

Veritas Access Appliance 8.0 Solutions Guide for NetBackup

Access Appliance Solutions Guide for NetBackup

Last updated: 2024-05-30

Legal Notice

Copyright © 2024 Veritas Technologies LLC. All rights reserved.

Veritas, the Veritas Logo, 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/about/legal/license-agreements>

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
2625 Augustine Drive
Santa Clara, CA 95054

<https://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 latest documentation is available on the Veritas website:

https://www.veritas.com/content/support/en_US/dpp.Appliances.html

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:

APPL.docs@veritas.com

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

<https://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	Access Appliance integration with NetBackup	
		7
	About Access Appliance as a NetBackup client	7
	About Access Appliance as backup storage for NetBackup	8
	Use cases for long-term data retention	8
Chapter 2	System requirements	11
	Supported configurations and versions for NetBackup with Veritas	
	Data Deduplication	11
	Supported configurations and versions for NetBackup with MSDP-C	
		12
Chapter 3	Configuring Veritas Data Deduplication with	
	Access Appliance	13
	About Veritas Data Deduplication	14
	Benefits of using Veritas Data Deduplication with Access Appliance	
		14
	Configuring Veritas Data Deduplication without WORM	15
	Configuring Veritas Data Deduplication using the GUI	15
	Configuring Veritas Data Deduplication using the Access CLISH	
		19
	Configuring Veritas Data Deduplication with WORM	21
	Configuring Veritas Data Deduplication with WORM using GUI	
		22
	Configuring Veritas Data Deduplication with WORM using the	
	Access CLISH	24
	Managing Veritas Data Deduplication using the Access CLISH	27
	Managing Veritas Data Deduplication using GUI	31
	Unconfiguring Veritas Data Deduplication	31
	Adding secondary IP for Veritas Data Deduplication	32
	Deleting secondary IP for Veritas Data Deduplication	32
	Accessing Access Appliance WORM storage shell for management	
	tasks	33
	About the Access Appliance WORM storage server shell	33

	Support for multiple domains across networks for Veritas Data Deduplication	52
	Veritas Data Deduplication storage layout	57
	Configuring a Veritas Data Deduplication storage unit on NetBackup	58
	Configuring global deduplication using the Veritas Data Deduplication storage server across the domain	70
	Enabling Veritas Data Deduplication encryption	70
	Support for bandwidth throttling during duplication	72
	Support for NetBackup Auto Image Replication	72
	Separating the duplication and replication network	88
Chapter 4	Configuring MSDP-C with Access Appliance	92
	Starting the Access S3 server and provisioning the S3 bucket	92
	Configuring Access S3 bucket with NetBackup MSDP-C	97
Chapter 5	Migrating the NetBackup images from existing storage to Veritas Access storage	111
	Migrating NetBackup images from CloudCatalyst/S3/MSDP-C to Veritas Data Deduplication storage	111
	Migrating the NetBackup images from the Veritas Data Deduplication STU to the MSDP-C STU	115
Chapter 6	Configuring Access Appliance with the NetBackup client	116
	Configuring Access Appliance for NetBackup client	117
	Installing the NetBackup client add-on packages	118
	Prerequisites for configuring the NetBackup client	120
	Configuring the NetBackup client	120
	Adding an optional media server	121
	Adding multiple primary servers	122
	Adding file systems to the backup configuration	123
	Removing file systems from backup configuration	123
	Changing the virtual IP address used by the NetBackup client	124
	Upgrade the NetBackup client	124
	Unconfiguring the NetBackup client	125
	Enabling Veritas Data Deduplication catalog backup with NetBackup client	125
	Disabling Veritas Data Deduplication catalog backup from NetBackup client	128
	Displaying the status of NetBackup services	129

	Configuring backup operations using NetBackup or other third-party backup applications	130
	Restoring filesystems backed up with NetBackup client	130
Chapter 7	Troubleshooting	132
	Additional resources	132
	Generating Access Appliance S3 server keys using the helper script	132
Index		134

Access Appliance integration with NetBackup

This chapter includes the following topics:

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

About Access Appliance as a NetBackup client

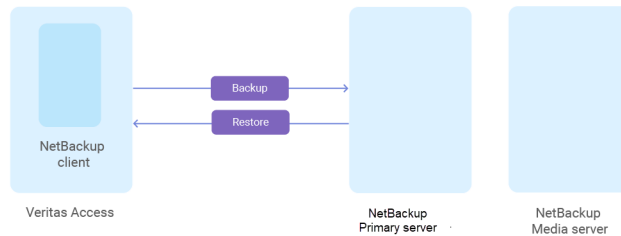
Access Appliance is integrated with Veritas NetBackup so that a NetBackup administrator can back up your Access Appliance file systems to NetBackup primary or media servers and retain the data as per your company policy. Once data is backed up, a storage administrator can delete unwanted data from Access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

You can configure NetBackup domain information using the command-line interface (CLI)

The Veritas Access command-line interface has a dedicated `Backup>` menu. From the `Backup>` menu, register the NetBackup client with the NetBackup domain. Information is saved in the `bp.conf` file.

See [“Configuring Access Appliance for NetBackup client”](#) on page 117.

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 Access Appliance.

Figure 1-1 Backing up Access Appliance using NetBackup

About Access Appliance as backup storage for NetBackup

This document describes how Access Appliance 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.

Access Appliance is based on the rock-solid and industry-proven Veritas CFS stack. It offers an AWS-compatible S3 protocol as object storage for NetBackup. Access Appliance also provides deduplication storage for NetBackup by using the NetBackup MSDP.

Use cases for long-term data retention

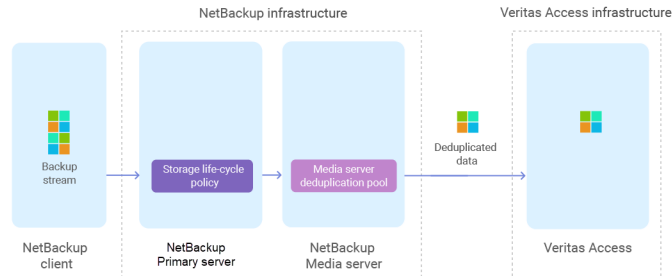
The following are the use cases for long-term data retention (LTR) using Access Appliance:

Use Case: Access Appliance with Veritas Data Deduplication

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

- Veritas Data Deduplication can also act as a source or destination while replicating deduplicated data using Auto Image Replication (AIR).

Figure 1-2 Access Appliance Veritas Data Deduplication with NetBackup

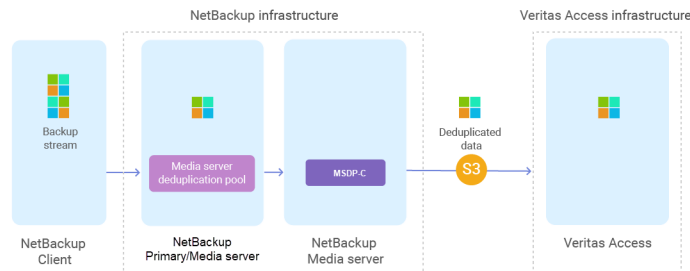


Use Case: Access Appliance with MSDP-C

- MSDP deduplicates the primary backup data and stores it on the NetBackup server.
- The same deduplicated data is moved to Access Appliance through SLP using MSDP-C.

See [“Configuring Access S3 bucket with NetBackup MSDP-C”](#) on page 97.

Figure 1-3 NetBackup MSDP-C over Access Appliance Object Access protocol (S3)



Note: If you want to use 2.4 PiB of storage, configure Veritas Data Deduplication with 1.2 PiB storage and configure MSDP-C with two buckets of size 600 TB each. Use the virtual IP of one node for Veritas Data Deduplication and use the virtual IP of another node for MSDP-C.

Note: Veritas does not support a deduplication pool of size greater than 1.2 PiB.

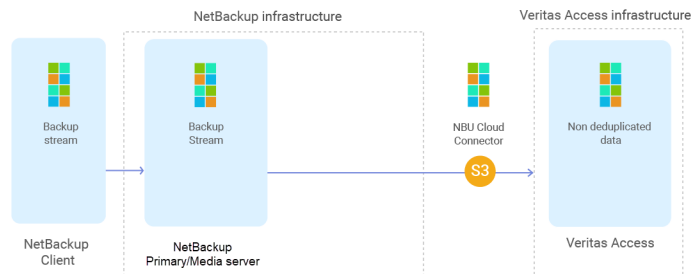
Use Case: Access Appliance as an S3 connector

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

Or

- MSDP duplicates the primary backup data and stores it on the NetBackup server.
- The deduplicated data is rehydrated and then moved to Access Appliance through SLP over the Access Appliance S3 protocol.

Figure 1-4 Backup data stored in non-deduplicated format on the NetBackup server as primary backup and the same backup data duplicates to Access Appliance over Access S3 protocol.



Note: Configurations and use cases beyond storing copies for long term retention periods require a Support Exception. Please contact your Veritas representative for details on the Support Exception approval process.

System requirements

This chapter includes the following topics:

- [Supported configurations and versions for NetBackup with Veritas Data Deduplication](#)
- [Supported configurations and versions for NetBackup with MSDP-C](#)

Supported configurations and versions for NetBackup with Veritas Data Deduplication

Table 2-1 Supported versions of NetBackup for Veritas Data Deduplication without WORM

Access Appliance	Veritas NetBackup primary servers	Veritas NetBackup media servers
8.0	8.3.x.x, 9.0.x.x, 9.1.x.x, 10.0.x.x and later versions	8.3.x.x, 9.0.x.x, 9.1.x.x, 10.0.x.x and later versions

Note: The version of the media server should be the same as or lower than the version of the primary server.

Table 2-2 Supported versions of NetBackup for Veritas Data Deduplication with WORM

Access Appliance	Veritas NetBackup primary servers	Veritas NetBackup media servers
8.0	10.0.x.x and later versions	10.0.x.x and later versions

Supported configurations and versions for NetBackup with MSDP-C

Table 2-3 Supported versions of NetBackup for MSDP-C without WORM

Access Appliance	Veritas NetBackup servers
8.0	9.0 and later versions

Table 2-4 Supported versions of NetBackup for MSDP-C with WORM

Access Appliance	Veritas NetBackup servers
8.0	10.0 and later versions

Configuring Veritas Data Deduplication with Access Appliance

This chapter includes the following topics:

- [About Veritas Data Deduplication](#)
- [Benefits of using Veritas Data Deduplication with Access Appliance](#)
- [Configuring Veritas Data Deduplication without WORM](#)
- [Configuring Veritas Data Deduplication with WORM](#)
- [Managing Veritas Data Deduplication using the Access CLISH](#)
- [Managing Veritas Data Deduplication using GUI](#)
- [Accessing Access Appliance WORM storage shell for management tasks](#)
- [Support for multiple domains across networks for Veritas Data Deduplication](#)
- [Veritas Data Deduplication storage layout](#)
- [Configuring a Veritas Data Deduplication storage unit on NetBackup](#)
- [Configuring global deduplication using the Veritas Data Deduplication storage server across the domain](#)
- [Enabling Veritas Data Deduplication encryption](#)
- [Support for bandwidth throttling during duplication](#)
- [Support for NetBackup Auto Image Replication](#)

About Veritas Data Deduplication

Access Appliance is integrated with a duplication engine which is based on Media Server Deduplication Pool (MSDP) technology for storing backup data. The storage server component of Veritas Data Deduplication runs on the Access Appliance nodes with high availability in active/passive mode. The deduplication plug-in of the NetBackup media server does segmentation and finger printing of the backup data and sends the deduplicated data to Access Appliance. The Veritas Data Deduplication storage server stores and manages the deduplicated data. The deduplication storage server provides high availability to protect against storage, node, and network failures. It supports client direct as well as media server deduplication configurations.

Considerations before configuring Veritas Data Deduplication:

- All storage that is provisioned for Veritas Data Deduplication is displayed as a single storage pool on NetBackup.
- Access Appliance supports only a single storage pool for Veritas Data Deduplication and it requires minimum (or multiple) of five disks in the storage pool.

Benefits of using Veritas Data Deduplication with Access Appliance

- Capability of writing the deduplicated data from the media server to Access Appliance.
- Support global deduplication across media servers within the same domain and across different NetBackup domains.
- The storage server components reside directly on the Access Appliance nodes with high availability in active/passive mode to protect against storage, node, and network failures.
- Includes WORM storage that provides immutable and indelible data protection, ensuring data cannot be changed for a determined length of time to protect data against cyber criminal intrusion and internal threats.
- All software meet stringent security standards and are Federal information Processing Standard (FIPS) 140-2-compliant.

Configuring Veritas Data Deduplication without WORM

You can configure Veritas Data Deduplication without WORM using the Access Appliance GUI as well as command-line interface. Veritas recommends that you configure Veritas Data Deduplication using the GUI as it ensures that the configuration is performed with the appropriate filesystem size, and volume layout along with catalog filesystem creation.

You can configure Veritas Data Deduplication without WORM when the lockdown mode is Normal, Enterprise or Compliance.

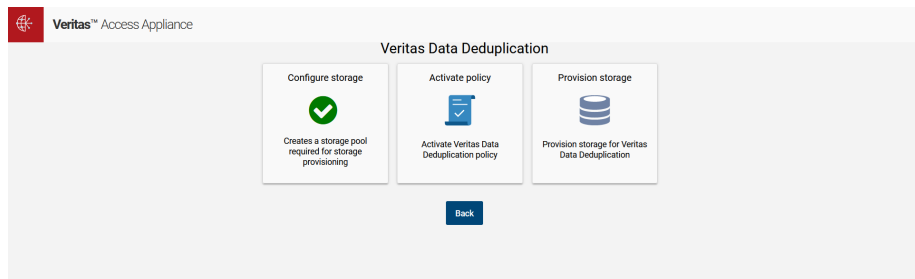
For more information, see the *About lockdown modes* section in the *Access Appliance Administrator's Guide*.

Configuring Veritas Data Deduplication using the GUI

This section describes how you can configure Veritas Data Deduplication using the Access Appliance GUI.

To configure Veritas Data Deduplication

- 1 Log on to the **Access Appliance** application.
 - The **Getting Started** page is displayed when you login for the first time. Click **Veritas Data Deduplication**.
 - Or, navigate to **Quick Actions > Provision Storage > Storage for NetBackup > Veritas Data Deduplication**.
 - Or, navigate to **Settings > Veritas Data Deduplication Management**.
- 2 A default storage pool is created at the time of initial configuration with all the available disks.



- 3 Under the **Activate Policy** tab, select the Veritas Data Deduplication policy.

 Veritas™ Access Appliance

Veritas Data Deduplication

Configure storage

Activate policy

Provision storage

Select and activate the policy for storage provisioning. ✕

Complete prerequisites

Policy name	Description	Capabilities	Prerequisite
☐ Veritas Data Deduplication	This policy provisions storage for Veritas Data Deduplicati...	Fault Tolerance	✓ Storage pool created
☐ Veritas Data Deduplication (WORM)	This policy provisions storage for Veritas Data Deduplicati...	Fault Tolerance,WORM	✓ Storage pool created ✕ Enterprise/Compliance mode configured

Items per page: 5 1 - 2 of 2 < > >|

Activate policy

- 4 Complete all the prerequisites such as, selecting the storage pool to activate the Veritas Data Deduplication policy and click **Activate policy**.

Veritas™ Access Appliance

Veritas Data Deduplication

Configure storage Activate policy Provision storage

Complete following prerequisite to activate Veritas Data Deduplication

Select storage pool : Selected storage pools:1, total size:297.05 GB

☒	Storage pool	Total size	Available size
☒	pool_default	300.00 GB	297.05 GB

Items per page: 5 1 - 1 of 1

Activate policy

After the policy is activated, click **Finish**.

5 Under the **Provision storage** tab, specify all the required fields.

Select storage policy	From the dropdown menu, choose <code>Veritas Data Deduplication policy</code> .
Storage size	Mention the capacity for Veritas Data Deduplication storage (size should be less than 1.2 PiB)
Select storage pool	Specify the name of the storage pool.
Username	Specify the username to be used
Password/Confirm Password:	Enter the password for the above username
VIP (Virtual IP address)	Specify a free virtual IP from the cluster (this IP should not be used by any protocol on the cluster) You can check if an IP is used by CIFS using the <code>cifs share show <sharename></code> command. Run the <code>network ip addr show</code> command from the Access command-line interface to find an available virtual IP address. Or navigate to Infrastructure > Nodes in the GUI, and click on the node name to see the virtual IP address. If a virtual IP is not available to configure the Veritas Data Deduplication server, you should add at least one virtual IP to the cluster using the Access command-line interface.

The screenshot shows the 'Veritas Data Deduplication' configuration page in the Veritas Access Appliance GUI. At the top, there are three tabs: 'Configure storage' (active), 'Activate policy', and 'Provision storage'. Below the tabs, the 'Provision storage' section is expanded, showing the following fields:

- Select storage policy:** A dropdown menu with 'Veritas Data Deduplication' selected.
- Specify storage requirements:**
 - Storage size:** A field with a value of '100' and a unit selector set to 'GB'.
 - Select storage pool:** A dropdown menu with 'pool_default' selected.
- Configure Veritas Data Deduplication:** A section with the instruction 'Set up credentials to communicate to the Veritas NetBackup deduplication engine.' containing:
 - Username:** A text field with the value 'testuser'.
 - Password:** A password field with masked characters.
 - Confirm password:** A password field with masked characters.
- VIP (Virtual IP Address):** A text field with the value '192.168.10.12'.

At the bottom right of the form, there is a blue button labeled 'Provision storage'.

Click **Provision storage**.

View the **Recent Activity** panel for the status of the task.

The storage provisioning is now complete.

An alert appears in the GUI when the memory usage of the Veritas Data Deduplication server is more than 75%. The alert displays the amount of memory used and the total RAM usage. If the situation persists for more than 24 hours, an AutoSupport alert is raised and an email is sent.

If you receive this alert, go to **Settings > Veritas Data Deduplication management** and restart the service once you reach this threshold. For information about the issues that are caused when the Veritas Data Deduplication service consumes large amount of memory, see

https://www.veritas.com/support/en_US/article.100045745.

Configuring Veritas Data Deduplication using the Access CLISH

This section describes how you can configure Veritas Data Deduplication without WORM using the Access Appliance command-line interface.

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

Prerequisites:

- The filesystem should be striped and should be already created with size not exceeding 100 TiB and the IP should be online before you start configuring Veritas Data Deduplication.
- If the total deduplication pool size required is larger than 100 TiB, then create multiple data filesystems.
- The total data filesystem size should not exceed 1.2 PiB.
- The data filesystems are used to store the deduplicated data and its metadata.
- You are required to create a separate catalog file system to store the Veritas Data Deduplication catalog. The minimum size of the catalog file system should be 5 TiB.
- The deduplication storage server uses the specified IP address to receive the backup data from NetBackup.

To configure the deduplication storage server

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

```
dedupe> config filesystem1[,filesystem2,...] IP username
[catfs_name] [worm=no] [minret] [maxret]
```

Where:

<i>filesystem1,</i> <i>filesystem2,...</i>	Specifies the data filesystem names.
<i>IP</i>	Specifies the interface IP. You can check for the IP using the <code>network IP address show</code> command.
<i>username</i>	Specifies the username.
<i>catfs_name</i>	Specifies the catalog filesystem of the deduplication server.
<i>worm</i>	Enables WORM. The possible values are <code>enable_worm=yes/enable_worm=no</code> . This is an optional parameter.
<i>minret</i>	Specifies the minimum image retention period. This is an optional parameter.
<i>maxret</i>	Specifies the maximum image retention period. This is an optional parameter.

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

Note: Make a note of the password that you use. You have to use the same password when you configure the storage server on NetBackup and also when you reconfigure Veritas Data Deduplication.

Note: Configuring Veritas Data Deduplication requires an FQDN entry which resolves to a specific IP. You can either have a DNS entry or you can add an entry in the `/etc/hosts` file of both the NetBackup media and primary servers on all the nodes to resolve the FQDN to a specific IP.

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

Note: If you have to reconfigure deduplication, you have to pass all the filesystems in the same order that is displayed in the output of the `dedupe show` command before deduplication was unconfigured.

You must use the same username and password that you used when you initially configured deduplication.

If a new IP is used for the deduplication server during reconfiguration, the new IP should map to the old FQDN. You can either have a DNS entry or add an entry in the `/etc/hosts` file on all the nodes to resolve the FQDN to a specific IP.

Configuring Veritas Data Deduplication with WORM

You can configure Veritas Data Deduplication with WORM using both the Access Appliance GUI and command-line interface. Veritas recommends that you configure Veritas Data Deduplication using the GUI as it ensures that the configuration is performed with the appropriate filesystem size, and volume layout along with catalog filesystem creation.

You can configure Veritas Data Deduplication with WORM when the lockdown mode is Enterprise or Compliance.

For more information, see the *About lockdown modes* section in the *Access Appliance Administrator's Guide*.

Only a single Veritas Data Deduplication pool is supported on Access Appliance. Veritas does not support converting an existing Veritas Data Deduplication pool (without WORM) to a Veritas Data Deduplication pool with WORM.

If you want to use the same appliance to configure a Veritas Data Deduplication pool with WORM, you must do the following:

- Duplicate the data to another storage unit.
- Expire all images from the Access Appliance deduplication pool.
- Unconfigure and destroy the file systems.

You cannot convert non-WORM images to WORM images directly. But it is possible to convert the images using other methods. For example, you can provision an MSDP-C instance using Access appliance if there is enough space to store a copy of the data present in Veritas Data Deduplication. You can also provision another Access Appliance with Veritas Data Deduplication and duplicate all images onto it. After duplicating the images to another storage unit, you can expire the images from Veritas Data Deduplication and unconfigure it. Then, you can proceed to configure Veritas Data Deduplication in WORM mode and duplicate the data back to the Access Appliance with WORM protection. After the configuration, the server is WORM-enabled but the existing images are not WORM-enabled.

Configuring Veritas Data Deduplication with WORM using GUI

This section describes how you can configure Veritas Data Deduplication with WORM using the Access Appliance GUI.

To configure Veritas Data Deduplication

- 1 Log on to the Access Appliance application.

Select the **Quick Actions** icon present on the dashboard page, and navigate to **Provision Storage > Storage for NetBackup > Veritas Data Deduplication**. Click **Next**. You have to use this option if any instance of Veritas Data Deduplication is already present on the cluster.

Or, navigate to **Settings > Veritas Data Deduplication Management**. Click **Configure**. This option is available only if no Veritas Data Deduplication instances are present on the cluster.

If you want to configure lockdown mode, refer to the *About lockdown modes* section in the *Access Appliance Administrator's Guide*.

- 2 Under the **Activate Policy** tab, enter the required details to activate the policy. Specify the maximum and minimum retention period. The retention period range is between 1 hour and 60 years.

Veritas Access Appliance

Veritas Data Deduplication

Configure storage | **Activate policy** | Provision storage

Complete following prerequisite to activate Veritas Data Deduplication (WORM)

Select storage pool: Selected storage pools (0), total size 0

Set WORM

Configure the retention time range that Appliance Administrators will be allowed to select from when setting WORM retention time. The minimum retention time you can set is 1 hour and the maximum is 60 years.

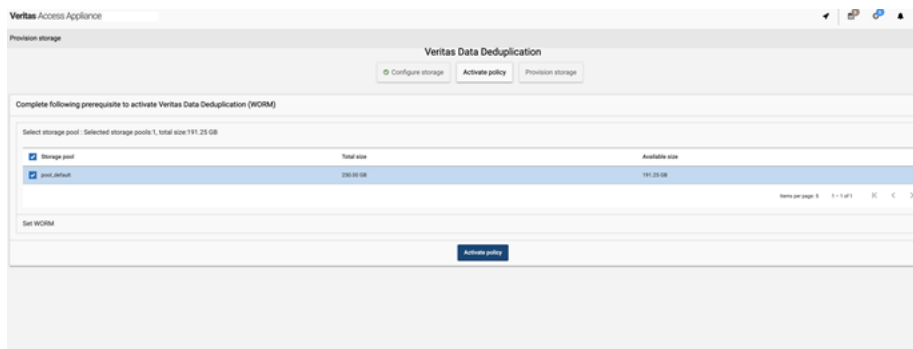
Minimum retention time: 1h

Maximum retention time: 1h, 1h

Days
Hours
Months
Years

Activate policy

3 Select the storage pools and click **Activate policy**.



The Veritas Data Deduplication policy is activated.

- 4** In the **Provision storage** page, select the Veritas Data Deduplication (WORM) policy and specify the storage requirements. Enter the required information.

Select storage policy	From the dropdown menu, choose the relevant Veritas Data Deduplication policy (WORM)
Storage size	Mention the capacity for Veritas Data Deduplication storage (size should be less than 1.2 PiB)
Username	Specify the username to be used
Password/Confirm Password:	Enter the password for the above username
VIP (Virtual IP address)	Specify a free virtual IP from the cluster (this IP should not be used by any protocol on the cluster). You can find this IP using the <code>network IP address</code> command.

Click **Provision storage**.

The screenshot shows the 'Provision storage' page in the Veritas Access Appliance interface. The page has a header with 'Veritas Access Appliance' and a sub-header 'Veritas Data Deduplication'. Below the sub-header are three tabs: 'Configure storage', 'Activate policy', and 'Provision storage'. The 'Provision storage' tab is active. The page contains several form fields: 'Select storage policy' (dropdown menu showing 'Veritas Data Deduplication (WORM)'), 'Storage size' (input field with '50' and a unit dropdown set to 'GB'), 'Select storage pool' (dropdown menu showing 'pool default'), 'Name' (input field with 'admin'), 'Password' (input field with a strength indicator), 'Confirm password' (input field with a strength indicator), and 'VIP (Virtual IP Address)' (input field with '10.22.51.88'). A blue 'Provision storage' button is located at the bottom right of the form.

View the **Recent Activity** panel for the status of the task.

Configuring Veritas Data Deduplication with WORM using the Access CLISH

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

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

Prerequisites:

- The filesystem should be striped and should be already created with size not exceeding 100 TiB and the IP should be online before you start configuring Veritas Data Deduplication.
- If the total deduplication pool size required is larger than 100 TiB, then create multiple data filesystems.
- The total data filesystem size should not exceed 1.2 PiB.
- The data filesystems are used to store the deduplicated data and its metadata.
- You are required to create a separate catalog file system to store the Veritas Data Deduplication catalog. The minimum size of the catalog file system should be 5 TiB.
- The deduplication storage server uses the specified IP address to receive the backup data from NetBackup.
- The lockdown mode should be enterprise or compliance.

To configure the deduplication storage server with WORM

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

```
dedupe> config filesystem1[,filesystem2,...] IP username
catfs_name [enable_worm=yes] [minret] [maxret]
```

Where:

<i>filesystem1, filesystem2,...</i>	Specifies the data filesystem names.
<i>IP</i>	Specifies the interface IP.
<i>username</i>	Specifies the user name.
<i>catfs_name</i>	Specifies the catalog file system of the deduplication server.
<i>worm</i>	Enables WORM. The possible values are <code>enable_worm=yes/enable_worm=no</code> .
<i>minret</i>	Specifies the minimum image retention period in seconds. It can contain: [1-9](s S). The minimum value is 3600s.
<i>maxret</i>	Specifies the maximum image retention period in seconds. It can contain: [1-9](s S). The maximum value is 1892160000s.

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

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

Note: Configuring Veritas Data Deduplication requires a FQDN entry which resolves to a specific IP. You can either have a DNS entry or you can add an entry in the `/etc/hosts` file on all the nodes to resolve the FQDN to a specific IP.

If the FQDN entry is not found, a random string is used as a FQDN entry during configuration.

Note: If you have to reconfigure deduplication, you have to pass all the file systems in the same order that is displayed in the output of the `dedupe show` command.

You must use the same user name and password that you used when you initially configured deduplication.

If a new IP is used for the deduplication server during reconfiguration, the new IP should map to the old FQDN. You can either have a DNS entry or add an entry in the `/etc/hosts` file on all the nodes to resolve the FQDN to a specific IP.

The default size of the stripe unit of the deduplication file system created is 64K. As a result of the creation of catalog file system and VxFS and VDD optimizations, performance improvements can be seen in optimized duplication and restore.

Managing Veritas Data Deduplication using the Access CLISH

This section describes the various operations that you can perform on the deduplication server using the Access CLISH.

To change the user password

- ◆ You can change the password of the deduplication server user.

To change the password, enter the following:

```
Dedupe> passwd user_name
```

You are prompted to enter your current password and the new password. After you confirm the new password, the password gets updated.

Note:

- If the user is not present on NetBackup, you have to add the user on the NetBackup server.

```
# /usr/openv/pdde/pdcr/bin/spauser -a -u user_name
```

- You also must update the password on NetBackup if you have updated the password for the Veritas Data Deduplication server from Access Appliance.

```
# /usr/openv/volmgr/bin/tpconfig -update -stype PureDisk  
-storage_server IP address -sts_user_id user_name
```

To start the deduplication storage server

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

To start the deduplication storage server, enter the following:

```
Dedupe> start
```

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

To display information the deduplication storage server

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

```
Dedupe> show
```

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

To display the deduplication storage server statistics

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

```
Dedupe> stats
```

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

To show the status of the deduplication storage server

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

```
Dedupe> status
```

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

To stop the deduplication storage server

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

```
Dedupe> stop
```

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

To increase the storage capacity of the deduplication storage server

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

```
Dedupe> grow size
```

The deduplication storage server should be online for this operation.

Note: The shrink operation is not supported. You cannot shrink the size of the deduplication storage server pool after configuration.

To add a new user to the deduplication storage server

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

```
Dedupe> adduser username
```

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

To show the list of users of the deduplication storage server

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

```
Dedupe> listuser
```

To unconfigure the deduplication storage server

Ensure that you make a note of the following configuration details before you unconfigure the Veritas Data Deduplication server. These details are required when you reconfigure the service.

- The virtual IP that you used to configure the Veritas Data Deduplication serve.
- Credentials to access the Veritas Data Deduplication server
- ◆ To unconfigure the deduplication storage server, enter the following:

```
Dedupe> unconfig destroy_fs=yes/no
```

The *destroy_fs* is an optional parameter with default value set to *no*.

If *destroy_fs=no*, the file systems that are used in the deduplication configuration (both data and catalog file systems) are not destroyed. You can later reconfigure deduplication using the same file systems.

If *destroy_fs=yes*,:

- If WORM was configured, a check is made to see if there are any backup images present in the system. If backup images are present, you cannot destroy the file system and the `dedupe unconfig` command fails. Before you unconfigure Veritas Data Deduplication and destroy the file systems, ensure that you have removed the storage unit, disk pool and storage server from the NetBackup primary server.
- If WORM is not configured, the file systems are destroyed after unconfiguring deduplication.

To add an IP to the deduplication cluster

- ◆ To add an IP to the deduplication cluster, enter the following:

```
Dedupe> addip IP
```

To remove an IP from the deduplication cluster

- ◆ To remove an IP from the deduplication cluster, enter the following:

```
Dedupe> removeip IP
```

- To change the primary IP of the deduplication server, enter the following:

```
Dedupe> changeip IP config_name
```

The *config_name* is the name of the deduplication server to which IP is being added. It must be specified if more than one deduplication server is configured on the cluster.

To add an FQDN to the deduplication server

The FQDNs of the NetBackup master and media servers should be added to the deduplication server. This configuration leads to faster backups on the storage server and should be done prior to adding the storage server in the NetBackup administration console or Web UI. Adding the FQDNs of the NetBackup servers allows for faster name resolution within the docker container.

Do not add the IP and FQDN of the deduplication service to the deduplication server as this can create issues when the MSDP services are started.

- To add an FQDN to the deduplication cluster, enter the following:

```
Dedupe> fqdn add IP fqdn
```

To remove an FQDN from the deduplication cluster

- ◆ To remove an FQDN from the deduplication cluster, enter the following:

```
Dedupe> fqdn remove IP
```

To grow the catalog file system of the deduplication server

- To grow the catalog file system of the deduplication server to a specific size, enter the following:

```
Dedupe> catgrow size
```

The deduplication server should be online for this operation. This operation is not supported from the Access Appliance GUI.

You can use the `dedupe catgrow <size>` command to grow the catalog file system to the specified size. The default `dedupe grow` command does not modify the size of the catalog file system. If there are multiple data file systems, specify the file system names in the same order in which you specified them in the `dedupe show` command previously.

See the `dedupe` man page for more information.

Managing Veritas Data Deduplication using GUI

This section describes the various operations that you can perform on the deduplication server using the GUI.

Unconfiguring Veritas Data Deduplication

You can unconfigure Veritas Data Deduplication.

Ensure that you make a note of the following configuration details before you unconfigure the Veritas Data Deduplication server with **Retain data** option. These details are required when you reconfigure the service.

- The virtual IP that you used to configure the Veritas Data Deduplication serve.
- Credentials to access the Veritas Data Deduplication server
- File system names (including data and catalog file systems)

Note: You can reconfigure Veritas Data Deduplication from the Access Appliance CLISH only.

To unconfigure Veritas Data Deduplication

- 1 Go to **Settings > Veritas Data Deduplication management**. Click on the kebab menu of the instance.
- 2 Click **Unconfigure**.

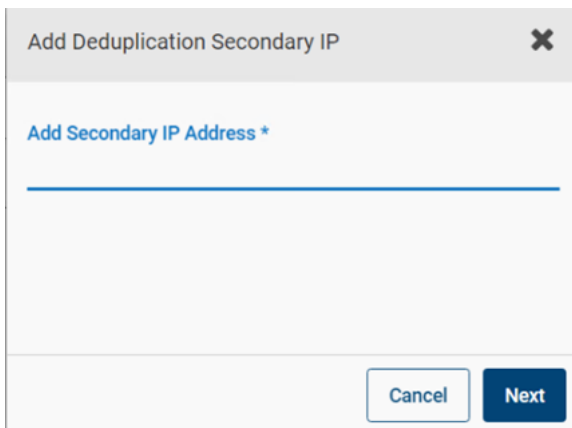
- 3 The **Unconfigure Veritas Data Deduplication** dialog box is displayed.
 Select one of the options - **Retain data** (if you want to keep the Veritas Data Deduplication utilized file systems) or **Delete data** (if you want to delete the file systems) and click **Save**.
- 4 View the **Recent Activity** panel for the status of the task.

Adding secondary IP for Veritas Data Deduplication

You can add a secondary IP for any instance of Veritas Data Deduplication.

To add secondary IP for any instance

- 1 Go to **Settings > Veritas Data Deduplication management**. Click on the configuration name for which you want to add a secondary IP.
- 2 Click **Add IP**.
- 3 The **Add Deduplication Secondary IP** dialog box is displayed. Enter the IP. Click **Next**.



Note: The restrictions which are applicable to the virtual IP field during configuring of Veritas Data Deduplication are also applicable here.

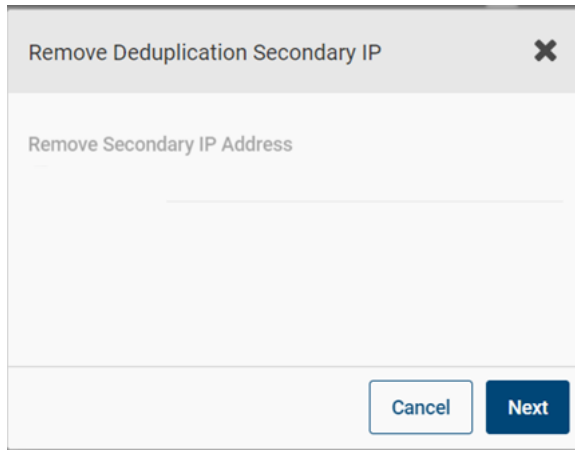
- 4 Click **Finish**.
- 5 View the **Recent Activity** panel for the status of the task.

Deleting secondary IP for Veritas Data Deduplication

You can delete the secondary IP for any instance of Veritas Data Deduplication.

To remove secondary IP for any instance

- 1 Go to **Settings > Veritas Data Deduplication management**. Click on the configuration name for which you want to delete the secondary IP.
- 2 Click **Remove** for the IP that you want to remove. The **Remove Deduplication Secondary IP** dialog box is displayed. Click **Next**.



- 3 Click **Finish**.
- 4 View the **Recent Activity** panel for the status of the task.

Accessing Access Appliance WORM storage shell for management tasks

To perform some management tasks on a WORM storage server instance, you must open an SSH session to the instance and log in to the WORM storage server shell. Any user with appliance administrator role can login and perform management tasks.

From the WORM storage shell, you can run commands to manage the instance and your WORM storage. See [“About the Access Appliance WORM storage server shell”](#) on page 33.

About the Access Appliance WORM storage server shell

Use the Access Appliance WORM storage server shell to configure the immutable and indelible data from the appliance. The interface provides tab-completed command options.

These are main categories of commands:

- `dedupe`
 This command lets you manage the deduplication service.
 See [“About the dedupe command”](#) on page 34.
- `retention`
 This command lets you manage image retention.
 See [“About the retention command”](#) on page 36.
- `setting`
 This command lets you manage the deduplication and system configuration settings.
 See [“About the setting command”](#) on page 36.
- `support`
 This command lets you access and upload the relevant logs and configuration files for troubleshooting.
 See [“About the support command”](#) on page 40.

About the dedupe command

The `dedupe` commands lets you manage the deduplication services.

The following table describes the options and arguments for the `dedupe` command.

Table 3-1 The options and arguments for the `dedupe` command.

Option and its description	Argument	Description
CRC Check and manage the deduplication CRC service.	<code>state</code>	Display the state of the CRC checking services.
	<code>enable</code>	Enable the CRC checking services.
	<code>enable-fixmode</code>	Enable the CRC checking services with a fix mode.
	<code>disable-fixmode</code>	Disable the fix mode of the CRC checking services.
	<code>disable</code>	Disable the CRC checking services.
	<code>fast</code>	Restart the CRC checking services in a mode.
	<code>fixmode-state</code>	Display the state of the fix mode of the CRC checking services.

Table 3-1 The options and arguments for the `dedupe` command. (*continued*)

Option and its description	Argument	Description
CRQP Manage the transaction log (Tlog) process service.	<code>status</code>	Display the status of the CRQP services.
	<code>start</code>	Start the CRQP services.
	<code>info</code>	Show the CRQP services information.
online-check Manage online checking services.	<code>enable</code>	Enable the online checking services.
	<code>status</code>	Display the status of the online checking services.
	<code>disable</code>	Disable the online checking services.
compaction Manage the MSDP compaction service.	<code>start</code>	Start the deduplication compaction services.
	<code>state</code>	Display the status of the deduplication compaction services.
	<code>disable</code>	Disable the deduplication compaction services.
	<code>enable</code>	Enable the deduplication compaction services.
MSDP Manage the MSDP services.	<code>start</code>	Start the deduplication (MSDP) services.
	<code>status</code>	Display the status of the deduplication (MSDP) services.
	<code>stop</code>	Stop the deduplication (MSDP) services.

Stopping and starting the MSDP services

To stop the MSDP services:

1. Check the health monitor status using the following command:
2. If the health monitor is enabled, stop the monitor using the following command:

```
setting health status
```

```
setting health disable
```

3. After disabling the health monitor, use the following command to stop the MSDP services:

```
dedupe MSDP stop
```

To start the MSDP services:

1. Start the MSDP services using the following command:

```
dedupe MSDP start
```

2. Start the health monitor using the following command:

```
setting health enable
```

About the retention command

The `retention` command lets you manage image retention.

The following table describes the options and arguments for the `retention` command.

Table 3-2 The options and arguments for the `retention` command.

Option and its description	Argument	Description
<code>policy</code> The backup policy to use for the image retention with a retention lock.	<code>list</code>	List the images that have a retention lock.
	<code>audit</code>	Display the audit information for the images with a retention lock.
	<code>disable</code>	Disable the image retention using the backup ID of the image. For example: <pre>retention policy disable backup_ID=<test_123> copynumber=<number></pre> You can find the backup ID and the copy number in the output of the <code>retention policy list</code> command.

About the setting command

The `setting` command lets you manage the deduplication and system configuration settings.

The following table describes the options and arguments for the `setting` command.

Table 3-3 The options and arguments for the `setting` command.

Option and its description	Argument	Description
FIPS Manage FIPS settings.	<code>status</code>	Display the status of FIPS in MSDP.
network Configure the network settings.	<code>ping</code>	Ping the network for a connection status. Use the <code>ip</code> parameter to enter the IP address of the network to check the connection status.
	<code>ifconfig</code>	Display the IP address of the network.
	<code>route</code>	Display the network route information.
WORM Configure the settings for immutable and indelible storage.	<code>status</code>	Display the status of WORM storage.
	<code>set-max</code>	Specify the maximum duration to keep the storage immutable and indelible. Use the <code>worm_max</code> parameter to specify the maximum duration in seconds to keep the storage immutable and indelible (WORM).
	<code>set-min</code>	Specify the minimum duration to keep the storage immutable and indelible. Use the <code>worm_min</code> parameter to specify the minimum duration in seconds to keep the storage immutable and indelible (WORM).
	<code>show-mode</code>	Display the WORM mode.

Table 3-3 The options and arguments for the `setting` command.
(continued)

Option and its description	Argument	Description
<code>set-MSDP-param</code> Set the parameters in the MSDP configuration files.	<code>write-thread-num</code>	Get and set the <code><WriteThreadNum></code> parameter. Use the <code>value</code> parameter to enter the value that is used by the MSDP parameters.
	<code>spoold-logging</code>	Get and set the <code><SpoolLogging></code> parameter.
	<code>allocation-unit-size</code>	Get and set the <code><AllocationUnitSize></code> parameter.
	<code>data-check-days</code>	Get and set the <code><DataCheckDays></code> parameter.
	<code>max-fp-cache-size</code>	Get and set the <code><MaxFPCacheSize></code> parameter.
	<code>max-retry-count</code>	Get and set the <code><MaxRetryCount></code> parameter.
	<code>spad-logging</code>	Get and set the <code><SpadLogging></code> parameter.
	<code>log-retention</code>	Get and set the <code><LogRetention></code> parameter.

Table 3-3 The options and arguments for the `setting` command.
(continued)

Option and its description	Argument	Description
<code>get-MSDP-param</code> Get the parameters from the MSDP configuration files.	<code>write-thread-num</code>	Get and set the <code><WriteThreadNum></code> parameter.
	<code>spoold-logging</code>	Get and set the <code><SpoolLogging></code> parameter.
	<code>allocation-unit-size</code>	Get and set the <code><AllocationUnitSize></code> parameter.
	<code>data-check-days</code>	Get and set the <code><DataCheckDays></code> parameter.
	<code>max-fp-cache-size</code>	Get and set the <code><MaxFPCacheSize></code> parameter.
	<code>max-retry-count</code>	Get and set the <code><MaxRetryCount></code> parameter.
	<code>spad-logging</code>	Get and set the <code><SpadLogging></code> parameter.
	<code>log-retention</code>	Get and set the <code><LogRetention></code> parameter.
<code>MSDP-user</code> Configure the settings for the MSDP user.	<code>random-password</code>	Generates a random password.
	<code>list</code>	List all the MSDP users.
	<code>verify-user</code>	Verify user password and user role.
	<code>reset-password</code>	Reset the password for the MSDP user.
<code>encryption</code> Configure the settings for MSDP encryption.	<code>status</code>	Display the current encryption status.
	<code>enable</code>	Enable encryption for MSDP.
<code>kernel</code> Get the information about the kernel.	<code>search-param</code>	Search for a keyword in the kernel parameters. Use the <code>keyword</code> to specify a keyword to search in the keyword parameters.

About the support command

The `support` command lets you access and upload the relevant logs and configuration files for troubleshooting.

The following table describes the options and arguments for the `support` command.

Table 3-4 The options and arguments for the `support` command.

Option and its description	Argument	Description
MSDP-history Access the MSDP history files.	tail	Append the last 10 lines of each file to standard output. This command requires the following parameters: ■ <code>file</code> Enter the filename. This is a required parameter. ■ <code>options</code> Enter the supported options for <code>grep</code>: <code>-i</code>, <code>-w</code>, <code>-E</code>, or <code>tail</code>: <code>-f</code>, <code>-n</code>.
	collect	Collect files for transferring to the target host. This command requires the following parameters: ■ <code>mmin</code> Find files that are modified <code>n</code> minutes ago. Same as <code>mmin</code> option in <code>find</code> command. For example, 15, +15, -15. ■ <code>pattern</code> Specify the naming pattern to find and select matching files and folders. For example, <code>spoold</code>, or <code>spad*</code>. ■ <code>mtime</code> Finds files that are modified <code>n*24</code> hours ago. Same as <code>mtime</code> option in <code>find</code> command. For example, 2, +2, -2.
	ls	List information about the FILES. Use the <code>dir</code> parameter to enter the directory name.
	scp	

Table 3-4 The options and arguments for the `support` command.
(continued)

Option and its description	Argument	Description
		Securely transfer selected files to the target host. This command requires the following parameters: ■ <code>scp_port</code> Specifies the port to connect to on the remote host. ■ <code>scp_target</code> Specifies the target host and path for transferring files. Use the <code>user@host:/directory path/</code> format. This is a required parameter.
	<code>cat</code>	Concatenate files and print on the standard output. Use the <code>file</code> parameter to enter the file name.
	<code>grep</code>	Print lines that match patterns. This command requires the following parameters: ■ <code>pattern</code> Specify the naming pattern to find and select matching files and folders. For example, <code>spoold</code>, or <code>spad*</code>. This is a required parameter. ■ <code>file</code> Enter the filename. This is a required parameter. ■ <code>options</code> Enter the supported options for <code>grep</code>: <code>-i</code>, <code>-w</code>, <code>-E</code>, or <code>tail: -f</code>, <code>-n</code>.

Table 3-4 The options and arguments for the `support` command.
(continued)

Option and its description	Argument	Description
process Displays information about the MSDP processes.	MSDP-process	Display the MSDP processes.
	htop	Display the CPU and memory information.
	atop	Display information about the operating system.
	pidstat	Display the PID statistics.
	memory-usage	Displays the free and used memory.
software Displays information about the software.	show-MSDP-version	Display the MSDP version.
	show-OS-version	Display the operating system information.

Table 3-4 The options and arguments for the `support` command.
(continued)

Option and its description	Argument	Description
MSDP-log Access the MSDP log files.	tail	Append the last 10 lines of each file to standard output. This command requires the following parameters: ■ <code>file</code> Enter the filename. This is a required parameter. ■ <code>options</code> Enter the supported options for <code>grep</code>: <code>-i</code>, <code>-w</code>, <code>-E</code>, or <code>tail</code>: <code>-f</code>, <code>-n</code>.
	collect	Collect files for transferring to the target host. This command requires the following parameters: ■ <code>mmin</code> Find files that are modified <code>n</code> minutes ago. Same as <code>mmin</code> option in <code>find</code> command. For example, 15, +15, -15. ■ <code>pattern</code> Specify the naming pattern to find and select matching files and folders. For example, <code>spoold</code>, or <code>spad*</code>. ■ <code>mtime</code> Finds files that are modified <code>n*24</code> hours ago. Same as <code>mtime</code> option in <code>find</code> command. For example, 2, +2, -2.
	ls	List information about the files. Use the <code>dir</code> parameter to enter the directory name.
	scp	

Table 3-4

The options and arguments for the `support` command.

(continued)

Option and its description	Argument	Description
		Securely transfer selected files to the target host. This command requires the following parameters: ■ <code>scp_port</code> Specifies the port to connect to on the remote host. ■ <code>scp_target</code> Specifies the target host and path for transferring files. Use the <code>user@host:/directory path/</code> format. This is a required parameter.
	<code>cat</code>	Concatenate files and print on the standard output. Use the <code>file</code> parameter to enter the file name.
	<code>grep</code>	Print lines that match patterns. This command requires the following parameters: ■ <code>pattern</code> Specify the naming pattern to find and select matching files and folders. For example, <code>spoold</code>, or <code>spad*</code>. This is a required parameter. ■ <code>file</code> Enter the filename. This is a required parameter. ■ <code>options</code> Enter the supported options for <code>grep</code>: <code>-i</code>, <code>-w</code>, <code>-E</code>, or <code>tail: -f</code>, <code>-n</code>.
<code>hardware</code> Displays information about the hardware.	<code>cpumem</code>	Display the CPU and memory information.

Table 3-4 The options and arguments for the `support` command.
(continued)

Option and its description	Argument	Description
MSDP-config Access the MSDP configuration files.	tail	Append the last 10 lines of each file to standard output. This command requires the following parameters: ■ <code>file</code> Enter the filename. This is a required parameter. ■ <code>options</code> Enter the supported options for <code>grep</code>: <code>-i</code>, <code>-w</code>, <code>-E</code>, or <code>tail</code>: <code>-f</code>, <code>-n</code>.
	collect	Collect files for transferring to the target host. This command requires the following parameters: ■ <code>mmin</code> Find files that are modified <code>n</code> minutes ago. Same as <code>mmin</code> option in <code>find</code> command. For example, <code>15</code>, <code>+15</code>, <code>-15</code>. ■ <code>pattern</code> Specify the naming pattern to find and select matching files and folders. For example, <code>spoold</code>, or <code>spad*</code>. ■ <code>mtime</code> Finds files that are modified <code>n*24</code> hours ago. Same as <code>mtime</code> option in <code>find</code> command. For example, <code>2</code>, <code>+2</code>, <code>-2</code>.
	ls	List information about the FILES. Use the <code>dir</code> parameter to enter the directory name.
	scp	

Table 3-4

The options and arguments for the `support` command.
(continued)

Option and its description	Argument	Description
		Securely transfer selected files to the target host. This command requires the following parameters: ■ <code>scp_port</code> Specifies the port to connect to on the remote host. ■ <code>scp_target</code> Specifies the target host and path for transferring files. Use the <code>user@host:/directory path/</code> format. This is a required parameter.
	<code>cat</code>	Concatenate files and print on the standard output. Use the <code>file</code> parameter to enter the file name.
	<code>grep</code>	Print lines that match patterns. This command requires the following parameters: ■ <code>pattern</code> Specify the naming pattern to find and select matching files and folders. For example, <code>spoold</code>, or <code>spad*</code>. This is a required parameter. ■ <code>file</code> Enter the filename. This is a required parameter. ■ <code>options</code> Enter the supported options for <code>grep</code>: <code>-i</code>, <code>-w</code>, <code>-E</code>, or <code>tail: -f</code>, <code>-n</code>.

Table 3-4 The options and arguments for the `support` command.
(continued)

Option and its description	Argument	Description
diskio Displays information about the disk I/O.	iostat	Displays the information about the disk I/O.
	vmstat	Displays the information on the wait on the disk I/O.
	nmon	Display the information about the monitor system.
	disk-volume	Display information about the disk volume.

Table 3-4 The options and arguments for the `support` command.
(continued)

Option and its description	Argument	Description
syslogs Access the system logs.	tail	Append the last 10 lines of each file to standard output. This command requires the following parameters: ■ <code>file</code> Enter the filename. This is a required parameter. ■ <code>options</code> Enter the supported options for <code>grep</code>: <code>-i</code>, <code>-w</code>, <code>-E</code>, or <code>tail</code>: <code>-f</code>, <code>-n</code>.
	collect	Collect files for transferring to the target host. This command requires the following parameters: ■ <code>mmin</code> Find files that are modified <code>n</code> minutes ago. Same as <code>mmin</code> option in <code>find</code> command. For example, 15, +15, -15. ■ <code>pattern</code> Specify the naming pattern to find and select matching files and folders. For example, <code>spool</code>, or <code>spad*</code>. ■ <code>mtime</code> Finds files that are modified <code>n*24</code> hours ago. Same as <code>mtime</code> option in <code>find</code> command. For example, 2, +2, -2.
	ls	List information about the FILES. Use the <code>dir</code> parameter to enter the directory name.
	scp	

Table 3-4

The options and arguments for the `support` command.
(continued)

Option and its description	Argument	Description
		Securely transfer selected files to the target host. This command requires the following parameters: ■ <code>scp_port</code> Specifies the port to connect to on the remote host. ■ <code>scp_target</code> Specifies the target host and path for transferring files. Use the <code>user@host:/directory path/</code> format. This is a required parameter.
	<code>cat</code>	Concatenate files and print on the standard output. Use the <code>file</code> parameter to enter the file name.
	<code>grep</code>	Print lines that match patterns. This command requires the following parameters: ■ <code>pattern</code> Specify the naming pattern to find and select matching files and folders. For example, <code>spoold</code>, or <code>spad*</code>. This is a required parameter. ■ <code>file</code> Enter the filename. This is a required parameter. ■ <code>options</code> Enter the supported options for <code>grep</code>: <code>-i</code>, <code>-w</code>, <code>-E</code>, or <code>tail: -f</code>, <code>-n</code>.

Table 3-4 The options and arguments for the `support` command.
(continued)

Option and its description	Argument	Description
<code>proc</code> Access process information about the pseudo-filesystem.	<code>tail</code>	Append the last 10 lines of each file to standard output. This command requires the following parameters: ■ <code>file</code> Enter the filename. This is a required parameter. ■ <code>options</code> Enter the supported options for <code>grep</code>: <code>-i</code>, <code>-w</code>, <code>-E</code>, or <code>tail</code>: <code>-f</code>, <code>-n</code>.
	<code>ls</code>	List information about the FILES. Use the <code>dir</code> parameter to enter the directory name.
	<code>cat</code>	Concatenate files and print on the standard output. Use the <code>file</code> parameter to enter the file name.
	<code>grep</code>	Print lines that match patterns. This command requires the following parameters: ■ <code>pattern</code> Specify the naming pattern to find and select matching files and folders. For example, <code>spoold</code>, or <code>spad*</code>. This is a required parameter. ■ <code>file</code> Enter the filename. This is a required parameter. ■ <code>options</code> Enter the supported options for <code>grep</code>: <code>-i</code>, <code>-w</code>, <code>-E</code>, or <code>tail</code>: <code>-f</code>, <code>-n</code>.

Here are some examples of the `support` command usage:

```
support MSDP-log ls dir=spoolld
support MSDP-log ls dir=spad/soflvm08.tec.com/spoolld/spad/072320.log
support MSDP-log cat file=pdde-config.log
support MSDP-log cat file=spad/soflvm08.tec.com/spoolld/spad/072320.log
support MSDP-log tail file=pdde-config.log
support MSDP-log tail file=pdde-config.log options="-f"
support MSDP-log tail file=pdde-config.log options="-n 5"
support MSDP-log tail file=spad/sofia11vm08/spoolld/spad/072320.log
options="-f -n 5"
support MSDP-log grep file=spad* pattern=sessionStartAgent
options="-r"
support MSDP-log grep file=pdde-setup.log pattern="pid 455"
support MSDP-log grep file=pdde-setup.log pattern="Pid" options="-w
-i"
support MSDP-log grep file=spoolld* pattern="Pid" options="-w -i -r"
support MSDP-log grep file=pdde-setup.log pattern="MSDP-X|PureDisk"
options="-w -i -r -E"
```

Examples to uploading logs, history, or config files:

Uploading logs is a two-step process:

- Run the `collect` command for the desired category to collect files of interest. For example:

```
support MSDP-log collect pattern=spoolld* mmin="+2"
support MSDP-history collect
support MSDP-config collect
support syslogs collect pattern=crash mmin="-2"
```

- Transfer files using `scp` command

Run the `scp` command from any category to create a tarball of all previously collected files (from all categories) and transfer the tarball to the target host using the `scp` protocol.

```
support MSDP-config scp scp_target=user@example.com:/tmp
```

Support for multiple domains across networks for Veritas Data Deduplication

You can use a single deduplication pool to backup data from multiple NetBackup domains. The Veritas Data Deduplication server deduplicates backups originating from different subnets. Use the `network ip addr show` command to list the multiple subnets that have been created.

```
Network> ip addr show
```

IP	Netmask/Prefix	Device	Node	Type	Status
192.168.10.5	255.255.255.0	eth5	vaupg_01	Physical	
192.168.10.13	255.255.255.0	eth5	vaupg_02	Physical	
192.168.30.2	255.255.255.0	eth4	vaupg_01	Physical	
192.168.30.10	255.255.255.0	eth4	vaupg_02	Physical	
10.209.192.206	255.255.252.0	eth1	vaupg_01	Physical	
10.209.192.208	255.255.252.0	eth1	vaupg_02	Physical	
10.209.194.38	255.255.252.0	eth1	vaupg_01	Virtual	ONLINE (Con IP)
192.168.10.22	255.255.255.0	eth5	vaupg_01	Virtual	ONLINE
192.168.10.25	255.255.255.0	eth5	vaupg_02	Virtual	ONLINE
192.168.30.15	255.255.255.0	eth4	vaupg_02	Virtual	ONLINE
192.168.30.20	255.255.255.0	eth4	vaupg_01	Virtual	ONLINE

You can use the following command to configure the deduplication server with a virtual IP.

```
Dedupe> config fs_name IPaddress username catalogfilesystem
```

For example:

```
Dedupe> config fs1 192.168.10.22 user1 CAT_257091
Enter Password:
ACCESS dedupe INFO V-493-10-0 configuring deduplication server...
ACCESS dedupe INFO V-493-10-0 Deduplication server configured successfully
```

You can verify that the IP has been added successfully using the `dedupe show` command.

```
Dedupe> show
```

Parameter	Value
Virtual_IP	192.168.10.22
Catalog_Filesystem	CAT_257091
Filesystem	fs1
Deduplication_Storage_Size_GB	5000
WORM_enabled	False
Hostname	vaupg_01
Server_Status	ONLINE
Max_Cache_Size	50%
Percentage_Memory_Usage	4.58%
Minimum_Retention_Value	
Maximum_Retention_Value	

You can add another IP from a different subnet.

```
Dedupe> addip <IPaddress>
```

For example:

```
Dedupe> addip 192.168.10.25
ACCESS dedupe INFO V-493-10-0 IP has been successfully added to the
deduplication server.
Dedupe> addip 192.168.30.15
ACCESS dedupe INFO V-493-10-0 IP has been successfully added to the
deduplication server.
Dedupe> addip 192.168.30.20
ACCESS dedupe INFO V-493-10-0 IP has been successfully added to the
deduplication server.
```

You can verify that the virtual IP is added successfully. The `dedupe show` command is used to display information about the deduplication server that has been configured. The output of this command includes the file system(s) being used, deduplication server status, storage capacity, secondary IPs used, percentage of memory usage, maximum cache size, and the IP and the cluster node on which the server is running.

```
Dedupe> show
Parameter                                Value
=====                                =====
Secondary_IP                             192.168.10.25,192.168.30.15,192.168.30.20
Virtual_IP                               192.168.10.22
Catalog_FileSystem                       CAT_257091
Filesystem                               fs1
Deduplication_Storage_Size_GB            5000
WORM_enabled                             False
Hostname                                 vaupg_01
Server_Status                            ONLINE
Max_Cache_Size                           50%
Percentage_Memory_Usage                   4.79%
Minimum_Retention_Value                   -
Maximum_Retention_Value                   -
```

Use the `network ip addr show` command to list the multiple subnets that have been created.

```
Network> ip addr show
IP                               Netmask/Prefix  Device Node      Type      Status
```

IP Address	Subnet	Interface	Port	Type	Status	Domain
192.168.10.5	255.255.255.0	eth5	vaupg_01	Physical		
192.168.10.13	255.255.255.0	eth5	vaupg_02	Physical		
192.168.30.2	255.255.255.0	eth4	vaupg_01	Physical		
192.168.30.10	255.255.255.0	eth4	vaupg_02	Physical		
10.209.192.206	255.255.252.0	eth1	vaupg_01	Physical		
10.209.192.208	255.255.252.0	eth1	vaupg_02	Physical		
10.209.194.38	255.255.252.0	eth1	vaupg_01	Virtual	ONLINE	(Con IP)
192.168.10.22	255.255.255.0	eth5	vaupg_01	Virtual	ONLINE	(Dedupe IP)
192.168.10.25	255.255.255.0	eth5	vaupg_01	Virtual	ONLINE	(Dedupe IP)
192.168.30.15	255.255.255.0	eth4	vaupg_01	Virtual	ONLINE	(Dedupe IP)
192.168.30.20	255.255.255.0	eth4	vaupg_01	Virtual	ONLINE	(Dedupe IP)

You can also add a second user. The second user is used to add the second NetBackup domain, if required. You should use a different user for every new NetBackup domain.

```
Dedupe> adduser user1
Enter Password:
Confirm Password:
ACCESS dedupe INFO V-493-10-0 Adding new user user2 to deduplication server.
ACCESS dedupe INFO V-493-10-0 Added new user user2 to deduplication server
successfully.
```

You can perform backup and restore operations from the NetBackup domains from the two subnets.

Note: You can remove the virtual IP that you added later after the initial configuration. But you cannot remove the virtual IP specified during the initial configuration.

```
Dedupe> removeip IPaddress
```

For example:

```
Dedupe> removeip 192.168.30.15
ACCESS dedupe INFO V-493-10-0 IP has been successfully removed from the
deduplication server.
```

You can verify that the second virtual IP has been removed from the configuration using the `dedupe show` command.

```
Dedupe> show
Parameter                                     Value
=====
```

```

Secondary_IP          192.168.10.25,192.168.30.20
Catalog_FileSystem    CAT_257091
Virtual_IP            192.168.10.22
Filesystem            fs1
Deduplication_Storage_Size_GB 5000
WORM_enabled          False
Hostname              vaupg_01
Server_Status         ONLINE
Max_Cache_Size        50%
Percentage_Memory_Usage 4.79%
Minimum_Retention_Value -
Maximum_Retention_Value -

```

You can use the `dedupe unconfig` command to free up all the virtual IPs added to the deduplication server. This command also unconfigures Veritas Data Deduplication from the cluster.

```

Dedupe> unconfig destroy_fs=yes
ACCESS dedupe INFO V-493-10-0 Removing deduplication server configuration...
ACCESS dedupe INFO V-493-10-0 Deduplication server unconfigured successfully.

```

Upgrade considerations

You cannot use the same virtual IP for both the CIFS and Veritas Data Deduplication server. So, if a virtual IP is used by the Veritas Data Deduplication server, then you cannot use the same virtual IP for adding CIFS shares or setting the CIFS home directory.

Note: If Veritas Access 7.4.2.x is installed in your system and the same virtual IP is being shared by both the CIFS and Veritas Data Deduplication server, and you want to upgrade, ensure that an additional free virtual IP is available in the configuration.

During the upgrade, the virtual IP which is shared between CIFS and Veritas Data Deduplication server is removed from the CIFS configuration and the next available free virtual IP is assigned to the CIFS server.

- If a free virtual IP is available, the deduplication continues to work without any issues once the upgrade is complete.
- If there is no free virtual IP, then the upgrade fails. You can add a free virtual IP to the configuration and try to upgrade again.
- If the virtual IP is shared between the Veritas Data Deduplication server and a segregated CIFS share, then the upgrade fails even if an additional free virtual

IP is available in the configuration. You can move the segregated CIFS share to different virtual IP and try the upgrade again.

Veritas Data Deduplication storage layout

The layout of the Veritas Data Deduplication storage is such that when you configure Veritas Data Deduplication, multiple file systems of 100TiB and a separate catalog file system of size 5TiB are created.

The `dedupe grow` command creates a new file system for every 100TiB. If you perform upgrade and you had previously configured Veritas Data Deduplication, then the old layout of Veritas Data Deduplication is preserved. If a separate catalog file system existed before upgrade, the same catalog file system is present after the upgrade also. If the size of data filesystems is more than 100 TiB, then those filesystems remain as it is but new data filesystems are created for every 100 TiB that is grown using the `dedupe grow` command.

Note: Veritas Data Deduplication configuration requires 5 TiB for creating the catalog file system. This is over and above the size specified for the deduplication pool in the GUI.

Reconfiguration is a two-step process involving unconfiguring the Veritas Data Deduplication without destroying the filesystems and configuring it again with the same existing filesystems. After an upgrade, if you want to reconfigure the Veritas Data Deduplication service, the following checks are performed:

- If a separate catalog file system existed before reconfiguration, then the same catalog file system is passed to the `dedupe config` command during reconfiguration.
- If a separate catalog file system did not exist before reconfiguration, then the catalog file system cannot be passed to the `dedupe config` command during reconfiguration.

After unconfiguration, you can use `dedupe config` command to reconfigure the deduplication server.

Reconfiguration of Veritas Data Deduplication can be done only using CLISH.

To reconfigure Veritas Data Deduplication

- 1 Run the `dedupe show` command and make a note of the file system names for both the data and catalog file system.
- 2 Unconfigure Veritas Data Deduplication using the `dedupe unconfig` command.

```
Dedupe> unconfig
```

- 3 Run the following command to configure Veritas Data Deduplication:

```
Dedupe> config filesystem_list virtual_IP username [catfs_name]
```

where the *catfs_name* depends on the configuration and *filesystem_list* is a comma-separated list of filesystems without space.

The credentials should be the same that you used when you previously configured Veritas Data Deduplication.

The catalog file system needs to be mentioned only if the previous Veritas Data Deduplication configuration had a catalog file system.

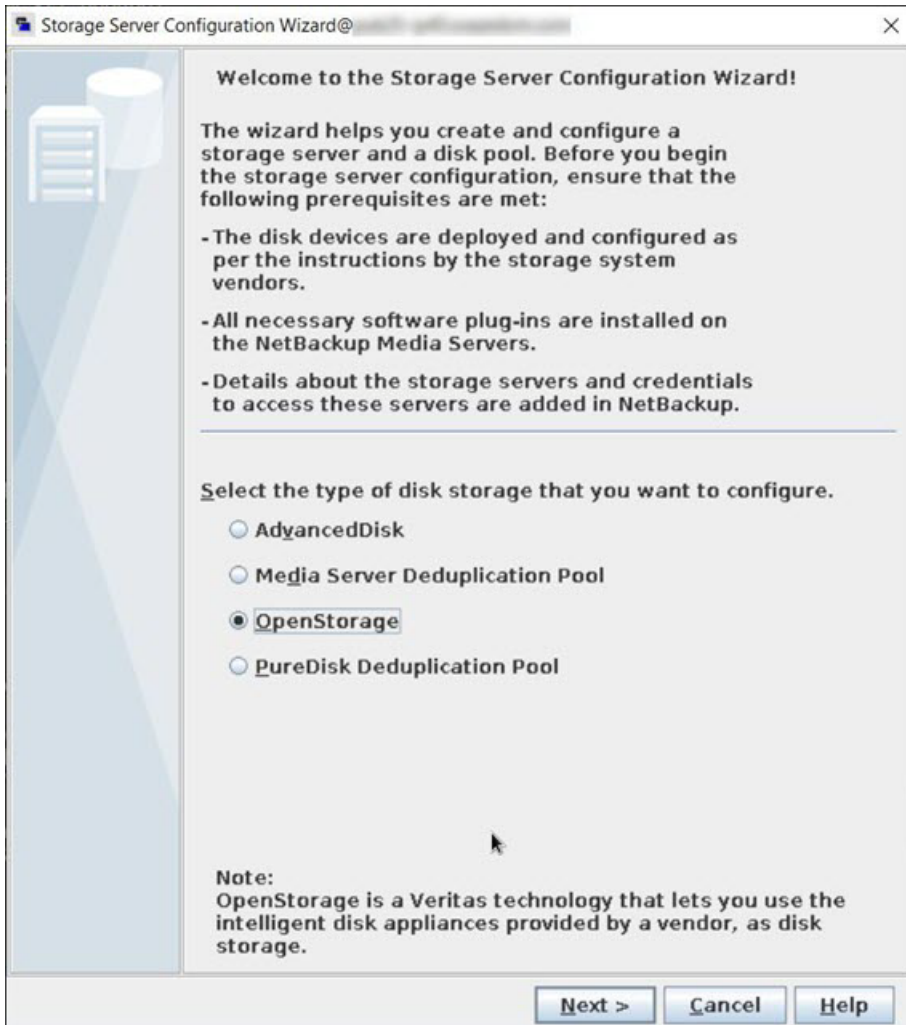
Configuring a Veritas Data Deduplication storage unit on NetBackup

Veritas recommends that you run a maximum of 80 parallel duplication streams on Veritas Data Deduplication.

To create a storage server on NetBackup

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

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



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

Note: If you want to use a host name for the storage server instead of the deduplication IP's FQDN, ensure that it is resolvable to the FQDN configured for the deduplication storage server with DNS.

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

Click **Next**.



The image shows a 'Storage Server Configuration Wizard' window. The title bar reads 'Storage Server Configuration Wizard@'. The window has a header bar with the text 'Add Storage Server' and 'Provide storage server details.' on the left, and a red icon on the right. The main content area contains the following elements:

- Instructional text: '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:' dropdown menu with a selected value.
- 'Storage server type:' dropdown menu with 'PureDisk' selected.
- Text 'PureDisk' displayed below the storage server type dropdown.
- 'Storage server name:' text input field.
- A section titled 'Enter storage server credentials' containing:
 - 'User name:' text input field.
 - 'Password:' text input field with masked characters (dots).
 - 'Confirm password:' text input field with masked characters (dots).
- At the bottom, four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

- 5 In the **Additional Media Server Configuration for OpenStorage Devices** form, specify the media servers that should have access to the OpenStorage device. Click **Next**.
- 6 In the **Storage Server Configuration Summary** form, verify the storage server configuration. Click **Next**.



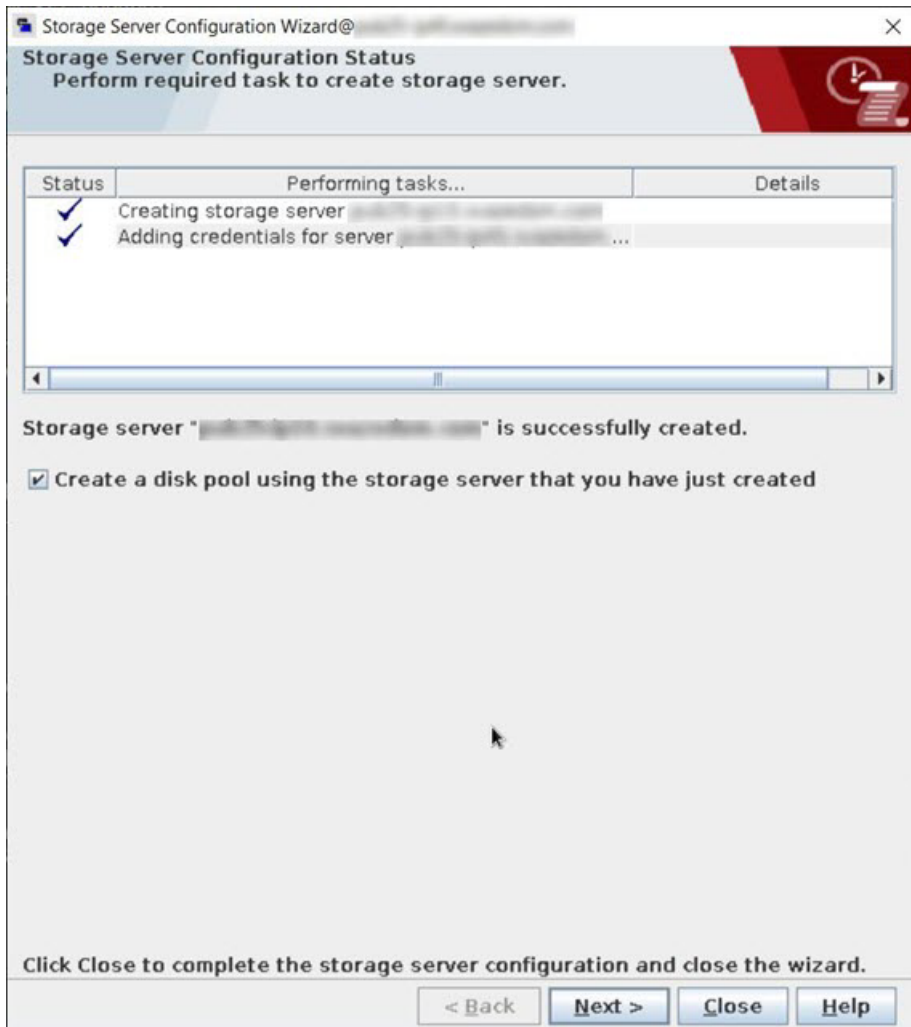
The image shows a screenshot of the 'Storage Server Configuration Wizard' window. The title bar reads 'Storage Server Configuration Wizard@'. The window has a red header bar with the text 'Storage Server Configuration Summary' and 'Verify the storage server configuration.' Below the header, there is a red icon of a document with a clock. The main content area contains the text 'Review the storage server configuration summary. You can change the configuration, if required.' Below this, there is a table with the following information:

Storage server type:	PureDisk
Storage server name:	[Redacted]
Media server name:	[Redacted]
User name:	[Redacted]

At the bottom of the window, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

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

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



9 The **Volume Selection** form lists all the volumes.

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

Storage Server Configuration Wizard@

Volume Selection

Select volumes to use in the disk pool.

Storage server:

Storage server type: PureDisk

Select storage server volumes to add to the disk pool.

Volume Na...	Available S...	Raw Size	Replication	WORM Cap...	Minimum L...	Maximum L...
☒ PureD...	9.02 GB	9.27 GB	None	Yes	1 hour	7 hours 1...

Disk Pool Size

Total available space: 9.02 GB

Total raw size: 9.27 GB

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

< Back

Next >

Cancel

Help

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

The screenshot shows a window titled "Storage Server Configuration Wizard@". The main heading is "Additional Disk Pool Information" with the instruction "Provide additional disk pool information." Below this, the "Storage server:" field is populated with "pdr-fgprk-mcswdsk-001". The "Storage server type:" is set to "PureDisk". A section titled "Disk Pool Size" displays "Total available space: 9.02 GB" and "Total raw size: 9.27 GB". The "Disk Pool name:" field contains "ltr-pool". There is a large empty text area for "Comments:". Below this, the "High water mark:" is set to "98 %" and the "Low water mark:" is set to "80 %". A section titled "Maximum I/O Streams" contains an information icon and the text "Concurrent read and write jobs affect disk performance. Limit I/O streams to prevent disk overload." Below this, there is a checkbox for "Limit I/O streams:" which is currently unchecked, followed by a spinner box set to "-1" and the text "per volume". At the bottom of the window are four buttons: "< Back", "Next >", "Cancel", and "Help".

Storage Server Configuration Wizard@

Additional Disk Pool Information
Provide additional disk pool information.

Storage server: pdr-fgprk-mcswdsk-001

Storage server type: PureDisk

Disk Pool Size
Total available space: 9.02 GB
Total raw size: 9.27 GB

Disk Pool name: ltr-pool

Comments:

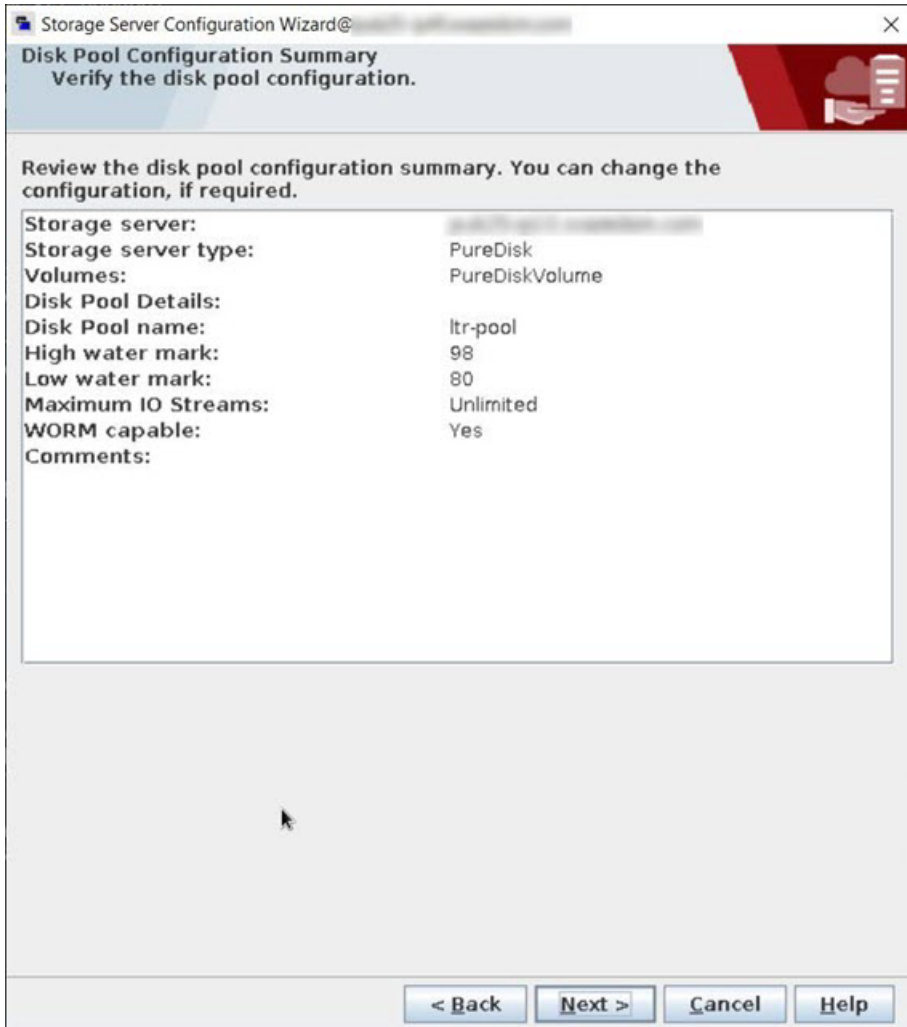
High water mark: 98 %

Low water mark: 80 %

Maximum I/O Streams
Concurrent read and write jobs affect disk performance.
Limit I/O streams to prevent disk overload.
☐ Limit I/O streams: -1 per volume

< Back Next > Cancel Help

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



The screenshot shows a window titled "Storage Server Configuration Wizard@". The main heading is "Disk Pool Configuration Summary" with the instruction "Verify the disk pool configuration." Below this, a text box says "Review the disk pool configuration summary. You can change the configuration, if required." A table lists the configuration details:

Storage server:	
Storage server type:	PureDisk
Volumes:	PureDiskVolume
Disk Pool Details:	
Disk Pool name:	ltr-pool
High water mark:	98
Low water mark:	80
Maximum IO Streams:	Unlimited
WORM capable:	Yes
Comments:	

At the bottom, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

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

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

Storage Server Configuration Wizard@

Disk Pool Configuration Status
 Perform disk pool creation task.

Status	Performing tasks...
✓	NetBackup Disk Pool created

Disk pool "ltr-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.
 Click 'Next' to create storage unit.

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

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

If the Access Appliance Veritas Data Deduplication is configured with the WORM option and you want to store the WORM-enabled images from NetBackup, then select the **Use WORM** check-box

To use this option, you should have created a WORM capable storage server on Access Appliance.

See [“Configuring Veritas Data Deduplication with WORM using GUI”](#) on page 22.

Click **Next**.

Storage Server Configuration Wizard@ [redacted] X

Storage Unit Creation
Enter details to create storage unit.

Disk pool: ltr-pool
Storage server type: PureDisk
Storage unit name: ltr-pool-stu
☒ Use WORM

Media Server

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

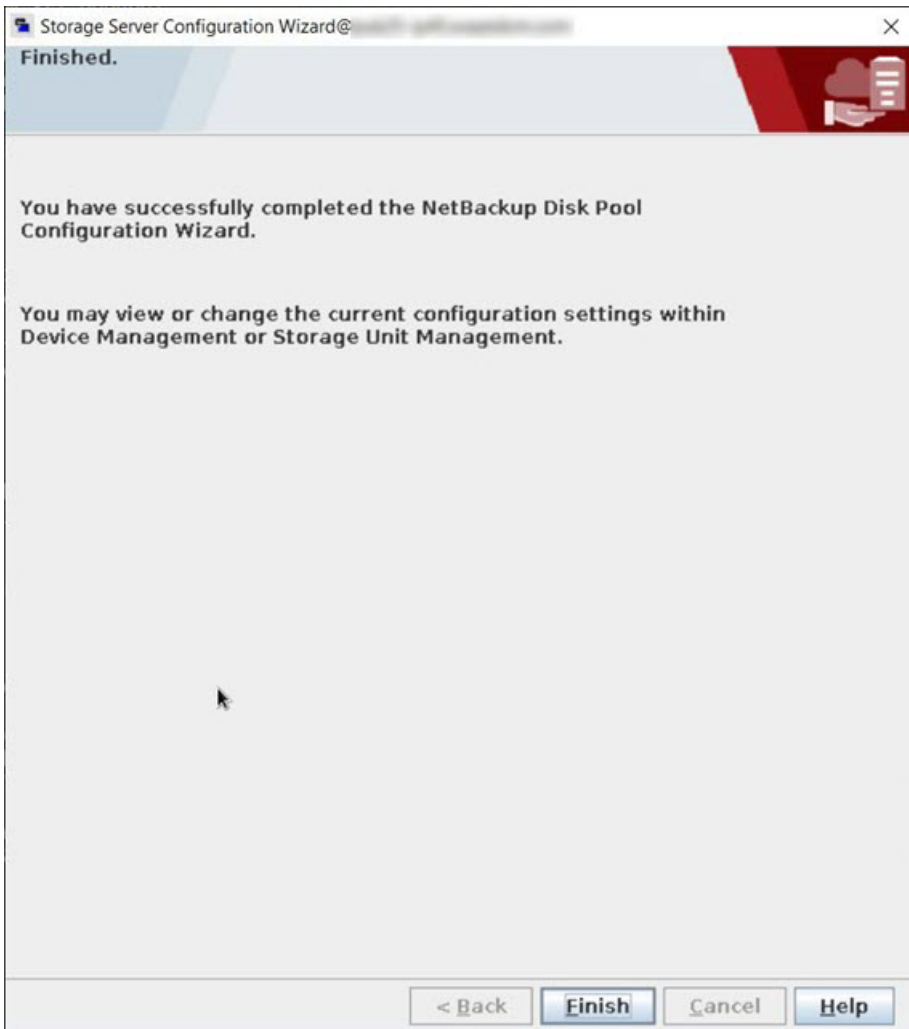
Media Servers

☐ [redacted]

Maximum concurrent jobs: 1
Maximum fragment size: 51200 Megabytes

< Back Next > Cancel Help

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



- 15** Go to **NetBackup Management > Storage Units** and verify that the storage server has been added successfully.
- 16** Go to **Media and Device Management > Disk Pools** and verify that the disk pool is created successfully.

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

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

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

```
dedupe> adduser username
```

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

The command should be run on the Access Appliance cluster.

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

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

```
dedupe> listuser
```

The command should be run on the Access Appliance cluster.

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

Enabling Veritas Data Deduplication encryption

Access Appliance supports Veritas Data Deduplication encryption for all backup and deduplication jobs. This section describes how to enable encryption for the backup jobs.

You can do it in two different ways.

Method 1:

Note: In NetBackup long-term data retention (LTR) use case, the server side refers to Access Appliance and the client refers to the media server.

For details on the MSDP compression and encryption settings, see the *MSDP compression and encryption settings matrix* section in the *Configuring deduplication* chapter in the *Veritas NetBackup Deduplication Guide* on SORT.

For details on configuring encryption for MSDP backups, see the *Configuring encryption for MSDP backups* section in the *Configuring deduplication* chapter in the *Veritas NetBackup Deduplication Guide* on SORT.

Method 2:

You can also enable encryption in the `contentrouter.cfg` file. If encryption is enabled in the `contentrouter.cfg` file, then any data coming from any media server is encrypted.

If Veritas Data Deduplication is configured with WORM

1. Log on to the restricted shell and type `setting encryption enable`.
2. Restart Veritas Data Deduplication services through the restricted shell.
3. Disable the health monitor and restart MSDP.

See [“Stopping and starting the MSDP services”](#) on page 35.

If Veritas Data Deduplication is configured without WORM

1. Log on to the appliance console by connecting to the management IP and elevate to shell using `support elevate`.
2. Enable Encryption on the Veritas Access cluster.
 - Append the *encrypt* keyword in `contentrouter.cfg` file which is located in the first Veritas Data Deduplication file system. For example:
`/vx/D3_588101/dedupe/etc/puredisk/contentrouter.cfg`.
 - Before appending the *encrypt* keyword, it appears as *ServerOptions=verify_so_references,fast*. After appending the *encrypt* keyword, it appears as *ServerOptions=verify_so_references,fast,encrypt*.
3. Restart the Veritas Data Deduplication services from the Access CLISH.

Support for bandwidth throttling during duplication

Veritas Data Deduplication supports bandwidth throttling during duplication.

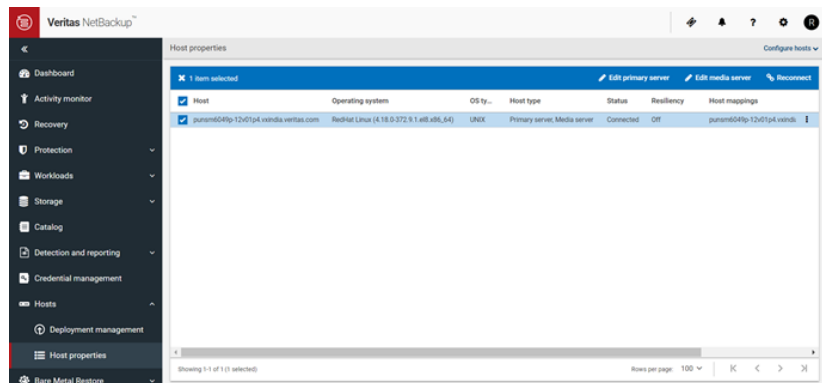
For more details, see https://www.veritas.com/support/en_US/article.100037976

Support for NetBackup Auto Image Replication

You can use the NetBackup Auto Image Replication (AIR) feature to replicate from one media to another media with Veritas Data Deduplication storage: You have to create a trust relationship between two NetBackup primary/media servers to configure NetBackup AIR.

To set up trust between NetBackup primary servers

- 1 Log on to the NetBackup primary server (*NBU1*) from the web UI.
- 2 Navigate to **Hosts > Host properties**. Select the **Edit primary server** tab.



- 3 Click on **Servers > Trusted primary servers**. Click **Add**. Provide the target NetBackup primary server (*NBU2*) FQDN. Click on the **Validate Certificate Authority** option.

Add trusted primary server [X]

When you establish trust between two primary servers, it allows the servers to securely communicate and perform replication operations.
Note: A trusted primary server is not required to be added for Isolated Recovery Environment.

Trusted primary server *

punsm6049p-12v01p2.vxindia.veritas.com

The primary server must be at NetBackup 8.1 or later.

[Validate Certificate Authority]

[Cancel] [Create trust]

- 4 After verifying the CA fingerprint, click **Next**.

- 5 Generate token on the target NetBackup primary server (*NBU2*) and use it for authentication. Or, you can specify the target NetBackup primary server (*NBU2*) credentials for authentication. Click on **Create trust**. The NetBackup primary server (*NBU2*) is listed in the **Trusted primary servers** tab.

Add trusted primary server
✕

Validate Certificate Authority

The primary server must be at NetBackup 8.1 or later.

☐ Specify authentication token of the trusted primary server

☒ Specify credentials of the trusted primary server

User name *

⚠ For a Windows host, specify the domain name along with the username. For example, domain name\username.

Password *

⚠ Enter the password. If multi-factor authentication is configured for the user on the target host, append the one-time password.

Cancel

Create trust

- 6 Repeat the same steps on the target NetBackup primary server (*NBU2*) to set up trust with the NetBackup primary server (*NBU1*).

To configure storage servers for NetBackup Auto Image replication (AIR)

- 1 Configure the deduplication servers on the Access Appliances (both source and target) for AIR configuration.
- 2 Add storage servers on the target NetBackup primary server (*NBU2*) with the target Access Appliance MSDP server's FQDN and credentials.

- 3** Log on to the target NetBackup primary server (*NBU2*) with the web UI.
Navigate to **Storage > Storage configuration > Add Storage server**.
Configure the storage server, disk pool and STU to complete the storage server configuration on the target.
- 4** Log on to the source NetBackup primary server (*NBU1*) with the web UI.
Navigate to **Storage > Storage configuration > Add Storage server**. Add the storage server.

- 5 While adding the MSDP disk pool, add the replication target. Select the trusted primary server (*NBU2*) and the target storage server.

Add replication targets

Search...

Trusted primary server

☒ punsm6049p-12v01p2.vxindia.ve...

1 Records (1 selected)

Select target storage server

These settings apply only to A.I.R. between NetBackup domains.

Search...

Target storage server	Target volume	Target storage server type
☒ dl365g10p-014v49p3.vxindia.veri...	PureDiskVolume	PureDisk

1 Records (1 selected)

Login credentials for the replication target storage server:

Cancel

Add

Scroll down and provide login credentials for the replication target storage servers. Click **Add**.

Add replication targets

×

Select target storage server

These settings apply only to A.I.R. between NetBackup domains.

Search...

Q

Target storage server	Target volume	Target storage server type
☒ dl365g10p-014v49p3.vxindia.veri...	PureDiskVolume	PureDisk

1 Records (1 selected)

Login credentials for the replication target storage server:

Username *

dedupeuser

Password *

.....

Cancel

Add

6 Review the MSDP pool configuration and click **Finish**.

Disk pool configuration

×

Replication configuration operations continue in the background when this window is closed. You can review the status of these operations on the storage review page.

✓

Configuring the disk pool.

✓

✓

Validating the credentials and configuring replication for storage options

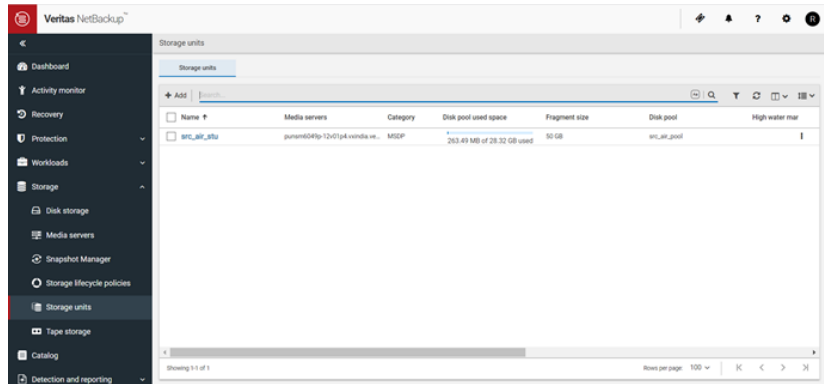
1 of 1 successful

✓

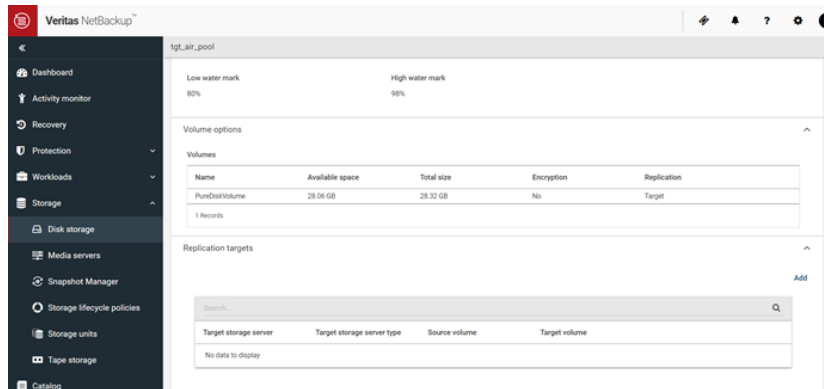
Target storage server: dl365g10p-014v49p3.vxindia.veritas.com

Close

- 7 Create an STU to complete the storage server configuration for the source.



- 8 Rlogin to the target NetBackup primary (*NBU2*) and navigate to the earlier configured disk pool. Click on the disk pool name and navigate to replication target option. Click **Add**.



- 9 Select a trusted primary server (*NBU1*) and storage server. Enter the password for the deduplication service on the storage server.

Add replication targets

Note: A replication target is not required to be added for Isolated Recovery Environment in this window.

Select trusted primary server

Search...

Trusted primary server

☒ punsm6049p-12v01p4.vxindia.ve...

1 Records (1 selected)

Select target storage server

These settings apply only to A.I.R. between NetBackup domains.

Search...

Target storage server	Target volume	Target storage server type
☒ dl365g10p-014v54p1.vxindia.veri...	PureDiskVolume	PureDisk

1 Records (1 selected)

Cancel

Add

Add replication targets

Select target storage server

These settings apply only to A.I.R. between NetBackup domains.

Search...

Target storage server

Target volume

Target storage server type

dl365g10p-014v54p1.vxindia.veri...

PureDiskVolume

PureDisk

1 Records (1 selected)

Login credentials for the replication target storage server:

Username *

dedupeuser

Password *

.....

Cancel

Add

10 Verify that the replication target is added.

Veritas NetBackup™

Dashboard

Activity monitor

Recovery

Protection

Workloads

Storage

Disk storage

Media servers

Snapshot Manager

Storage lifecycle policies

Storage units

Tape storage

Catalog

Detection and reporting

tgair_pool

Low water mark

High water mark

80%

95%

Volume options

Volumes

Name	Available space	Total size	Encryption	Replication
PureDiskVolume	28.06 GB	28.32 GB	No	Target

1 Records

Replication targets

Search...

Target storage server	Target storage server type	Source volume	Target volume
dl365g10p-014v54p1.vxindia.veri...	PureDisk	PureDiskVolume	PureDiskVolume

1

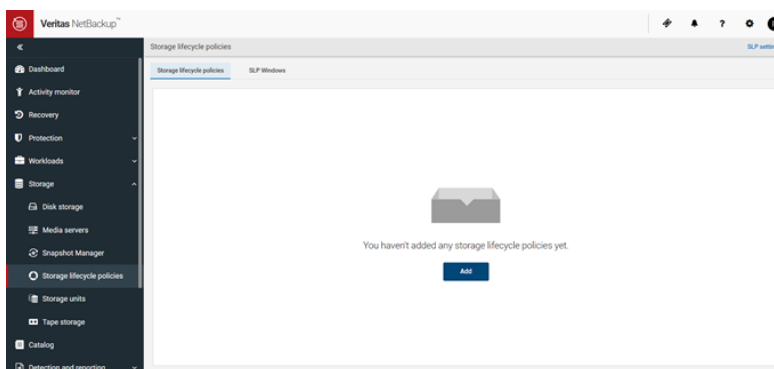
NetBackup AIR process:

1. Backup - This is performed on the originating primary server (source domain, *NBU1*). Clients are backed up according to a backup policy that is indicated by the SLP specified in the Policy storage selection. The SLP must include at least one replication operation to a similar storage in the target domain.

2. Duplication - Images are duplicated to the source domain secondary storage server.
3. Replication - Images are replicated from the source domain to the target domain.
4. Device notifies NetBackup - The storage server in the target domain recognizes that a replication event has occurred. It notifies the NetBackup primary server in the target domain.
5. Import - NetBackup imports the image immediately, based on an SLP that contains an import operation. NetBackup can import the image quickly because the metadata is replicated as part of the image.

To create Storage LifeCycle Policy (SLP) for AIR

- 1 Create SLP Policy (import) on the target: cluster.
 - On the target NetBackup primary (*NBU2*), navigate to **Storage > Storage lifecycle policies**. Click **Add**.



- Provide the SLP name. Click **Add** to add the import operation. Select **Import** from the drop-down. Select the destination storage STU. Click **Create**.

New operation

Properties Window

Source storage: Not applicable

Operation
Import

Destination storage attributes
Destination storage
tgt_all_sfu

Retention
Retention type
Target retention

Import
☐ Override default priority
Operation Priority
A higher number is greater priority.

Advanced

Cancel Create

- Verify the import operation, storage and SLP name. Click **Create**.

Storage Lifecycle Policy

Storage lifecycle policy Validation report

Storage lifecycle policy name
import_SLP

Data classification
No data classification

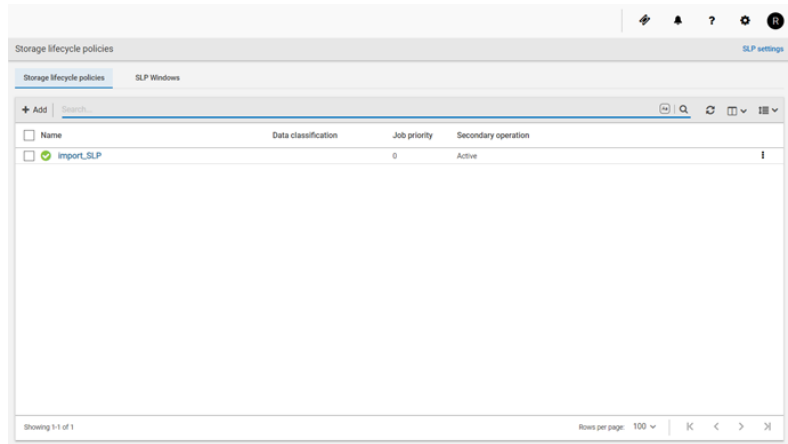
Priority for secondary operations
0
A higher number is greater priority.

+ Add

Operation	Window	Target primary	Storage	Storage type	Volume pool
☐ Import	Default_24x7_Window		tgt_all_sfu	PureDisk	

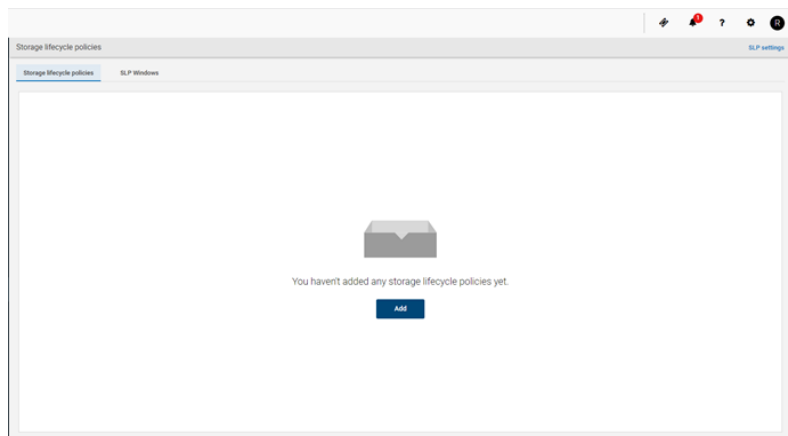
Cancel Create

- Verify that the Import SLP has been added.



2 Create SLP Policy (backup, duplication and replication) on the source NetBackup primary (NBU1):

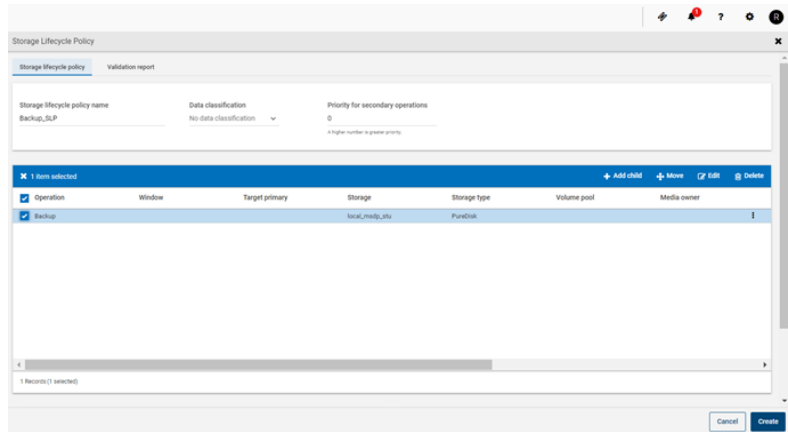
- Log on to the source NetBackup primary (*NBU1*). Navigate to **Storage > Storage lifecycle policies**. Click **Add**.



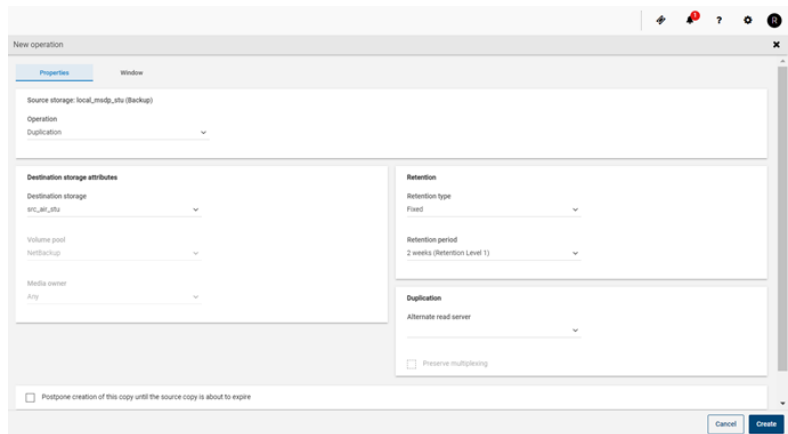
- Provide the SLP name. Click **Add**.

- Select **Backup** from the drop-down. Select the destination storage pool as the local MSDP pool which stores the primary data backup. Provide retention type and retention period. Click **Create**.

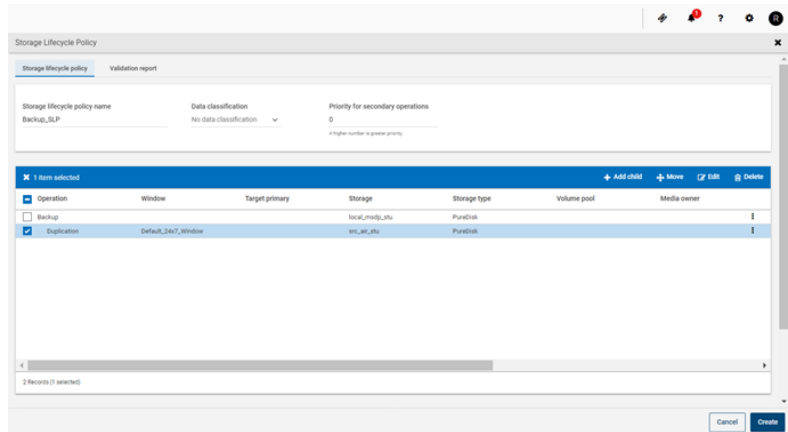
- Select the created backup operation on the SLP window, click on **Add child** to add the duplication operation as a child for backup operation.



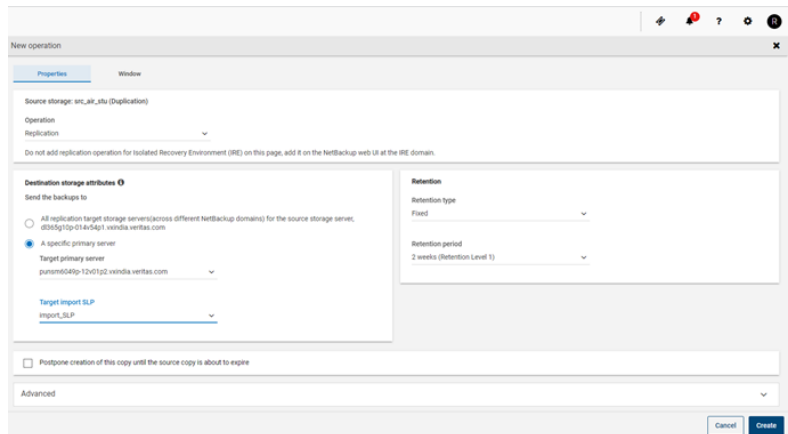
- Set the destination storage attributes.



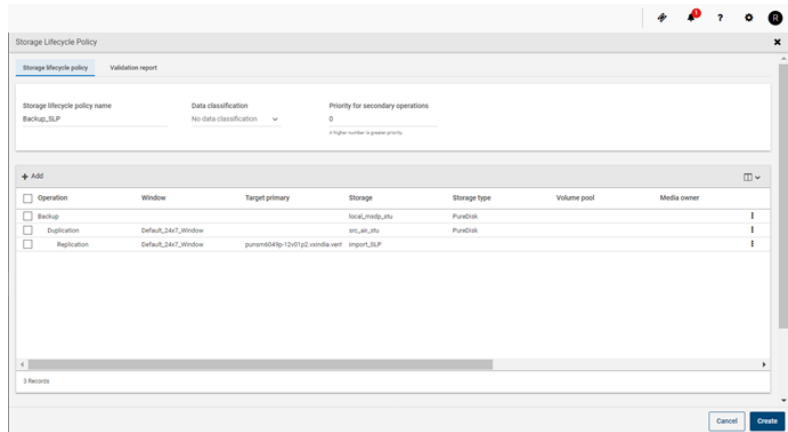
- Select the created duplication operation on the SLP window. Click **Add child** to add the replication operation as a child for duplication operation.



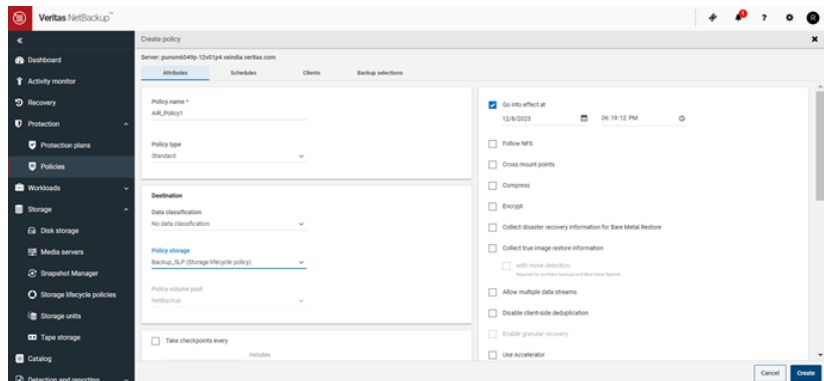
- Set the destination storage attributes. Choose the target primary server and target import SLP policy.



- Verify that the backup, duplication and replication operations are added correctly. Click **Create**.



- 3 On the source NetBackup primary server (*NBU1*), create a policy and select the policy storage as the SLP you created. Configure the policy **Attributes**, **Schedules**, **Clients** and **Backup selections**.



- Run the policy manually. The backup job is responsible for the data backup. The duplication job is responsible for duplicating backed up data on source storage server. The replication job is responsible for the replication of data to the target NetBackup primary server.

Job ID	Type	Client or display name	Job state	Status code	Policy name	Schedule	Schedule type	Elapsed time	State	Active elapsed	Accel
19	Duplication	pernm04lhp12-0719k-vc...	Done	0	SLP_Backup_SLP	Default_24k7...		00:02:04	Done	00:02:04	
18	Backup	pernm04lhp12-0719k-vc...	Done	0	AIR_Policy1	Full backup	Full backup	00:00:10	Done	00:00:10	
17	Backup	pernm04lhp12-0719k-vc...	Done	0	AIR_Policy1	Full backup	Full backup	00:00:12	Done	00:00:12	
16	Duplication	pernm04lhp12-0719k-vc...	Done	0	SLP_Backup_SLP	Default_24k7...		00:12:22	Done	00:12:22	
15	Duplication	pernm04lhp12-0719k-vc...	Done	0	SLP_Backup_SLP	Default_24k7...		00:02:04	Done	00:02:04	
14	Backup	pernm04lhp12-0719k-vc...	Done	0	AIR_Policy1	Full backup	Full backup	00:00:10	Done	00:00:10	
13	Backup	pernm04lhp12-0719k-vc...	Done	0	AIR_Policy1	Full backup	Full backup	00:00:13	Done	00:00:13	
12	Duplication	pernm04lhp12-0719k-vc...	Done	0	SLP_Backup_SLP	Default_24k7...		00:02:04	Done	00:02:04	
11	Backup	pernm04lhp12-0719k-vc...	Done	0	AIR_Policy1	Full backup	Full backup	00:00:13	Done	00:00:13	
10	Duplication	pernm04lhp12-0719k-vc...	Done	0	SLP_Backup_SLP	Default_24k7...		00:02:07	Done	00:02:07	
9	Backup	pernm04lhp12-0719k-vc...	Done	0	AIR_Policy1	Full backup	Full backup	00:00:13	Done	00:00:13	
7	Backup	pernm04lhp12-0719k-vc...	Done	0	AIR_Policy1	Full backup	Full backup	00:00:10	Done	00:00:10	
6	Backup	pernm04lhp12-0719k-vc...	Done	0	AIR_Policy1	Full backup	Full backup	00:00:12	Done	00:00:11	
5	Image Cleanup		Partial success	1				00:00:01	Done	00:00:01	
4	Image Cleanup		Partial success	1				00:00:01	Done	00:00:01	
3	Image Cleanup		Partial success	1				00:00:01	Done	00:00:01	
2	Image Cleanup		Partial success	1				00:00:01	Done	00:00:01	
1	Image Cleanup		Partial success	1				00:00:01	Done	00:00:01	

- On the target NetBackup primary server (**NBU2**), verify that the **Activity** monitor lists the import job.

Job ID	Type	Client or display name	Job state	Status code	Policy name	Schedule	Schedule type	Elapsed time	State
7	Import from replica		Done	0	SLP_import_SLP	Default_24k7...		00:00:02	Done
6	Import from replica		Done	0	SLP_import_SLP	Default_24k7...		00:00:03	Done
5	Image Cleanup		Partial success	1				00:00:01	Done
4	Image Cleanup		Partial success	1				00:00:01	Done
3	Image Cleanup		Partial success	1				00:00:01	Done
2	Image Cleanup		Partial success	1				00:00:01	Done
1	Image Cleanup		Partial success	1				00:00:01	Done

Separating the duplication and replication network

You can separate the duplication and replication network by performing an AIR from the source Access Appliance MSDP server to the target Access Appliance MSDP server. With the default configuration, the AIR traffic follows the same network route as the duplication traffic (eth4). You can separate both the traffic by running the following steps on the Access Appliance cluster.

Consider the following scenario:

- The deduplication server is configured on source Access Appliance cluster (*NBU1*) with primary IP as *10.10.10.11* and FQDN as *primary1.access.com*.
- The deduplication server is configured on the target cluster (*NBU2*) with primary IP as *10.10.10.12* and FQDN as *primary2.access.com*.
- The primary IPs are online on device *eth4*.
- The storage server is configured with *primary1.access.com* on (*NBU1*) and *primary2.access.com* on (*NBU1*).
- *10.10.10.13* and *10.10.10.14* are unused IPs with FQDNs as *vip1.access.com* and *vip2.access.com* respectively.

To separate the duplication and replication network

- 1 Log on to source Access Appliance cluster with management console IP.
- 2 On the source cluster, add a virtual IP. Select a device other than the one already used for deduplication of the primary IP.

```
network> ip addr add <virtual_ip> <netmask> [device] [nodename] [fqdns]
```

Example:

```
network> ip addr add 10.10.10.13 255.255.240.0 eth5
```

- 3 Repeat step 2 with the other IP on the target Access Appliance cluster.

Example:

```
network> ip addr add 10.10.10.14 255.255.255.0 eth5
```

- 4 On the source cluster, add a route to the new target virtual IP.

```
network ip route add all <target_vip> 255.255.255.255 via
<source_gateway> dev <device_name> scope=global
```

Where

target_vip	Newly added virtual IP on target Access Appliance cluster.
source_gateway	Gateway IP of the source cluster
device_name	Device on which the newly added virtual IP is present on the source cluster.

Example:

```
network> ip route add all 10.10.10.14 255.255.255.255 via 10.10.10.1
dev eth5
```

- 5 Add the virtual IP to Access Appliance MSDP server on both the source and target cluster with the respectively added virtual IPs.

```
dedupe> addip <virtual_ip>
```

Example:

On the source cluster:

```
dedupe> addip 10.10.10.13
```

On target: cluster:

```
dedupe> addip 10.10.10.14
```

- 6 Add the mapping of the target virtual IP to the target deduplication primary FQDN on the source deduplication instance.

If you have an instance of WORM-enabled Veritas Data Deduplication, run the following command on the source cluster.

```
dedupe> fqdn add <target_vip> <target_primary_fqdn>
```

Where

target_vip	Newly added virtual IP on the target Access Appliance cluster.
target_primary_fqdn	FQDN with which the storage server has been added to the target NetBackup primary server.

Example:

```
dedupe> fqdn add 10.10.10.14 primary2.access.com
```

If the instance of Veritas Data Deduplication is not WORM-enabled, add the IP/FQDN to the /etc/hosts file of each node.

- 7 If you want to replicate from the target cluster to the source cluster, you can perform the same steps on the target cluster with the source cluster IP.

If you have an instance of WORM-enabled Veritas Data Deduplication, run the following command on the target cluster.

```
dedupe> fqdn add 10.10.10.13 primary1.access.com
```

If the instance of Veritas Data Deduplication is not WORM-enabled, add the IP/FQDN to the /etc/hosts file of each node.

Configuring MSDP-C with Access Appliance

This chapter includes the following topics:

- [Starting the Access S3 server and provisioning the S3 bucket](#)
- [Configuring Access S3 bucket with NetBackup MSDP-C](#)

Starting the Access S3 server and provisioning the S3 bucket

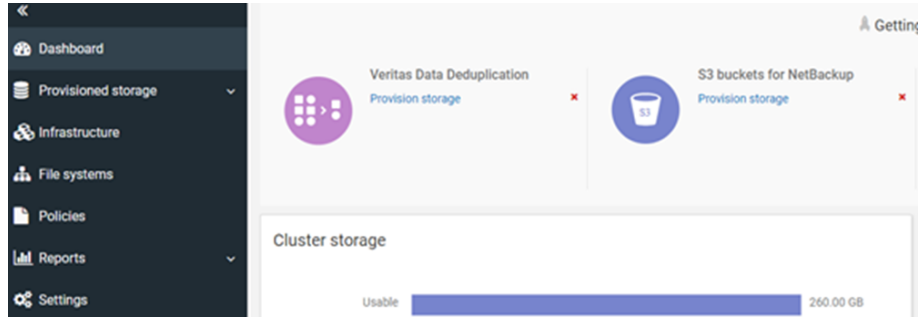
You can use the following procedure to start the S3 server and provision the S3 bucket.

Note: The size of the bucket for MSDP-C should not be more than 1 PiB.

Note: NetBackup bucket with WORM-enabled is only supported with Compliance mode.

To start the S3 server and provision the S3 bucket using the Access GUI

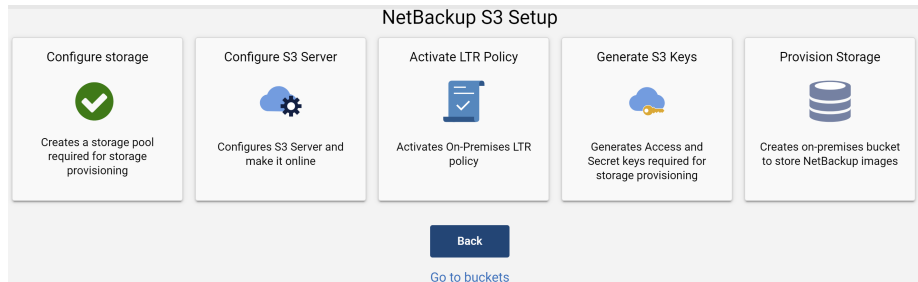
- 1 In **S3 buckets for NetBackup** area, click **Provision storage**.



Or

Navigate to **Quick Actions > Provision Storage > Storage for NetBackup > S3 without cloud**. Click **Next**.

- 2 Click **Configure S3 server**.



- 3 Select the storage pool and click **Start S3 server**. If you want to enable SSL for S3 server. then turn on the **Enable SSL** toggle button.

Start S3 server

This step configures S3 server and make it online. This configuration enables the Veritas Access server to create S3 bucket(s) on-premises. This step will also start the server and bring it online after the default settings are configured.

Select storage pool :

	Storage pool	Total size	Available size
☒	pool_default	250.00 GB	201.50 GB

Items per page: 2 1 - 1 of 1 < >

i Access keys and secret keys should be regenerated if this setting is changed in future.

☐ Enable SSL

Start S3 server

- 4 Click **Activate LTR Policy**.

S3 Setup

Configure storage

✓

Creates a storage pool required for storage provisioning

Configure S3 Server

✓

Configures S3 Server and make it online

Activate LTR Policy

✓

Activates On-Premises LTR policy

Generate S3 Keys

☁

Generates Access and Secret keys required for storage provisioning

Provision Storage

🗄

Creates on-premises bucket to store NetBackup images

Back

- 5 If you want to configure NetBackup MSDP-C on a non-WORM bucket, select **NetBackup LTR S3 Bucket policy** and click **Complete prerequisites**.

If you want to configure NetBackup MSDP-C on a WORM bucket, select **NetBackup LTR S3 Bucket (WORM) policy** and click **Complete prerequisites**.

Select and activate the policy for storage provisioning.

Complete prerequisites

Policy name	Description	Capabilities	Prerequisite
☐ NetBackup LTR S3 bucket	This policy provisions an S3 bucket to store...	Fault Tolerance	✓ Storage pool created
☒ NetBackup LTR S3 Bucket (WORM)	This policy provisions an S3 bucket to store...	Fault Tolerance,WORM	✓ Storage pool created ✓ Enterprise/Compliance mode configured

Items per page: 5 1 - 2 of 2 < >

Activate policy

- 6** For non-WORM use case, select the storage pool. Click **Activate policy**.
 For WORM use case, select the storage pool.

Complete following prerequisite to activate NetBackup LTR S3 Bucket (WORM)

Select storage pool :Selected storage pools:1, total size:201.50 GB

☒	Storage pool ↑	Total size	Available size
☒	pool_default	250.00 GB	201.50 GB

Items per page: 5 1 ~ 1 of 1 < > >>

- 7** Perform this step only for WORM use case. During activation, under **Set WORM**, the minimum and maximum retention period should be left as blank for MSDP-C buckets. This will be applied from NetBackup during configuration. Click **Activate policy**.

Set WORM

Configure the retention time range that Appliance Administrators will be allowed to select from when setting WORM retention time. The minimum retention time you can set is 1 hour and the maximum is 60 years.

Minimum retention time Maximum retention time

0 0 Hours ▾

- 8** Generate S3 keys. You can use any local//AD/LDAP user credentials. Under **Name**, enter the username for which you want to create keys and under **Password**, specify the user password.
 Click on **Generate S3 Keys**.

S3 Setup

Generate S3 access key and secret key.

i You need an access and secret key to access the S3 buckets.

Enter user credentials to generate the keys.

Name *

admin

Password *

Generate S3 Keys

- 9 Note down the access key and secret key.

S3 Setup

Configure storage

Configure S3 Server

Activate LTR Policy

Generate S3 Keys

Provision Storage

Generate S3 access key and secret key.

Generating S3 keys

View details

Save the access key and secret key in a safe location for future use. These keys are required for storage provisioning.

Access key

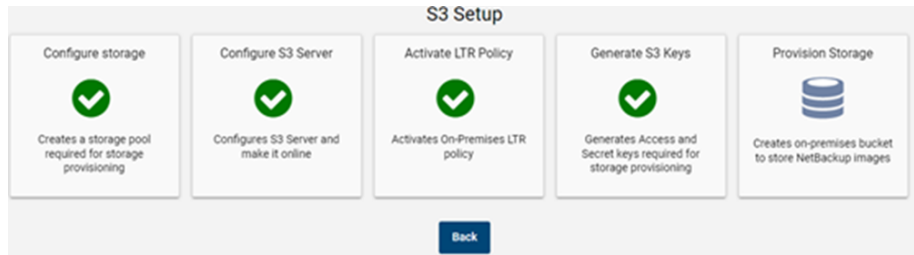
NTM0MDMyMzFIMDZjZml

Secret key

YmRjYmRiZGYxZGNmMTRkMzM4YWE2OTZIMDZjYTU

Finish

10 Click Provision Storage.



11 Select the storage policy according to the activation, set the bucket size as per the requirement, and specify the access and the secret keys.

Provision storage

i This step provides storage to store NetBackup images. You have to enter the access and secret keys created in the previous step.

On-premises storage options

Select storage policy
 NetBackup LTR S3 Bucket (WORM) ▼

Bucket size
 100 GB ▼

Access key

Secret key

Configure storage

Configuring Access S3 bucket with NetBackup MSDP-C

This section describes how to configure an Access S3 bucket with NetBackup MSDP-C.

Pre-requisite to configuring MSDP-C with Access S3 server configured in SSL mode

If Access S3 is started with SSL, perform the following steps to add the Access S3 certificate to the OS trust store of NetBackup media servers:

1. Copy the certificate obtained after running the `objectaccess certificate show` CLISH command to the `s3cert.pem` file. Append the following file with the obtained certificate on the NetBackup servers:

For NetBackup 9.x: `/usr/openv/var/global/wmc/cloud/cacert.pem`

For NetBackup 10.x: `/usr/openv/var/global/cloud/cacert.pem`

2. Run the following commands on the NetBackup primary server:

```
cp s3cert.pem /usr/share/pki/ca-trust-source/anchors/
```

```
update-ca-trust force-enable
```

```
update-ca-trust extract
```

```
update-ca-trust
```

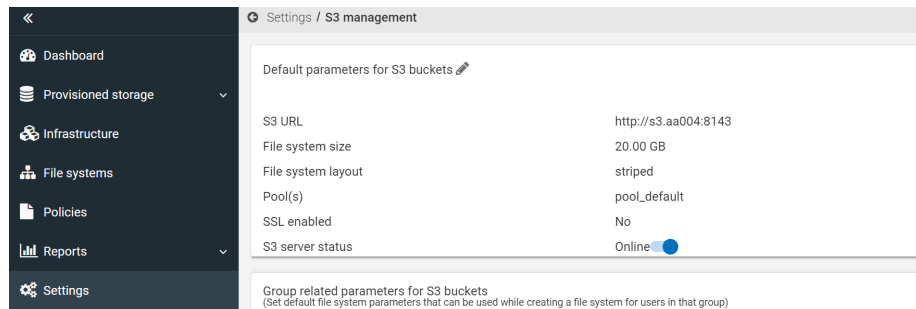
Pre-requisite to configuring MSDP-C with WORM

If you want to configure NetBackup MSDP-C WORM with Access S3 WORM bucket, then you must add the volume to the bucket using the `msdpcloudutil` command from the NetBackup server's bash.

To add volume to the bucket

- 1 Log in to NetBackup primary and set the following environment variables:

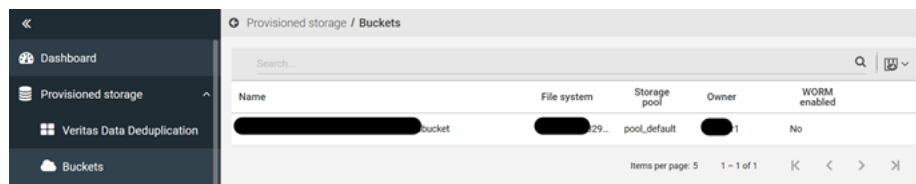
```
export MSDPC_ACCESS_KEY=<access-key>
export MSDPC_SECRET_KEY=<secret-key>
export MSDPC_REGION=us-east-1
export MSDPC_PROVIDER=vtas-access
export MSDPC_ENDPOINT=<endpoint name> (find it from GUI Dashboard.
Go to Settings > S3 management. For example: http://<cluster>:8143)
```



- 2 Run the following command to create a volume. Use the bucket name from the Access Appliance GUI (**Provisioned storage > Buckets**).

```
/usr/openv/pdde/pdcr/bin/msdpclutil create --bucket <bucketname>
--volume <volumename> --mode COMPLIANCE --max <maxdays>
--min <mindays> --live <date>
```

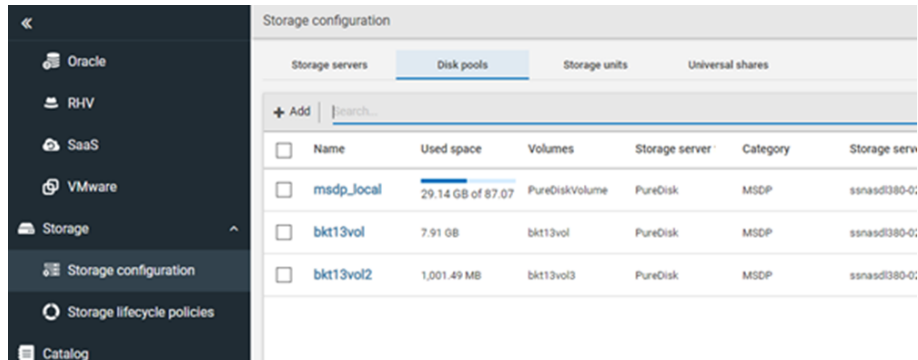
Refer to the `msdpclutil` command's help for more details.



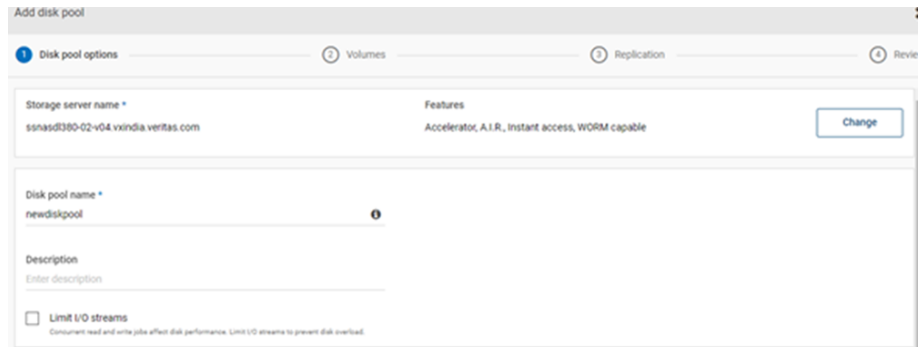
Log in to the NetBackup GUI and perform the following steps to configure MSDP-C with Access S3 bucket, create disk pool and create STU.

To configure MSDP-C with Access S3 bucket

- 1 Go to **Storage > Storage Configuration > Storage servers** and add the MSDP storage server on the NetBackup media server using which you want to configure MSDP-C.
- 2 Go to **Storage > Storage Configuration > Disk pools** and add a new pool.



- 3 Select a storage server and enter the name of pool and click **Next**.



4 Select **Add volume**.

For MSDP-C with WORM use case, enter the volume name which was provided as part of `msdpclldutil` command during S3 configuration.

For MSDP-C with non-WORM use case, you can enter any volume name.

Volume

Add volume

Volume name *

testvol

5 Under **Select cloud storage provider**, search for Veritas Access.

Select cloud storage provider

1 item selected

Cloud storage provider	Description	Storage API type
☐ Microsoft Azure	Microsoft Azure Storage Service	Azure
☐ Microsoft Azure Government	Microsoft Azure Storage Service	Azure
☐ NetBackup Recovery Vault Azure	NetBackup Recovery Vault Azure Storage Service	Azure
☐ NetBackup Recovery Vault Azure Government	NetBackup Recovery Vault Azure Storage Service	Azure
☒ Veritas Access	Veritas Access Scale-out software-defined storage	S3

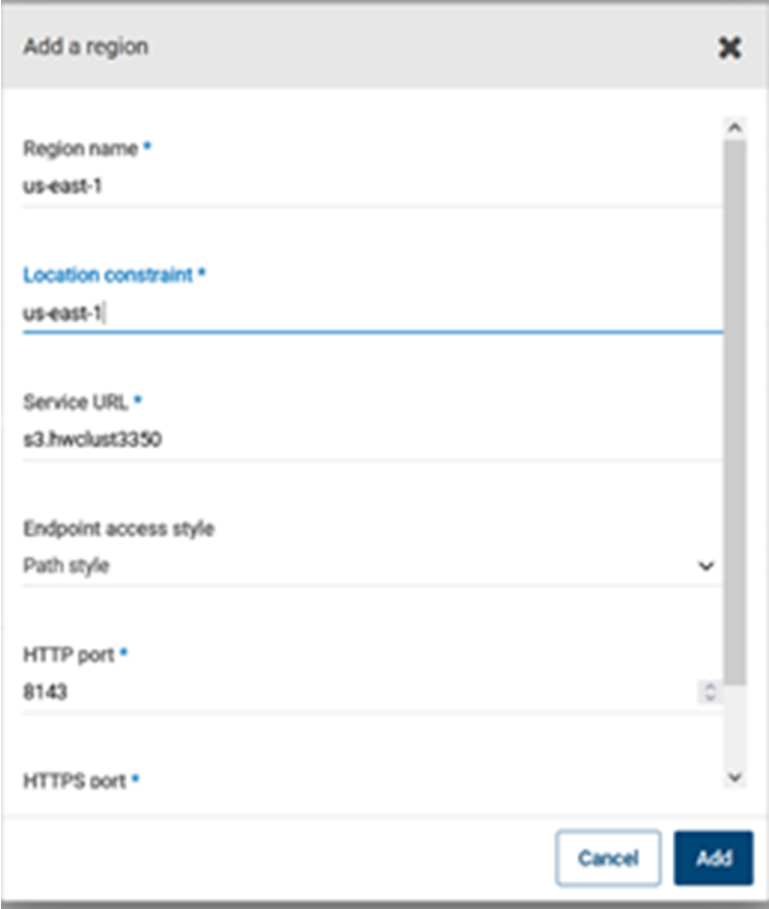
5 Records (1 selected)

Cancel

Select

- 6 Add **Region name** and **Location Constraint** as *us-east-1*. Service URL should be endpoint name (<http://<cluster>:8143>). Note that the endpoint name refers to only the *<cluster>* part listed in the URL and not the entire URL.

You can find the Access S3 endpoint URL by running the `objectaccess show` command from the Access CLISH. Specify the HTTP and HTTPS port number which is mentioned in S3 endpoint URL. Click **Add** to proceed.



The screenshot shows a dialog box titled "Add a region" with a close button (X) in the top right corner. The dialog contains the following fields and values:

- Region name ***: us-east-1
- Location constraint ***: us-east-1
- Service URL ***: s3.hwclust3350
- Endpoint access style**: Path style (with a dropdown arrow)
- HTTP port ***: 8143
- HTTPS port ***: (empty)

At the bottom right of the dialog, there are two buttons: "Cancel" and "Add". The "Add" button is highlighted in blue.

7 Add access key and secret key.

Access details for the account

Access key ID *

NDvjMTlmAGUSNzBhMDQ

Secret access key *

.....

Advanced settings

Security

☐ Use SSL

Proxy

☐ Use proxy server

8 Uncheck the **Use SSL** option, if Access S3 server is configured on HTTP. If Access S3 server is configured with SSL/HTTPS then select the **Use SSL** option with **Authentication and data transfer**.

Security

☒ Use SSL

☐ Authentication only

☒ Authentication and data transfer

☐ Check certificate revocation (IPv6 not supported for this option)

- 9 You can either enter an existing bucket name or select a cloud bucket by clicking **Retrieve list**. Click **Next**.

Cloud buckets

☒ Enter an existing cloud bucket name

Cloud bucket name
 88c143b8-7917-4aeb-86cf-8a008d01a1des3bucket

☐ Select or create a cloud bucket

☒ Select or create a cloud bucket

Complete all required fields to view available cloud buckets.

Retrieve list

- 10 Skip the addition of replication target by clicking **Next**.

Add MSDP disk pool

✓ Disk pool options ✓ Volumes 3 Replication 4 Review

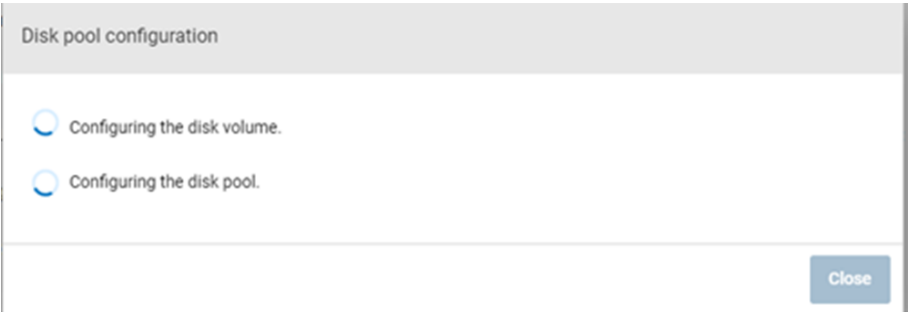
You have not added any replication targets

Add

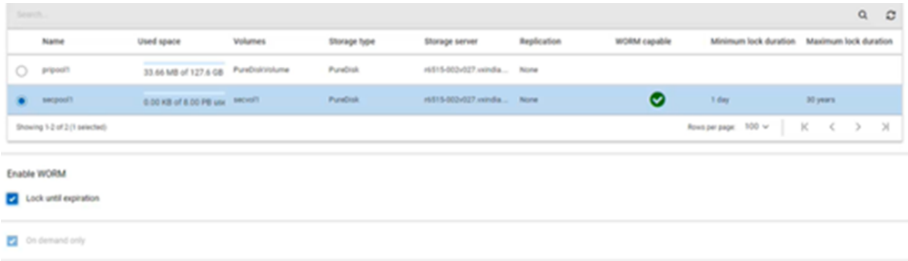
Activate Windows
 Go to Settings to activate Windows.

Cancel Previous Next

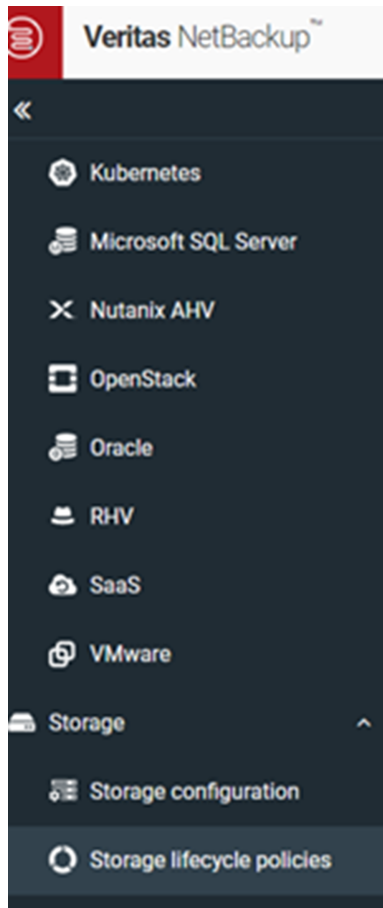
- 11
- Review the configuration and click **Finish**. The disk volume and disk pool will get configured.



- 12
- Go to **Add storage unit** and select the created pool. For MSDP-C with WORM use case, check the **Lock until expiration** option to enable WORM.



- 13 Create storage lifecycle policies. Go to **Storage > Storage lifecycle policies**.

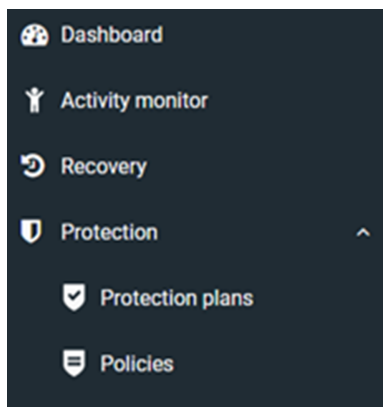


- 14 Add Storage lifecycle policy (SLP) with backup on the primary STU and deduplication on the secondary STU (the STU which is configured with MSDP-C).

For MSDP-C with WORM use case, the retention period selected should be between the maximum and minimum value given while configuring the volume using the `msdpclutil` command.

The screenshot shows the 'New operation' dialog box with the 'Properties' tab selected. The 'Source storage: pri0stuf (Backup)' is listed at the top. Below it, the 'Operation' is set to 'Duplication'. The 'Destination storage attributes' section includes 'Destination storage' (secstuf1), 'Volume pool' (netbackup), and 'Media owner' (Any). The 'Retention' section shows 'Retention type' as 'Fixed' and 'Retention period' as '2 weeks (Retention Level 1)'. The 'Duplication' section has 'Alternate read server' set to a dropdown menu. At the bottom, there is a 'Preserve multiplexing' checkbox.

- 15 After defining the SLP, create a policy to perform backup. Go to **Protection > Policies**.



- 16 Add a policy name. Under **Policy storage**, select the SLP created in the previous step.

Attributes

Schedules

Clients

Backup selections

Policy name

policy1

Policy type

Standard

Destination

Data classification

No data classification

Policy storage

slp1 (Storage lifecycle policy)

Policy volume pool

- 17 Go to **Schedules** to create automatic schedules.

Attributes

Start window

Exclude dates

Name *

full

Type of backup *

Full Backup

☐ Synthetic backup

☐ Accelerator forced rescan

Destination

☐ Multiple copies

☐ Override policy storage selection

slp1 (Storage lifecycle policy)

Schedule type

☐ Calendar

☐ Retries allowed after the run day

☒ Frequency

10

hours

Retention *

Determined by SLP

Cancel

Add

18 Add the client.

Add client - Policy pol1

Server

r6515-002v027.vxindia.veritas.com

Client name

r6515-002v027.vxindia.veritas.com

☒ Detect client operating system

Hardware and operating system

HP-UX-IA64, HP-UX11.31

Cancel

Add

- 19
- In the **Add backup selection** dialog box, select the file or directory that needs to be backed up.

Add backup selection

Server

ssnasdl380-02-v03.vxindia.veritas.com

Construct a list of pathnames (and directives, if applicable) to add to the selection list.

Pathname or directive

List of pathnames and directives to add to the selection list.

/data

Cancel

Add

20

Click **Create**.

21

Activate the policy.

Dashboard

Activity monitor

Recovery

Protection

Protection plans

Policies

Workloads

Cloud

Policies

+ Add

Search

	Name	Type	Data classification	Storage	Volume paths	Media owner	Checkpoint interval (min)	Job Policy	Priority	
☐	pol1	Standard		s3	netbackup	any	0	0	0	

Edit

Copy policy

Delete

Activate

Internal backup

Migrating the NetBackup images from existing storage to Veritas Access storage

This chapter includes the following topics:

- [Migrating NetBackup images from CloudCatalyst/S3/MSDP-C to Veritas Data Deduplication storage](#)
- [Migrating the NetBackup images from the Veritas Data Deduplication STU to the MSDP-C STU](#)

Migrating NetBackup images from CloudCatalyst/S3/MSDP-C to Veritas Data Deduplication storage

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

Table 5-1

When CloudCatalyst is configured as the secondary/LTR storage in the NetBackup policy

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

Table 5-1 (continued)

When CloudCatalyst is configured as the primary storage in the NetBackup policy	To migrate the NetBackup images from the CloudCatalyst STU to the Veritas Data Deduplication STU when CloudCatalyst is configured as the primary storage in the NetBackup policy
When S3 is configured as the primary storage in the NetBackup policy	To migrate the NetBackup images from the S3 STU to the Veritas Data Deduplication STU when S3 is configured as the primary storage in the NetBackup policy
If you want to migrate the NetBackup images from the MSDP-C STU to the Veritas Data Deduplication STU	To migrate the NetBackup images from the MSDP-C STU to the Veritas Data Deduplication STU

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

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

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

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

- 1 Configure the Veritas Data Deduplication STU.
- 2 Change the SLP to point to the Veritas Data Deduplication STU instead of the CloudCatalyst STU so that the new images get created on the Veritas Data Deduplication STU.
- 3 As optimized duplication from CloudCatalyst to Veritas Data Deduplication is not supported, the administrator is required to add the `RESUME_ORIG_DUP_ON_OPT_DUP_FAIL = TRUE` flag in the `/usr/openv/netbackup/bp.conf` file of both the primary and media server.
- 4 Go to the **NetBackup Management > Catalog** and select the **Action as Duplicate** from the drop-down menu.
- 5 In the **NetBackup Management > Catalog**, right-click on the image that is stored on the CloudCatalyst STU and that you want to duplicate on the Veritas Data Deduplication STU. Select **Duplicate**.
- 6 In the pop-up window that appears, select the Veritas Data Deduplication STU and click **OK**.
- 7 In the confirmation screen, click **OK** to start duplication.
You can check the progress of the image duplication in the **NetBackup Activity Monitor**.
- 8 After the completion of duplication, the status of the duplication job appears as **The requested operation was partially successful**. In the job detail status, some error messages appear that are expected.
- 9 After duplication is complete, expire the backup image stored on the CloudCatalyst STU.

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

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

To migrate the NetBackup images from the MSDP-C STU to the Veritas Data Deduplication STU

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

Migrating the NetBackup images from the Veritas Data Deduplication STU to the MSDP-C STU

You can migrate the NetBackup images from the Veritas Data Deduplication STU to the MSDP-C STU.

To migrate the NetBackup images from the Veritas Data Deduplication STU to the MSDP-C STU which is configured on bucket of Veritas Access Objectaccess server

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

Configuring Access Appliance with the NetBackup client

This chapter includes the following topics:

- [Configuring Access Appliance for NetBackup client](#)
- [Installing the NetBackup client add-on packages](#)
- [Prerequisites for configuring the NetBackup client](#)
- [Configuring the NetBackup client](#)
- [Adding an optional media server](#)
- [Adding multiple primary servers](#)
- [Adding file systems to the backup configuration](#)
- [Removing file systems from backup configuration](#)
- [Changing the virtual IP address used by the NetBackup client](#)
- [Upgrade the NetBackup client](#)
- [Unconfiguring the NetBackup client](#)
- [Enabling Veritas Data Deduplication catalog backup with NetBackup client](#)
- [Disabling Veritas Data Deduplication catalog backup from NetBackup client](#)
- [Displaying the status of NetBackup services](#)

- [Configuring backup operations using NetBackup or other third-party backup applications](#)
- [Restoring filesystems backed up with NetBackup client](#)

Configuring Access Appliance for NetBackup client

Access Appliance 8.0 supports NetBackup client versions 8.1.2.1, 8.2, 9.0, 9.0.0.1, 9.1, and 10.0.

Certificates are deployed as a part of the NetBackup client configuration to enable secure communication between NetBackup primary and NetBackup client to perform backup and restore related operations successfully.

To back up your data present on filesystems which are present on Access Appliance with NetBackup, you must register the installed and configured NetBackup primary server with Access Appliance.

To configure NetBackup Client for Access Appliance, perform the following tasks in the following order:

Table 6-1 Workflow for configuring the NetBackup client

Task	Details
Make sure that the prerequisites are met.	See “Prerequisites for configuring the NetBackup client” on page 120.
Configure the NetBackup client.	See “Configuring the NetBackup client” on page 120.
Add an optional media server.	See “Adding an optional media server” on page 121.
Add multiple primary servers.	See “Adding multiple primary servers” on page 122.
Add file systems for backup.	See “Adding file systems to the backup configuration” on page 123.

You can also perform the following tasks:

Table 6-2 Other operations that you can perform on the NetBackup client

Task	Details
Unconfigure the NetBackup client.	See “Unconfiguring the NetBackup client” on page 125.

Table 6-2 Other operations that you can perform on the NetBackup client
(continued)

Task	Details
Remove file systems from backup configuration.	See “Removing file systems from backup configuration” on page 123.
Change the virtual IP address used by NetBackup client.	See “Changing the virtual IP address used by the NetBackup client” on page 124.
Upgrade the NetBackup client.	See “Upgrade the NetBackup client” on page 124.
Enable Veritas Data Deduplication catalog backup with NetBackup client.	See “Enabling Veritas Data Deduplication catalog backup with NetBackup client” on page 125.
Disable Veritas Data Deduplication catalog backup with NetBackup client.	See “Disabling Veritas Data Deduplication catalog backup from NetBackup client” on page 128.
Remove file systems from backup configuration.	See “Removing file systems from backup configuration” on page 123.
Display the current status of the NetBackup client.	See “Displaying the status of NetBackup services” on page 129.
Verify that Access Appliance is configured with the NetBackup client.	See “Displaying the status of NetBackup services” on page 129.

If Access Appliance 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 running the `bpgetconfig` command.

```
# bpgetconfig
IP_ADDRESS_FAMILY = AF_UNSPEC
```

- Restart the services after making this change.

Installing the NetBackup client add-on packages

The supported NetBackup clients can be installed as add-on packages.

Considerations while installing the NetBackup client add-on packages:

- If the nodes are configured in the cluster, the NetBackup client add-on packages are installed on both nodes.
- If the nodes are not configured in the cluster, you have to download and install the NetBackup client add-on packages on both the nodes.
- To create a file system, refer the section *Creating a file system* section in the *Access Appliance Administrator's Guide* on [SORT](#). The file system used for the NetBackup client configuration should be a minimum of 10 GB with a 5-way striped layout. The client configuration uses 1 GB or less of space of the file system, and the remaining space is used for NetBackup Accelerator track logs. The NetBackup file system is used to store NetBackup client configuration and NetBackup Accelerator track logs. You can grow the file system as per your requirement.
- The virtual IP should be pingable and online. You can check the status of the virtual IP using the `network ip addr show` command.

To install the add-on packages

- 1 Download the add-on packages for the NetBackup client from the Download Centre:
 - VRTSaccess-app-ADDON-NBUClient-8.1.2.1-1.0.1-1.x86_64.rpm
 - VRTSaccess-app-ADDON-NBUClient-8.2-1.0.1-1.x86_64.rpm
 - VRTSaccess-app-ADDON-NBUClient-9.0-1.0.1-1.x86_64.rpm
 - VRTSaccess-app-ADDON-NBUClient-9.0.0.1-1.0.1-1.x86_64.rpm
 - VRTSaccess-app-ADDON-NBUClient-9.1-1.0.1-1.x86_64.rpm
 - VRTSaccess-app-ADDON-NBUClient-10.0-1.0.1-1.x86_64.rpm
- 2 Go to the Appliance CLISH. Navigate to **System > Software > Share Open**.
- 3 Mount the path specified as a part of the `share open` command on NFS or CIFS client.
- 4 Copy the add-on packages to the `/inst/patch/appliance/available/` folder using NFS or CIFS.

For more details, see the *Downloading software updates to an Access appliance node using a client share* section in the *Veritas Access Appliance Upgrade Guide*.

- 5 In the Appliance CLISH, navigate to **System > Software > Downloaded** to confirm that the add-on packages are downloaded successfully.

- 6 Navigate to **System > Software > Install update** *update-name=<add-on pkg name>* to install the package.
- 7 Navigate to **System > Software > Installed-addons** to confirm that the package has been installed.
- 8 Navigate to **System > Software > Share close** to close the shares.

To remove the add-on packages

- 1 Go to the Appliance CLISH. Navigate to **System > Software > Rollback-update** *update-name=<pkg name>* to uninstall the packages.
- 2 Navigate to **System > Software > Installed-addons** to confirm that the package has been removed.

Prerequisites for configuring the NetBackup client

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

- Add the valid licenses on the NetBackup primary server.
- Make sure that host names of the primary server and the NetBackup client installed on Access Appliance can be resolved and the reverse lookup is working.
- The file system used for the NetBackup client configuration should be a minimum of 10 GB with a 5-way striped layout. The client configuration uses 1 GB or less of space of the file system, and the remaining space is used for NetBackup Accelerator track logs. The size of the file system must be decided based on the the backup policies that have been created. See https://www.veritas.com/support/en_US/article.100045746 for more details.

Configuring the NetBackup client

The `backup config` CLISH command configures the specified version of the NetBackup client. The NetBackup client version must be 8.1 or higher. Required certificates are generated as part of this command.

To configure the NetBackup client

- ◆ Configure the NetBackup client.

```
Backup> config <virtual_name> <virtual_IP> fs_name  
client_version auth_token primary_server_name [primary_server_ip]
```

virtual_name	Hostname to be used by a NetBackup client configuration on the nodes. Make sure that name can be resolved through DNS and its IP address can be resolved back to name through a DNS reverse lookup. Also make sure that name resolves to the IP address parameter <i>ipaddr</i> that is provided for configuration.
virtual_IP	Virtual IP address to be used by the NetBackup client configuration on the nodes. Make sure that IP address can be resolved back to the name we use for configuration.
fs_name	Name of the file system used to store NetBackup client configuration.
client_version	NetBackup client version to be installed.
auth_token	Authentication token from NetBackup primary server to enable backup/restore in a secure environment.
primary_server_name	FQDN of the primary server
primary_ip	IP of the server to be used as the NetBackup primary server. Specify this parameter if DNS is not configured in the cluster. This is an optional parameter.

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

Adding an optional media server

You can optionally add a media server to be used by the NetBackup client. If the media server name is not added, the local NetBackup client uses the NetBackup primary server as the NetBackup media server. But it is not mandatory that the NetBackup primary server be the NetBackup media server. In production environments, the NetBackup media server is separate from the NetBackup primary server.

To add an optional NetBackup media server

- ◆ Add an optional NetBackup media server.

```
Backup> netbackup media-server add media_server_name
[media_server_IP]
```

For example:

```
Backup> netbackup media-server add FQDN_of_primary_server
```

Make sure that the server hostname can be resolved through DNS, and its IP address can be resolved back to the NetBackup media server hostname through the DNS reverse lookup. If DNS is not configured in the cluster, specify the *media_server_IP* in the `/etc/hosts` file of all nodes of the cluster. to create a mapping between the server hostname and its IP address.

You can also delete an already configured NetBackup media server.

To delete an already configured NetBackup media server

- ◆ Delete an already configured NetBackup media server.

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

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

Adding multiple primary servers

The NetBackup primary server is registered with Access Appliance during NetBackup client configuration so that it can communicate with the Access Appliance. If necessary, you can add multiple primary servers with the same NetBackup client.

To add an additional NetBackup primary server

- ◆ Add an additional new NetBackup primary server to the existing client configuration. Required certificates of the new primary server are generated as part of this command.

```
Backup> netbackup primary-server add auth_token primary_server
[primary_ip]
```

<code>primary_server</code>	FQDN of the primary server
<code>auth_token</code>	Authorization token to generate th host ID based certificates
<code>primary_ip</code>	IP address of the primary server. This is optional field when the primary server is not resolvable to the FQDN,

To delete a NetBackup primary server

- ◆ Remove a primary server from the existing client configuration.

```
Backup> netbackup primary-server del primary_server
```

where *primary_server* is the FQDN of the primary server.

CA and host ID certificates for the specified primary server is deleted and its associated entry from the configuration files also removed.

See the `backup` man page `fs` module for detailed examples.

Adding file systems to the backup configuration

You can add the file systems required to be backed up with the NetBackup client. Once the file system is configured for backup, it is available for backup and restore operation from NetBackup primary server side.

To add file systems for backup

- ◆ Add the file system to the NetBackup client configuration to enable backup and restore operations from NetBackup primary server.

```
Backup> fs add fs_name
```

See the `backup` man page `fs` module for detailed examples.

Removing file systems from backup configuration

You can remove the file system from the NetBackup client configuration. Once the file system is removed from the backup configuration, it is not available for backup and restore operations from NetBackup primary server side.

To remove the file systems for backup

- ◆ Remove the file system from the NetBackup client configuration.

```
Backup> fs remove fs_name
```

See the `backup` man page `fs` module for detailed examples.

Changing the virtual IP address used by the NetBackup client

You can alter the virtual IP address of the NetBackup client. This address is a highly-available virtual IP address in the cluster.

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

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

To change the virtual IP address used by NetBackup

- ◆ Configure the virtual IP address of NetBackup on Access Appliance.

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

This command configures the built-in NetBackup client to use *ipaddr* as its virtual IP address and *device* as the network interface. A network mask can be provided with the IP address as the prefix length for the *ipaddr*.

Ensure that the NetBackup primary server is able to resolve the NetBackup client's FQDN to the new IP.

Upgrade the NetBackup client

You can upgrade the NetBackup client on your appliance by specifying the version. Ensure that the client image version that is specified is pre-installed on the cluster. Also, the version to be installed must be higher than the already configured version. Download the Add-Ons before you begin the upgrade operation.

To upgrade the NetBackup client to a specified version

- ◆ Upgrade the NetBackup client on the appliance by specifying the version.

```
Backup> upgrade <version>
```

Unconfiguring the NetBackup client

The `backup unconfig` command removes the existing NetBackup client configuration.

To unconfigure the NetBackup client

- ◆ Removes the NetBackup client configuration for the client,

```
Backup> unconfig
```

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

Enabling Veritas Data Deduplication catalog backup with NetBackup client

You can configure the built-in NetBackup client to perform a backup and restore of the deduplication catalog.

To enable the Veritas Data Deduplication catalog backup with NetBackup client

- 1 Enable the NetBackup client to perform a backup and restore of the deduplication catalog.

```
Backup> dedupe-catalog enable
```

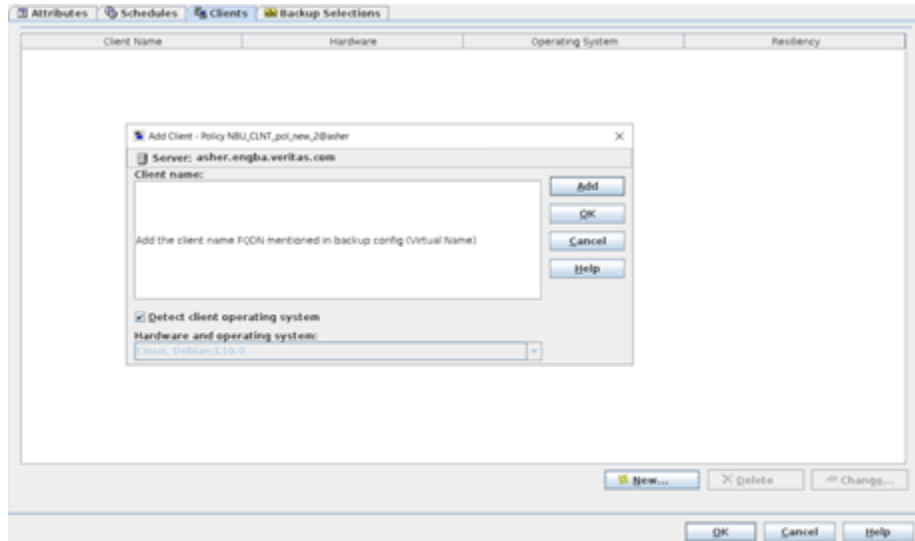
- 2 Create a new policy. Navigate to the **Attributes** tab, select *MSDP local STU* (*Storage unit*) in **Policy storage** drop-down. You have to create a local STU as data is written to the media server.

Note: During policy creation, you must select the **Policy Type** as Standard and also select the **Cross Mount Point** check box for successful backup operation.

The screenshot shows the 'Attributes' tab of the NetBackup Policy Attributes dialog box. The 'Policy type' is set to 'Standard'. The 'Destination' is set to '<No data classification>'. The 'Policy storage' is set to 'new_local_stu'. The 'Policy volume pool' is set to 'NetBackup'. The 'Take checkpoints every' is set to '0' minutes. The 'Limit jobs per policy' is set to '1'. The 'Job priority' is set to '0'. The 'Media Owner' is set to 'Any'. The 'Snapshot Client and Replication Director' section is expanded, showing 'Perform block level incremental backups', 'Use Replication Director', 'Enable vendor change tracking for incremental backups', 'Perform snapshot backups', 'Retain snapshot for Instant Recovery or SLP management', 'Hyper-V server', and 'Perform off-host backup'. The 'Microsoft Exchange Server Attributes' section is expanded, showing 'Exchange DAG or Exchange 2007 replication (LCR/CCR)', 'Database backup source', 'Preferred server list...', and 'Dynamic Data Streaming Attributes'. The 'Dynamic Data Streaming Attributes' section is expanded, showing 'Allow Dynamic Streaming', 'Maximum number of streams per volume' set to '4', and 'Maximum number of files in a batch' set to '300'. The 'Go into effect at' date is set to 'Jul 20, 2023 9:31:07 AM'. The 'Cross mount points' checkbox is checked. The 'Compress' and 'Encrypt' checkboxes are unchecked. The 'Collect disaster recovery information for' section is expanded, showing 'Bare Metal Restore', 'Collect True Image Restore information', 'with move detection', 'Allow multiple data streams', 'Disable client-side deduplication', 'Enable granular recovery', 'Use Accelerator', and 'Enable optimized backup of Windows deduplicated volumes'. The 'Keyword phrase (optional)' field is empty. The 'OK', 'Cancel', and 'Help' buttons are at the bottom right.

- 3 Navigate to the **Schedules** tab and create a new schedule as per your requirement.

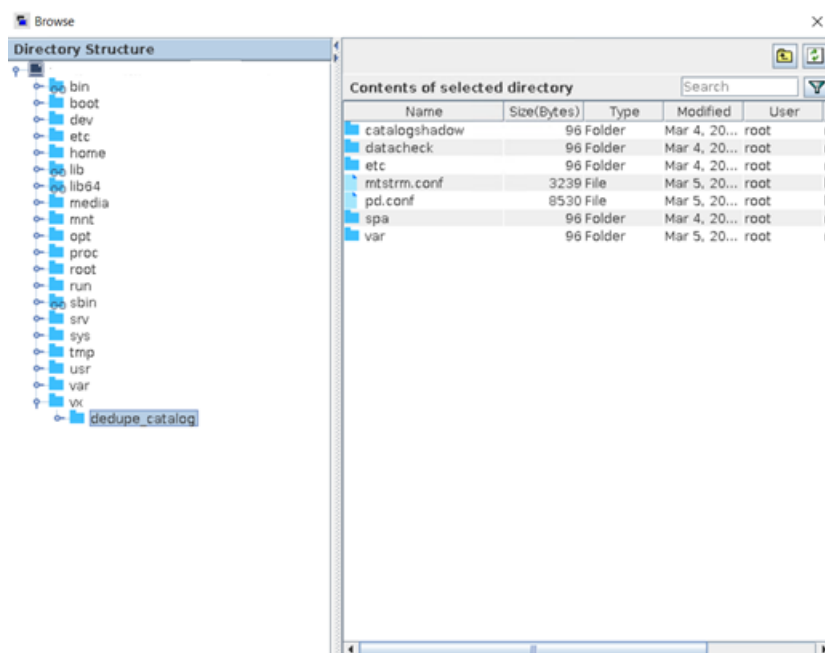
- 4 Navigate to the **Clients** tab. Click **New** and add the client name (FQDN) which is mentioned during backup configuration (Virtual Name). Select the check box **Detect client operating system** and click **OK**.



- 5 Navigate to the **Backup Selection** tab. Click **Browse**.

Double click on the `vx` folder. Select the `dedupe_catalog` folder. The list of all the files and directories which are to be backed up appears. Click **OK**.

Note: When you run the `dedupe-catalog enable` command from CLISH, all the catalog files and folders that are required for back up are automatically added to the `dedupe_catalog` folder. You need not select any files manually.



- 6 Run the policy manually or as per schedule.

Disabling Veritas Data Deduplication catalog backup from NetBackup client

You can disable the NetBackup client from performing a backup and restore of the deduplication catalog.

To disable the Veritas Data Deduplication catalog backup from the NetBackup client

- ◆ Disable Veritas Data Deduplication catalog backup from the NetBackup client.

```
Backup> dedupe-catalog disable
```

Displaying the status of NetBackup services

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

See the following man pages for detailed examples:

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

To display NetBackup services

- ◆ Display the current NetBackup services.

```
Backup> show
```

If the settings were configured while the backup and the restore services were online, run the `backup stop` command followed by the `backup start` command to make the changes come into effect.

To display the status of backup services

- ◆ Display the status of backup services.

```
Backup> status
```

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

To start or stop backup services

- 1 Start the backup services.

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

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

- 2 Stop the backup services.

```
Backup> stop
```

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

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

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

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

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

Restoring filesystems backed up with NetBackup client

This section describes how you can restore filesystems (which are backed up using the NetBackup client) that get corrupted in the Access Appliance environment.

You can backup a filesystem with the NetBackup client using the `backup fs add` command. The backup of the filesystem is created on the NetBackup media server. If the filesystem goes corrupt and is destroyed, you can restore the filesystem.

To restore a corrupted filesystem

- 1 Create a new filesystem. You can use the same name as that of the existing filesystem if a filesystem with that name is no longer present, else use a different name.
- 2 Add the filesystem back to the NetBackup client's backup filesystem configuration using the `backup fs add fs_name` command.
- 3 Restore the data backed up from the filesystem to the respective path on the new filesystem.

To restore the MSDP catalog filesystem

- ◆ Restore the MSDP catalog filesystem.

If the NetBackup client is enabled with deduplication catalog backup and the catalog filesystem goes corrupt, you will need to format the catalog filesystem.

- Disable the catalog backup.

```
backup> dedupe-catalog disable
```

- Format the catalog filesystem or re-create it with the same name.
- Add the catalog filesystem as a backup filesystem.

```
backup> fs add fs_name
```

- From the deduplication catalog backup, restore the content that was backed up to `/vx/<catalog_fs>/dedupe/databases` by selecting **Restore to a different location** on the NetBackup primary.
- Enable the deduplication catalog to continue backing up the deduplication catalog.

```
backup> dedupe-catalog enable
```

Note: In case the MSDP catalog filesystem is destroyed, ensure that a new filesystem is created with same name as the old MSDP catalog filesystem. You can then follow the steps to add, restore and enable the catalog filesystem.

Troubleshooting

This chapter includes the following topics:

- [Additional resources](#)
- [Generating Access Appliance S3 server keys using the helper script](#)

Additional resources

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

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

Generating Access Appliance S3 server keys using the helper script

Create the access and the secret keys using the Access Appliance 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 Access Appliance S3 server credential keys.

- Location of the helper script:
`/opt/VRTSnas/scripts/utils/objectaccess/objectaccess_client.py`
- The Access Appliance 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. The `ADMIN_URL` has the format **admin.<cluster_name>:port number** . The port number should be 8144. This url should point to the Access Appliance management console IP address.
- Create the access and the secret key using the Access Appliance helper script by providing the user name, password, and `ADMIN_URL` (check the online Help of the Access Appliance 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 Access Appliance 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 Data Deduplication 14
- additional resources
 - documentation 132

B

- backup services
 - displaying the status of 129
 - starting 129
 - stopping 129
- backup storage for NetBackup 8

C

- configuring
 - backups using NetBackup or other third-party backup applications 130
 - Veritas Data Deduplication 19
- configuring NetBackup
 - prerequisites 120

D

- displaying
 - NetBackup configurations 129
 - status of backup services 129

G

- generating Access Appliance S3 server keys
 - using the helper script 132
- global deduplication
 - Veritas Data Deduplication 70

I

- integration with Access Appliance
 - NetBackup 7

M

- migrating
 - Veritas Data Deduplication 111

N

- NetBackup
 - configuring 130
 - displaying configurations 129
 - integration with Access Appliance 7

P

- prerequisites
 - configuring NetBackup 120

S

- starting
 - backup services 129
- stopping
 - backup services 129
- supported configurations and versions
 - NetBackup with MSDP-C 12
 - NetBackup with Veritas Data Deduplication 11
- system requirements
 - supported configurations and versions for
 - NetBackup with MSDP-C 12
 - supported configurations and versions for
 - NetBackup with Veritas Data Deduplication 11

U

- use case
 - long-term data retention 8
- using the helper script
 - generating Access Appliance S3 server keys 132
- using Veritas Data Deduplication
 - benefits 14

V

- Veritas Data Deduplication
 - about 14

Veritas Data Deduplication *(continued)*

- configuring 19
- global deduplication 70
- migration 111