Veritas Access Solutions Guide for Enterprise Vault

7.4.2 Linux

December 2020

VERITAS™

Veritas Access Solutions Guide for Enterprise Vault

Last updated: 2020-12-01

Document version: 7.4.2 Rev 1

Legal Notice

Copyright © 2018 Veritas Technologies LLC. All rights reserved.

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

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

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

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

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

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

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

http://www.veritas.com

Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

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

https://sort.veritas.com/documents

Documentation feedback

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

accessdocs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 1 Introduction 6

About Veritas Access 6
About this document 6
About Veritas Access as archival storage for Enterprise Vault 6
Veritas Access versions certified by Enterprise Vault 7

Chapter 2 System Requirements 8

Server roles 8
Hardware requirements 9
Software requirements 10

Chapter 3 Installing and configuring Enterprise Vault with Veritas Access 12

Enterprise Vault deployment 12
Veritas Access deployment 12

Chapter 4 Veritas Access features for Enterprise Vault archival storage 13

Write-Once-Read-Many support 13
Partition Secure Notification 15

Chapter 5 Veritas Access archival policy configuration for Enterprise Vault 17

Configuring CIFS for the Active Directory domain mode 17
Veritas Access GUI policies for archival storage 19
Configuring the storage pool 21
Configuring the replication job 22
Configuring the archival policy using GUI 25
Configuration of CIFS shares for archival using Veritas Access CLISH 28
Storage provisioning using policies 30
Configuring Veritas Access storage with Enterprise Vault store partition 33

Chapter 6 Troubleshooting 36

Log locations for troubleshooting 36
Additional resources 36

Index 37

Chapter 1

Introduction

This chapter includes the following topics:

- About Veritas Access
- About this document
- About Veritas Access as archival storage for Enterprise Vault
- Veritas Access versions certified by Enterprise Vault

About Veritas Access

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

About this document

This document describes how Veritas Access 7.4.2 can be configured as archival storage with Enterprise Vault. Veritas Enterprise Vault helps automate retention management, classification and supervision, while simplifying search and eDiscovery of unstructured data.

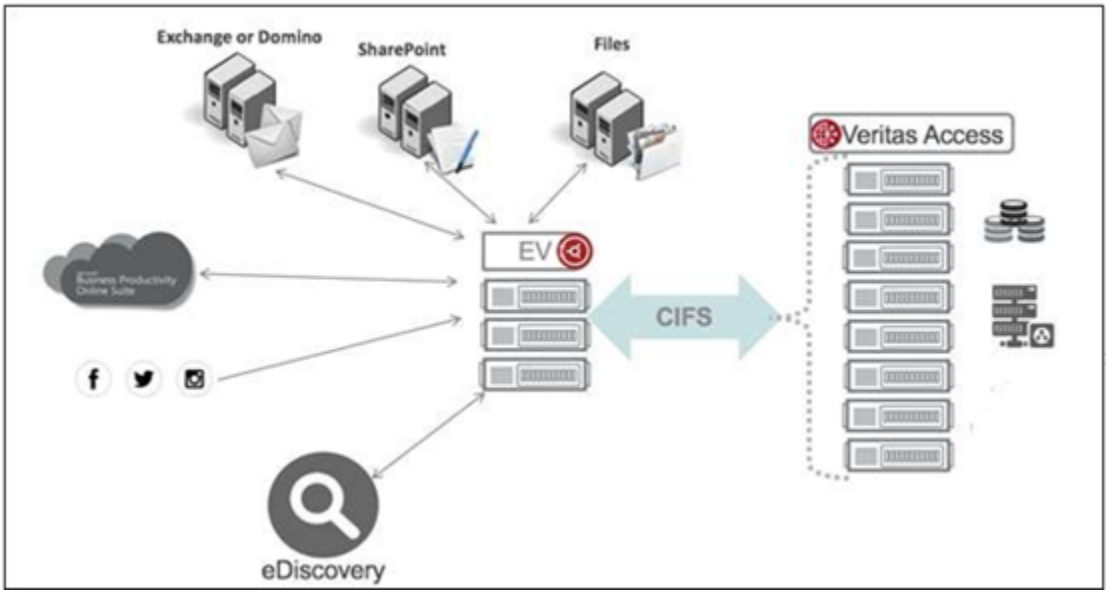
About Veritas Access as archival storage for Enterprise Vault

Veritas Access can be used as both primary storage and secondary storage for Enterprise Vault.

- Primary storage: Enterprise Vault can archive data directly to the storage system vault store partition.
- Secondary storage: Enterprise Vault can migrate collections of files from an NTFS or network share vault store partition to a secondary storage location.

Figure 1-1 shows how Veritas Access works as a primary archive datastore for Enterprise Vault.

Figure 1-1 Veritas Access as a primary archive datastore for Enterprise Vault



Veritas Access versions certified by Enterprise Vault

Veritas Access is certified for archival storage by Enterprise Vault.

See "Software requirements" on page 10. for details on Enterprise Vault Certification.

Chapter 2

System Requirements

This chapter includes the following topics:

- Server roles
- Hardware requirements
- Software requirements

Server roles

Figure 2-1 shows the roles of different servers in an Enterprise Vault configuration.

Figure 2-1

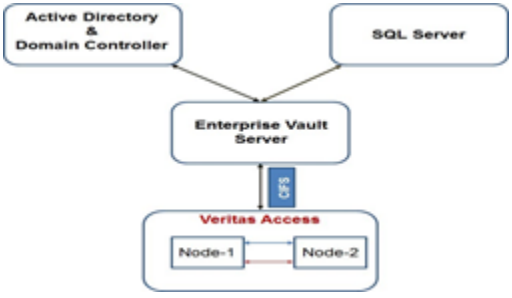


Table 2-1 gives the list of required servers and their use.

Table 2-1

Server	Use
Active Directory and Domain Controller	Required for user authentication for Enterprise Vault.

Table 2-1 *(continued)*

Server	Use
Enterprise Vault server	Required to configure Enterprise Vault services.
SQL server	Required by Enterprise Vault server to host its back-end database.
Veritas Access	Required as a storage system for archival by Enterprise Vault.

Hardware requirements

Four physical or virtual servers are required to host the following:

1. Active Directory and Domain Controller server

2. SQL server

The SQL servers should have the following minimum specifications:

- Number of CPUs: 8 (recommended)
- Power of CPUs: 2.8 GHz or more
- Memory: 16 GB (recommended)

The SQL server requires three fast local partitions (composed of one or more disks) to hold the following:

- SQL Server installation (OS Drive)
- SQL Server Data
- SQL Server Logs

3. Enterprise Vault server

The Enterprise Vault servers should have the following minimum specifications:

- Number of CPUs: 8 (recommended)
- Power of CPUs: 2.8 GHz or more
- Memory: 16 GB (recommended)

Each Enterprise Vault server requires three fast local partitions (composed of one or more disks) to hold the following:

Table 2-2

Disk use	Disk size (minimum)
OS Drive: Enterprise Vault installation Enterprise Vault Cache Enterprise Vault Storage Queue	100 GB
Enterprise Vault Indexes	75 GB
Target data for archiving This disk is only required for EVSCEV01	75 GB

4. Veritas Access cluster

See the *Veritas Access Installation Guide* for the system requirements.

Software requirements

Table 2-3 shows the software requirements for the involved software components are as follows:

Table 2-3 Software requirements

Component	Requirements
Enterprise Vault	See the software requirements to configure the Enterprise Vault server at Veritas Enterprise Vault 12.0 – Installing & Configuring Guide.
Veritas Access	See the software requirements to configure the Enterprise Vault server at Veritas Access Installation Guide.

Table 2-4 shows the Enterprise Vault certification details for Veritas Access as a primary archival storage.

Table 2-4 Certification details

	Enterprise Vault 11	Enterprise Vault 12
Veritas Access 7.2.1 and later versions	Non-WORM	Non-WORM
Veritas Access 7.3 and later versions	N/A	WORM

See the *Veritas Access Release Notes* for operating system compatibility list.

Chapter 3

Installing and configuring Enterprise Vault with Veritas Access

This chapter includes the following topics:

- Enterprise Vault deployment
- Veritas Access deployment

Enterprise Vault deployment

Before you install Enterprise Vault, the Enterprise Vault Deployment scanner should be run on each of the intended Enterprise Vault servers.

If you want to configure partitions in both IPv6 and IPv4 modes, the following network settings are required on Enterprise Vault and the Active Directory (AD) server.

Network settings> **NIC Properties**> **Enable IPv6 and Enable IPv4**.

For more information, see Enterprise Vault installation and configuration.

Veritas Access deployment

For deploying Veritas Access, see the *Veritas Access Installation Guide*.

Chapter 4

Veritas Access features for Enterprise Vault archival storage

This chapter includes the following topics:

- Write-Once-Read-Many support
- Partition Secure Notification

Write-Once-Read-Many support

When a file is committed as Write-Once-Read-Many (WORM), the data in the file can be read but cannot be altered. The retention time for a WORM file specifies the time period for which the file must be retained after it is committed to WORM storage. The file cannot be deleted till the retention period expires. Once the retention time period has expired, the storage system allows the deletion of the file.

In the Veritas Access 7.4.2 release, the maximum value for the retention time period is *19 January 2038, 03:14:07 UTC*. The WORM property is set at the file level. The file can be committed or enabled as WORM on a file system created with 'WORM' support. A new option has been added in the `Storage> fs create` command to enable WORM support.

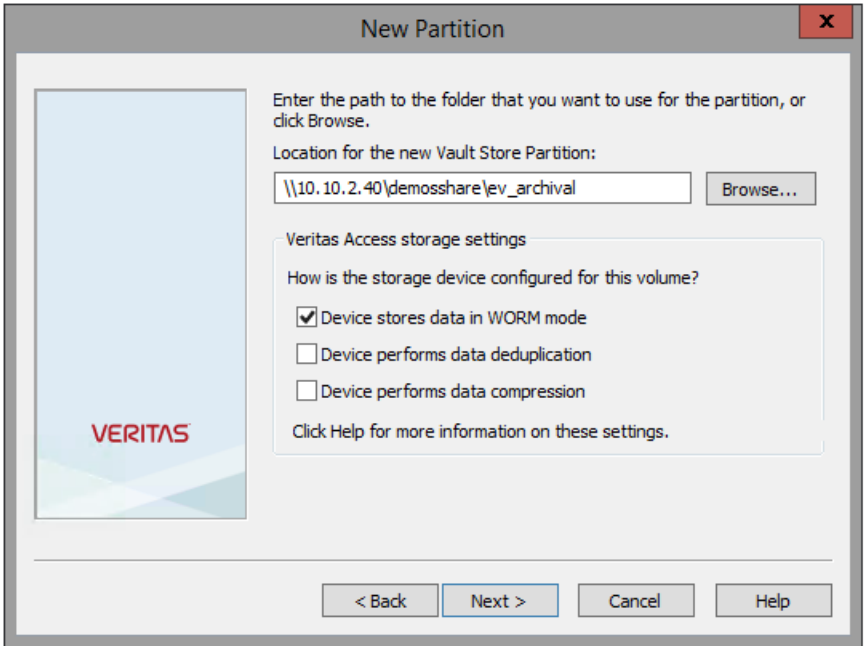
You can find out whether a given file system is WORM-enabled or not using the `Storage> fs list` command.

See the `Storage> fs list` man page for more details.

A new option has been added in the Veritas Access GUI as a policy to enable WORM support. You can find out whether a specific file system is WORM-enabled or not using the **File Systems** tab in the Veritas Access GUI.

While creating a partition in the Enterprise Vault Administration Console, select **Device stores data in WORM mode**.

Figure 4-1 Creating a new partition



Enterprise Vault archiving processes check the target servers for items to archive at scheduled times. When an item is archived, it is automatically assigned a retention category, which defines how long it must be kept in the archives (retention time). The administrator can define different retention categories for different types of data. Enterprise Vault monitors the archives and deletes items when the retention period expires.

Enterprise Vault sets a retention time on individual files. It sets the retention time by setting the access time of the file to a date in the future. For WORM-committed files, the access time of the file indicates the retention time.

Enterprise Vault uses a CIFS share, which exports the WORM-supported file system to archive data in WORM mode. Create the CIFS share with the `full_acl` option.

Any file system and CIFS share created in this way can be used as WORM storage for Enterprise Vault's archival on WORM-enabled storage.

Note: When using Veritas Access file systems as WORM-enabled storage for Enterprise Vault, once WORM retention period is set on archived items from Enterprise Vault, it can be extended for the associated files on the Veritas Access file systems only through the Veritas Access command-line interface.

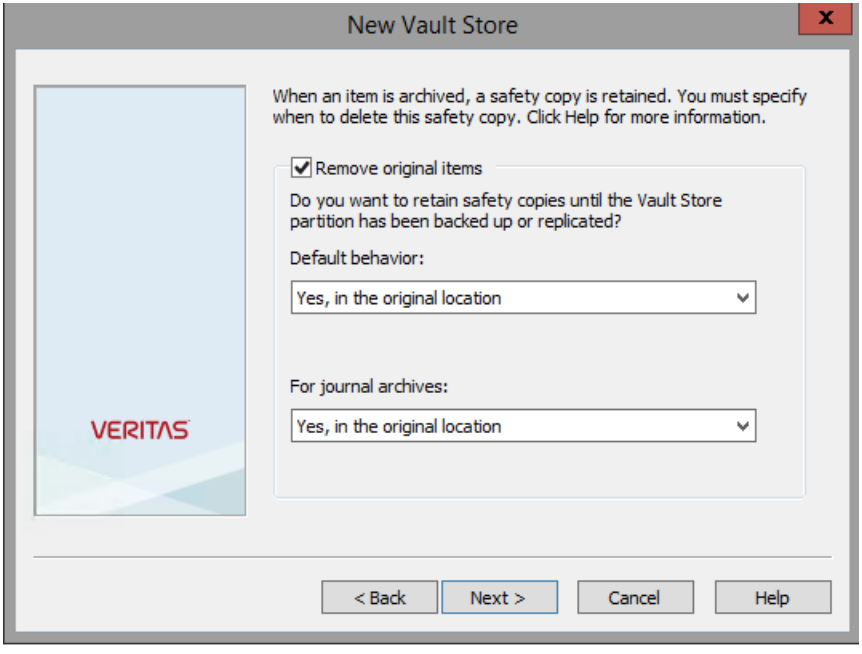
Partition Secure Notification

You can configure Enterprise Vault to retain original items until the vault store partition in which they are archived has been backed up. During the time between archival and removal, the original items are treated as safety copies by Enterprise Vault. A Partition Secure Notification (PSN) file is created at a source partition after the successful backup of the partition at the remote site. When the vault store partition has been backed up, Enterprise Vault removes the safety copies and creates placeholders.

The Veritas file-level replication is used to take a backup of a single partition. The Partition Secure Notification feature is enabled in the Veritas Access `replication job create` interface when an optional argument called `evpsn` is enabled.

Figure 4-2 shows the Enterprise Vault store settings when safety copies are removed after the partition has been backed up.

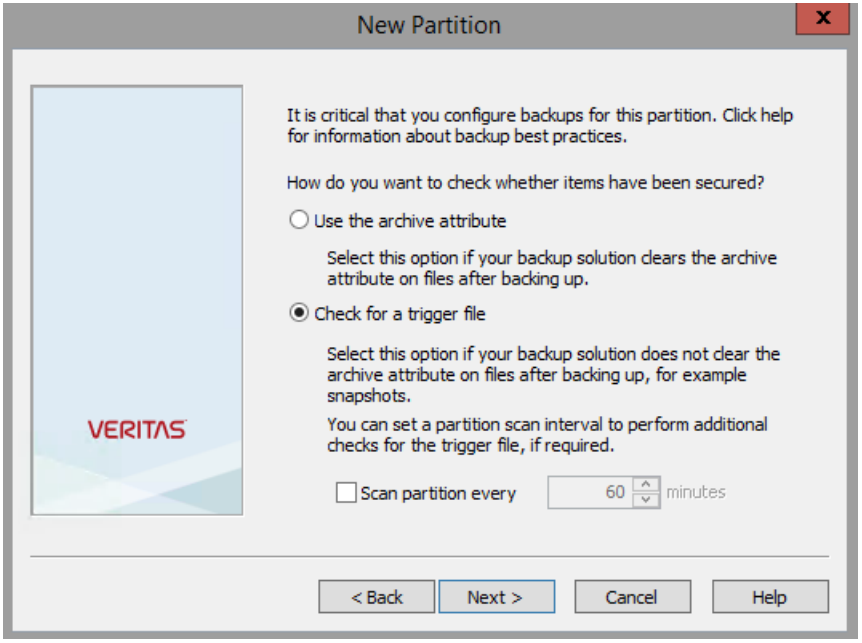
Figure 4-2



Enterprise Vault keeps the original items until the partition that contains the archived items has been backed up if **Yes, in the original location** option has been selected.

Figure 4-3 shows the Enterprise Vault store setting when a partition is created.

Figure 4-3



If the **Check for a trigger file** option is selected, Enterprise Vault refers to the PSN file to confirm that the archived data is secure. Accordingly, Enterprise Vault deletes safety copies and creates placeholders.

When the Enterprise Vault store is configured to delete the safety copies, it is important to configure how Enterprise Vault checks to ensure that the partition has been secured. Enterprise Vault checks for a trigger file when its Storage service starts and the back mode is cleared

See the `replication job create` man page for more details.

See the *Configuring replication* chapter in the *Veritas Access Administration Guide* for more details on replication.

Chapter 5

Veritas Access archival policy configuration for Enterprise Vault

This chapter includes the following topics:

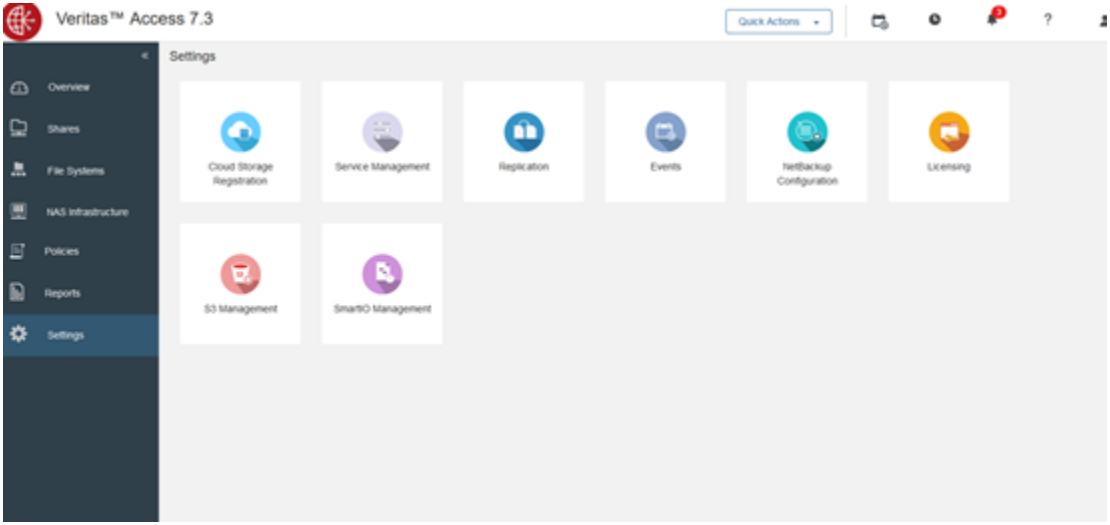
- Configuring CIFS for the Active Directory domain mode
- Veritas Access GUI policies for archival storage
- Configuring the storage pool
- Configuring the replication job
- Configuring the archival policy using GUI
- Configuration of CIFS shares for archival using Veritas Access CLISH
- Storage provisioning using policies
- Configuring Veritas Access storage with Enterprise Vault store partition

Configuring CIFS for the Active Directory domain mode

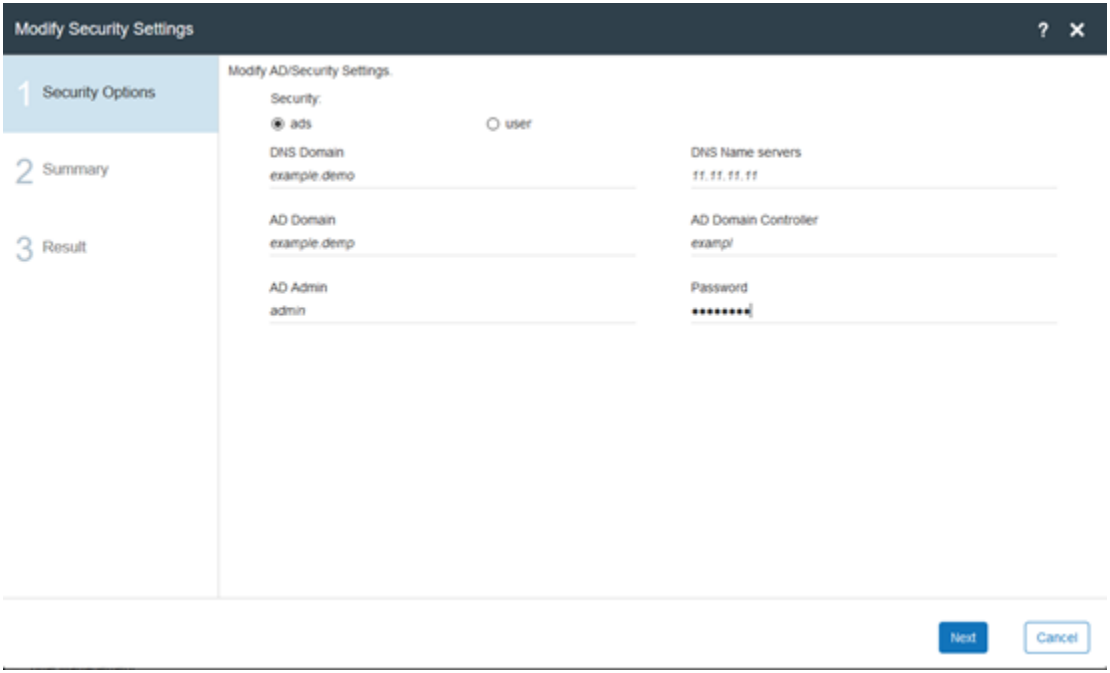
You have to configure Active Directory (AD) using the Veritas Access GUI.

To configure Active Directory

1 Click **Settings** > **Service Management** to configure AD.



2 Click **Settings** and modify the AD security settings.



Veritas Access GUI policies for archival storage

The Veritas Access GUI policies provide quick and easy configuration of archival storage for Enterprise Vault. The following policies are supported:

WORM

This policy gives Write Once Read Many storage and mirrors data across two devices, thus protecting against devices failures.

The key features of this archival policy are:

- Fault tolerance
- WORM

Prerequisites for this archival policy:

- Storage pool should be configured.

Non-WORM

This policy protects data against device failures by creating mirrored data across two devices.

The key features of this archival policy are:

- Fault tolerance

Prerequisites for this archival policy:

- Storage pool should be configured.

Non-WORM with replication

This policy protects the data against device, node, and site failures. It replicates data across two clusters. Veritas recommends that these clusters should be in different data centers. This policy mirrors data across two devices and protects against device failures.

The key features of this archival policy are:

- Fault tolerance
- Replication

Prerequisites for this archival policy:

- Storage pool should be configured.
- Replication link should be set up.

WORM with replication

This policy provides Write Once Read Many (WORM) storage and protects data against device, node, and site failures. It replicates data across two clusters. Veritas recommends that these clusters should be in different data centers. This policy mirrors data across two devices and protects against device failure.

The key features of this archival policy are:

- Fault tolerance
- WORM
- Replication

Prerequisites for this archival policy:

- Storage pool should be configured.

Note: For Enterprise Vault PSN to show expected behavior with episodic replication, it is recommended to configure episodic replication jobs from the Veritas Access GUI.

Note: To ensure seamless disaster recovery for vault stores, it is important to collect simultaneously consistent point-in-time copies of the Enterprise Vault partitions, Enterprise Vault database, and associated Enterprise Vault indices on the disaster recovery site regularly. If simultaneously consistent point-in-time copies are not collected regularly for vault stores at the disaster recovery site, the recovery points and the recovery times for those vault stores may be adversely affected.

Veritas recommends that every vault store that is protected against disasters using episodic replication should have backup mode set for it before the scheduled episodic replication jobs start for partitions in that vault store. The set of simultaneously consistent point-in-time copies should then be collected for that vault store. Once the set of simultaneously consistent point-in-time copies have been collected, backup mode can be unset for that vault store resuming archival in the vault store.

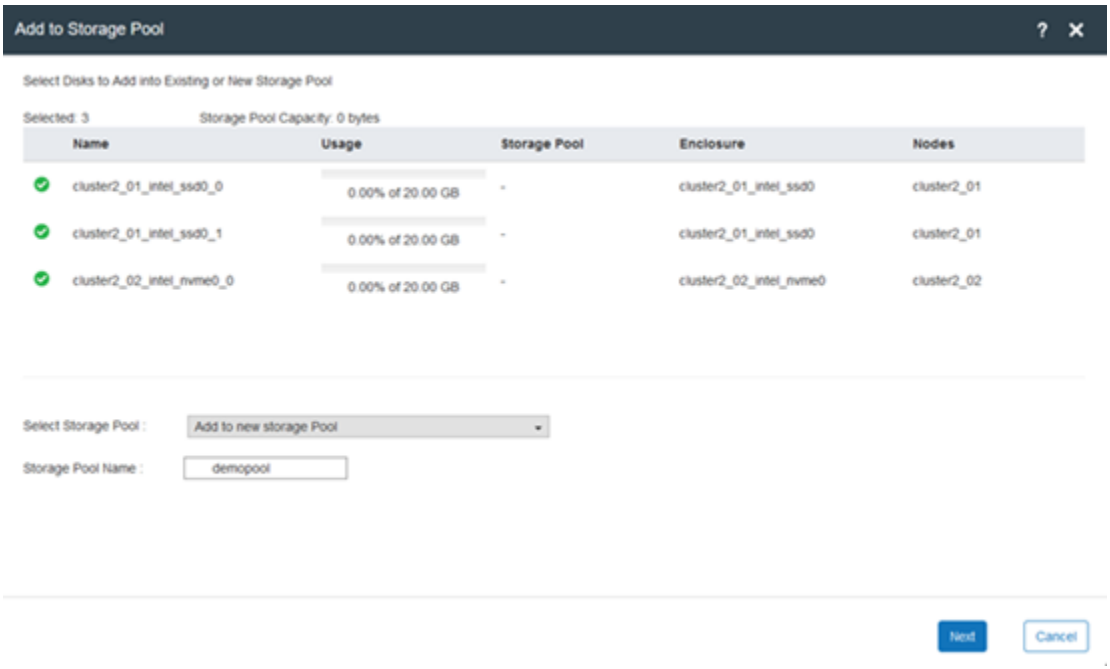
See “Configuring the storage pool” on page 21.

Configuring the storage pool

You have to configure the storage pool for archival storage.

To configure the storage pool

1. Log on to the Veritas Access GUI.
2. Click **NAS Infrastructure**. Select the disks to create the pool.
3. Enter a pool name. Click **Next** to create the pool.



Configuring the replication job

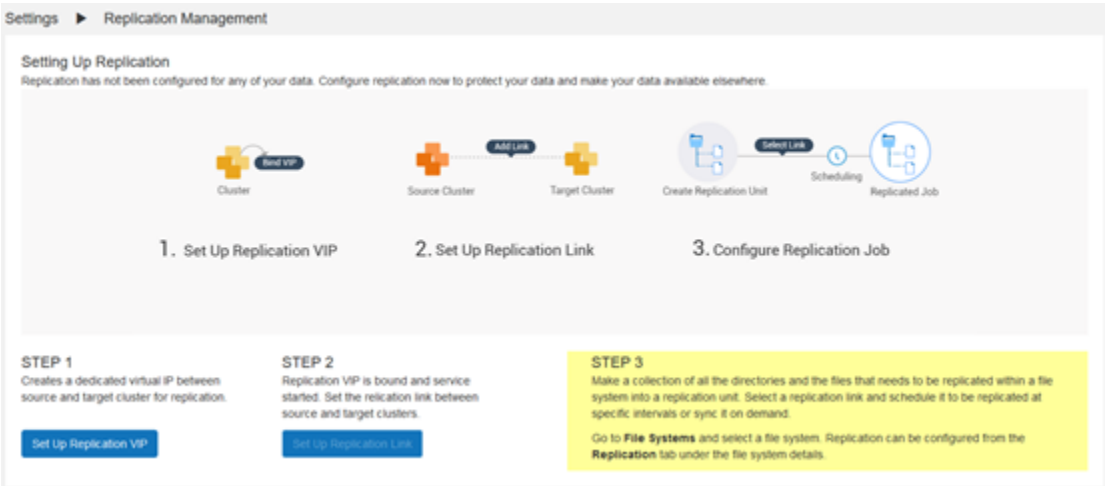
You have to configure replication for activating replication-related policies. As part of this configuration, you have to set up the replication VIP and replication link.

Archival policies use Veritas file-level replication.

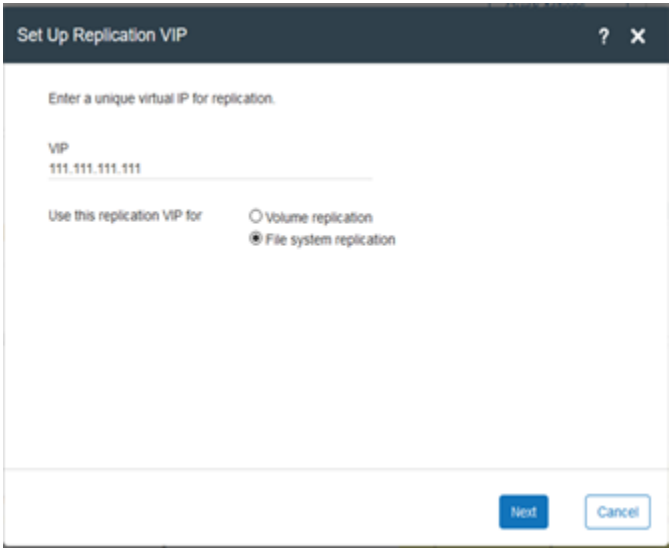
See the *Veritas Access Administration Guide* for more information on configuring replication.

To configure replication

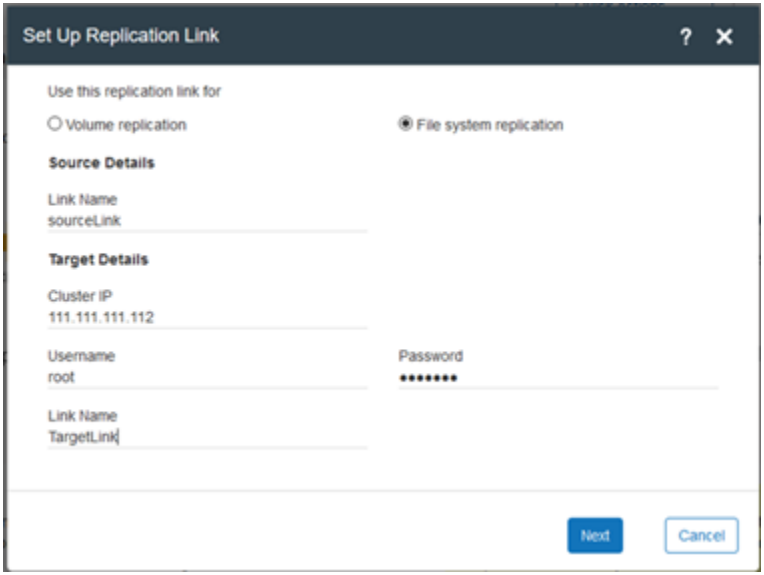
1. Log on to the Veritas Access GUI.
2. Click **Settings** -> **Replication Management**



3 Enter the required information for setting up the replication VIP.



4 Enter the required information to set up the replication link.



Configuring the archival policy using GUI

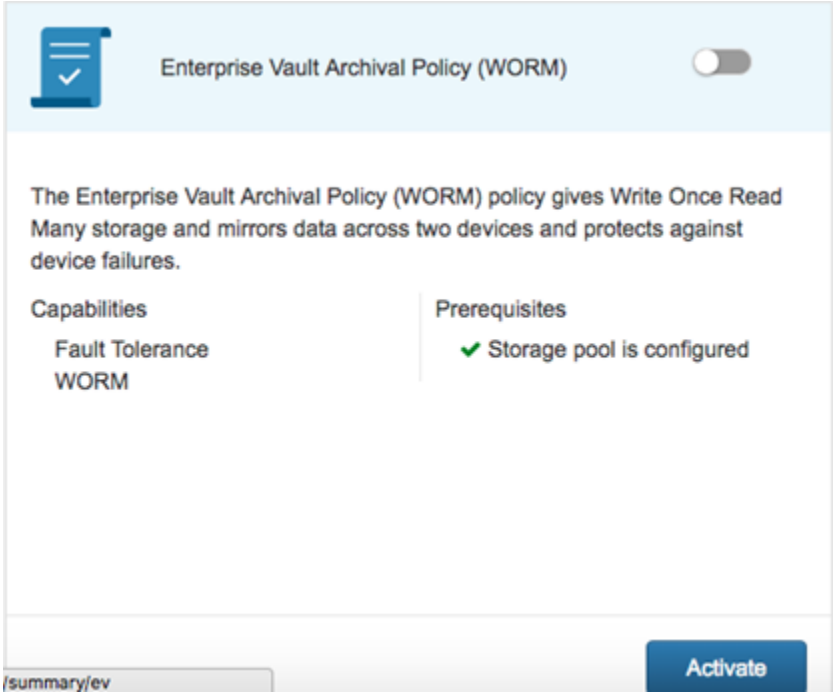
Once policy prerequisites are completed (like configuring storage pool and replication set up), you have to activate the archival policy.

Note: To use the archival policy, ensure that you have five disks in the configured pool as the policy creates five column striped file system layout. Else, you can perform similar operations using the Veritas Access CLISH. See "Configuration of CIFS shares for archival using Veritas Access CLISH" on page 28.

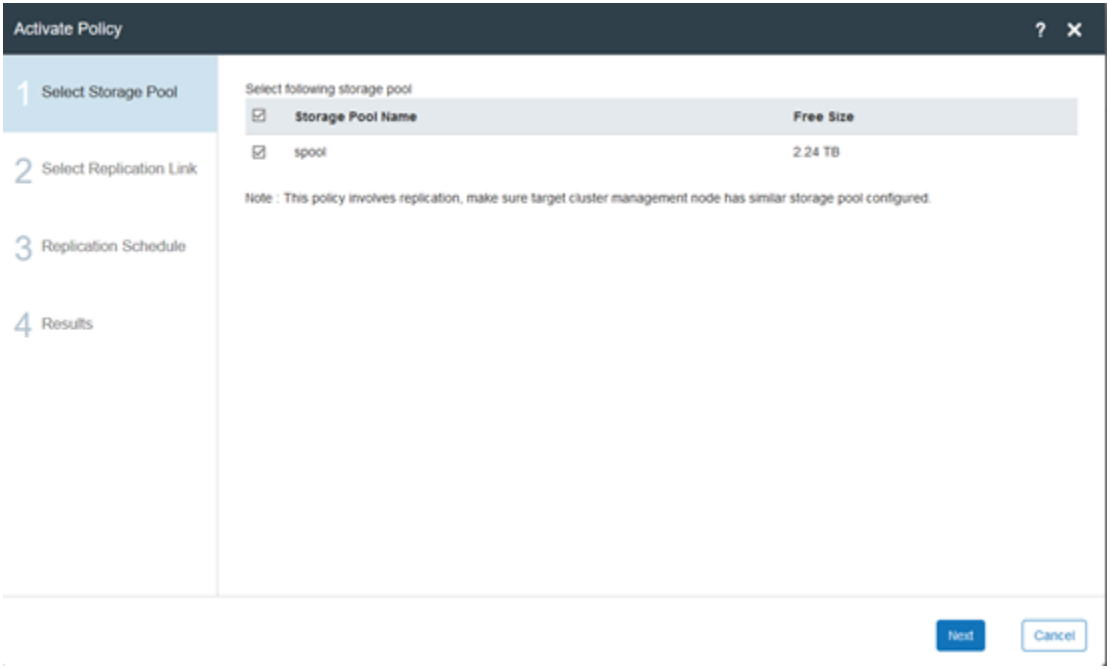
To configure the archival policy using GUI

1. Log on to the Veritas Access GUI.
2. Click on **Policies & Select Archival Policy**. Activate the required policy by clicking **Activate** on the policy.

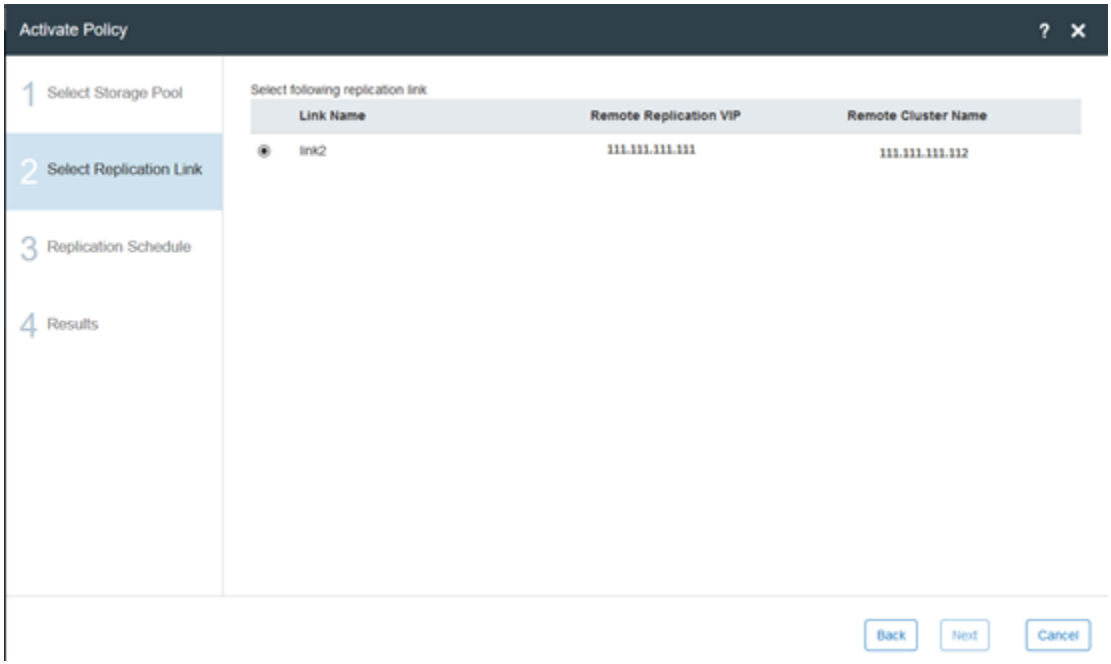
   The figure below shows activation of Enterprise Vault WORM policy.



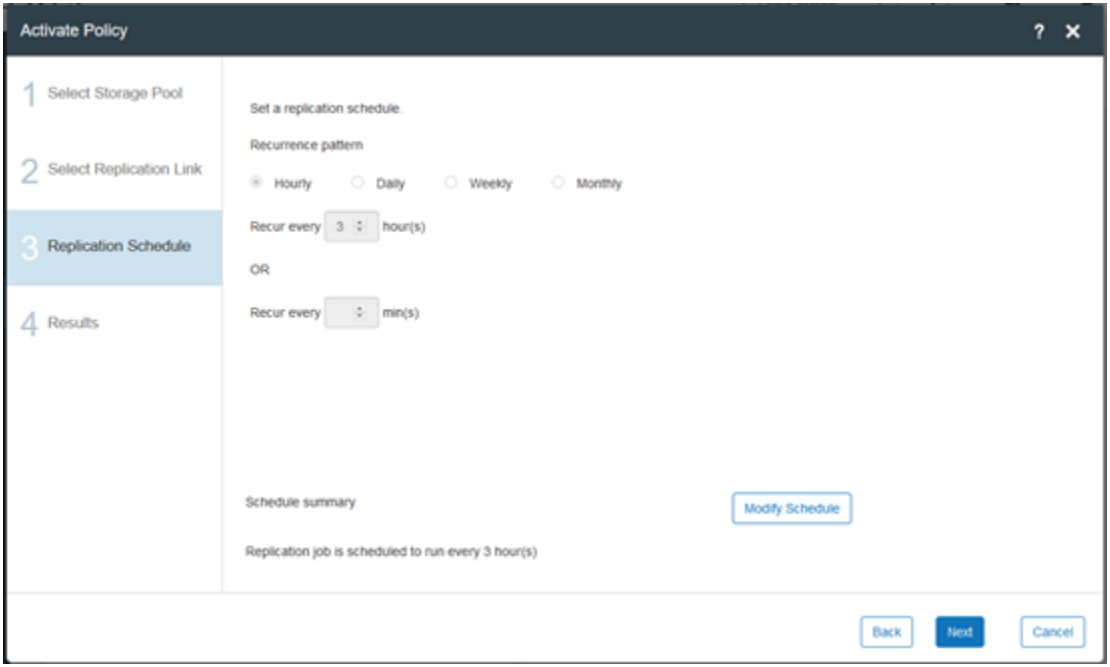
3 Select the storage pool during policy activation.



4 Select the replication link if the replication-related policy is activated. Select the file-level replication link that has been configured.



5 Provide replication job schedule information.



Once you activate the archival policy, storage for archival can be provisioned using the activated policy.

Note: Enterprise Vault partition rollovers show expected behavior only if there is a one-to-one mapping between the Enterprise Vault partitions and Veritas Access shares.

See “Storage provisioning using policies” on page 30.

Configuration of CIFS shares for archival using Veritas Access CLISH

Ensure that all the prerequisites are completed such as AD settings, configuration of storage pool and setting up the replication links.

To set up the archival folder for Enterprise Vault

1. Create a file system with a supported layout using the following command:

```
Storage> fs create striped testfs 10G 5 testpool stripeunit=128
blksize=1024 pdir_enable=no encrypt=off worm=yes
```

Note: To use WORM capabilities, make sure that you turn on the WORM flag during file system creation. You can also enable WORM flag for an already created file system using the `storage fs worm set` command.

2. Create a CIFS share by adding a directory inside the file system, with share options as `rw`, `full_acl`, and `allow domain user`.

```
CIFS> share create testfs testfs/test_directory
allow=accessra.local\evuser,noguest,rw,full_acl
```

Where the `testfs/test_directory` is the CIFS share.

3. Go to the bash prompt by elevating to root. Create an empty directory inside the share, which is used as a root folder for archival data by Enterprise Vault.

```
cd /vx/testfs/testfs
mkdir -m 0777 ev_archival
```

Note: After the empty folder creation, full permission should be given to Enterprise Vault user for archival from Windows client (Enterprise Vault server). You can access the share from the Windows client (Enterprise Vault server) and configure partition.

The Veritas Access policies provide quick and easy configuration of archival storage for Enterprise Vault. You have an option to configure WORM or Non-WORM policies with or without replication.

See "Veritas Access GUI policies for archival storage" on page 19.

If you want to configure your archival policy with replication, perform the following steps.

To set the replication of archived files to target site

1. Create a replication unit for the root folder that was created for episodic replication.

   ```
   Replication> episodic repunit create source_rep1
   testfs/test_directory/ev_archival
   ```

2. Create a replication schedule.

   ```
   Replication> episodic schedule creates schedule1 */15
   ```

3. Create a replication job and enable the job.

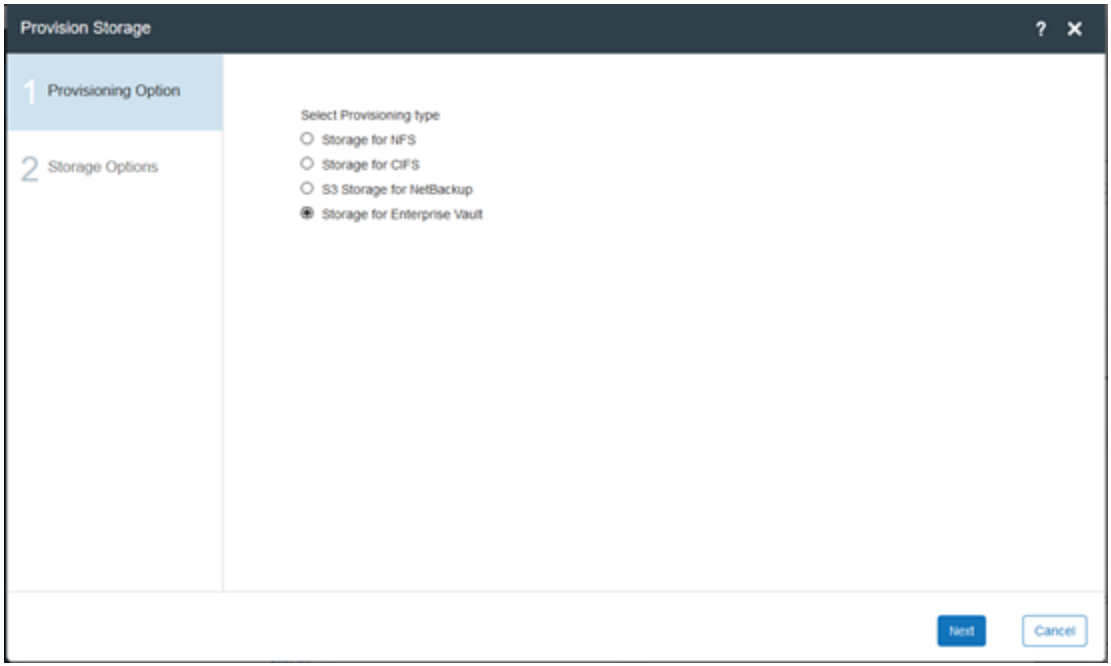
   ```
   Replication> episodic job create replicationjob sourcerep targetrep
   src_to_destination schedule1 evpsn=yes
   ```

Storage provisioning using policies

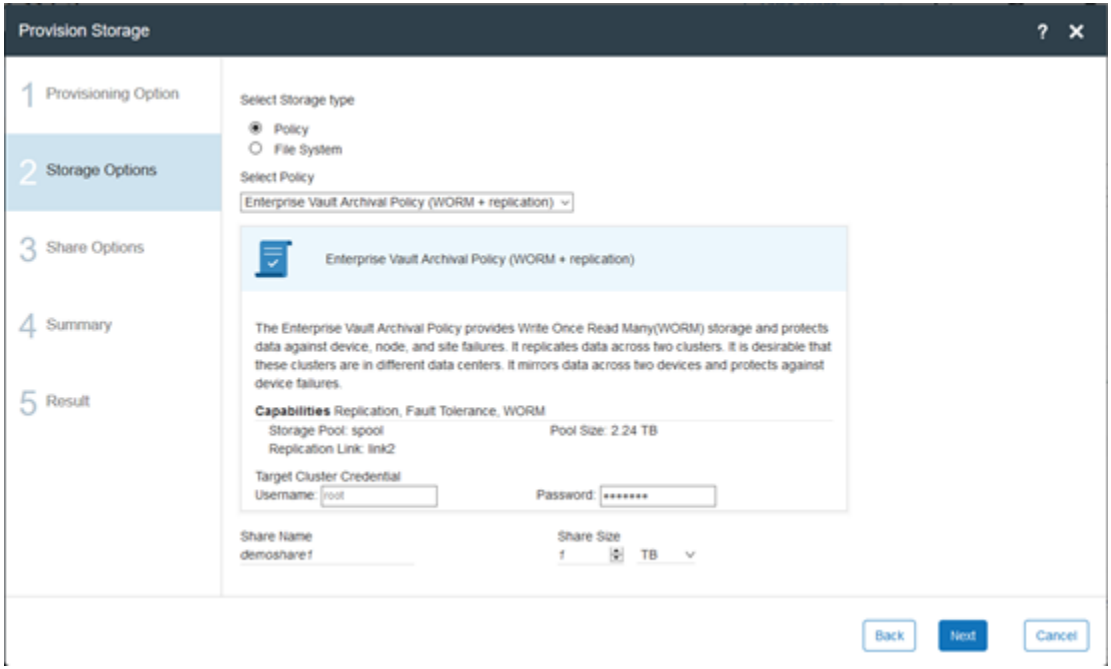
You have to configure replication and set up the replication VIP and replication link.

To configure replication

1. On the **Quick actions** tab on top right corner of the Veritas Access GUIDashboard, select **Provision Storage**.
2. In the menu, select **Storage for Enterprise Vault**.



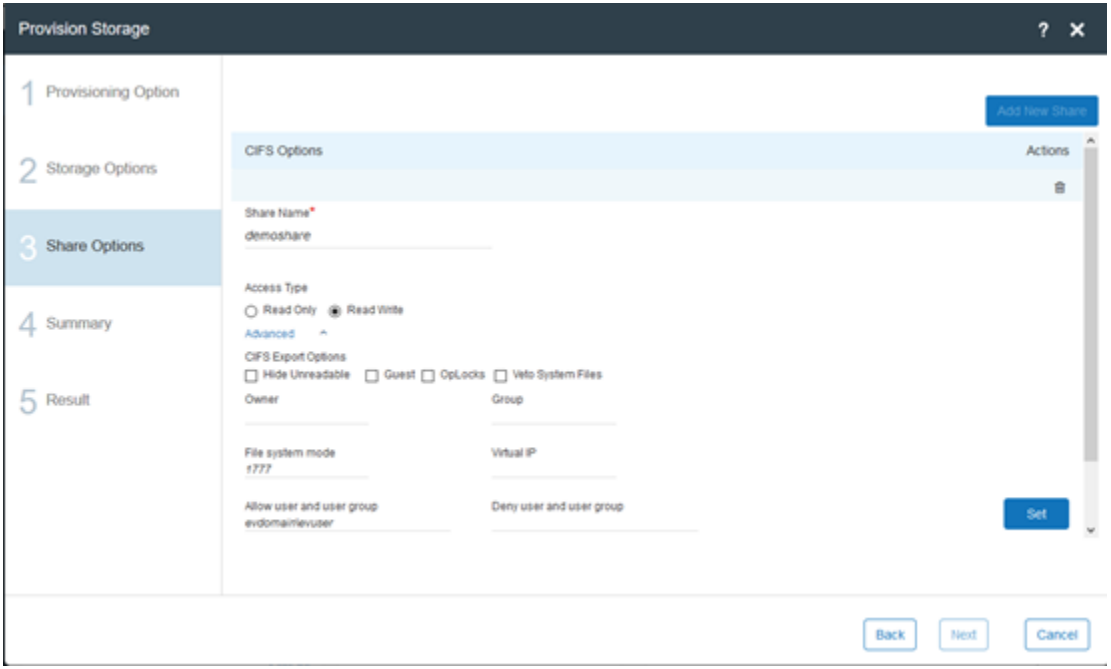
3 Provide the CIFS share name and other details.



The share configuration creates an empty directory called **ev_archival** inside the share, which is used for archival data by Enterprise Vault.

In the example above, CIFS network share path used for Enterprise Vault is `demoshare1\ev_archival`

4 Specify the Enterprise Vault user permissions while creating the share.



Create the share with 'full_acl' mode and allow read-write access for the Enterprise Vault user.

Note: After the share is created, full permissions should be given to the `EV user` for the `ev_archival` directory in a CIFS share from the Windows client (Enterprise Vault server).

To give ownership of `ev_archival` directory to `evuser` in `EVSC` domain using the `chown` command:

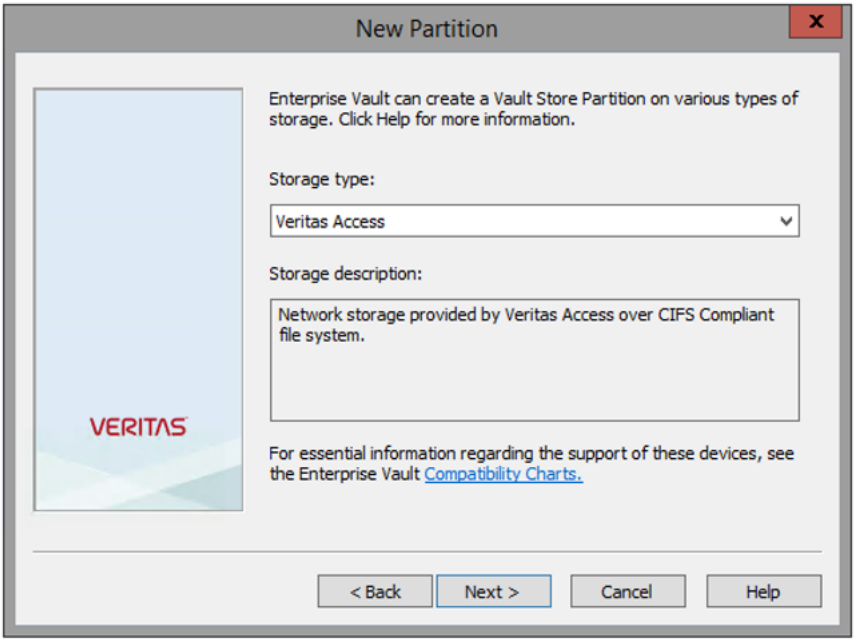
```
# chown "EVSC\evuser" ev_archival
```

Configuring Veritas Access storage with Enterprise Vault store partition

Once a CIFS share is created for archival storage provisioning, you can configure the Enterprise Vault store partition. Veritas Access is now listed as a storage type

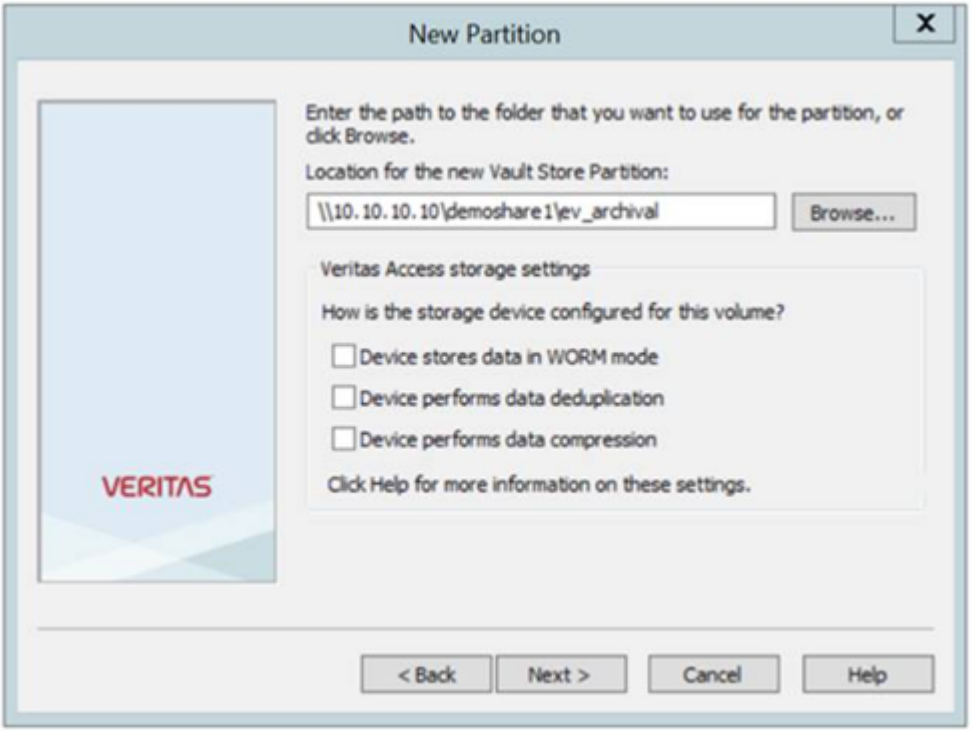
in the **New Partition** dialog of Enterprise Vault. You can create a new partition under the vault store as shown in Figure 5-1.

Figure 5-1 Creating a new partition



Select **Veritas Access** as the Storage Type.

Figure 5-2



When you configure the Enterprise Vault store partition, specify the full path of the directory created in the CIFS share configuration step as a vault store partition location as shown in Figure 5-2.

`demoshare1` is the Veritas Access CIFS share and `ev_archival` is the empty directory in this share that is created through the GUI archival policy.

Chapter 6

Troubleshooting

This chapter includes the following topics:

- Log locations for troubleshooting
- Additional resources

Log locations for troubleshooting

- See Veritas Access CIFS-related logs at `/opt/VRTSnas/log/cifs.log` for issues related to accessing CIFS shares.
- See Windows Event Log for errors related to the Enterprise Vault server.
  - Go to **Run**. Type **eventvwr**.
  - The Windows Event Viewer opens up.
    Select **Applications and Services logs**-> **Microsoft** -> **Veritas Enterprise Vault**.
- See **Recent Activity** at the top right corner of Veritas Access GUI for GUI-related status information

Additional resources

See the following documentation for more information on Veritas Access and Enterprise Vault.

- *Veritas Access Installation Guide*
- *Veritas Access Administration Guide*
- *Veritas Access Online Help*
- Enterprise Vault product documentation on the Enterprise Vault website.

Index

A

about
    policies for archival storage 19
additional resouces
    documentation 36

C

configuring
    replication job 22
    storage pool 21
configuring CIFS
    Active Directory domain 17
configuring using GUI
    archival policy 25
Configuring Veritas Access storage
    with Enterprise Vault store partition 33

E

Enterprise Vault
    PSN file 15
    WORM enabled file support 13
Enterprise Vault deployment
    installing and configuring 12

P

PSN file
    Enterprise Vault 15

S

storage provisioning
    using policies 30
System requirements
    hardware requirements 9
    server roles 8
    software requirements 10

T

troubleshooting
    log locations 36

V

Veritas Access
    archival storage for Enterprise Vault 6
    certifications by Enterprise Vault 7
Veritas Access deployment
    installing and configuring 12
Veritas Access GUI
    policies for archival storage 19

W

WORM enabled file support
    Enterprise Vault 13