Enterprise Vault Whitepaper

Configuring a NAS device as Enterprise Vault storage

This document provides background and guidance on how configure Symantec Enterprise Vault with generic Network Attached Storage (NAS). **Note this is restricted to using NAS as storage for Vault Store Partitions only, not Indexes or SQL databases. For use of NAS with Indexes or SQL, refer to the appropriate best practice guides.**

This document applies to the following version(s) of Enterprise Vault: 10.0.1

This document applies to any NAS that supports CIFS, including storage that is not specifically listed in the Enterprise Vault Compatibility Charts.

This document is provided for informational purposes only. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

Document Control

Contributors

Who	Contribution
Rick Krieger	Author

Revision History

Version	Date	Changes
1.0	April 4th, 2012	Initial release

Related Documents

Title	Link
Enterprise Vault 10.0 - Indexing Design and Implementation Best Practices	http://www.symantec.com/docs/DOC4250
Symantec Enterprise Vault 10.0: SQL Best Practices Guide	http://www.symantec.com/docs/DOC5365
Symantec Enterprise Vault Compatibility Charts	http://www.symantec.com/docs/TECH38537

Table of Contents

Overview

Symantec Enterprise Vault Storage

The key elements in the storage footprint of a Symantec Enterprise Vault (EV) environment are:

- **Databases** – EV databases in MS SQL Server holding configuration and operational data.
- **Indexes** – required for searching contents of EV archives.
- **Vault Store Partitions** – hold archived content.

EV **Databases and Indexes** should be stored on high performing block storage. NAS storage is not recommended for environments requiring high performance discovery searches, and connectivity via CIFS (or SMB) is not suitable for such environments. Please see the following document for more information: *Enterprise Vault 10.0 - Indexing Design and Implementation Best Practices***.**

Vault Store Partitions can be stored on a wide variety of storage platforms including NAS platforms which offer a good balance of scalability, performance and cost.

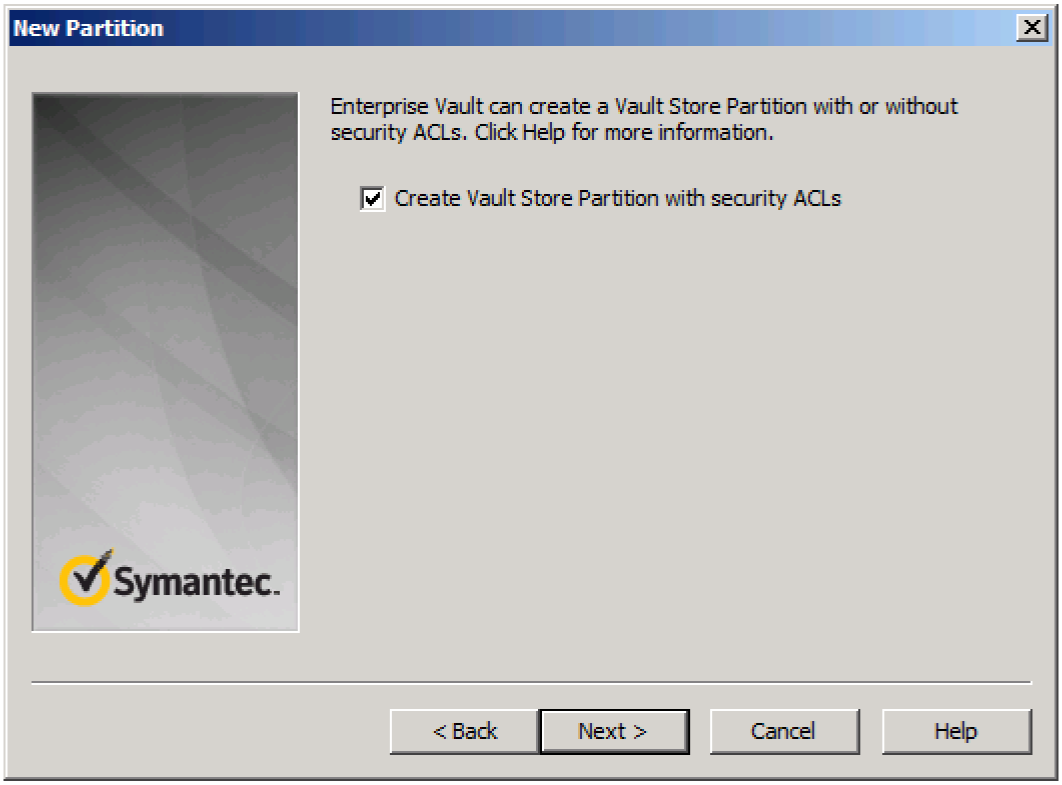
EV manages the retention and expiry of items it stores to Vault Store Partitions and can also send retention information to storage devices so they can provide additional functionality such as enforcing the retention of items at the storage layer, writing the items in a WORM state so they are immutable, API level integration, etc. Support for these advanced EV-storage features requires the storage vendor to become a member in the Symantec Technology Enabled Program (**STEP**) and self-certify their storage solutions for the desired functionality. These self-certified storage solutions are then listed in the *Enterprise Vault Compatibility Charts.*

Using Network Attached Storage (NAS) for Vault Store Partitions

Customer environments that do not require the storage device to provide retention management and/or WORM functionality and only require basic storage functionality do not require the storage device to be self-certified (and therefore are not required to be specifically listed in the EV Compatibility Charts) as long as the intended usage meets the criteria mentioned in Chapter 3 of the current *Enterprise Vault Compatibility Charts.* This currently includes support for archiving via Enterprise Vault to any high-performing Network Attached Storage (NAS) that is accessible over the CIFS/SMB protocol. In these cases it is still advisable that customers confirm operability of their specific configuration in a test/pre-production environment as part of their design and deployment process.

When configuring an EV Vault Store Partition for basic/generic non-WORM usage with NAS the customer will choose the “Network Share” partition type when creating a new EV Vault Store Partition in the EV Vault

Admin Console. The EV Vault Store Partition can be configured to have EV write ACLs on the root folder of the EV Vault Store Partition ***or*** the EV Vault Store Partition can be configured to allow the storage device to manage security of the items written to the EV Vault Store Partition via share permissions which are set when the share is created on the storage device (note that in some cases it may be necessary to allow the latter where the storage device manages security of the items). This is configured during EV Vault Store Partition configuration via the 'new partition' wizard in EV Vault Admin Console:



New Partition

Enterprise Vault can create a Vault Store Partition with or without security ACLs. Click Help for more information.

☑ Create Vault Store Partition with security ACLs

In most cases the best practice is to have EV write ACLs on the root folder of the EV Vault Store partition as shown above (which is the default configuration when creating a new EV Vault Store Partition).

More information on this configuration option can be found in the EV Vault Admin Console help page for this dialog as shown below:

New Partition

Create Vault Store Partition with security ACLs. It is usual to create a vault store partition with security ACLs in the folders in the partition. Some optical devices, however, do not allow Enterprise Vault to add the ACLs.

- If you are unsure about the behavior of the device you want to use, leave Create Vault Store Partition with security ACLs selected and try to create the vault store partition. If Enterprise Vault cannot add the security permissions, an error occurs and the partition is not created. You can then go back through the wizard, clear Create Vault Store Partition with security ACLs, and try again.

- If you decide to create the vault store partition without ACLs, be aware that there is no security on the vault store partition. In this case, we strongly recommend that you apply security manually, as described in the documentation for the device. You must restrict access to the vault store partition, including all subfolders and files, with the only access allowed being full control access to the Vault Service account.

IMPORTANT:

In EV 10.0.0 there was an issue for some NAS devices that prevented CIFS partitions from being created with EV writing ACLs to the root of the EV Vault Store Partition as shown in the configuration above. This was fixed in EV 10.0.1 so it is important that if you want to have EV manage the ACLs on the network share then you should ensure that you are using EV 10.0.1. Below is a explanation which is provided in the EV 10.0.1 'updated_en.htm' file:

> **Could not create new partition with ACLs on CIFS devices [Ref 13359, E2705819]**
>
> In Enterprise Vault 10.0 it was not possible to create a new partition on some CIFS/SMB devices when the 'Create Vault Store Partition with security ACLs' option was selected.
>
> This has been fixed.

This document focuses on the configuration specific to providing operability with Symantec Enterprise Vault with generic NAS for Vault Store Partition storage and non-WORM usage.

NAS Device Configuration

The following high level steps are to be performed on the NAS device:

- Join the NAS device/cluster to AD Domain
    - Most NAS devices provide the ability to join to an AD domain which allows for AD accounts to be given share permissions.
- Create a share to be used by the EV Vault Store Partition and give the EV Vault Service AD Account (VSA) 'Full' permissions to this share.

Symantec Enterprise Vault Configuration

The following steps are to be performed on the EV Server while logged in as the Vault Service Account (VSA).

Confirm Access to Share on NAS Device

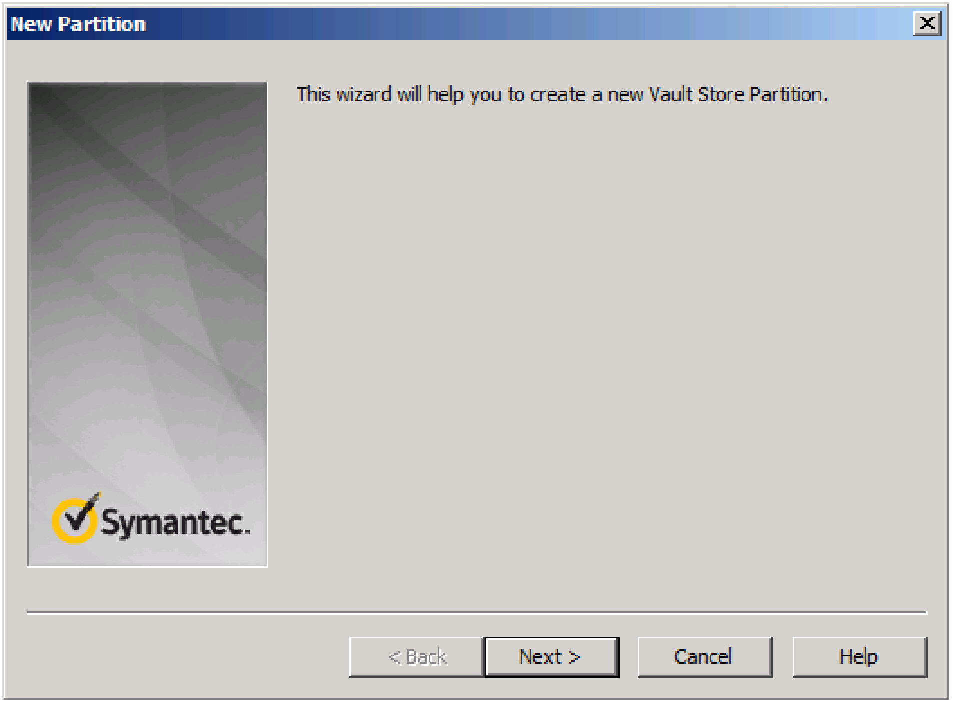
- Click **Start**->**Run**, type the following and press **Enter**:
    - \\<<fqdn of NAS device>>\<<share name>>
- Make sure you can access the NAS share.

Create Folders

- Using Windows Explorer create a new folder (such as “Vault Store Partitions”) at the root of the share which will be used to hold the vault store partition(s):
- Create subfolders here (such as “VSP1”) if it is necessary to store multiple vault store partitions:
    - NOTE: It is important that each vault store partition is stored within its own folder.

Create Partition

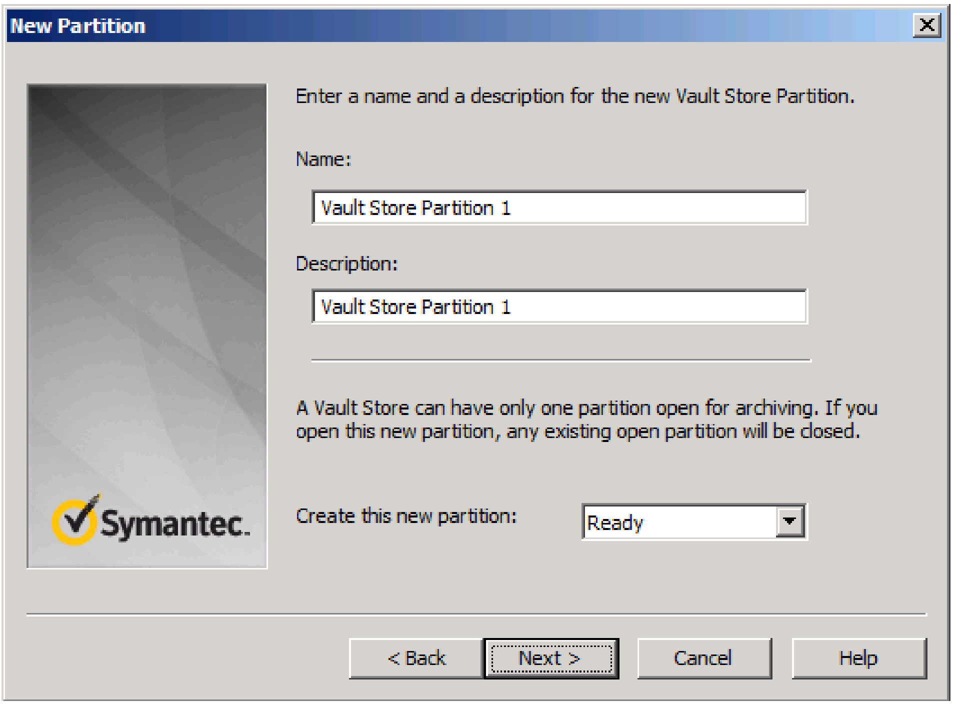
- Open the EV Vault Admin Console while logged into the EV Server as the Vault Service Account (VSA).
- Navigate to the **EV Site Object**->**Vault Store Groups**->***desired vault store sharing group***->***desired vault store***. Right click the desired vault store and choose **New**->**Partition**.
- Click **Next** to start the New Partition wizard.



New Partition

This wizard will help you to create a new Vault Store Partition.

- Enter a **Name** and **Description** for the partition (such as "Vault Store Partition 1"), leave the default setting for the partition **state** as **'Ready'**, click **Next**:



New Partition

Enter a name and a description for the new Vault Store Partition.

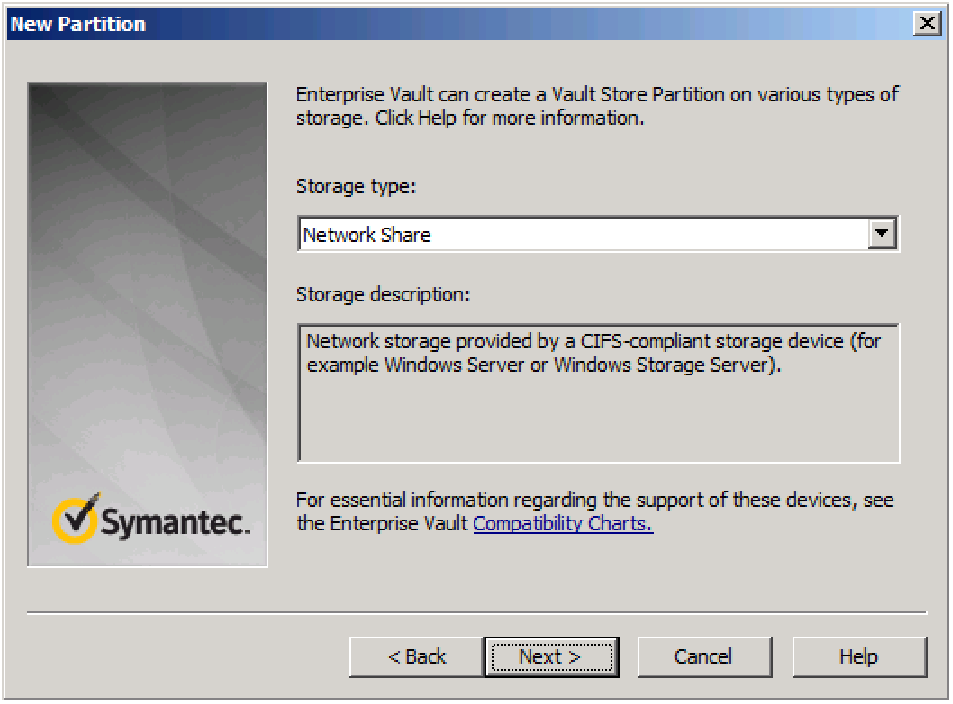
Name: Vault Store Partition 1

Description: Vault Store Partition 1

A Vault Store can have only one partition open for archiving. If you open this new partition, any existing open partition will be closed.

Create this new partition: Ready

- Select **Network Share** for the Storage Type, click **Next**.



New Partition

Enterprise Vault can create a Vault Store Partition on various types of storage. Click Help for more information.

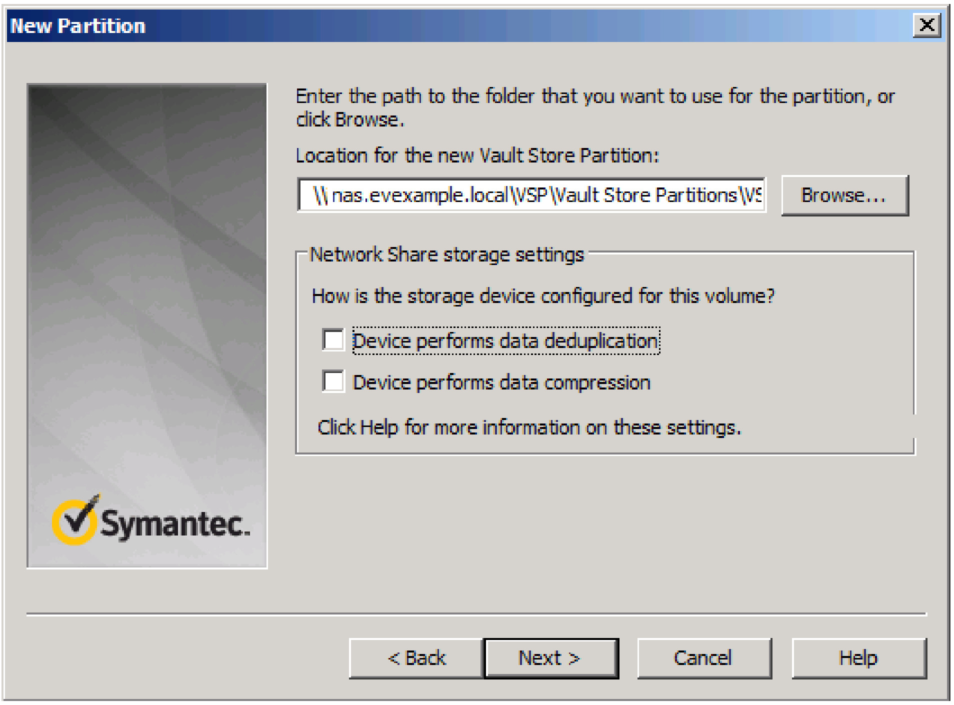
Storage type: Network Share

Storage description:

Network storage provided by a CIFS-compliant storage device (for example Windows Server or Windows Storage Server).

For essential information regarding the support of these devices, see the Enterprise Vault Compatibility Charts.

- Enter the UNC path to the folder in the share on the NAS device where the data for this partition is to be stored (such as \\nas.evexample.local\VSP\Vault Store Partitions\VSP1), do not choose any other options on this page, click **Next**.



New Partition

Enter the path to the folder that you want to use for the partition, or click Browse.

Location for the new Vault Store Partition: \\nas.evexample.local\VSP\Vault Store Partitions\VS

Network Share storage settings

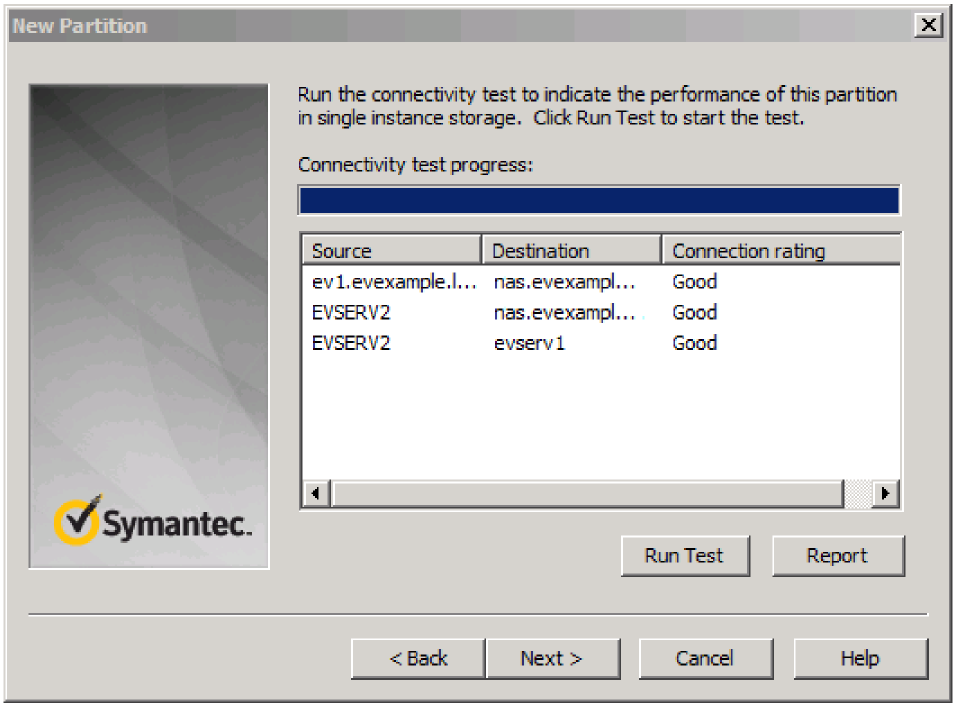
How is the storage device configured for this volume?

☐ Device performs data deduplication

☐ Device performs data compression

Click Help for more information on these settings.

- Click **Run Test**, confirm connection is ‘Good’, click **Next**.

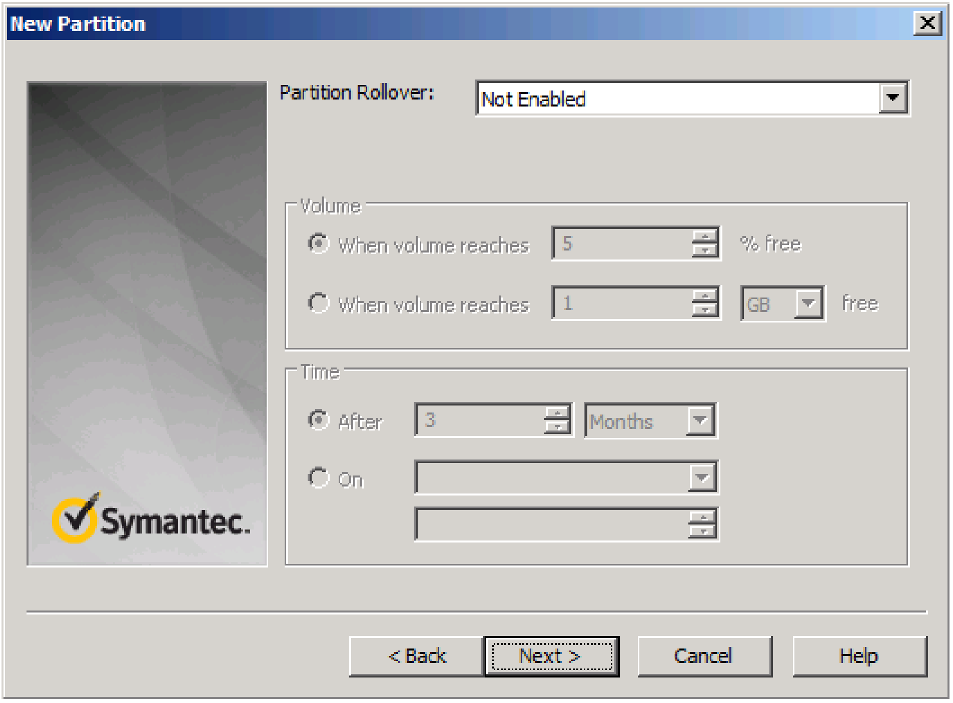


Run the connectivity test to indicate the performance of this partition in single instance storage. Click Run Test to start the test.

Connectivity test progress:

Source	Destination	Connection rating
ev1.evexample.l...	nas.evexampl...	Good
EVSERV2	nas.evexampl...	Good
EVSERV2	evserv1	Good

- Set Partition Rollover as desired, click **Next**.



Partition Rollover: Not Enabled

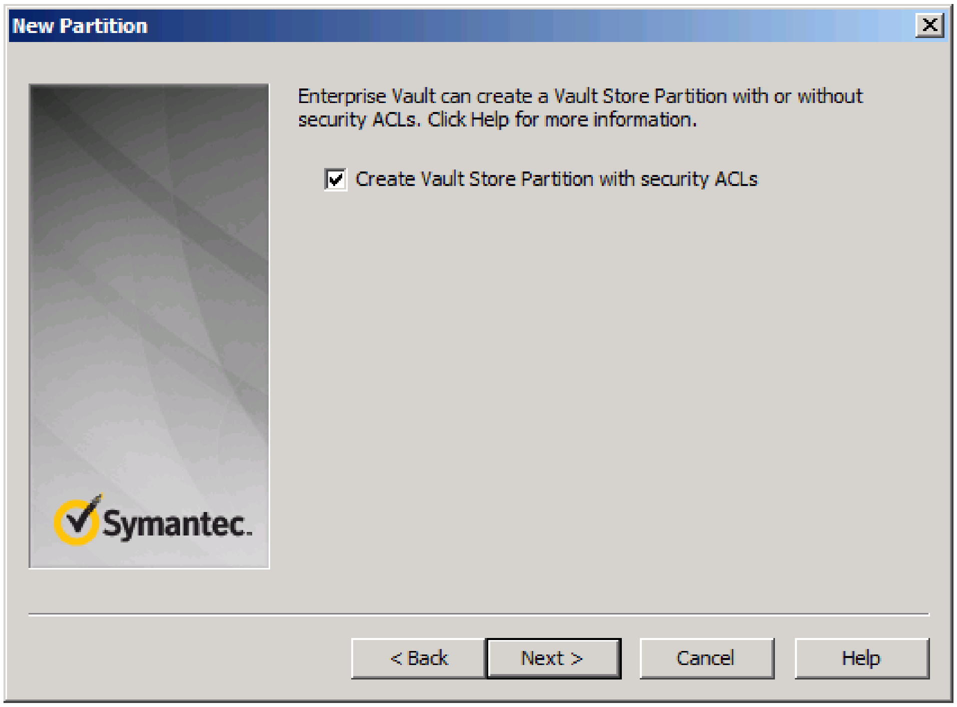
● When volume reaches 5 % free

○ When volume reaches 1 GB free

● After 3 Months

○ On

- **Check** or **Uncheck** the box for “**Create Vault Store Partition with security ACLs**” (depending on your requirements), click **Next**.

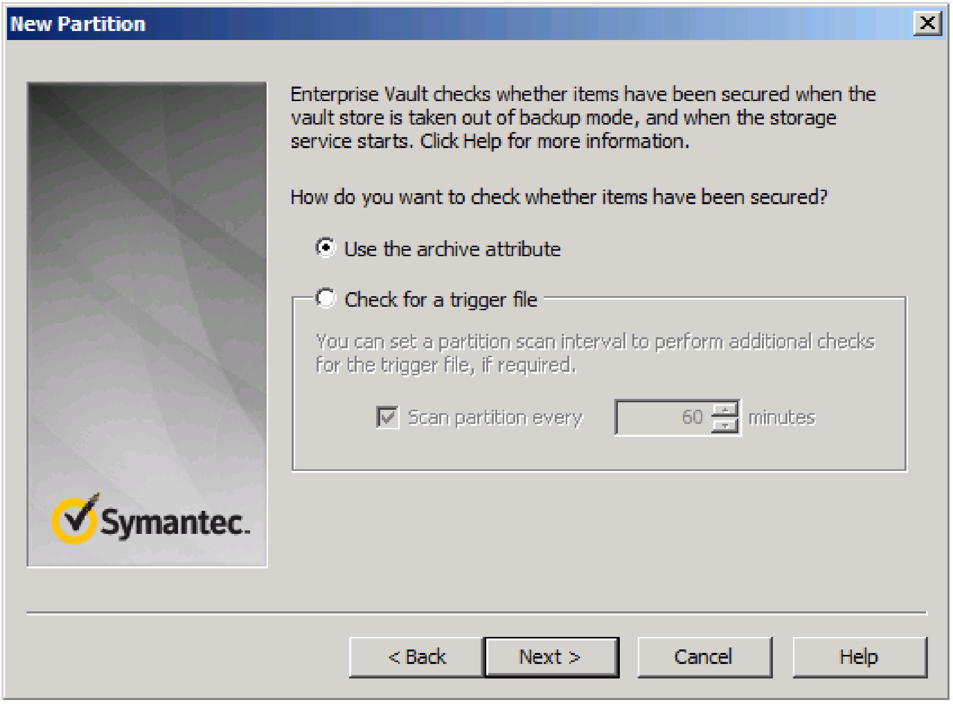


Enterprise Vault can create a Vault Store Partition with or without security ACLs. Click Help for more information.

☑ Create Vault Store Partition with security ACLs

- Choose the desired method for confirming that items have been secured (backed up) for the purposes of releasing safety copies, click **Next**.

NOTE: If the archive attribute method is selected it is important to test this functionality prior to going into full production to ensure that the archive attribute is being set and unset properly on the files in the vault store partition so the safety copies are released. If this does not work as expected then use the trigger file mechanism. More information can be found on the trigger file mechanism by clicking ‘Help’.



New Partition

Enterprise Vault checks whether items have been secured when the vault store is taken out of backup mode, and when the storage service starts. Click Help for more information.

How do you want to check whether items have been secured?

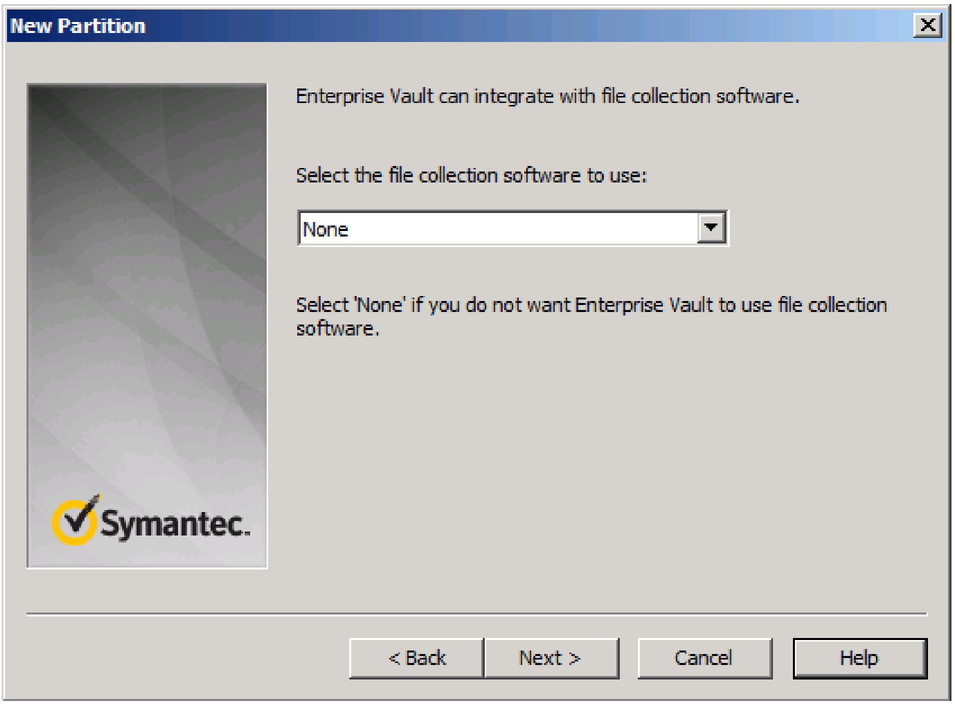
● Use the archive attribute

○ Check for a trigger file

You can set a partition scan interval to perform additional checks for the trigger file, if required.

☑ Scan partition every 60 minutes

- Select the desired option for Collections, click **Next**.
    - NOTE: If you are not sure what to select do **NOT** simply select the default below. Research this further and select the appropriate option for your environment.



New Partition

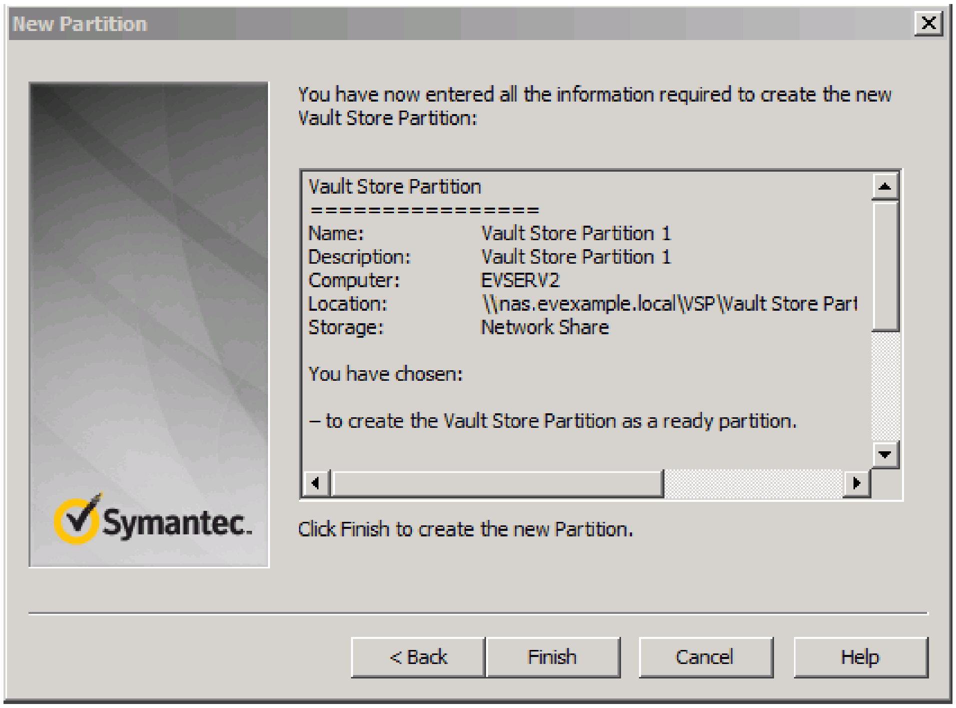
Enterprise Vault can integrate with file collection software.

Select the file collection software to use:

None

Select 'None' if you do not want Enterprise Vault to use file collection software.

- Confirm the configuration, click **Finish**.



You have now entered all the information required to create the new Vault Store Partition:

```
Vault Store Partition
================
Name:           Vault Store Partition 1
Description:    Vault Store Partition 1
Computer:       EVSERV2
Location:       \\nas.evexample.local\VSP\Vault Store Part
Storage:        Network Share

You have chosen:

– to create the Vault Store Partition as a ready partition.
```

Click Finish to create the new Partition.

Vault Store Partition
================
Name: Vault Store Partition 1
Description: Vault Store Partition 1
Computer: EVSERV2
Location: \\nas.evexample.local\vsp\vault store partitions\vsp1
Storage: Network Share

You have chosen:

– to create the Vault Store Partition as a ready partition.

– rollover not enabled.

– to use the archive attribute to indicate when files in the Vault Store Partition have been secured.

– to create the Vault Store Partition without security ACLs.

– not to use integrated file collection software.

– Connectivity Test executed. All the connections were rated as 'Good'.

- When ready to begin writing data to this partition change the state to “Open”.

About Symantec:

Symantec is a global leader in providing storage, security and systems management solutions to help consumers and organizations secure and manage their information-driven world.

Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For specific country offices and contact numbers, please visit our Web site: **www.symantec.com**

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
+1 (800) 721 3934