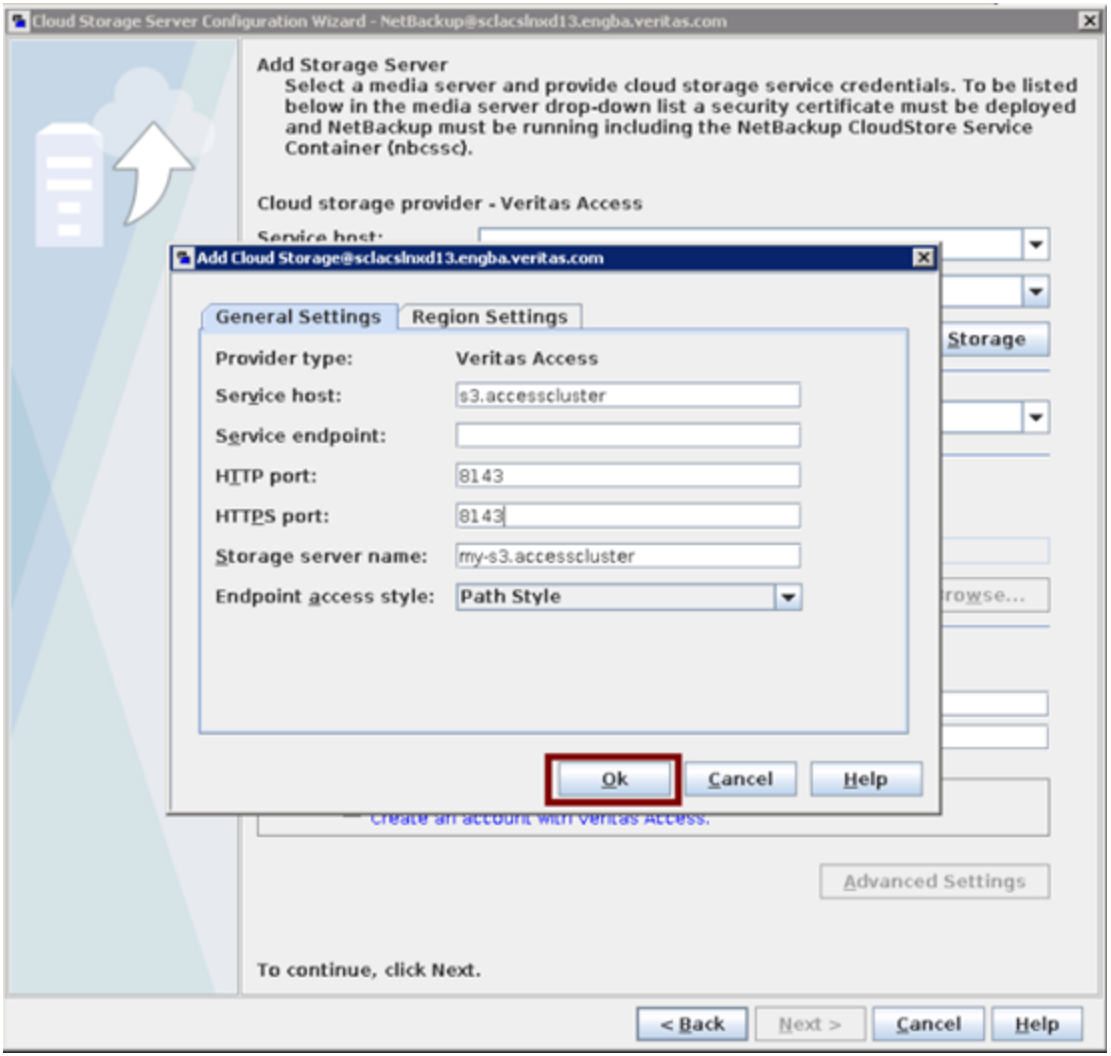


6 In the **Add cloud storage** wizard, enter the required information.

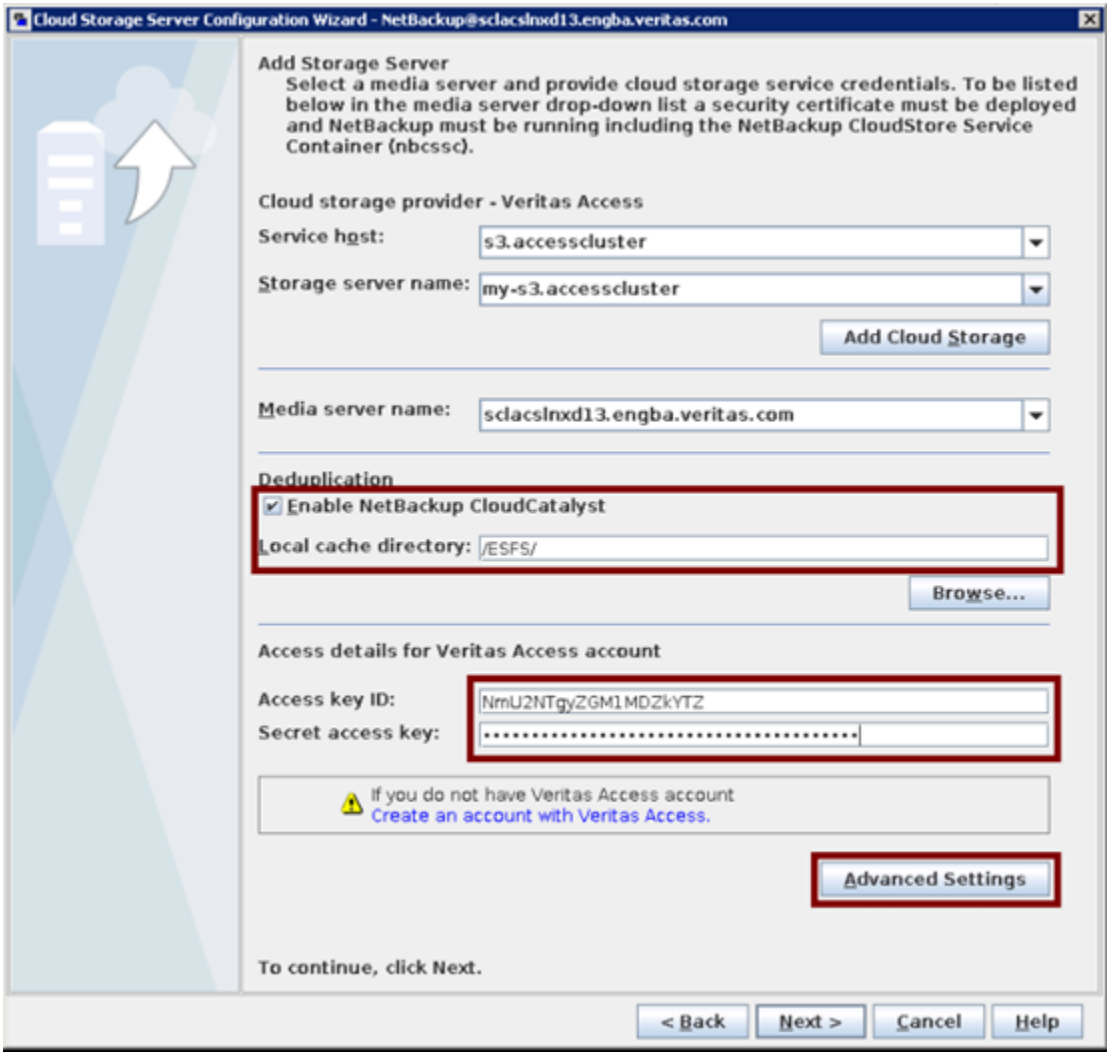
- Service host: s3.<veritas_access_cluster_name>
- HTTP port: 8143
- Https Port: 8143
- Storage server Name: Any string or any auto-generated name.

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

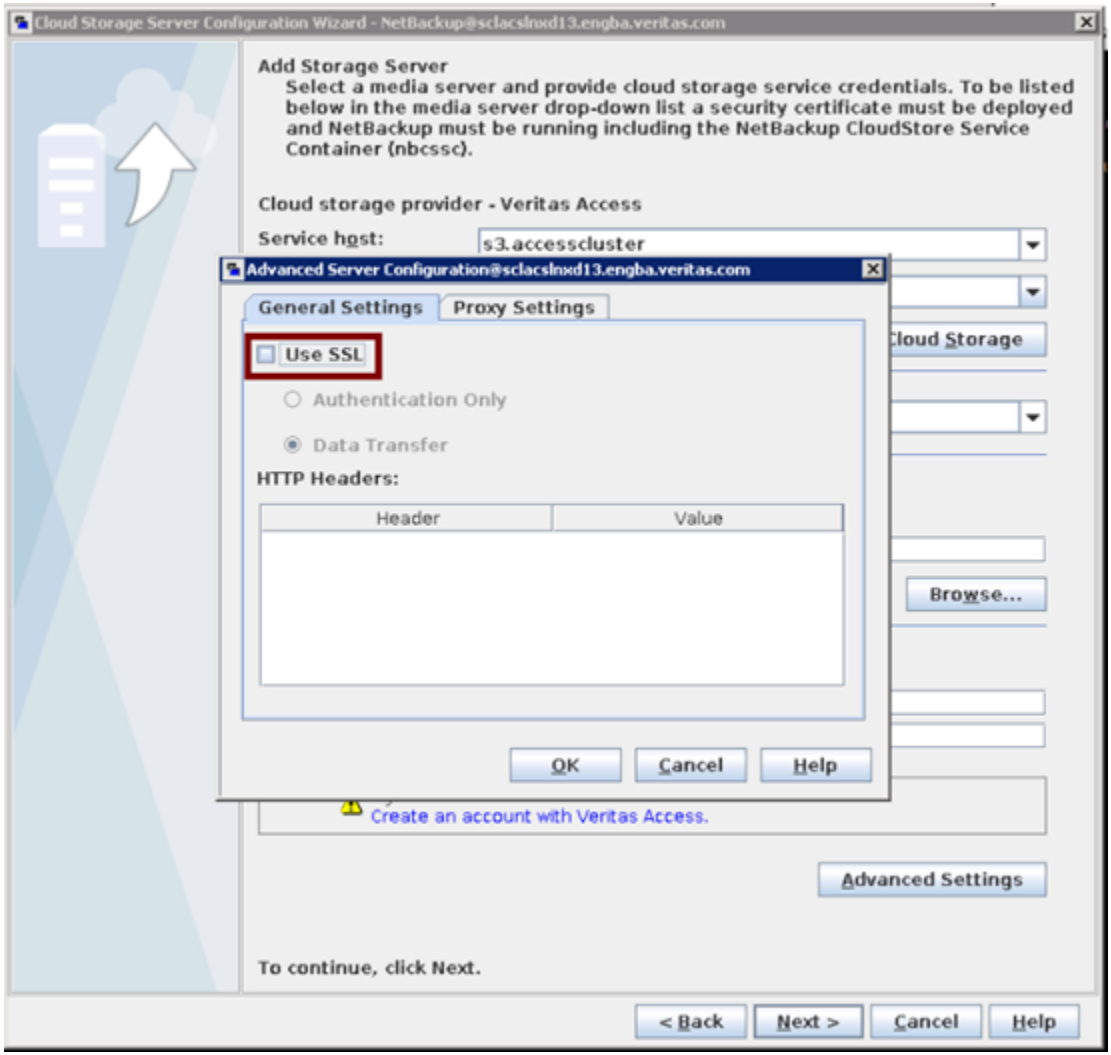
Click **Ok**.



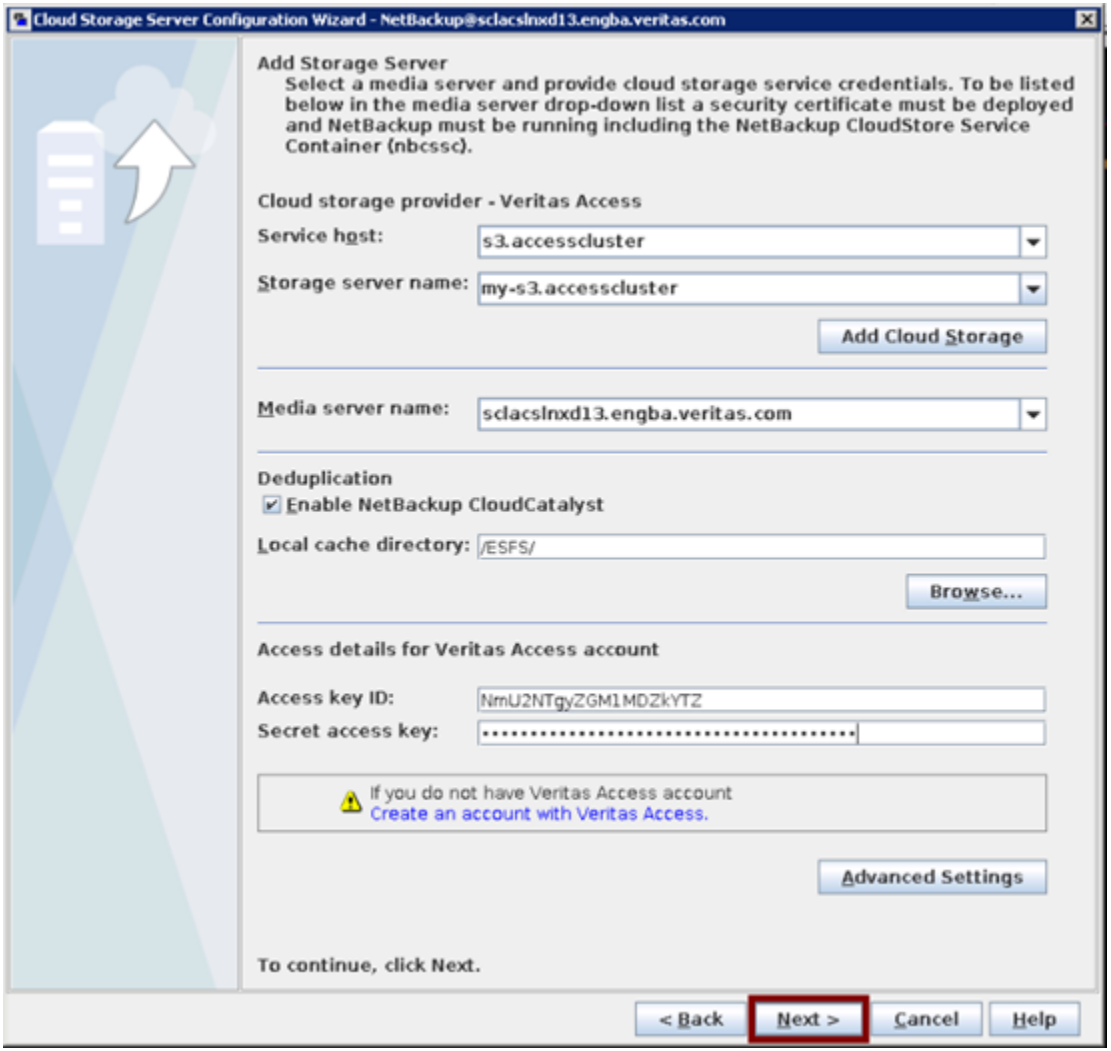
7 Select **Media server** from the **Media server name** drop-down box. Select the **Enable NetBackup CloudCatalyst** check box if you want to store the deduplicated MSDP backup data on Veritas Access's ObjectAccess bucket. Specify the path of local cache directory for CloudCatalyst. Enter the access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



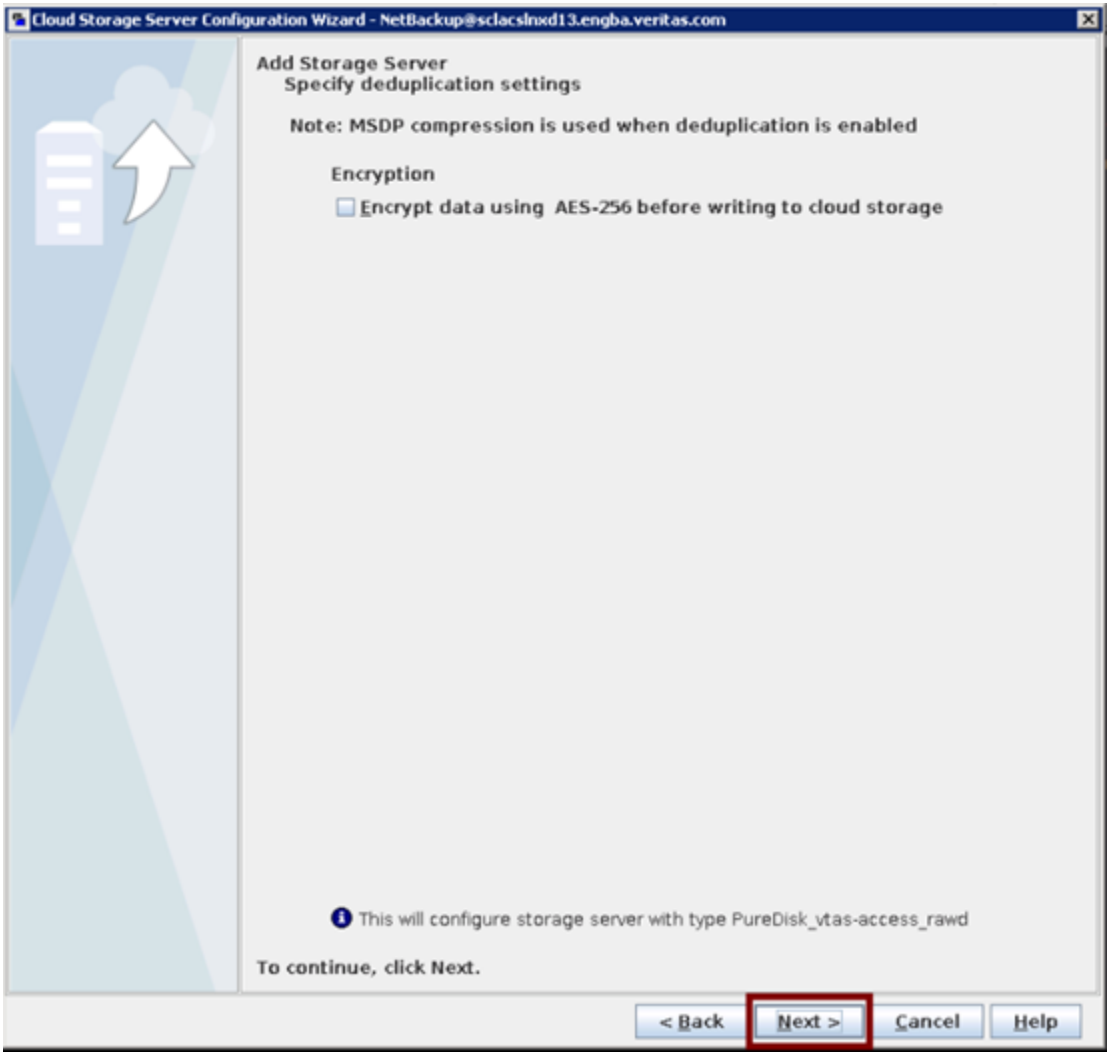
8 If the Veritas Access ObjectAccess server is configured with **No SSL**, then clear the **Use SSL** check box and click **Ok**.



9 Click **Next**

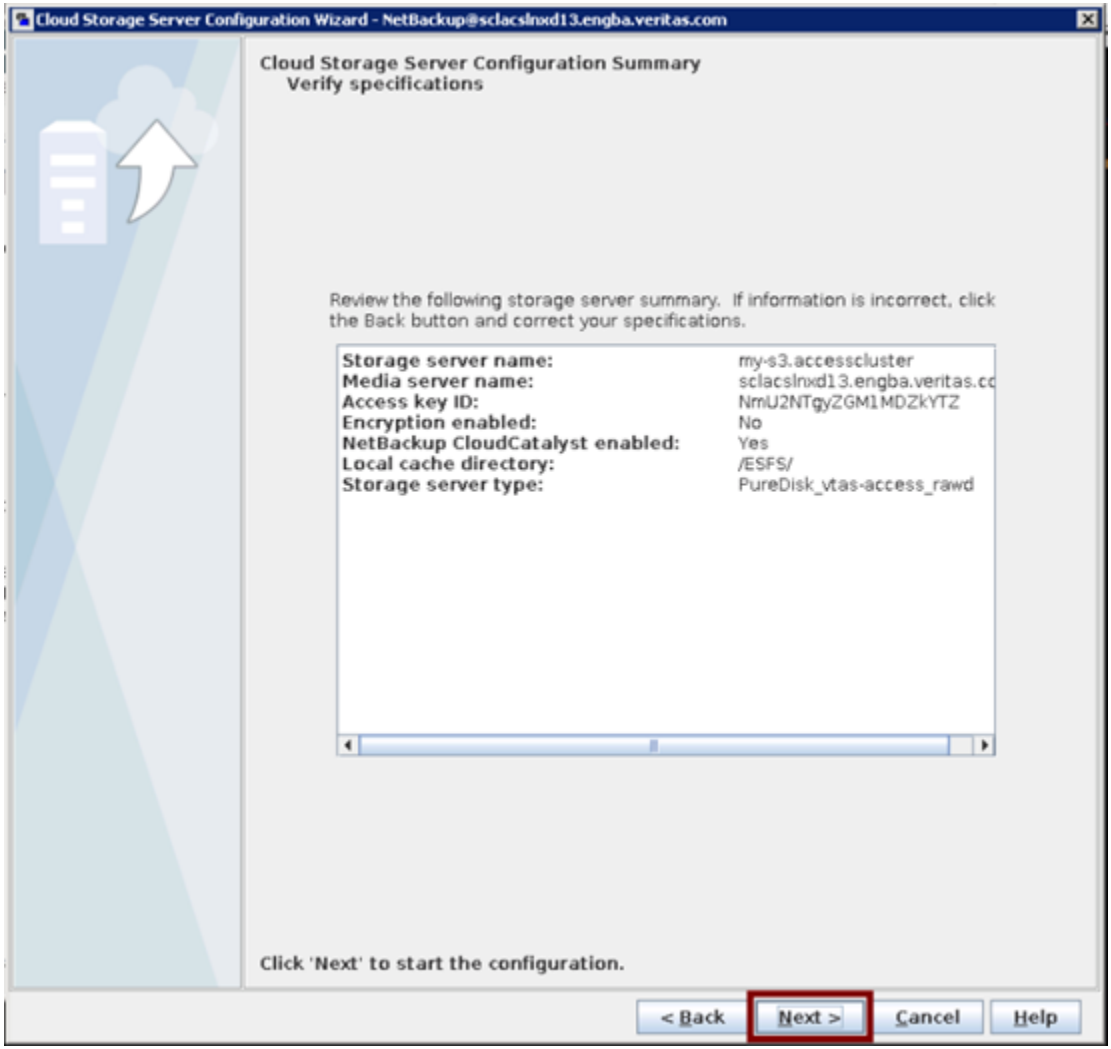

Cloud Storage Server Configuration Wizard - NetBackup@sclacslnxd13.engba.veritas.com
Add Storage Server
Select a media server and provide cloud storage service credentials. To be listed below in the media server drop-down list a security certificate must be deployed and NetBackup must be running including 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:
sclacslnxd13.engba.veritas.com
Deduplication
Enable NetBackup CloudCatalyst
Local cache directory:
/ESFS/
Browse...
Access details for Veritas Access account
Access key ID:
NmU2NTgyZGM1MDZkYTZ
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

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

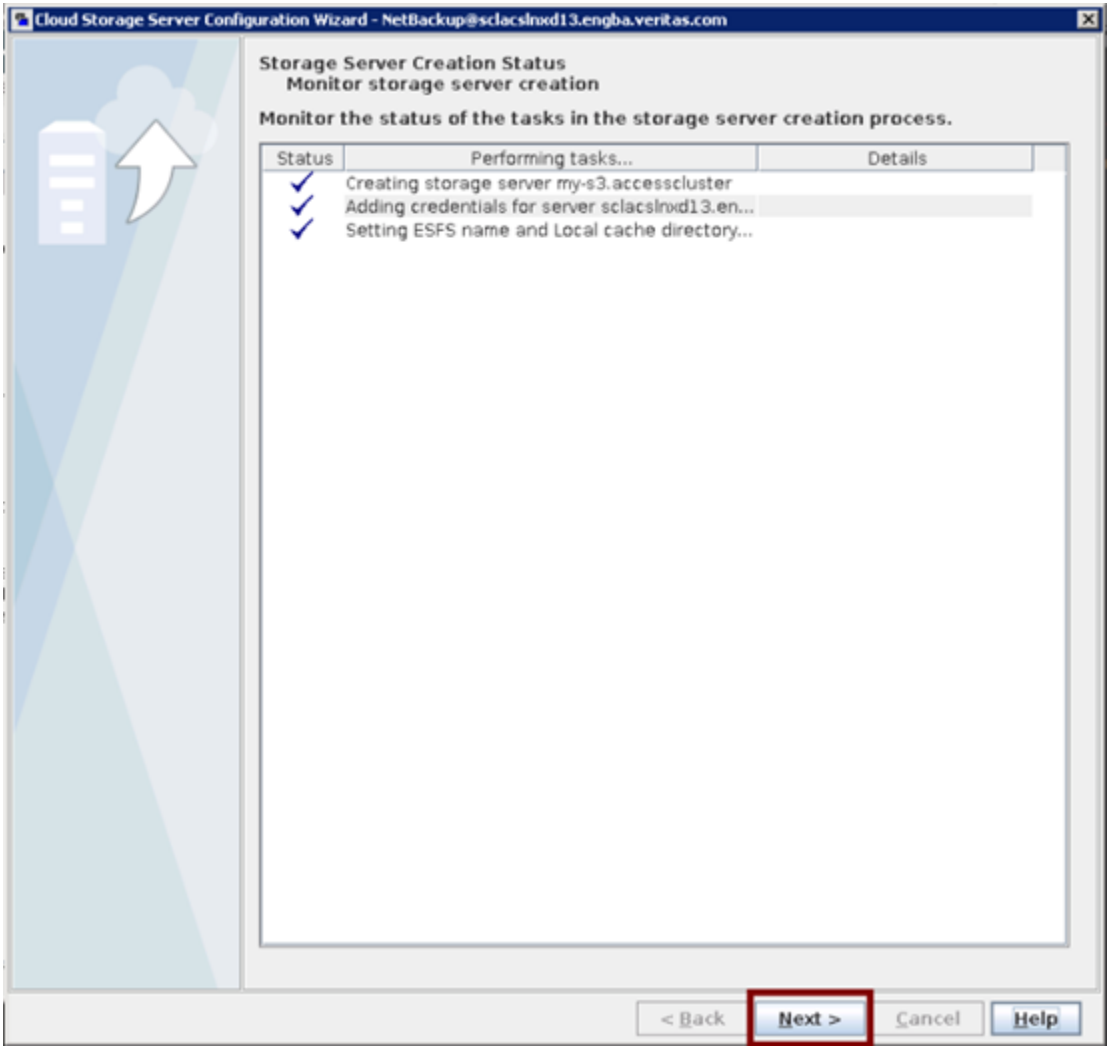


11 Messages related to setting the encryption appear. Click **Yes**.

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

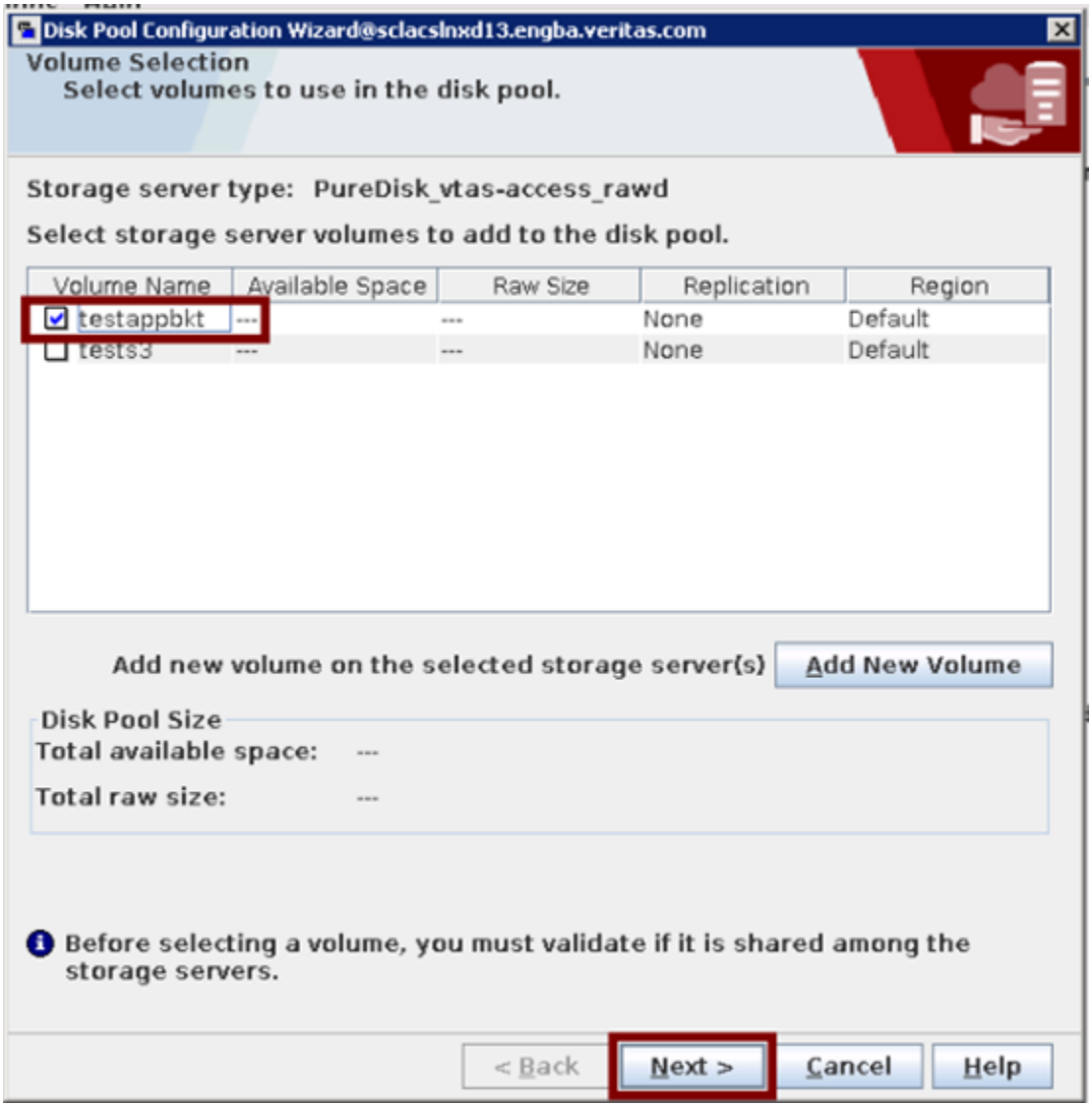


13 Check the status of the tasks in the storage server creation process. Click **Next**

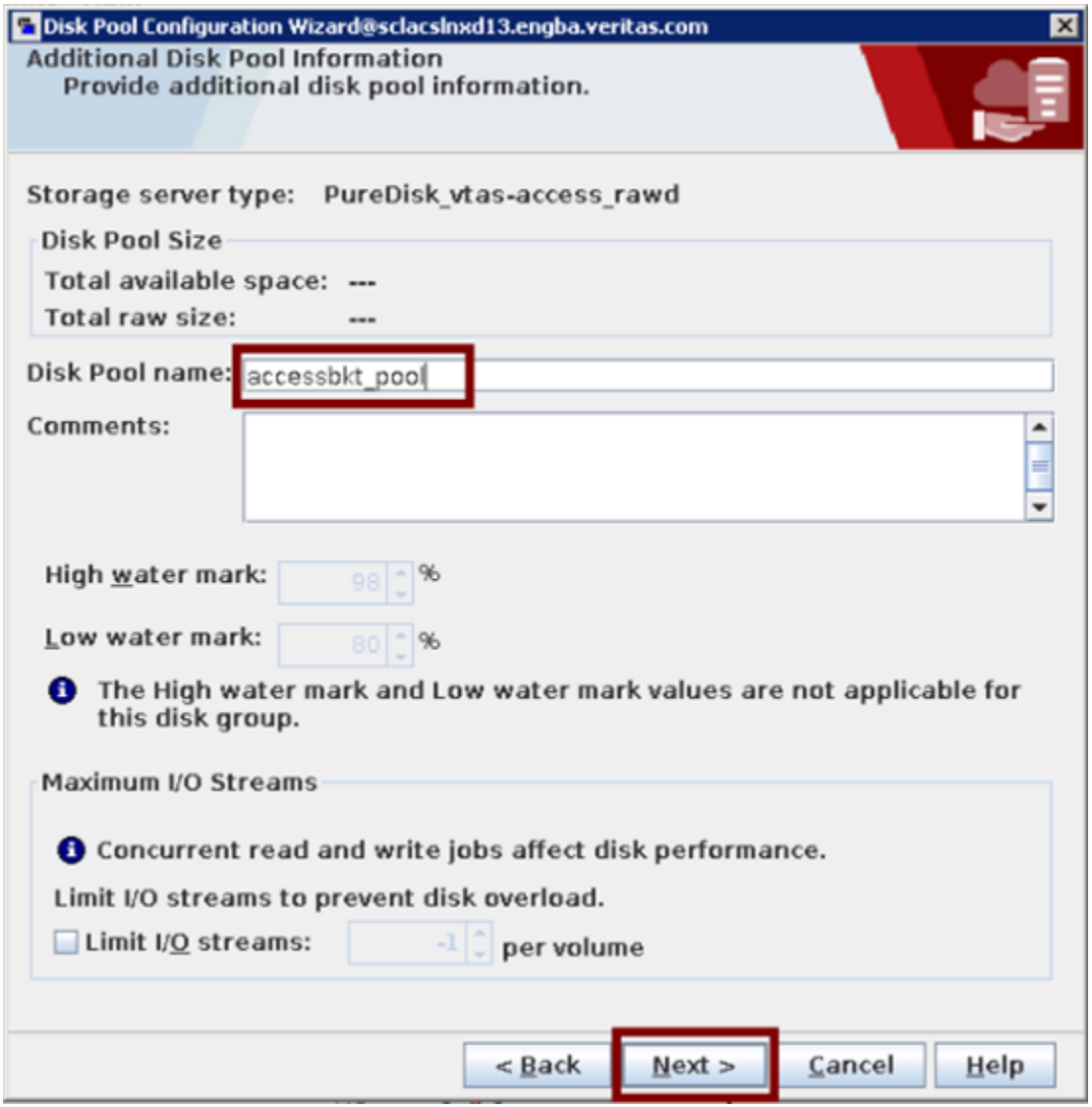


14 Verify that the storage server is successfully created and click **Next**.

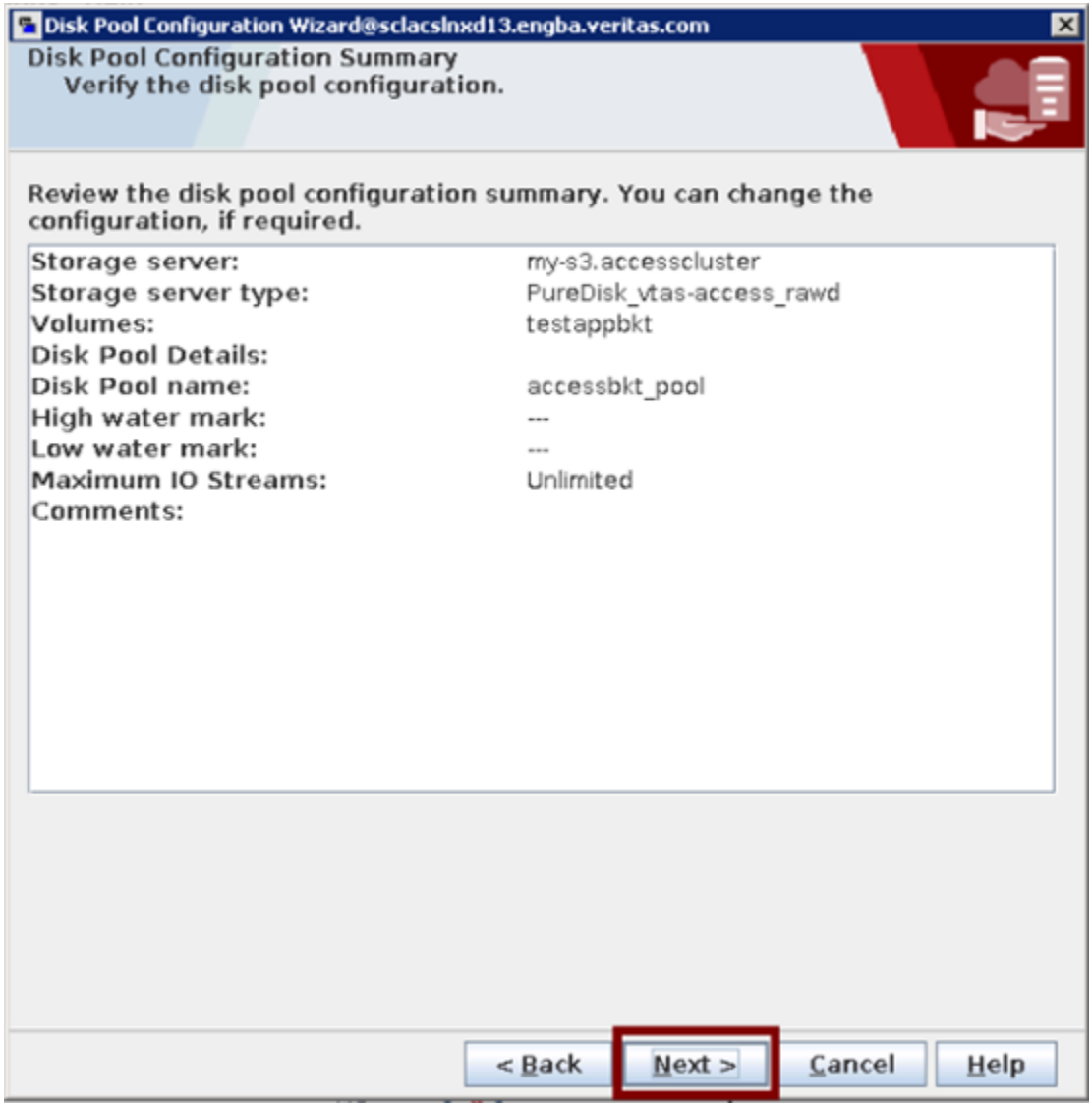
15 The **Volume selection to use in disk pool** form lists all the buckets that are created by a user on the Veritas Access cluster as a volume. If the bucket is not created from Veritas Access, then click on **Add volume** and specify the bucket name. After bucket creation, the bucket is listed as a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



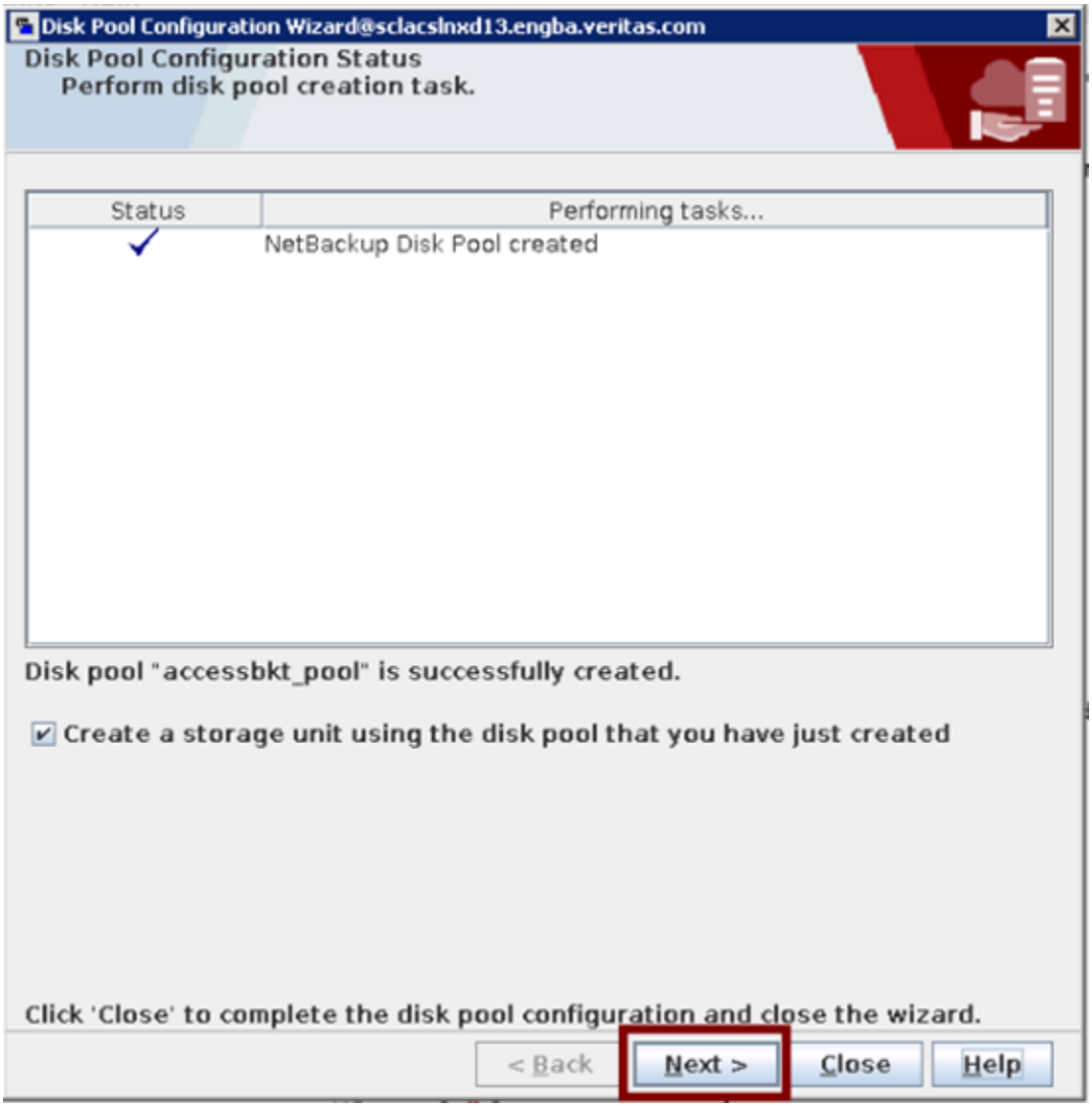
16 In the **Additional disk pool information** form, enter the disk pool name and click **Next**.



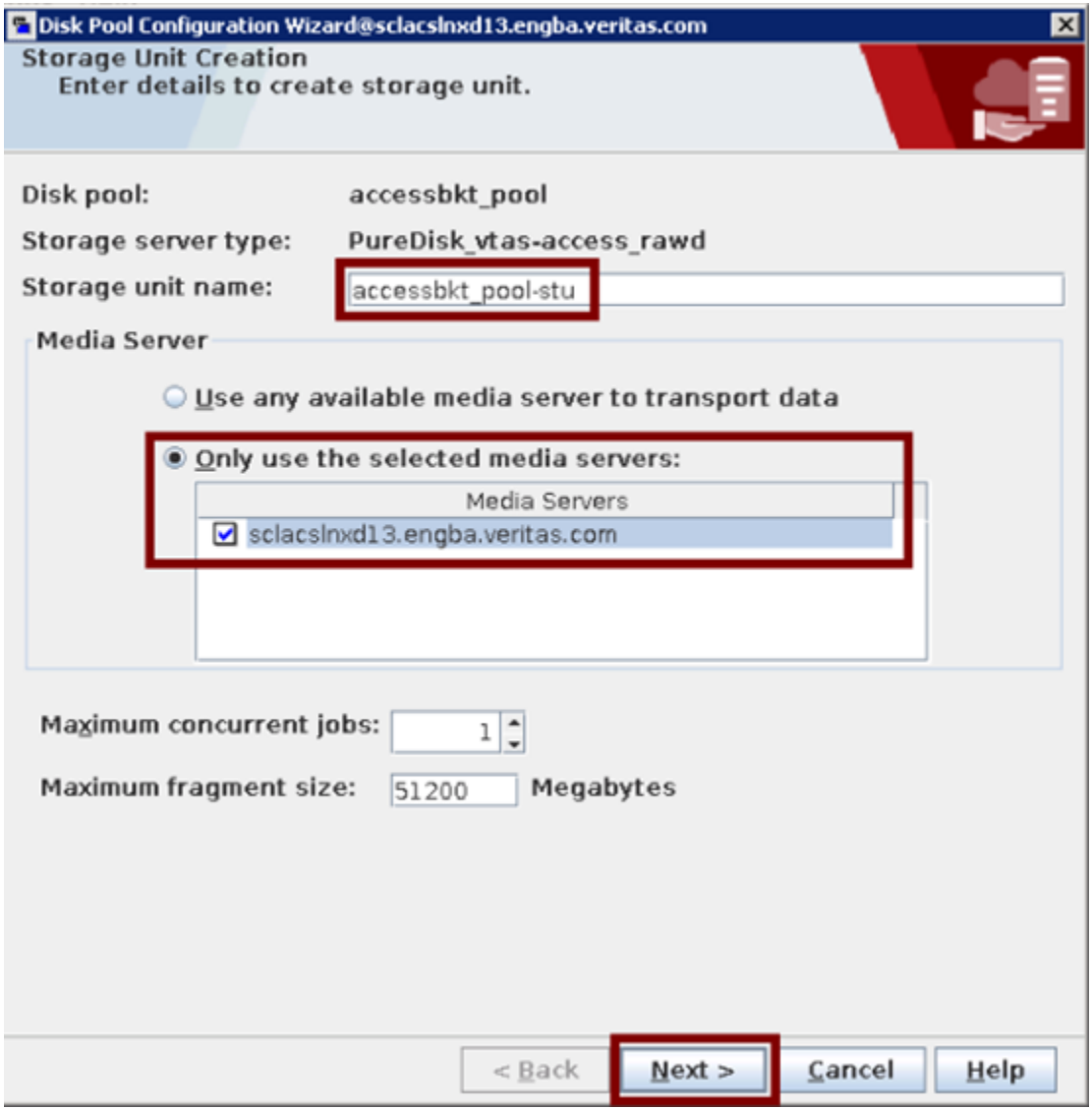
17 Review the disk pool configuration summary and click **Next**.



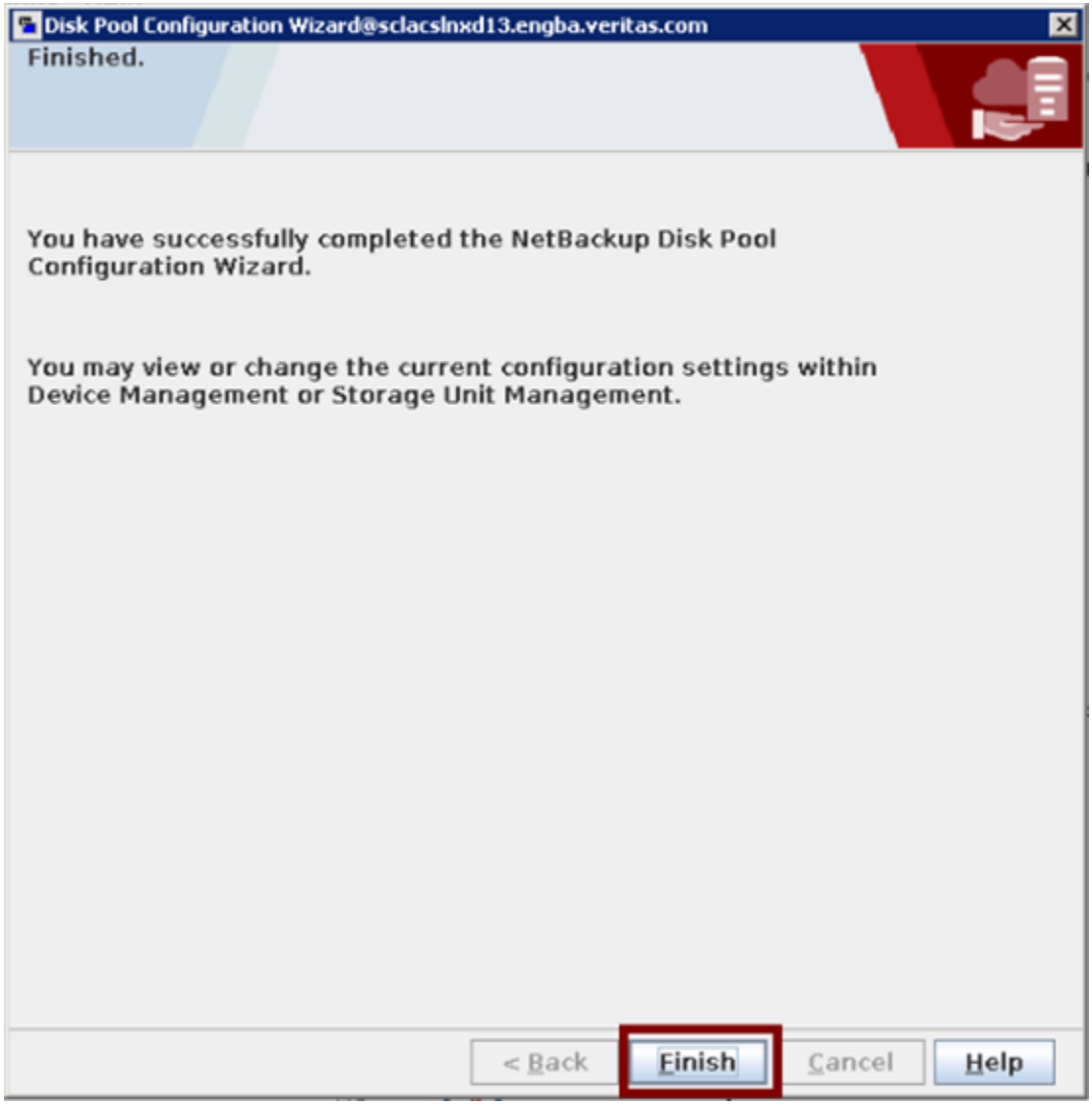
18 In the **Disk pool creation status** form, verify that the disk pool is created successfully. Make sure that the **Create storage unit using disk pool which you have just created** check box is selected.



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**.



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



Configuring Veritas Access SSL with NetBackup

To configure Veritas Access SSL with NetBackup

1 Enable SSL on Veritas Access.

```
Objectaccess > set ssl_enabled yes
Objectaccess > server stop

Objectaccess > server start
```

2 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

BAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRAwDgYDVQQKDAdWZXJpdGFzMQ8w

DQYDVQQLDAZBY2Nlc3MxFjAUBgNVBAMMDXMzLm5idTg3Mi1hcHAwHhcNMTgwMTAz

MTAwODAxWhcNMjEwMTAyMTAwODAxWjBdMQswCQYDVQQGEwJVUzETMBEGA1UECAwK

Q2FsaWZvcm5pYTEQMA4GA1UECgwHVmVyaXRhczEPMA0GA1UECwwGQWNjZXNzMRYw

FAYDVQQDDA1zMy5uYnU4NzItYXBwMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB

CgKCAQEAl+XkH9Buzz2KRYsoBbKxOExq2fRDhfTb1lplleiMN/1cryvMkguEFkFk

kjuTsi3lnuj0Sc5/FimzfnclXyvI9uWAB07wdxwjKFBlg0GvxSa/obQ/SMG8fEHL

qYl/baJKPoz7xvg+QJd/3A1ZJqLvA1i7DEErVuUyNrtjxKnPNIKzzRhBg9M5+HPp

b4ZOXUnFWU9w4CI1JBvYTBQ5X2wtGx9cLtHb9fF9XTv2SqWUUroGDc2DYlgo8j2n

AsTWzk+mJw12wRcE00FoBlYhOCNJlXkl4n4VSKbTUdCMkm6Ej5Yf+AIAbLiQNFgv

Sralc5TFMHjUUg5dgBPizCLTmuQz8QIDAQABo1AwTjAdBgNVHQ4EFgQUgBpm7gK1

q/M/3+Y0st8m2EMzulgwHwYDVR0jBBgwFoAUgBpm7gK1q/M/3+Y0st8m2EMzulgw

DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAcw4QIfXiuJMY/6BGBVAA

dnrRG11+hczHfbQVeDV9ApijEe/qiIx8QLL9fDx8MqsdIIHcgfuv5mzAQLzwa+tH

7USIqBfxfEytnKBuAYbYyOfXKJDUIAaWFjcM0rOP1z+Dv6zf7B65Mv3aKD1rENFT

UgPBphLACAU9CzLidJkoE3izOaZbiys/r24yRR8X/Pugsxy7VESN6WSqzYg0jdSf

iCJKgLEdOYcE85NhW8eaCsfqCkxoskTgu1Nnf4j0lMYP5d+4U8uAEc/uLrndD3Rn
```

```
n7MB0EeciPgqWZQWNLjyQNNZ/F58wlyTtHv48VM1ZXhIJBhjUwFZAEAg43R5n67o

Pw==

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

3 Restart the NetBackup services on both the master and media server.

```
# bp.kill_all
# bp.start_all
```

4 Configure the cloud storage server with SSL.

Chapter 4

Configuring backup and restore using NetBackup policies

This chapter includes the following topics:

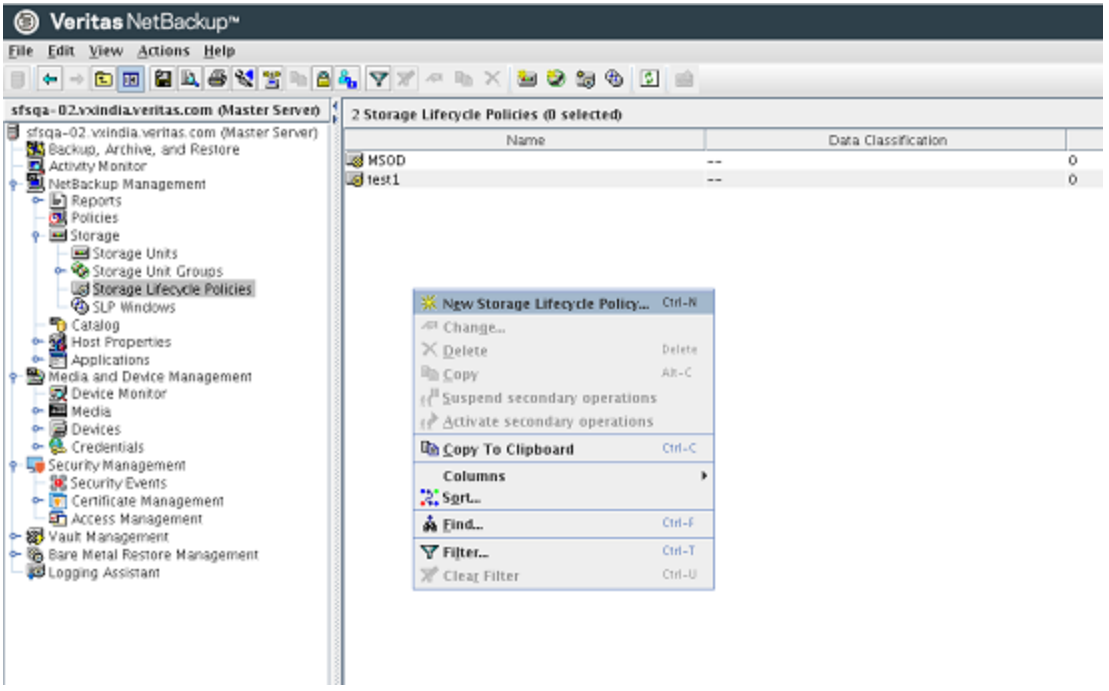
- Storage Lifecycle Policies
- Backup and restore
- Running a backup policy manually
- Restoring backed up files

Storage Lifecycle Policies

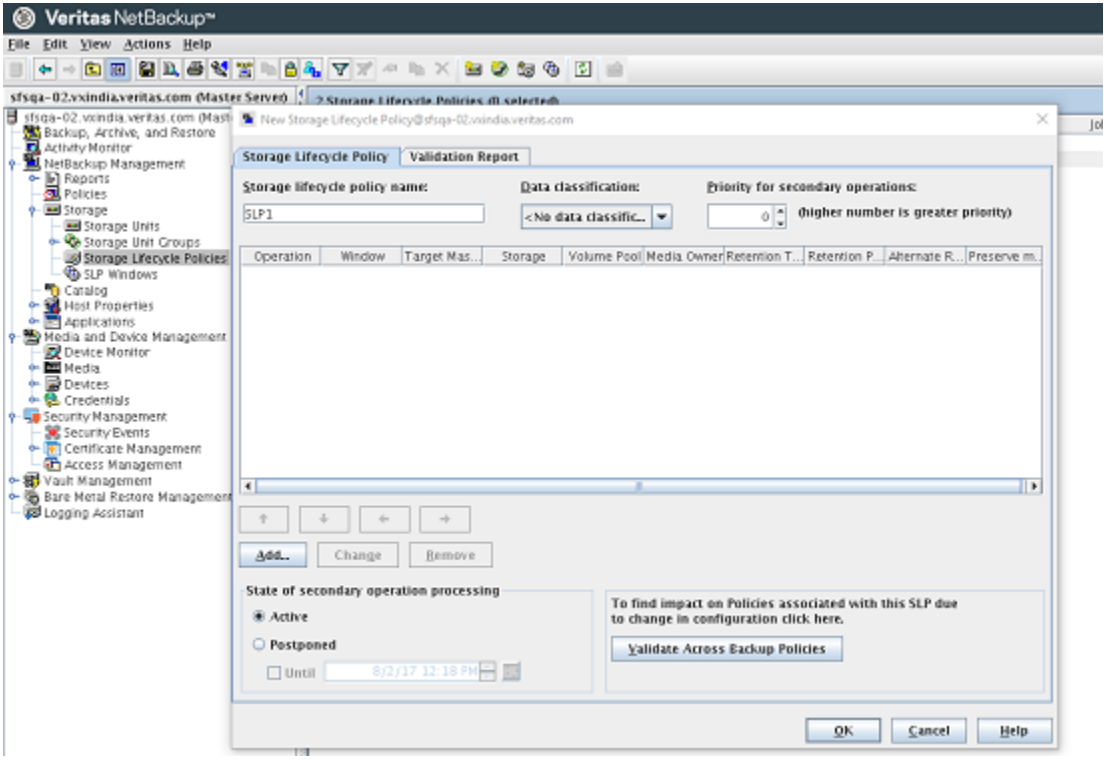
You can create Storage Lifecycle Policies (SLP).

To create Storage Lifecycle Policies

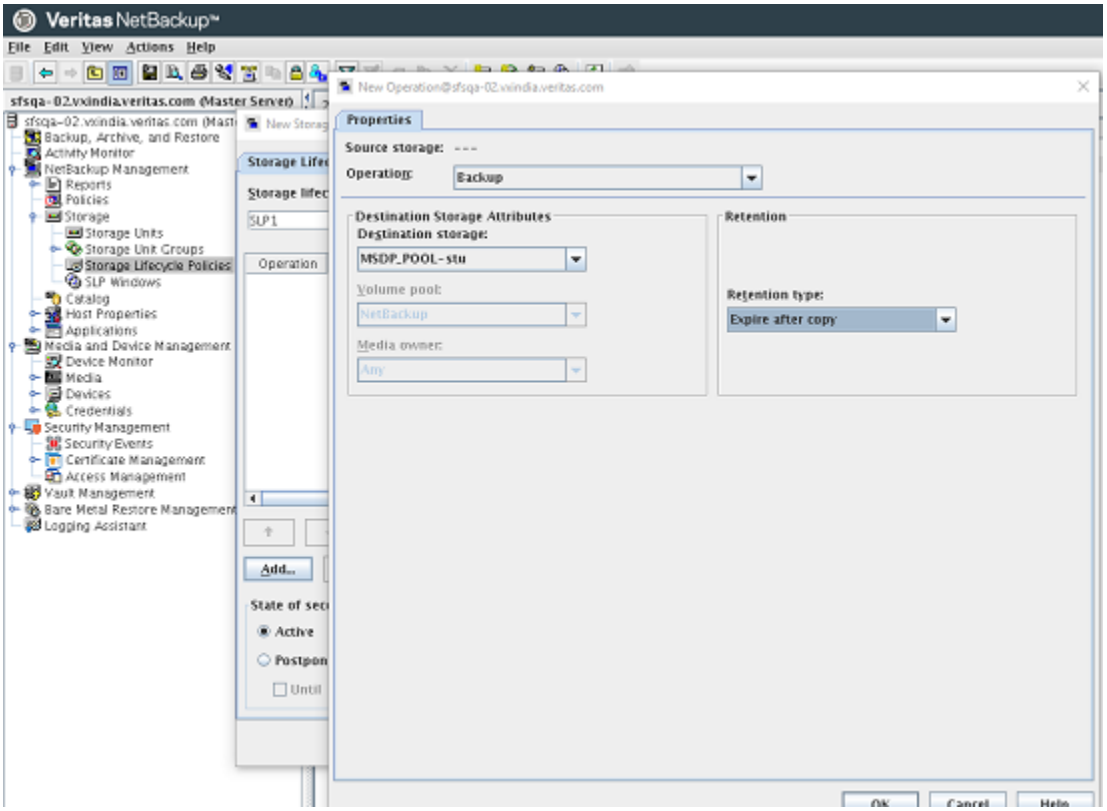
1 Click **Storage** -> **Storage Lifecycle Policies** on the NetBackup console. Select **New Storage Lifecycle Policy**.



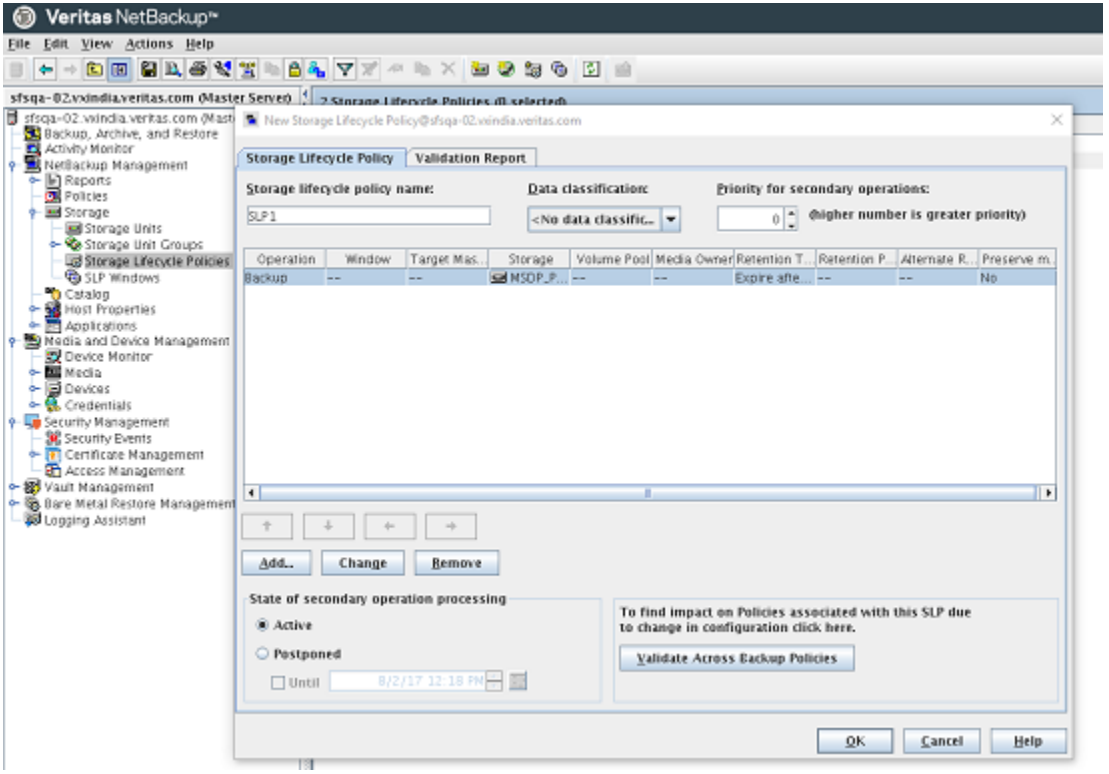
2 Enter a unique policy name for the policy. Click on the **Add** button.



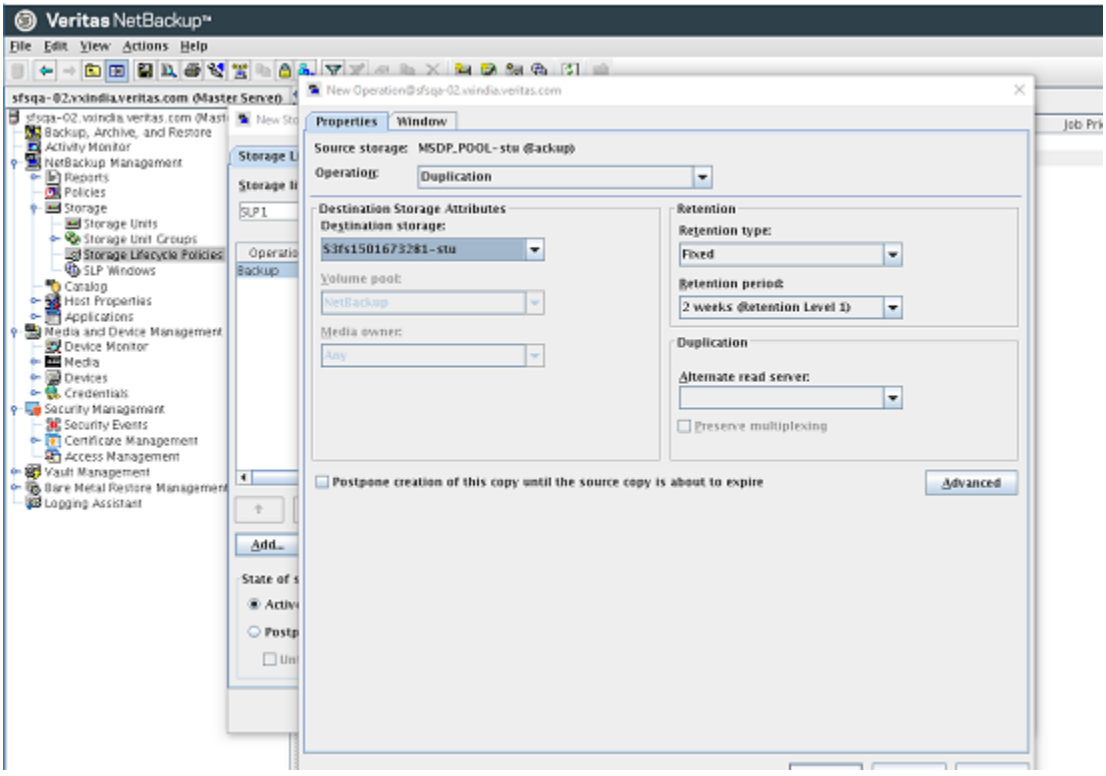
3 Select **Operation** as **Backup**, and set the destination pool to the MSDP pool that was created. Choose the **Retention type** based on your requirement.



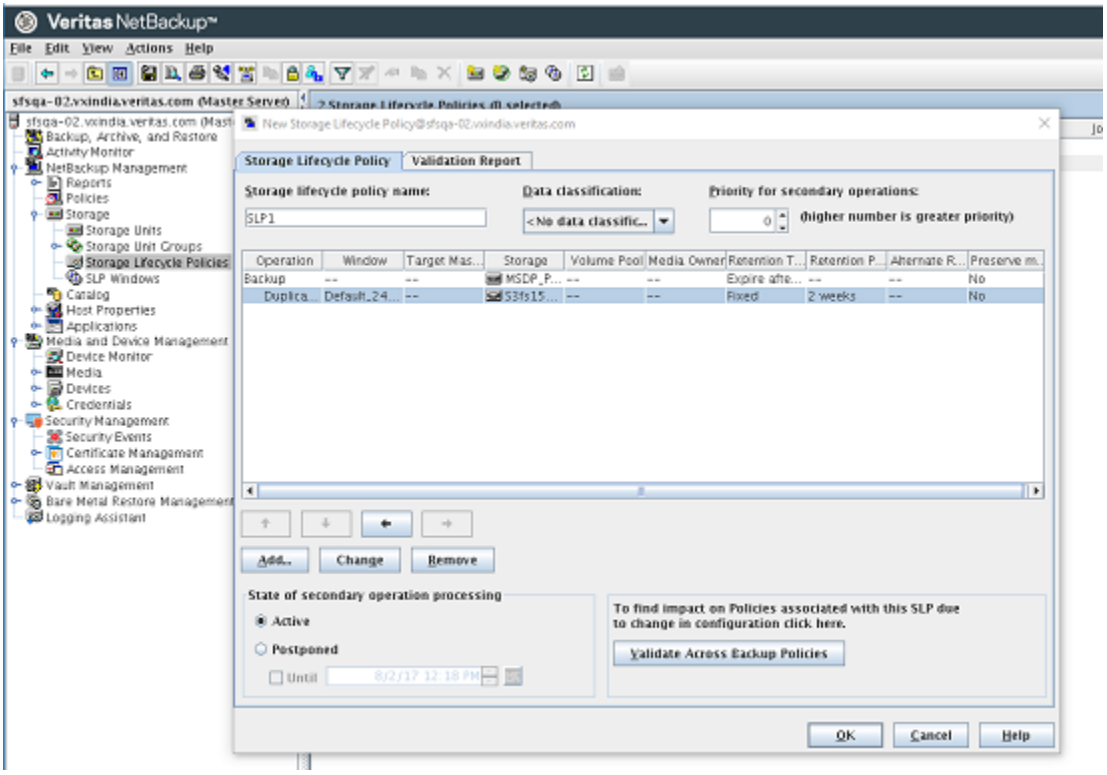
4 A new entry for Backup gets added. Click on the **Add** button again.



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.



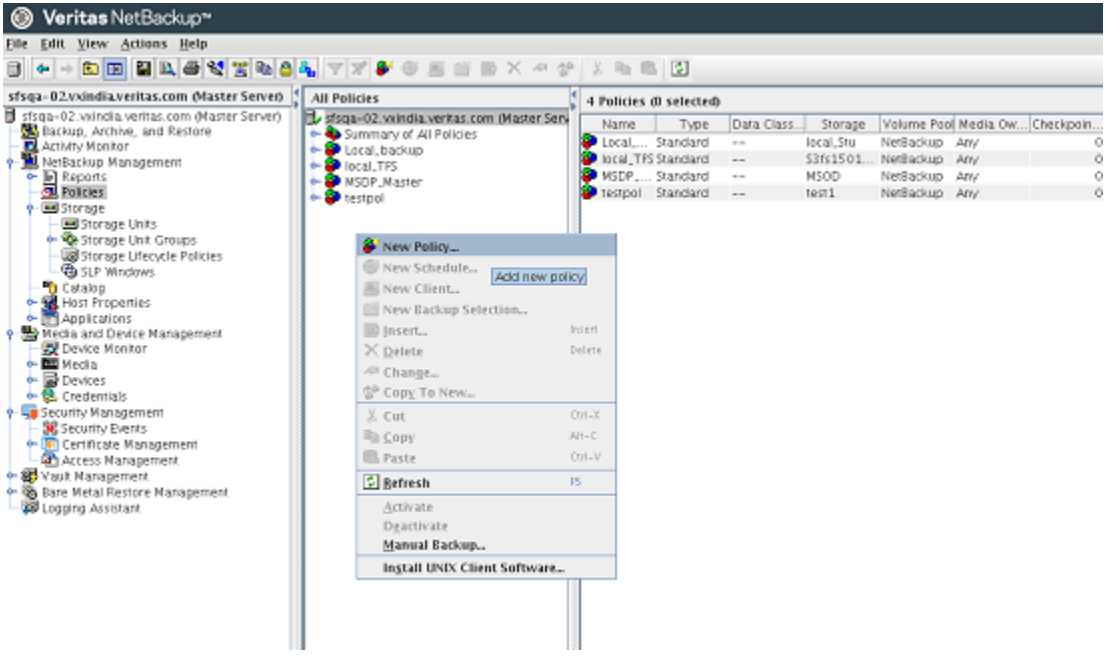
Backup and restore

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

Policy creation

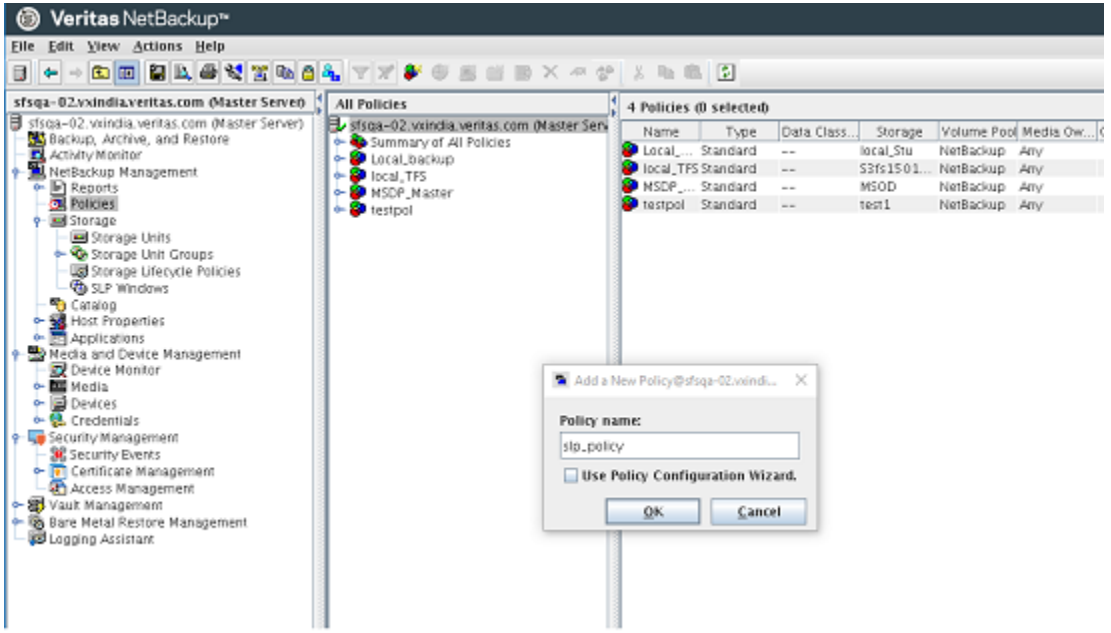
To create policies

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



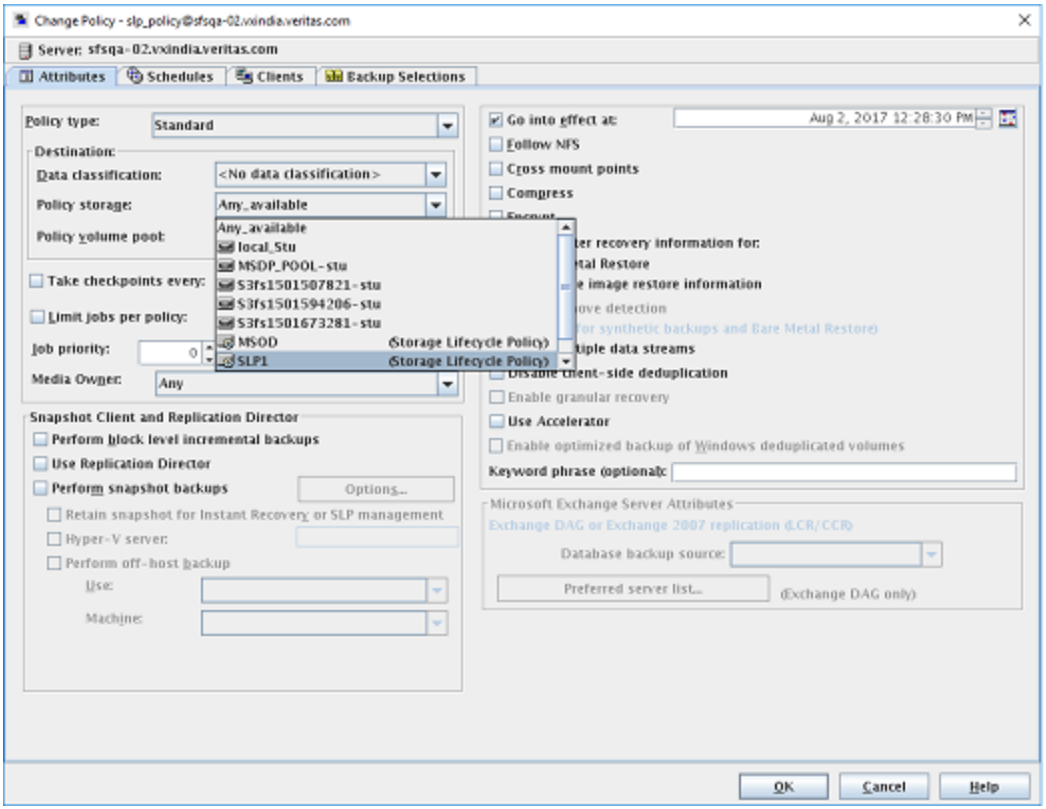
2 Provide the following information for policy creation.

- Policy name
- From the **Attributes** tab, select the appropriate storage unit under **Policy storage**.

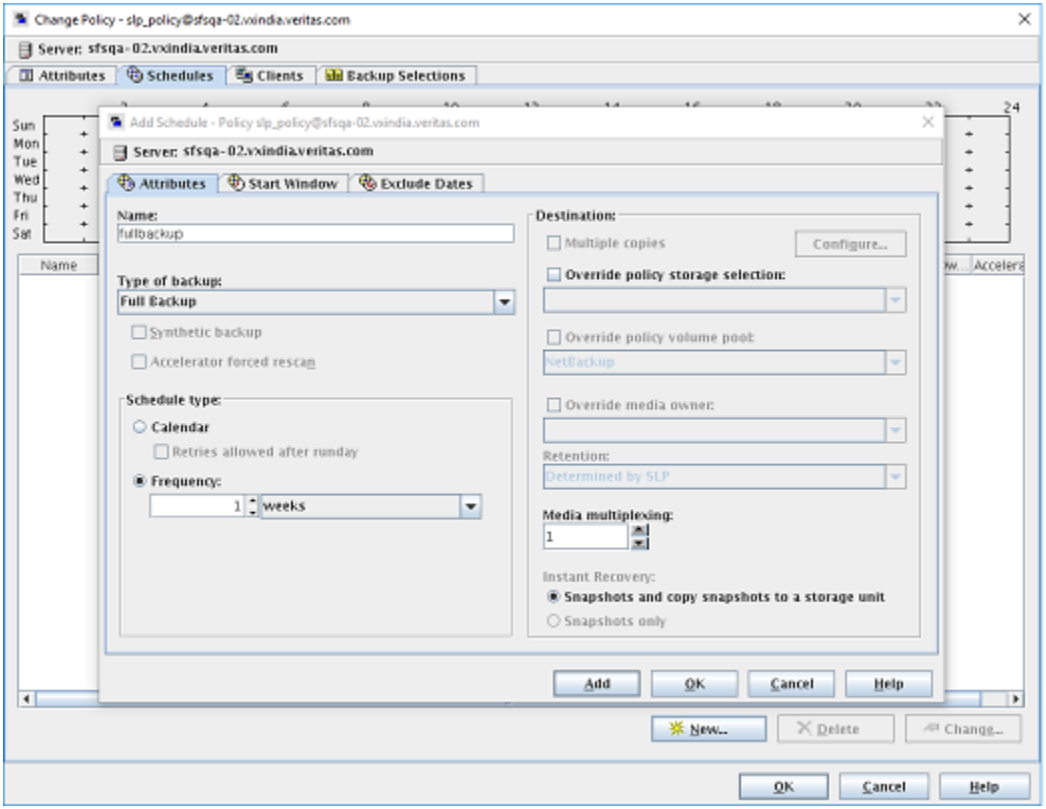

Veritas NetBackup™
File Edit View Actions Help
sfsqa-02.vxindia.veritas.com (Master Server)
sfsqa-02.vxindia.veritas.com (Master Server)
Backup, Archive, and Restore
Activity Monitor
NetBackup Management
Reports
Policies
Storage
Storage Units
Storage Unit Groups
Storage Lifecycle Policies
SLP Windows
Catalog
Host Properties
Applications
Media and Device Management
Device Monitor
Media
Devices
Credentials
Security Management
Security Events
Certificate Management
Access Management
Vault Management
Bare Metal Restore Management
Logging Assistant
All Policies
sfsqa-02.vxindia.veritas.com (Master Serv
Summary of All Policies
Local_backup
local_TFS
MSDP_Master
testpol
4 Policies (0 selected)
Name
Type
Data Class...
Storage
Volume Pool
Media Ow...
Local_...
Standard
--
local_Stu
NetBackup
Any
local_TFS
Standard
--
S3fs15 01...
NetBackup
Any
MSDP_...
Standard
--
MSOD
NetBackup
Any
testpol
Standard
--
test1
NetBackup
Any
Add a New Policy@sfsqa-02.vxindi...
Policy name:
slp_policy
Use Policy Configuration Wizard.
OK
Cancel

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

See “Storage Lifecycle Policies” on page 43.

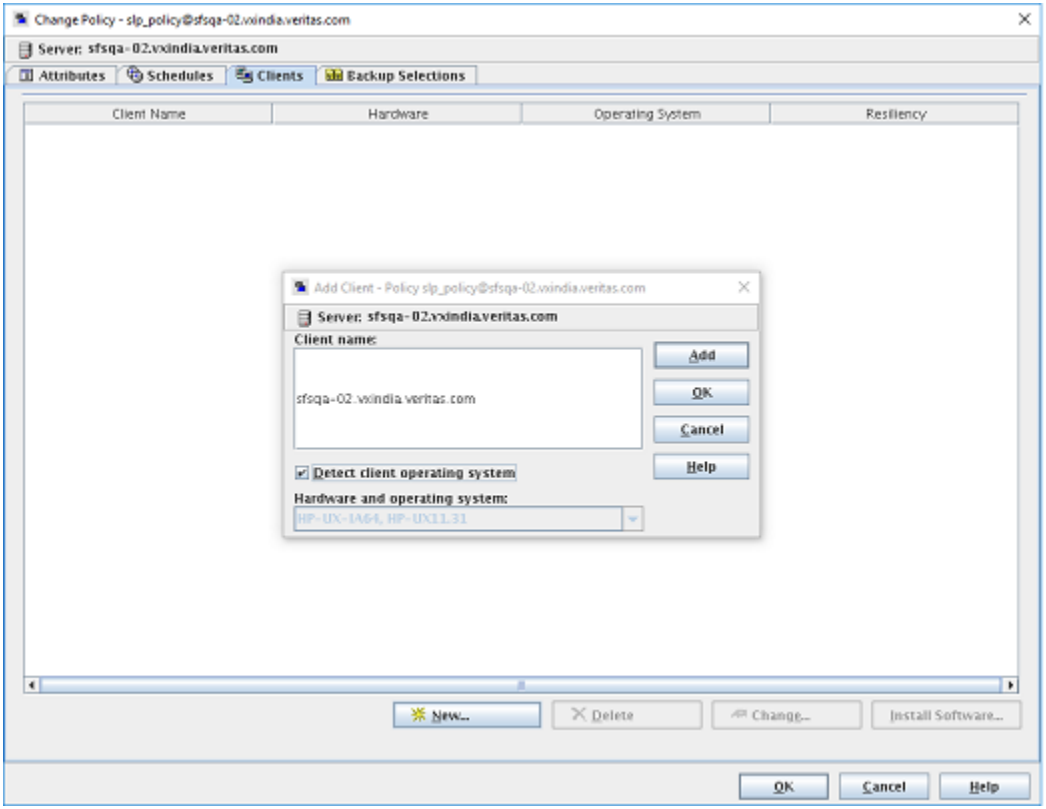


4 Enter the attribute information as per your requirement.

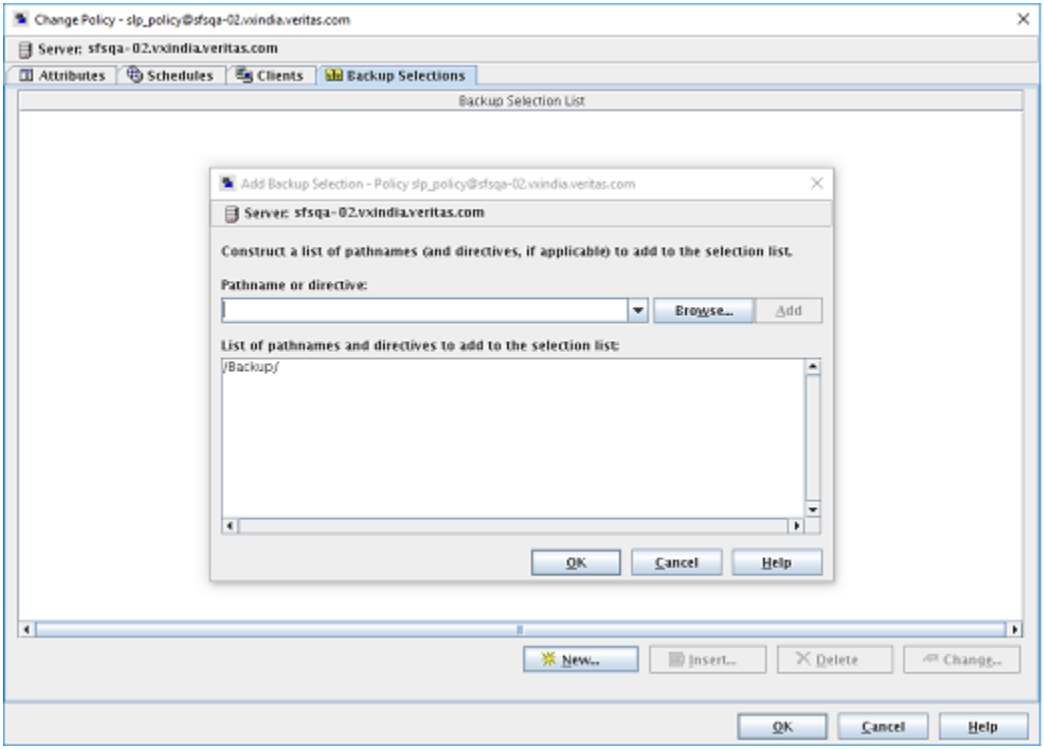


5 Under the **Schedule** tab, enter the name of the schedule. For example, **fullbackup**.

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



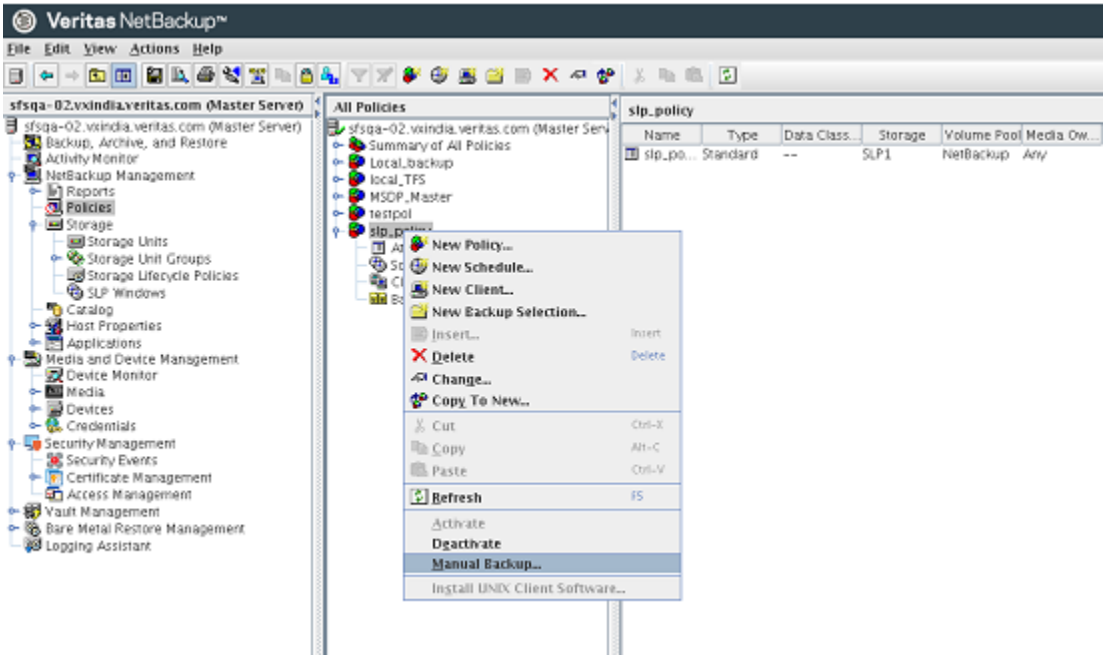
7 Select the folders that need to be backed up under **Backup Selections**.



Running a backup policy manually

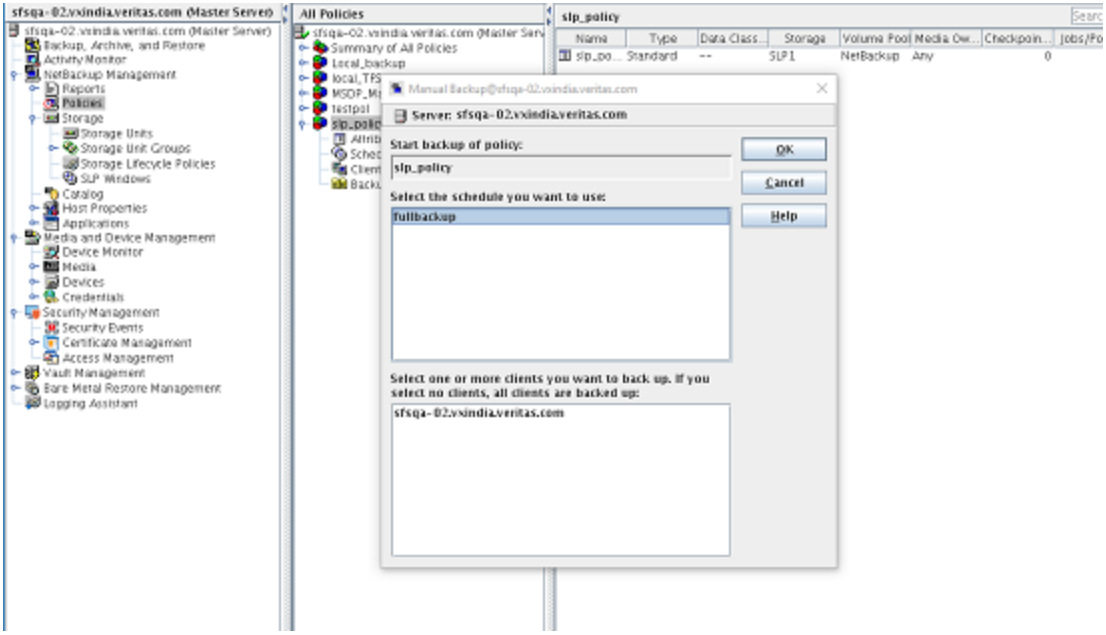
To run a backup policy manually

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**.

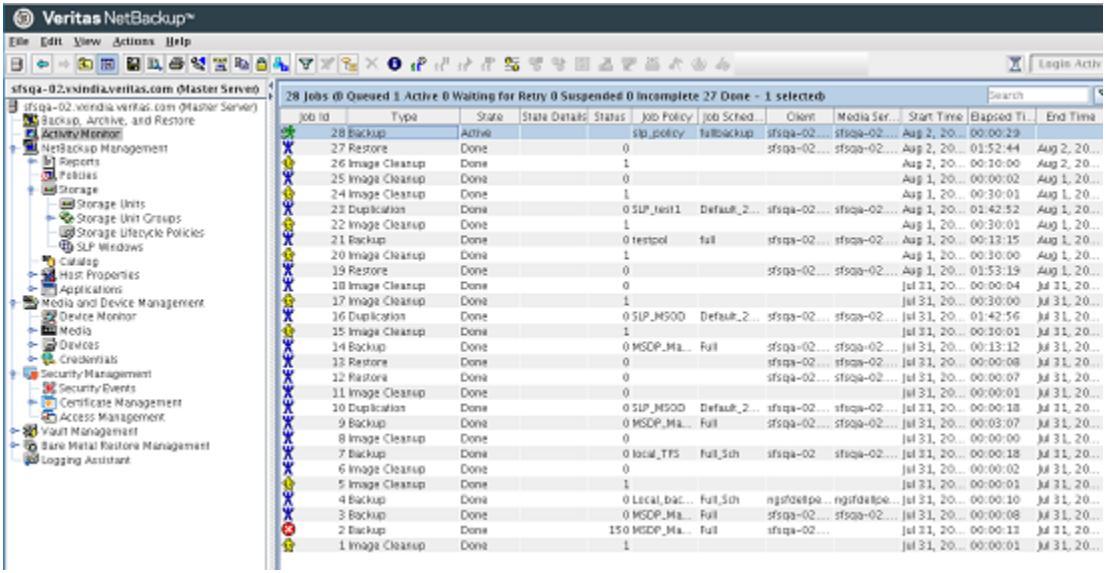


2 Select the schedule that you want to use and click **OK**.

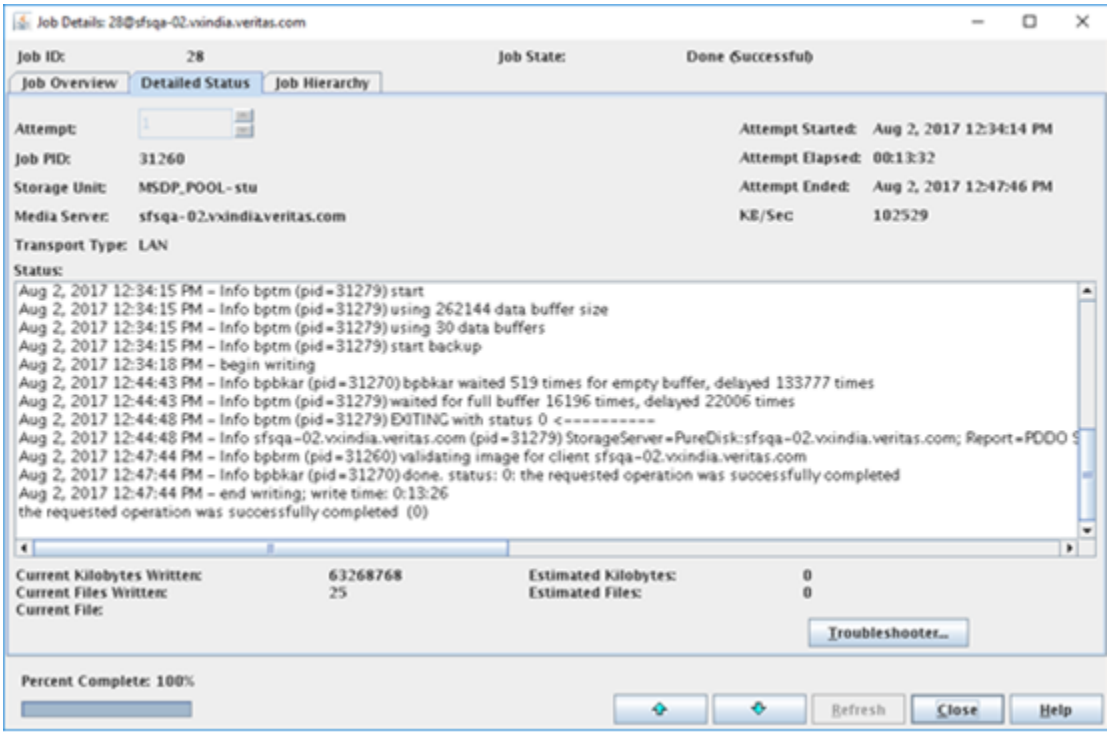
This starts the manual backup with the policy.



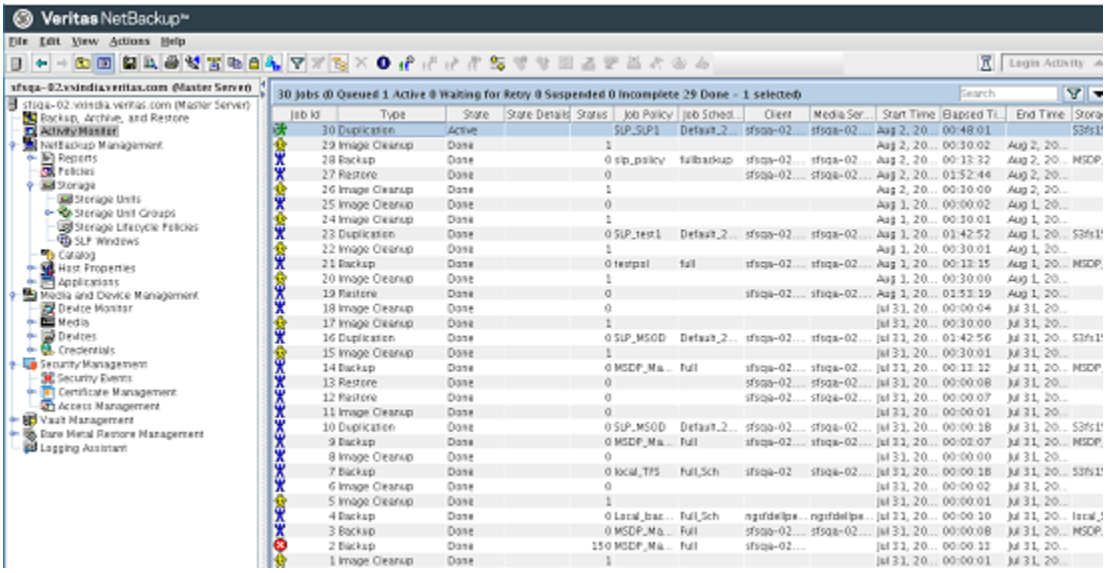
3 To verify the status of the backup, go to **Activity Monitor**.



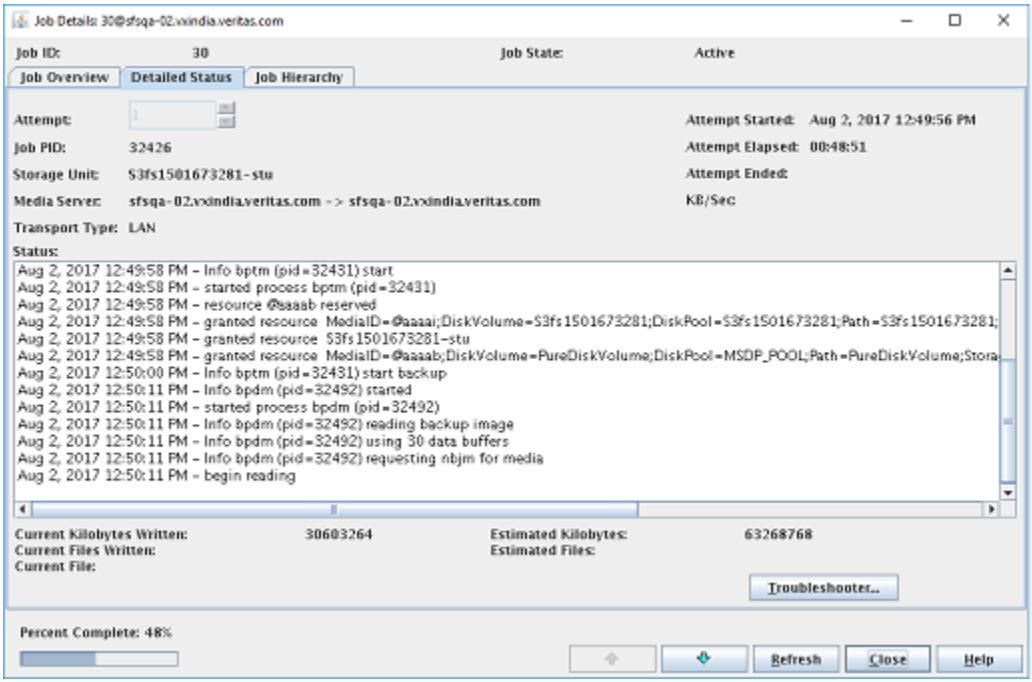
4 Select the appropriate job from the displayed jobs and click on the **Detailed status** tab in the new window to check on the status of the backup.



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



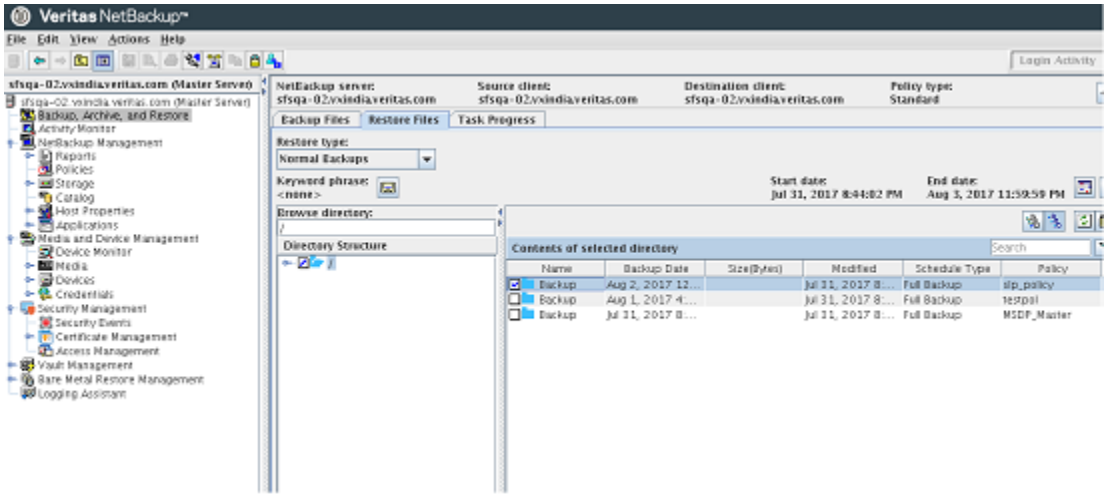
6 Click on that job and then select detailed status to check the status of the duplication job.



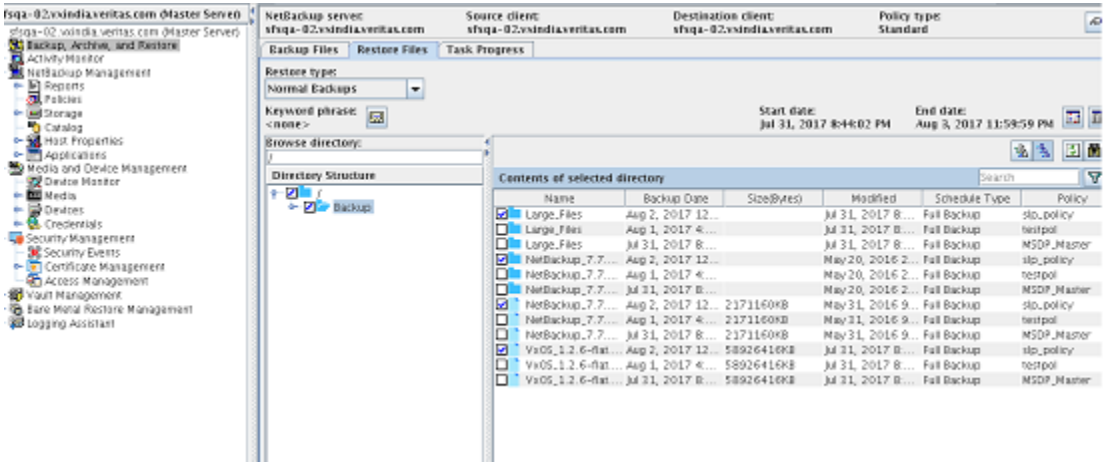
Restoring backed up files

To restore backed up files

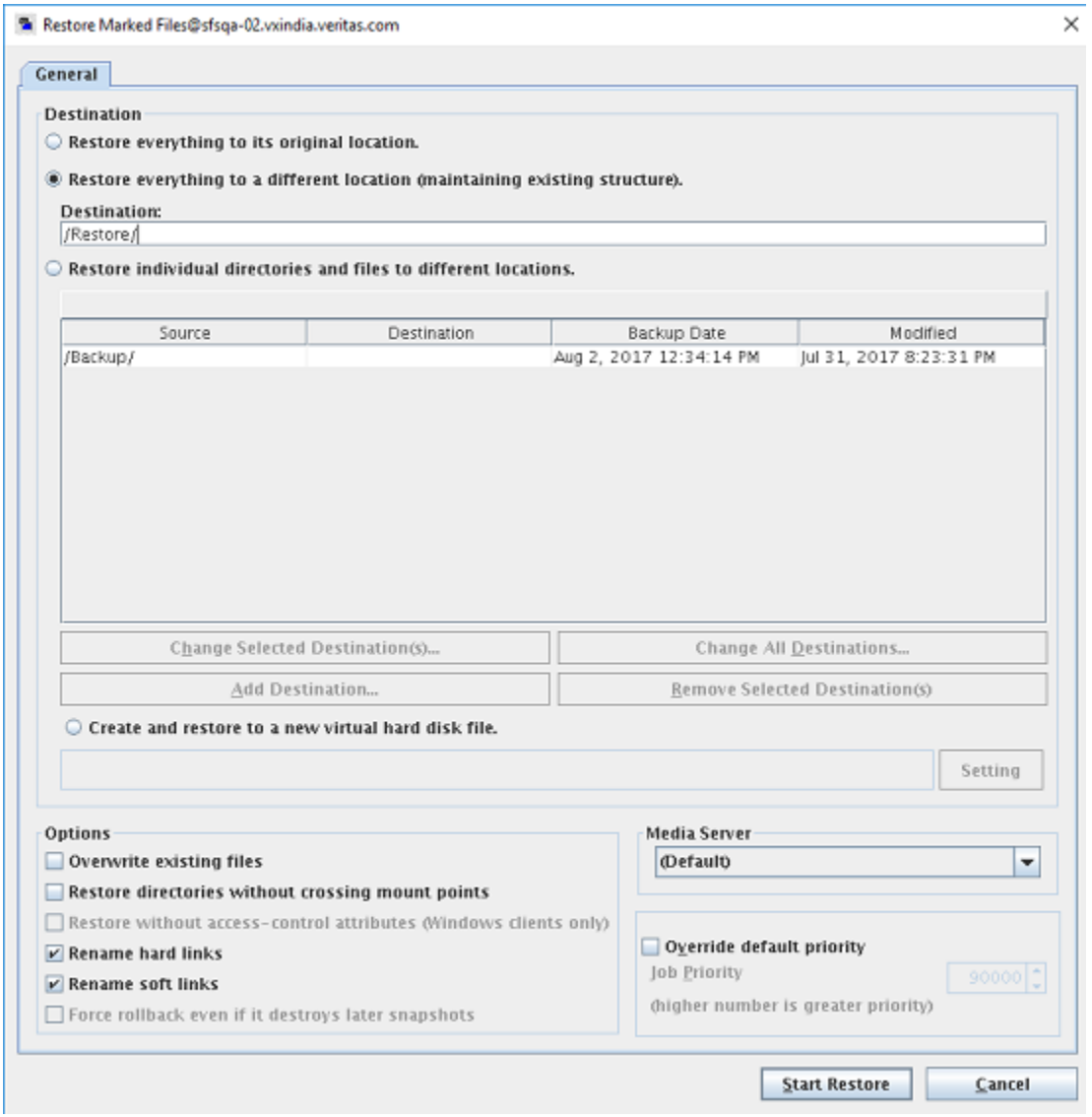
1. Create a directory where you want to restore the backed-up files.
2. Go to the **Restore Files** tab under **Backup, Archive, Restore**.



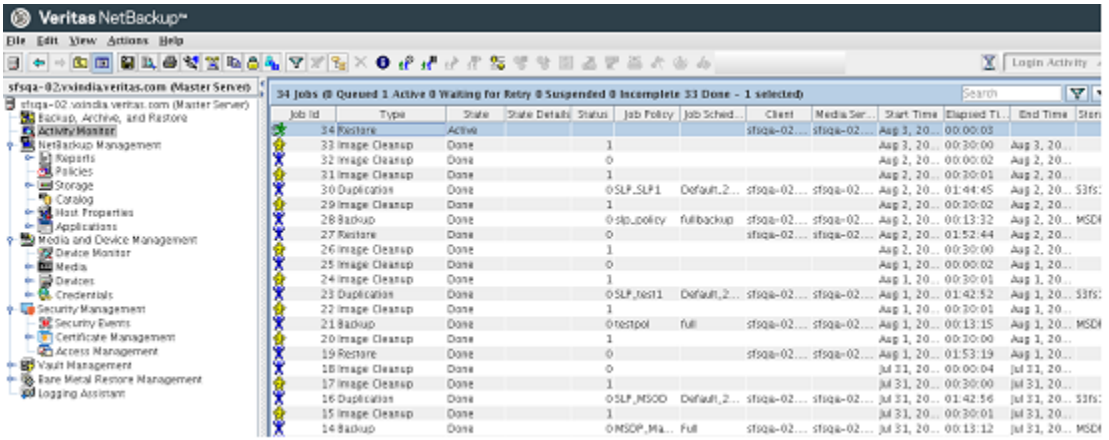
3. Go to the browse directory and select the appropriate files to restore and click **Restore**. The backup to be restored can reside either on NetBackup or on Veritas Access depending on the **Storage Lifecycle Policy** that is set. Hence, the restore location changes accordingly.



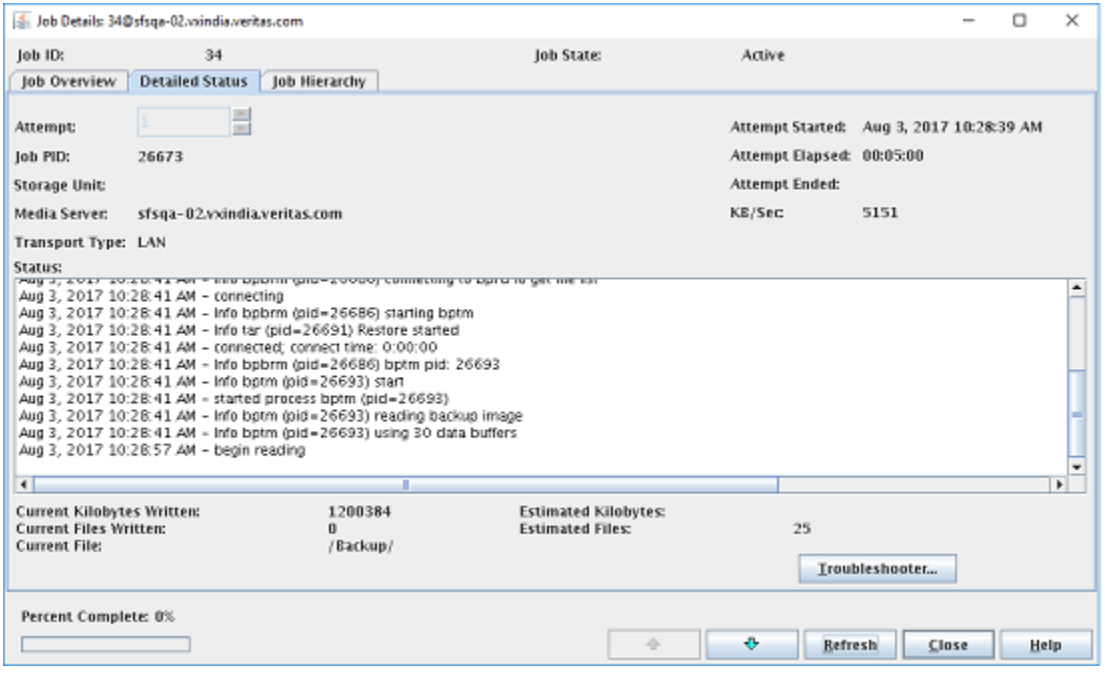
4 Enter the location where the files should be restored, and click on the **Start Restore** button.



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.



Chapter 5

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:

   ```
   # opendedup vol 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 7
    Veritas Access 6
additional resources
    documentation 66

B

backup and restore 49
backup storage for NetBackup 7

C

configuring
    Veritas Access SSL with NetBackup 40
configuring Veritas Access as a cloud storage server 23
creating
    Storage Lifecycle Policies 43
Creating a Media Server Deduplication Pool
    primary backup using NetBackup 15
creating a MSDP
    primary backup using NetBackup 15
creating S3 bucket
    storing deduplicated backup data 13

G

generating Veritas Access S3 server keys
    using the helper script 67

I

integration with Veritas Access
    NetBackup 6

L

log locations
    troubleshooting 66

N

NetBackup
    integration with Veritas Access 6

P

policy creation 49

R

restoring backup files 62
running a backup policy
    manually 56

S

SDFS volume
    unmounting before rebooting Veritas Access 65
Storage Lifecycle Policies
    creating 43
supported configurations and versions
    NetBackup with CloudCatalyst 11
system requirements
    supported configurations and versions for NetBackup with CloudCatalyst 11

T

troubleshooting
    log locations 66

U

unmounting
    SDFS volume before rebooting Veritas Access 65
use case
    long-term data retention 8
using the helper script
    generating Veritas Access S3 server keys 67
using Veritas Access with NetBackup and CloudCatalyst
    benefits 12