HITACHI
Inspire the Next

Hitachi Content Platform Streamer Adapter for Veritas Enterprise Vault

EV Streamer User Guide

MK-90ADPTR014-08
June 2018

Copyright © 2018 Hitachi, Ltd., Hitachi Vantara Corporation, ALL RIGHTS RESERVED

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for any purpose without the express written permission of Hitachi, Ltd., or Hitachi Vantara Corporation (collectively, "Hitachi").

Hitachi reserves the right to make changes to this document at any time without notice and assume no responsibility for its use. This document contains the most current information available at the time of publication. When new and/or revised information becomes available, this entire document will be updated and distributed to all registered users.

Some of the features described in this document may not be currently available. Refer to the most recent product announcement or contact your local Hitachi Vantara sales office for information on feature and product availability.

Notice: Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with HitachiVantara.com.

By using this software, you agree that you are responsible for:

a) Acquiring the relevant consents as may be required under local privacy laws or otherwise from employees and other individuals to access relevant data; and

b) Ensuring that data continues to be held, retrieved, deleted or otherwise processed in accordance with relevant laws.

Hitachi is a registered trademark of Hitachi, Ltd., in the United States and other countries.

All other trademarks, service marks, and company names are properties of their respective owners.

Enterprise Vault product screen shot(s) reprinted with permission from Veritas, Incorporated.

Contents

Contents

EV Streamer User Guide i
Preface v
Intended audience v
Software version v
Related documents v
Document conventions v
Getting help vi
Comments vii
EV Streamer overview 2
Requirements and installation 4
Installation and set-up prerequisites 4
Installing EV Streamer 4
Setting up EV Streamer 6
Configuring EV Streamer 8
Overview 8
Creating a new tenant in HCP 8
Creating a new namespace in HCP 9
Configuring an HCP namespace for CIFS 12
Configuring an EV server for CIFS 14
Creating a Vault Store Group in EV 17
Creating a Vault Store in EV 21
Creating an HCP Vault Store Partition in EV 26
Creating an HCP Vault Store Partition in EV with CIFS 32
Best practices 39
About Enterprise Vault Safety Copies 40
Troubleshooting 42
Access to HCP failed 42
Incorrect parameter 42

Preface

This document describes how to use the Hitachi Content Platform Streamer Adapter for Veritas Enterprise Vault (also referred to as EV Streamer).

This preface includes the following information:

- ☐ Intended audience
- ☐ Software version
- ☐ Related documents
- ☐ Document conventions
- ☐ Getting Help
- ☐ Comments

Notice: The use of Hitachi Content Platform Streamer Adapter for Veritas Enterprise Vault and all other Hitachi Vantara products is governed by the terms of your agreement(s) with Hitachi Vantara.

Preface

Intended audience

This document is intended for Enterprise Vault (EV) system administrators, Hitachi Ltd. representatives, and authorized service providers who are involved in installing, configuring, and operating Hitachi Content Platform (HCP).

This document assumes the following:

- The user is familiar with Enterprise Vault.
- The user is familiar with Hitachi Content Platform.
- The user is familiar with Veritas Enterprise Vault software and the Windows® host systems on which it is installed.

Software version

This document revision applies to Hitachi Content Platform Streamer Adapter for Veritas Enterprise Vault release version 1.4.*x*.

Related documents

- Enterprise Vault 12 Documentation
- Enterprise Vault 11 Documentation

Document conventions

This document uses the following typographic conventions:

Convention	Description
Bold	Indicates text on a window, other than the window title, including menus, menu options, buttons, fields, and labels. Example: Click **OK**.

Convention	Description
Italic	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: `copy source-file target-file` ***Note:*** Angled brackets (< >) are also used to indicate variables.
`screen/code`	Indicates text that is displayed on screen or entered by the user. Example: `# pairdisplay -g oradb`
< > angled brackets	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: `# pairdisplay -g <group>` ***Note:*** Italic font is also used to indicate variables.
[ ] square brackets	Indicates optional values. Example: [a | b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a | b } indicates that you must choose either a or b.
| vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [a | b] indicates that you can choose a, b, or nothing. { a | b } indicates that you must choose either a or b.

This document uses the following icons to draw attention to information:

Icon	Label	Description
	Note	Calls attention to important and/or additional information.
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
	Caution	Warns the user of adverse conditions and/or consequences (e.g., disruptive operations).
	WARNING	Warns the user of severe conditions and/or consequences (e.g., destructive operations).

Getting help

The Hitachi Vantara Support Center staff is available 24 hours a day, seven days a week. Provisions for patches and fixes are restricted to normal business hours, 8 a.m. to 5 p.m. PST.

To reach us, please visit the support Web site for current telephone numbers and other contact information: https://support.hitachivantara.com/en_us/contact-us.html. If you purchased this product from an authorized Hitachi reseller, contact that reseller for support.

Before calling the Hitachi Vantara Support Center, please provide as much information about the problem as possible, including:

- The circumstances surrounding the error or failure.
- The exact content of any error message(s) displayed on the host system(s).
- All Windows error log messages from Enterprise Vault that are relevant to the issue.

Comments

Please send us your comments on this document: HCPDocumentationFeedback@HitachiVantara.com. Include the document title, number, and revision, and refer to specific section(s) and paragraph(s) whenever possible. (All comments become the property of Hitachi Vantara Corporation.)

Thank you!

About EV Streamer

This chapter describes and provides an overview of EV, HCP, and EV Streamer.

- [EV Streamer overview]

EV Streamer overview

Veritas Enterprise Vault (EV) provides a software-based intelligent archiving platform that stores, manages, and enables the discovery of corporate data from e-mail systems, file server environments, instant messaging platforms, content management, and collaboration systems. When used with Hitachi Content Platform (HCP), the result is an open, highly scalable, intelligent archive that preserves and protects data, while at the same time greatly reducing storage capital and ongoing management costs.

Using the Hitachi Content Platform Streamer Adapter API interface, EV can take better advantage of HCP features, communicate with HCP over its REST-based enhanced interface, place data in secure and authenticated namespaces, and validate that the data has been successfully replicated to a remote HCP system.

2

Requirements and installation

This chapter provides the prerequisites and steps for installing and setting up EV Streamer.

- ☐ Installation and set-up prerequisites
- ☐ Installing EV Streamer
- ☐ Setting up EV Streamer

Requirements and installation

The following sections list the prerequisites for installing and setting up EV Streamer and include the steps to install and set up EV Streamer.

Installation and set-up prerequisites

Before installing EV Streamer, ensure that the following are installed first:

- Enterprise Vault Version 11.0.0 Hotfix 3 or later
- HCP 7.*x* or later

Before setting up EV Streamer, ensure the following:

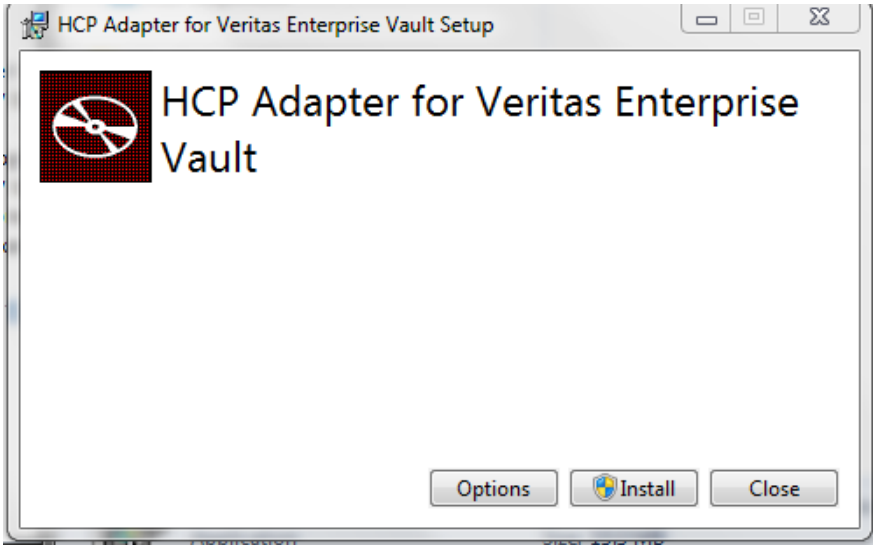
- Enterprise Vault Version 11 or later is installed and ready to create new Vault Store Partitions
- HCP 7.*x* or later is installed and has the following configurations:
  - The HCP DNS is integrated with the data center DNS
  - The tenant(s) and namespace(s) used for Vault Store Partitions are created before using the HCP Partition Wizard of EV
  - The Namespace Data Access User Account name and password are created prior to using the HCP Partition Wizard of EV
- EV Streamer is installed on each EV Server

Installing EV Streamer

The EV Streamer software is available for download from the Hitachi Vantara Support Portal. To install this software:

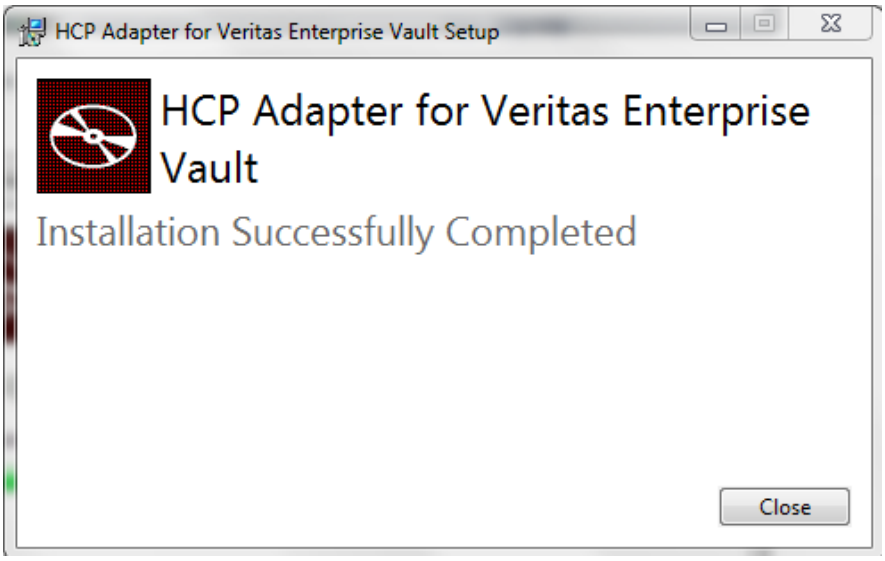
1. Stop the **File System Archiving Task**.
2. Stop the **Enterprise Vault Storage Service**.
3. Uninstall the earlier version of EV Streamer.
4. Double-click on **Hitachi Content Platform Streamer Adapter for Veritas Enterprise Vault** in its file location.

The first page of the Installation Wizard is displayed.



5. Click on **Install**.

   The Installation Wizard confirms that the installation was successfully completed.



6. When the installation is complete, click on **Close**.

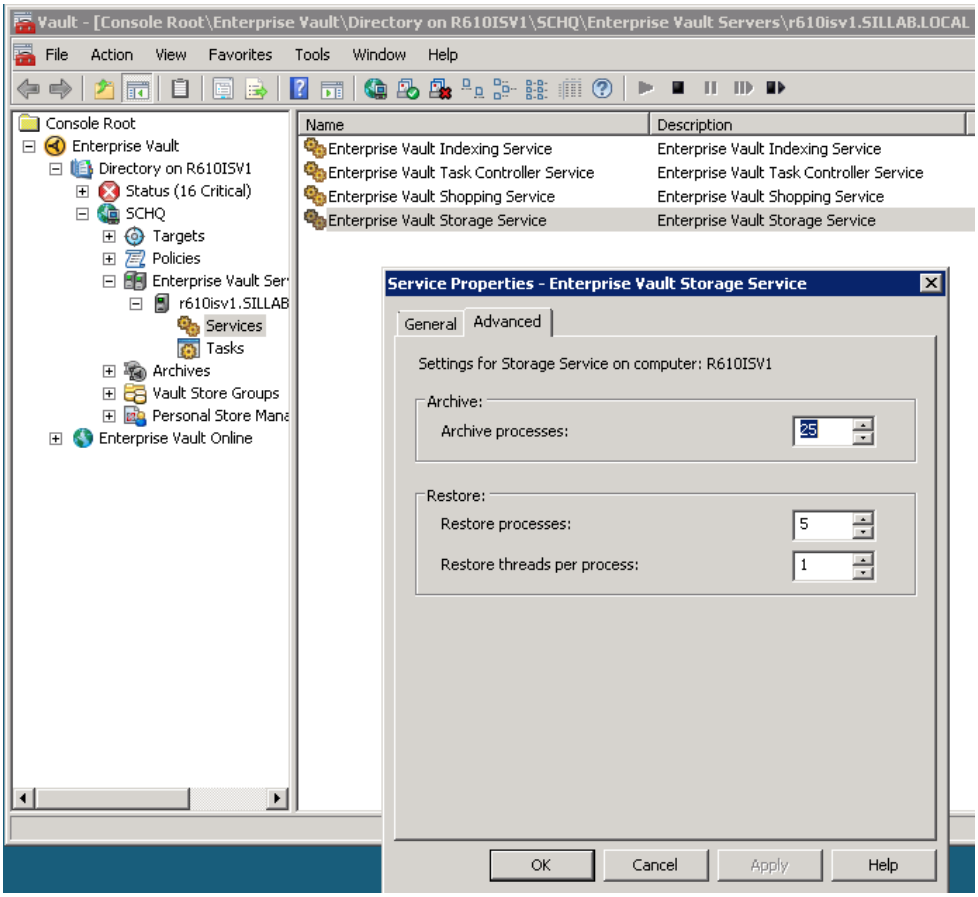
Setting up EV Streamer

To set up EV Streamer:

1. In the Enterprise Vault (EV) console, expand the Enterprise Vault Services in the Console Root tree and double-click on **Services**.

2. In the main window, select **Enterprise Vault Storage Service**.

   The Service Properties window is displayed.



3. Click on the **Advanced** tab.

4. Adjust the value of **Archive processes** as necessary to increase archive performance. The maximum value is 25.

5. Adjust **Restore** values as necessary.

6. Click on **OK**.

3

Configuring EV Streamer

This chapter provides the procedural steps for configuring EV Streamer and performing various EV Streamer operations.

- ☐ Overview
- ☐ Creating a new tenant in HCP
- ☐ Creating a new namespace in HCP
- ☐ Configuring an HCP namespace for CIFS
- ☐ Configuring an EV server for CIFS
- ☐ Creating a Vault Store Group in EV
- ☐ Creating a Vault Store in EV
- ☐ Creating an HCP Vault Store Partition in EV
- ☐ Creating an HCP Vault Store Partition in EV with CIFS

Configuring EV Streamer

The following sections include the procedural steps for configuring EV Streamer. These sections also include how to configure HCP as a CIFS Vault Store Partition within EV.

Overview

HCP 7.*x* and later supports multiple tenants, each tenant a peer of others, and for each tenant, multiple namespaces. Each tenant has its own disk quota, and each namespace of a given tenant can share that quota.

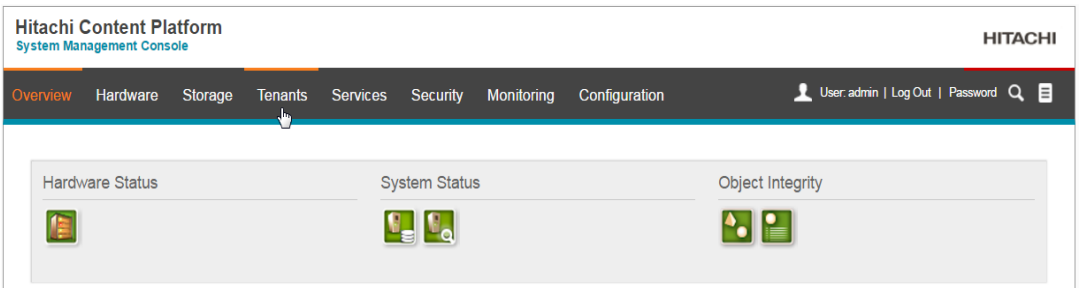
Multiple vault store partitions can share the same namespace as long as each partition has a unique root folder path.

When multiple EV servers exist, each server can share the same tenant, but each server should have its own dedicated namespace.

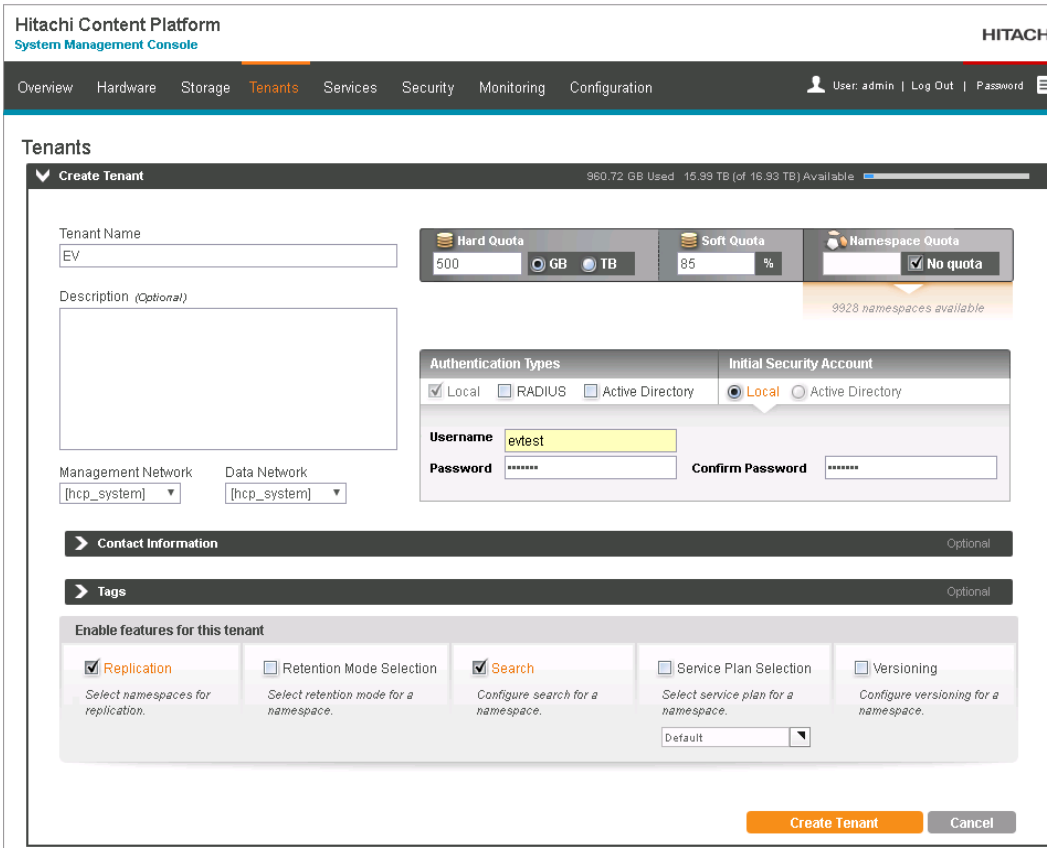
Recommended practice is to create all necessary EV vault store partitions that share the same namespace in a unique root folder path.

Creating a new tenant in HCP

1. Open the HCP System Management Console.



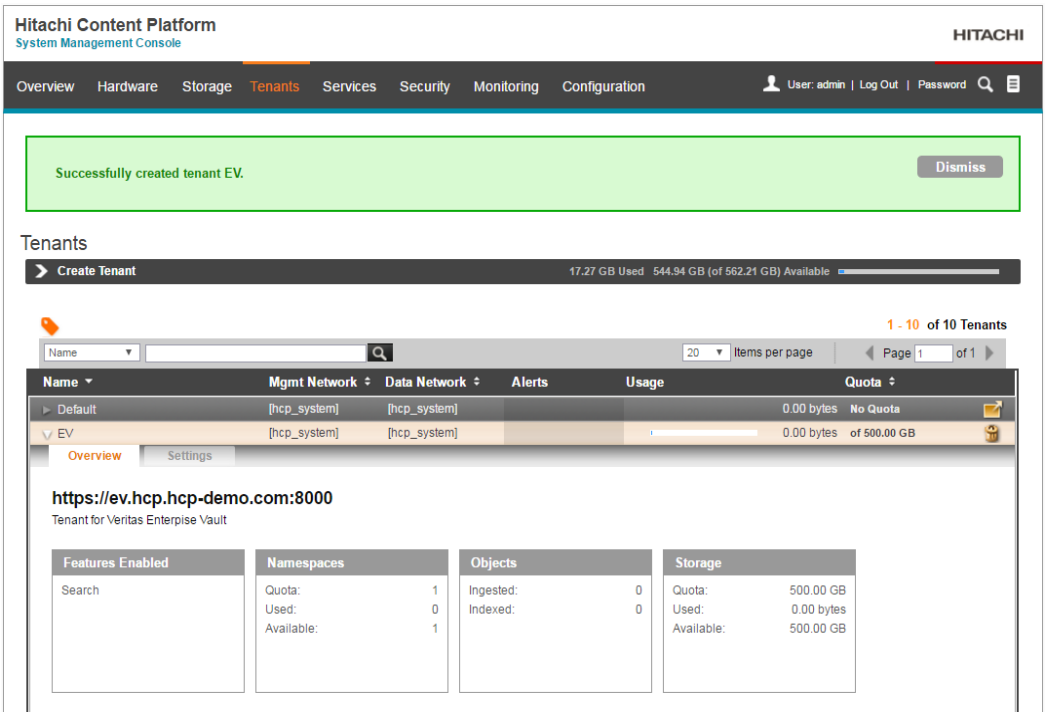
2. Click on the **Tenants** tab then click on **Create Tenant**.



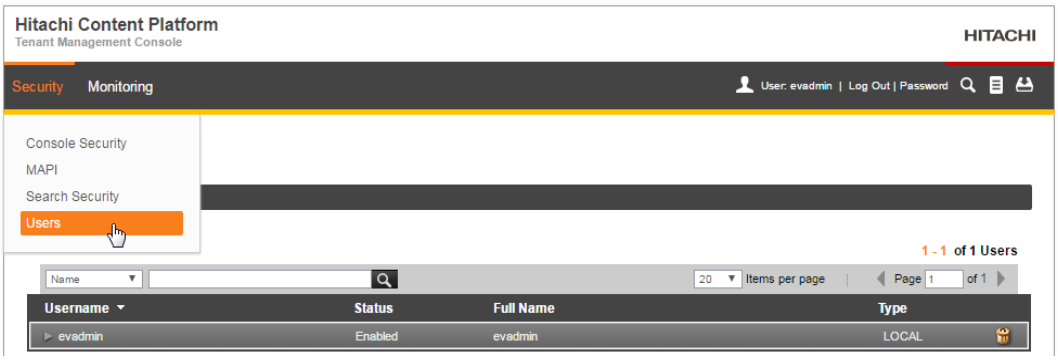
3. Assign a name and password for a new tenant in UTF-8 lowercase letters.
4. Assign a **Disk Quota** for anticipated data storage requirements.
5. Set a **Namespace Quota** (number of namespaces allowed in the tenant) to unlimited or to the number of EV servers that access HCP.
6. Disable **Disposition Service** and **Versioning** (the default values).
7. Enable **Search** and **Replication.**
8. Leave all other tenant settings in their default values.

Creating a new namespace in HCP

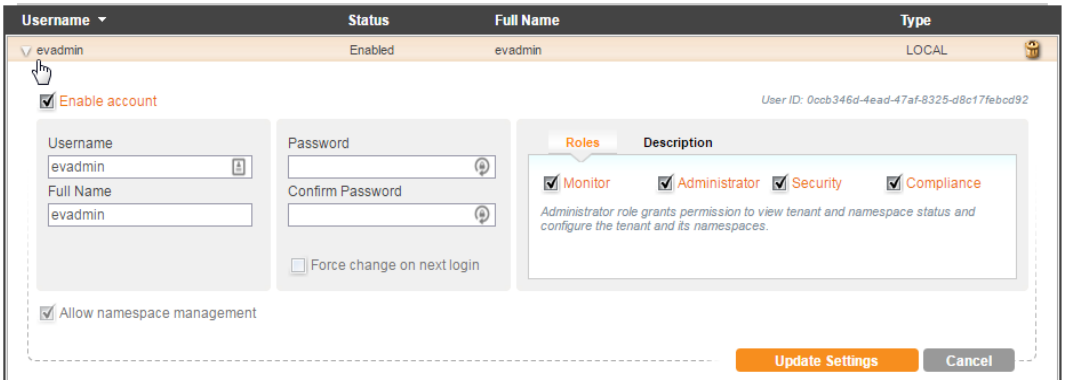
1. Open the HCP Tenant Management Console.



2. The tenant-level user must have administrative privileges to create a new namespace. Select the **Security** tab and then click on **Users**.

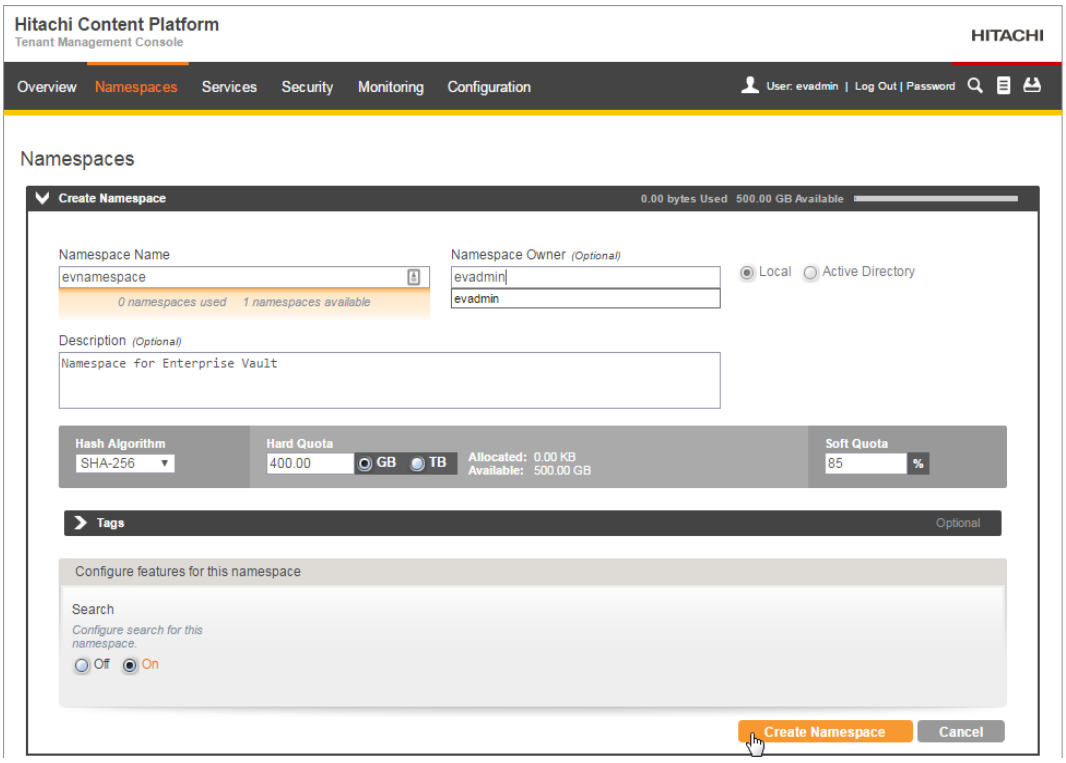


3. Click to **expand** the initial user and assign compliance and administrative privileges to the account. These assignments are immediately updated and are reflected in the menu options.



4. Select the **Namespaces** tab and then click on **Create Namespace**.

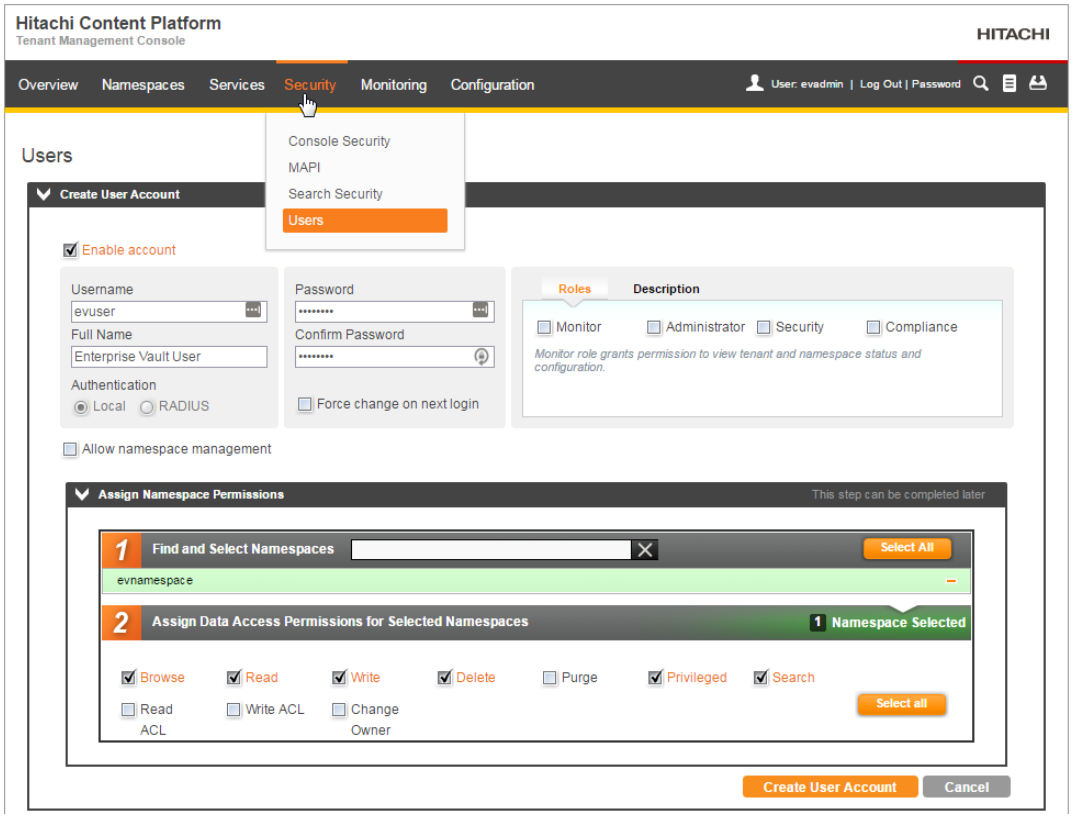
5. Assign a name for the new namespace in UTF-8 lowercase letters.



6. Assign a **Disk Quota** for anticipated data storage requirements.

7. At the bottom of the page under **Search**, select **On**. Search needs to be enabled to allow EV to query the storage structure on HCP when attempting to rebuild its internal database view.

8. Select the **Security** -> **Users** tab and create a User Access Account with a password that has required access permissions to the namespace.



Important: Do not change the default retention setting (**Deletion Allowed**) for the namespace.

9. If you want to enable HTTP access on the HCP partition in EV, enable the HTTP protocol in the **Protocol** tab of the Namespace Admin UI.

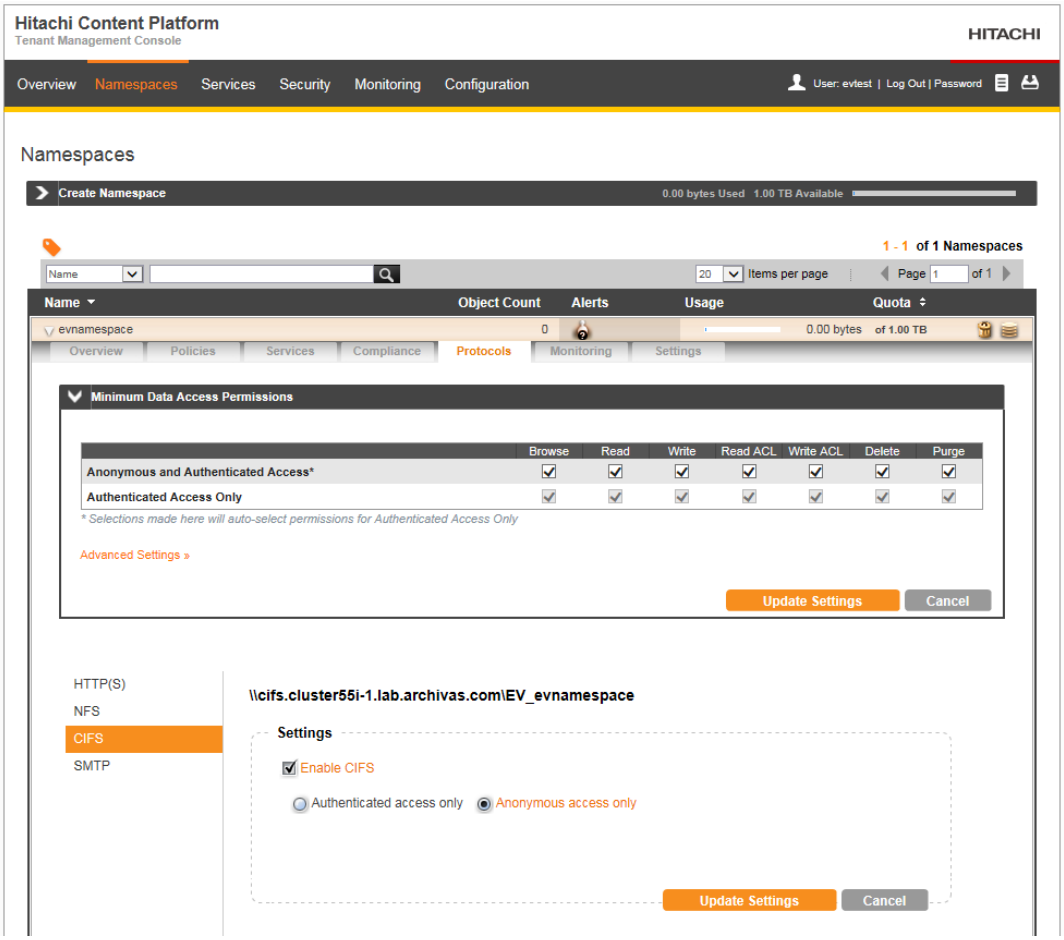
   The HTTP protocol should be used only on a network that is secure from malicious monitoring.

Configuring an HCP namespace for CIFS

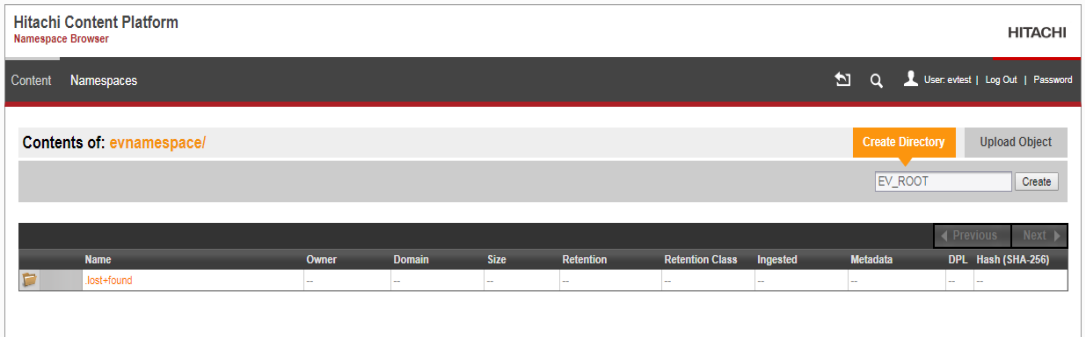
Optionally, after you have created an HCP namespace, you can configure that namespace to utilize the CIFS namespace access protocol. To configure an HCP namespace to use the CIFS protocol:

1. In the HCP Tenant Management Console, click on the **Protocols** tab of a namespace that you have created.

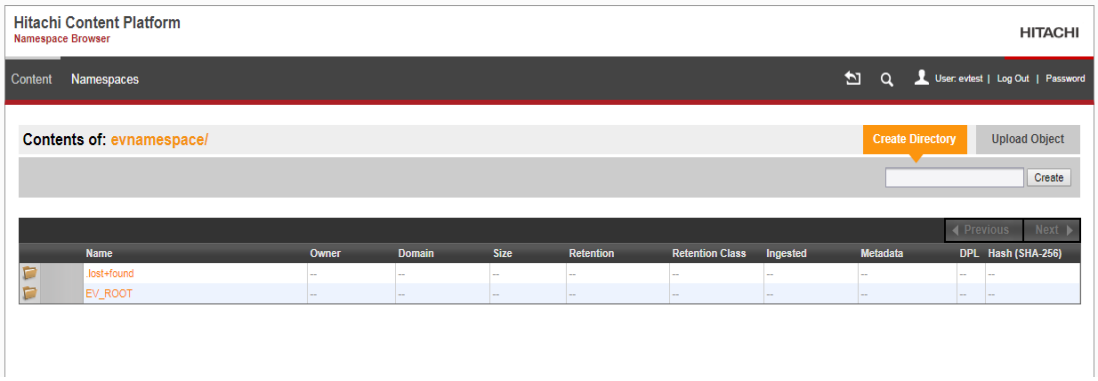
2. Select the **Enable CIFS** option.
3. Select the **Anonymous access only** option.
4. Under **Minimum Data Access Permissions**, select each of the checkboxes in the **Anonymous and Authenticated Access** row.



5. Under **Case Sensitivity**, select the **Make CIFS case sensitive** option.
6. Under **Case Sensitivity**, select the **Make CIFS case forcing** option, then select the **Uppercase** option.
7. Enter the **Namespace Browser** of the namespace that you have created.



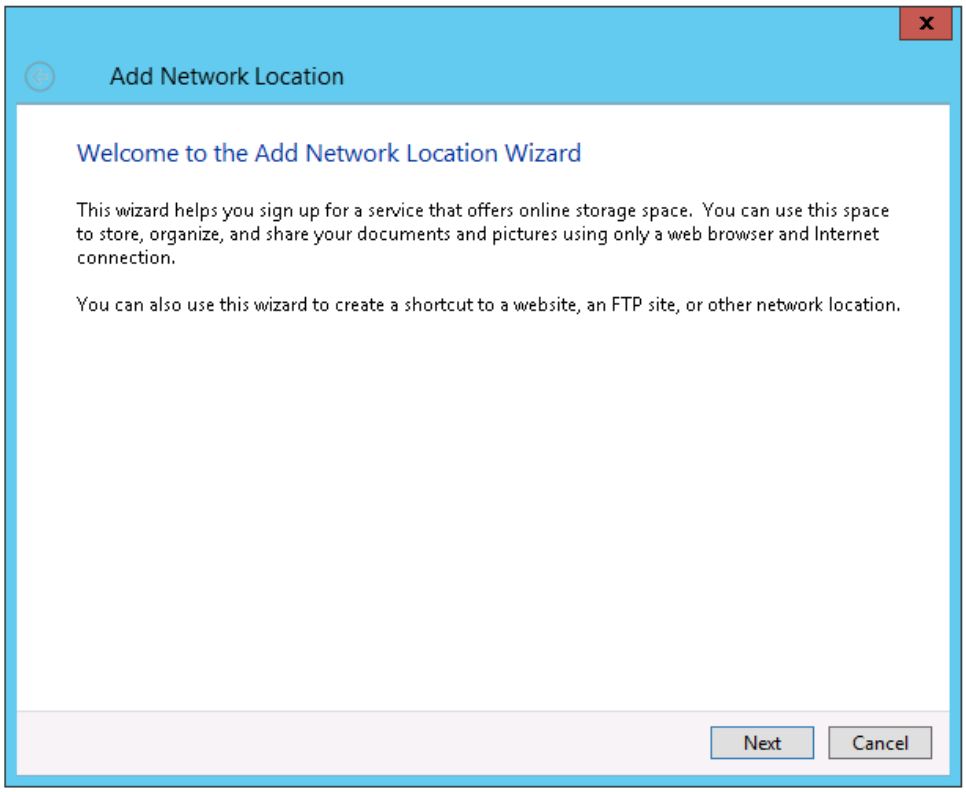
8. Under **Create Directory**, enter a name for the new top-level directory. **Do not use any lowercase letters in the directory name.** The directory that you create will be used to contain the archived EV data.



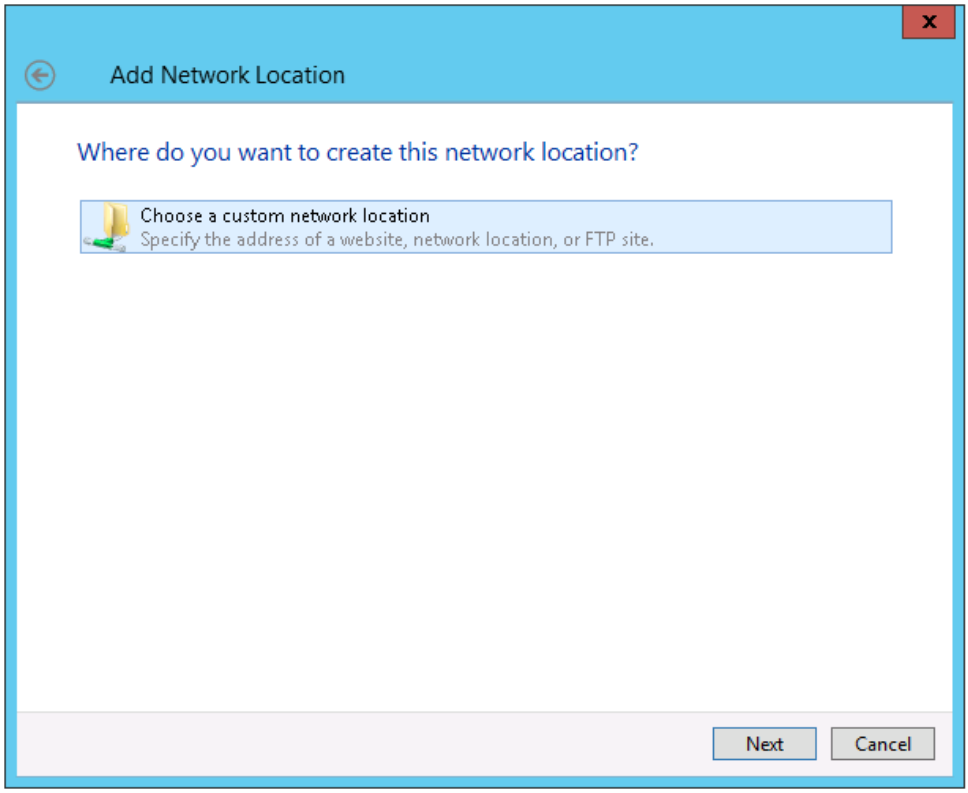
Configuring an EV server for CIFS

If you have configured an HCP namespace that you have created to use the CIFS protocol, you also need to configure an EV server for CIFS access. To configure an EV server for CIFS access:

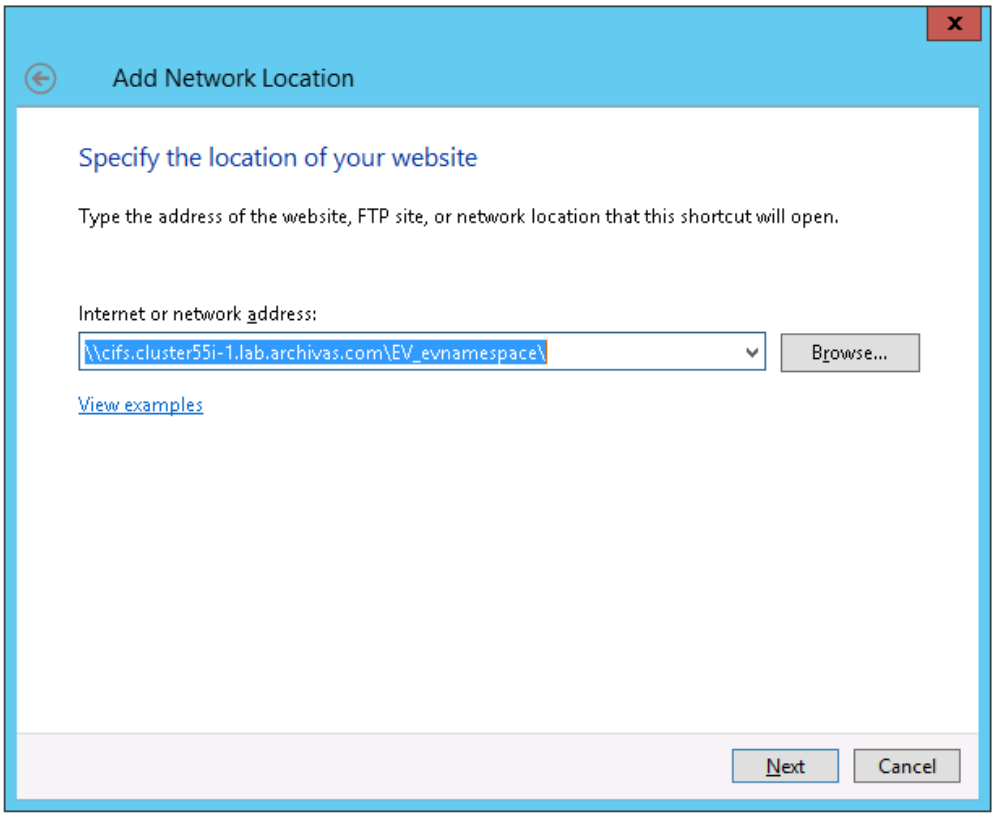
1. In your EV server, open the **Add Network Location** wizard, then click on **Next**.



2. Select **Choose a custom network location** then click on **Next**.

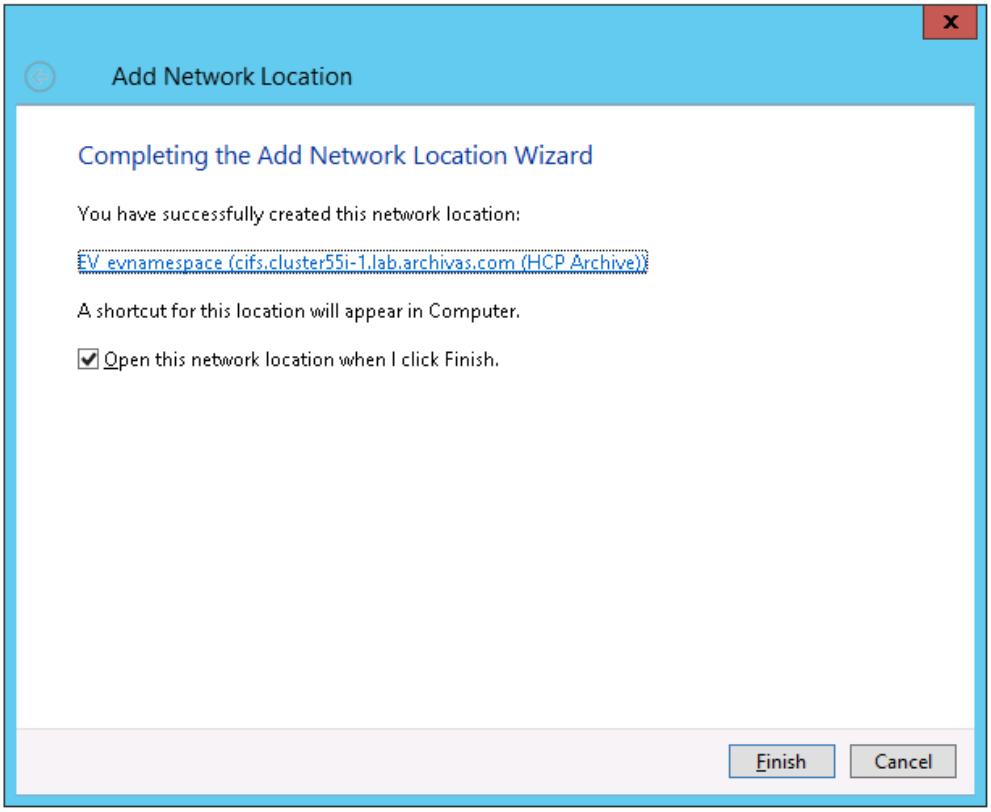


3. Enter the network address of the HCP namespace that you have created. This is the address on which you clicked to enter the **Namespace Browser** in the previous section.



4. Click on **Next**.

5. Confirm that you have successfully created the network location, then click on **Finish**.

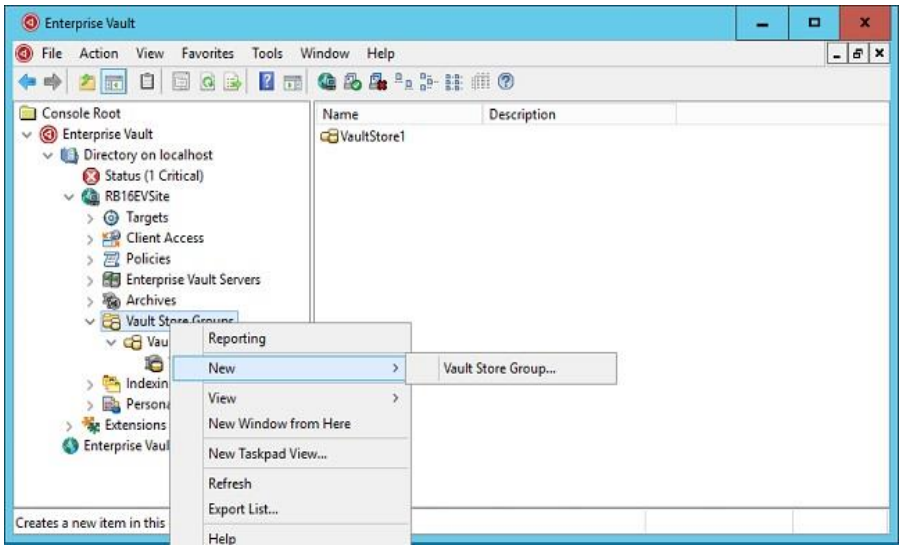


Creating a Vault Store Group in EV

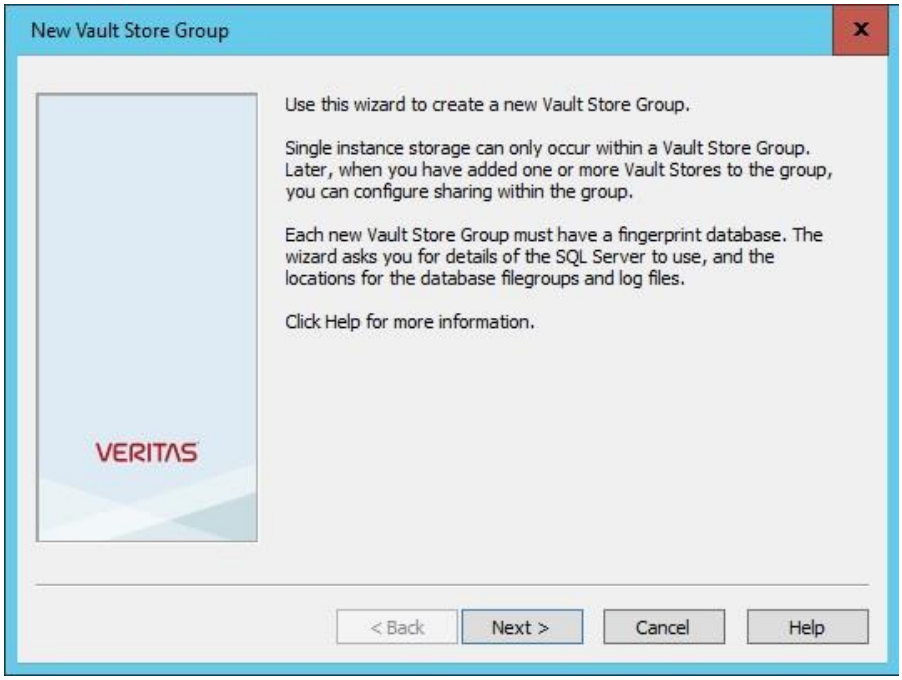
Vault Stores are grouped within Vault Store Groups. If you use Enterprise Vault single instance storage, a Vault Store Group forms an outer boundary for the sharing of SIS parts.

To create a Vault Store Group using the New Vault Store Group wizard:

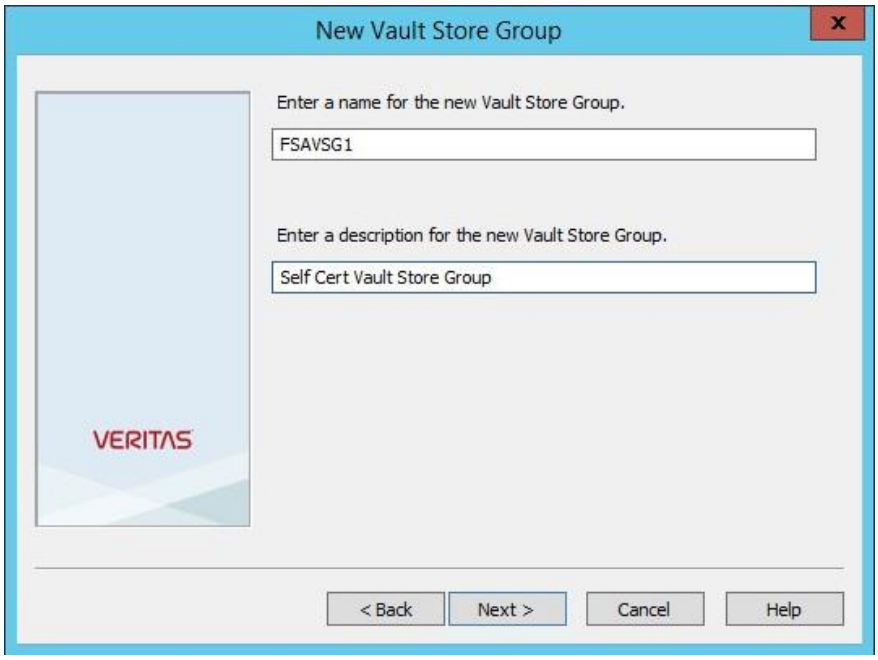
1. Right-click on **Vault Store Group** in the EV Administration Console. Select **New** -> **Vault Store Group**.



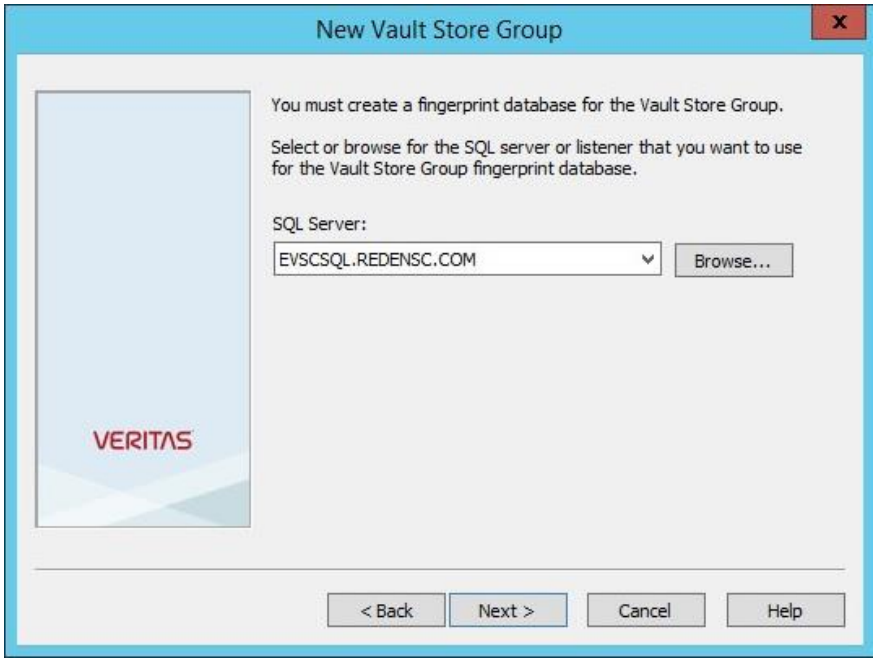
2. Click on **Next**.



3. Enter a name **(FSAVSG1)** and a description **(Any)** for the new Vault Store Group then click on **Next**.

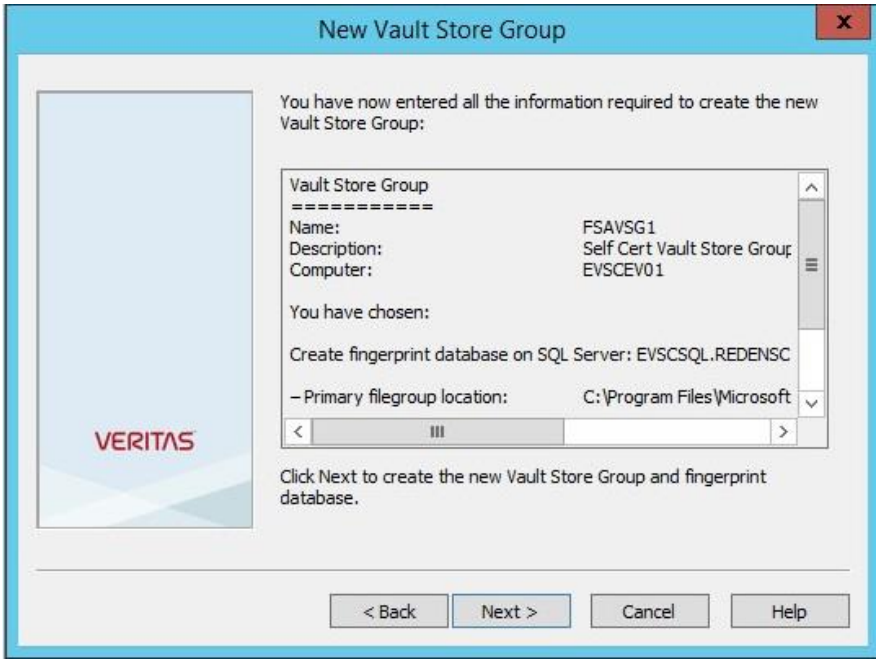


4. Enter the SQL server to be used for the Vault Store Group Fingerprint Database then click on **Next**.

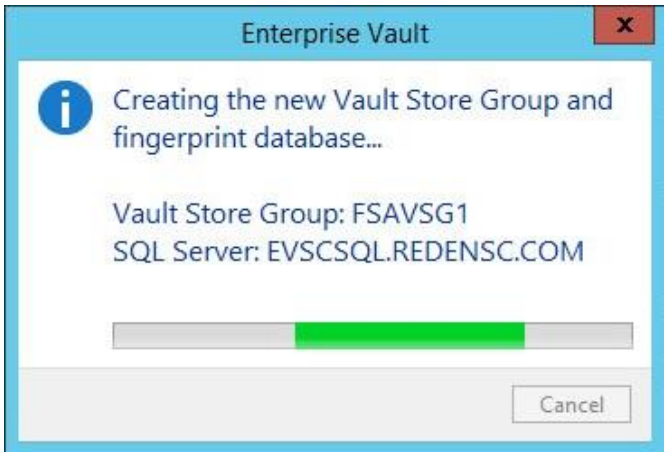


5. Enter the SQL Primary filegroup and Transaction log locations. Make sure that **Configure additional locations for the non-primary filegroups** is unchecked then click on **Next**.

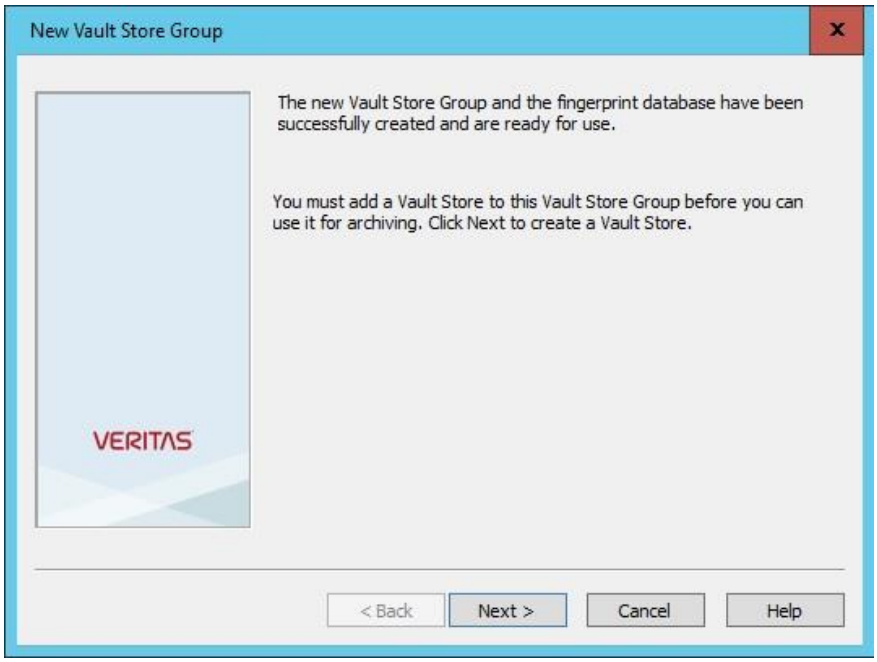
6. Confirm the **Vault Store Group** Information then click on **Next**.



7. Click on **Next** to create the new Vault Store Group and fingerprint database.



8. Check that the Vault Store Group and fingerprint database have been successfully created then click on **Next**.



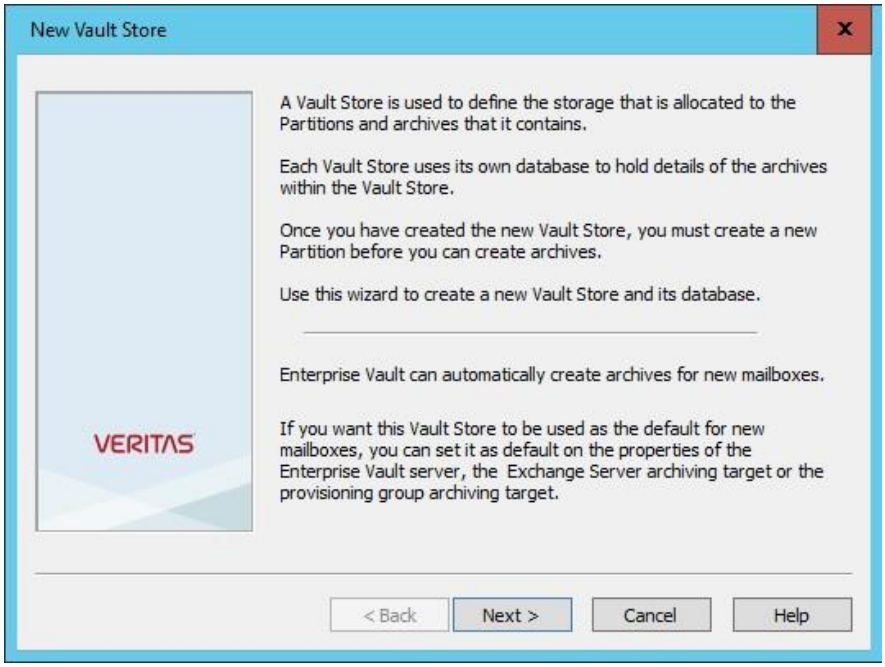
Creating a Vault Store in EV

When you create a Vault Store, you need to specify an Enterprise Vault Storage service to manage it and a location for the SQL Vault Store database.

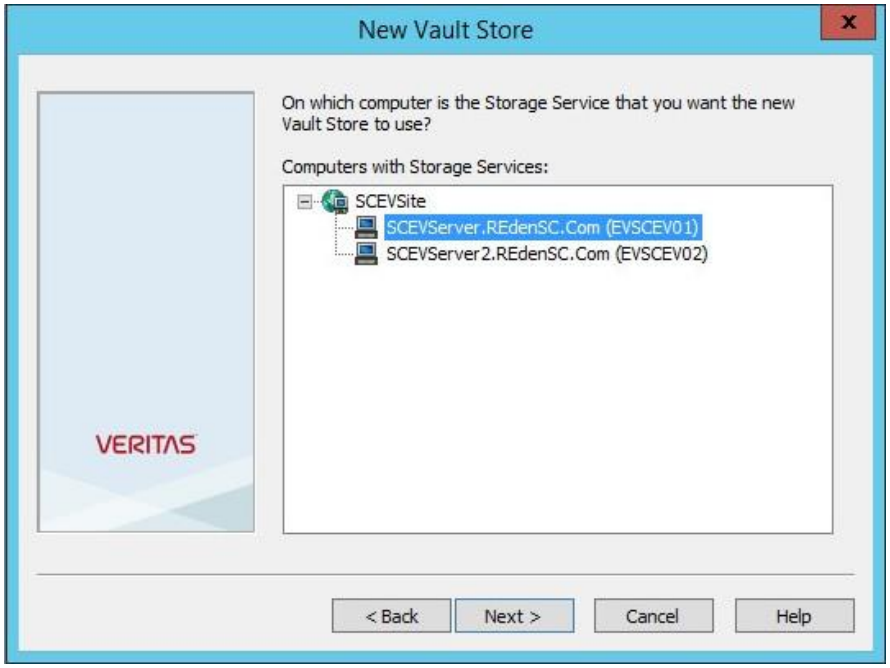
The Vault Store database holds information about the archives in the Vault Store and all the items that are stored in each archive. For example, when an archived item is backed up, this is reflected in the information held in the Vault Store database.

To create a Vault Store:

1. After creating a Vault Store Group in the New Vault Store Group wizard, click on **Next** to create a new Vault Store.

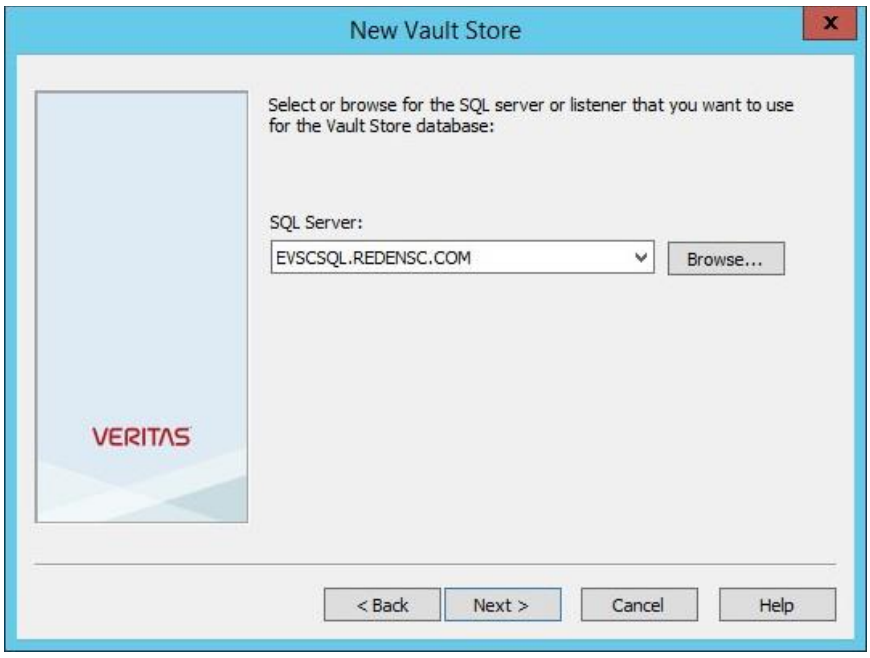


2. Select server **EVSCEV01** for the Storage Service that you want the new Vault Store to use then click on **Next**.

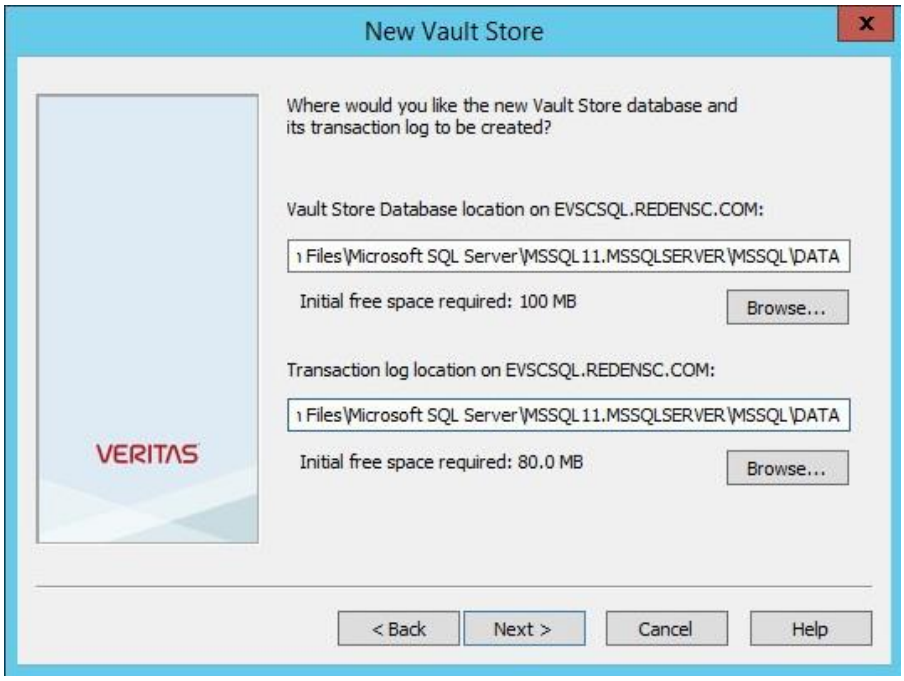


3. Enter a name **(FSAVS1)** and a description **(Any)** for the new Vault Store then click on **Next**.

4. Enter the SQL Server to be used for the Vault Store database then click on **Next**.

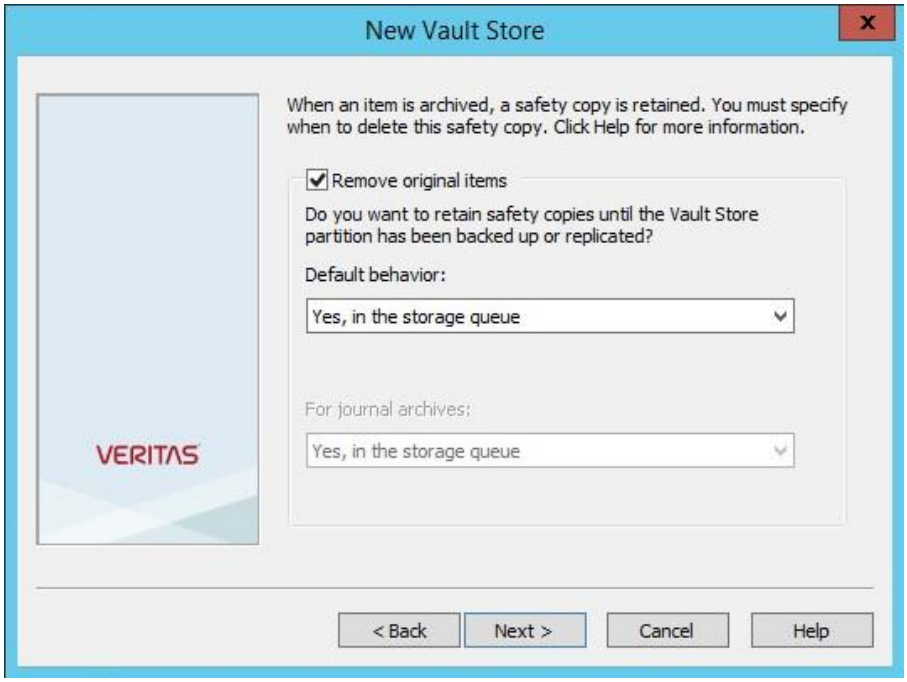


5. Enter the **Vault Store Database** and **Transaction log** locations then click on **Next**.

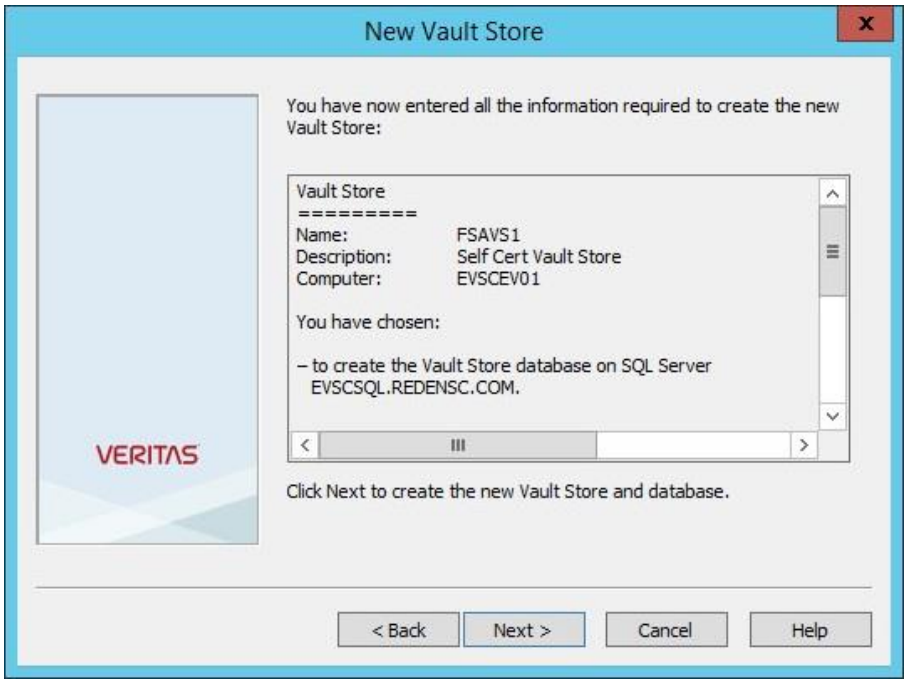


6. Ensure that **Remove original items** is selected. In the **Default Behavior** dropdown menu, select **Yes, in the storage queue** then click on **Next**.

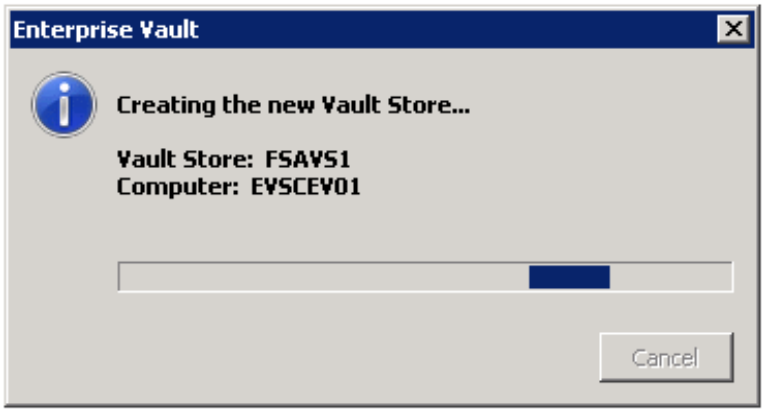
   For recommended configuration settings, see About Enterprise Vault Safety Copies.



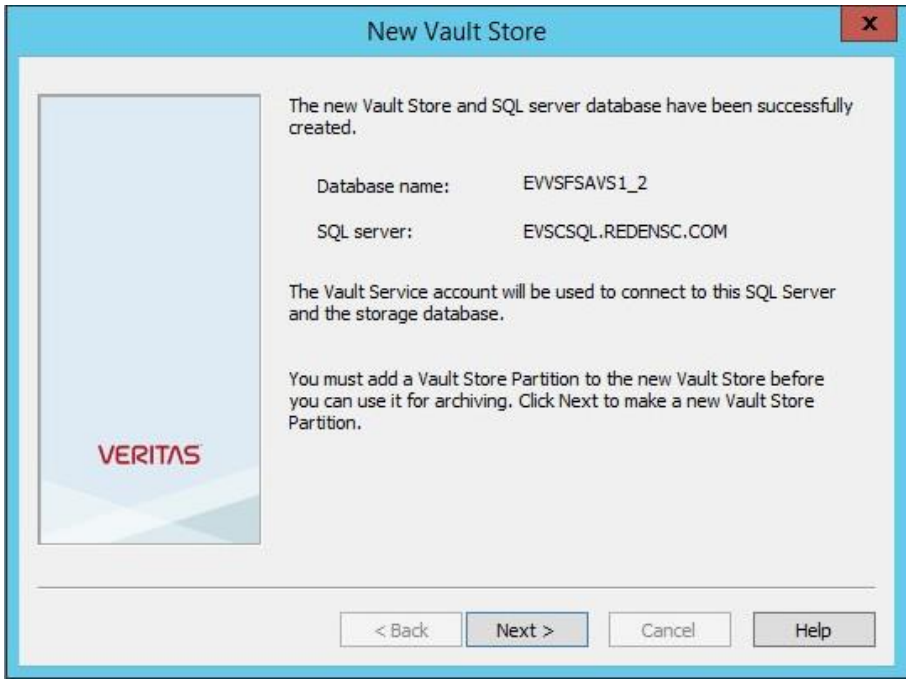
7. Confirm the Vault Store information then click on **Next**.



8. The installation window displays the setup progress.



9. Check that the Vault Store and SQL server database have been successfully created then click on **Next**.



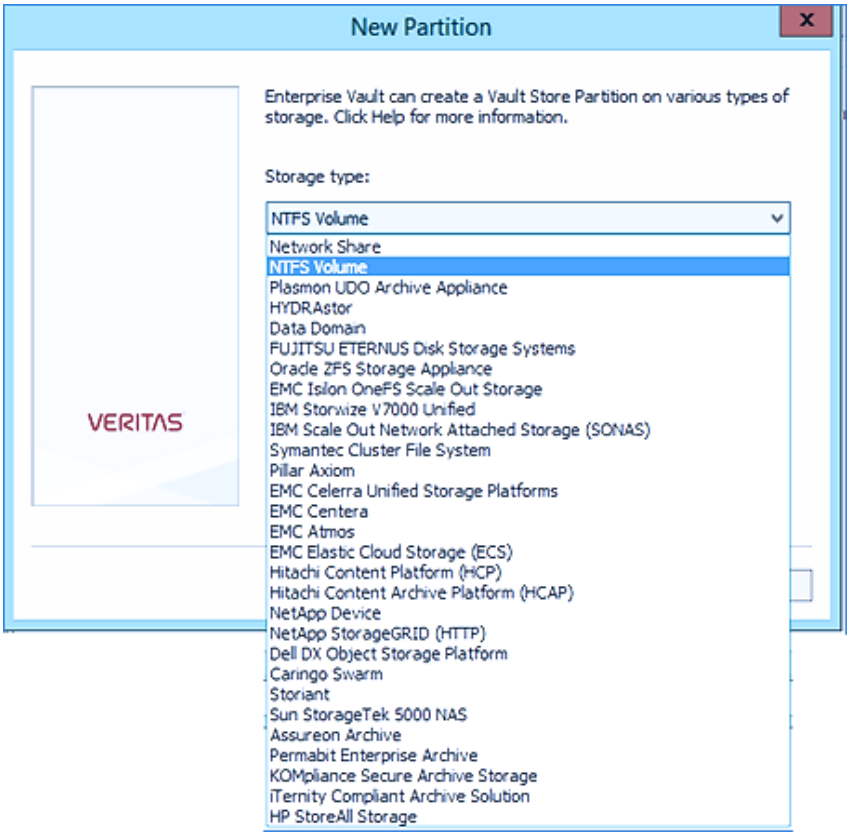
Creating an HCP Vault Store Partition in EV

The HCP Vault Store Partition can be created within any existing Vault Store Group and Vault Store within EV. A new Vault Store Group and/or Vault Store may be created for HCP using standard EV techniques.

To create an HCP Vault Store Partition in EV using the CIFS protocol, see Creating an HCP Vault Store Partition in EV with CIFS.

To create an HCP Vault Store Partition in EV (without CIFS):

1. Right-click on the selected Vault Store and select **New Partition**. In the Veritas **New Partition** window, select **Hitachi Content Platform (HCP)** from the dropdown menu.



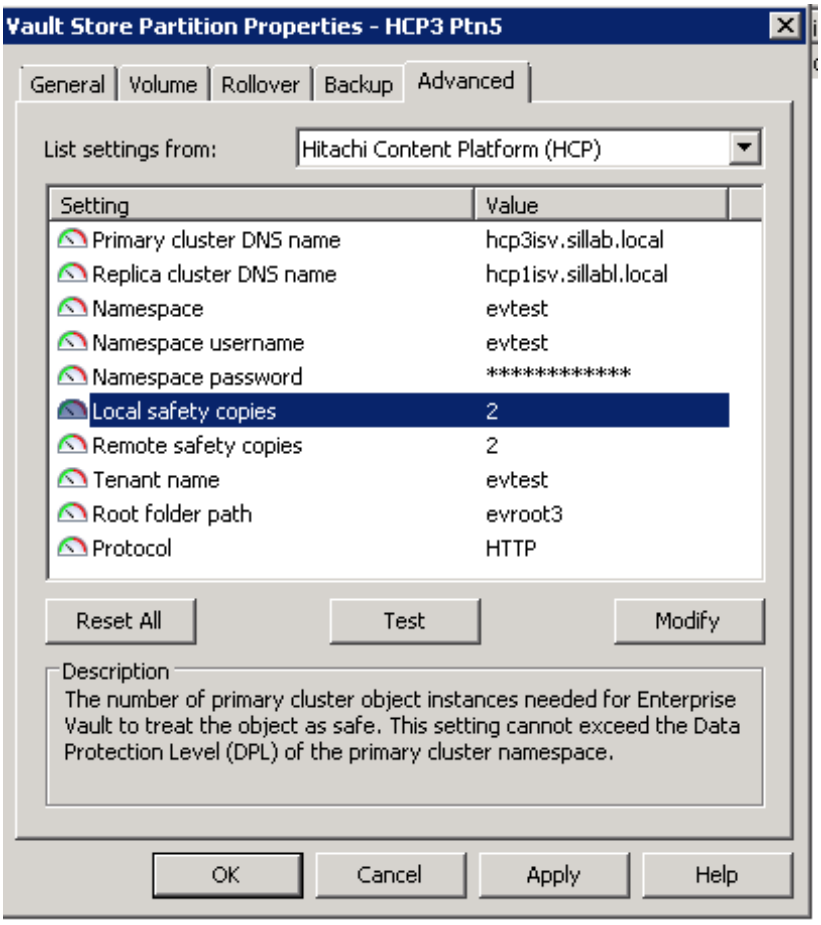
2. In the **Configuration** window, enter the **DNS**, **Tenant**, **Namespace**, and **Data Access User** information.

3. If you do not want to configure a replica, leave the **Replica Cluster Name** blank. A replica can be configured at a later time.

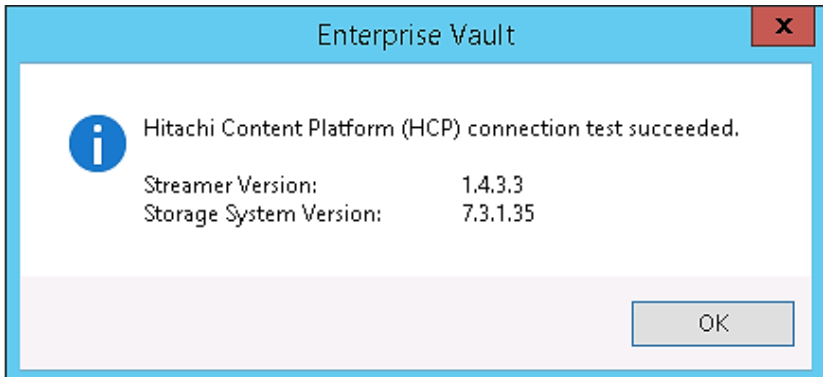
4. Set the number of **Local Safety Copies** to the DPL (data protection level) value of the local namespace accessed by EV.

5. Set the number of **Remote Safety Copies** to the DPL (data protection level) value of the remote HCP namespace accessed by EV. If EV is not accessing a remote HCP namespace, set the value to **0**.

6. Click the **Advanced** tab to view the new settings.

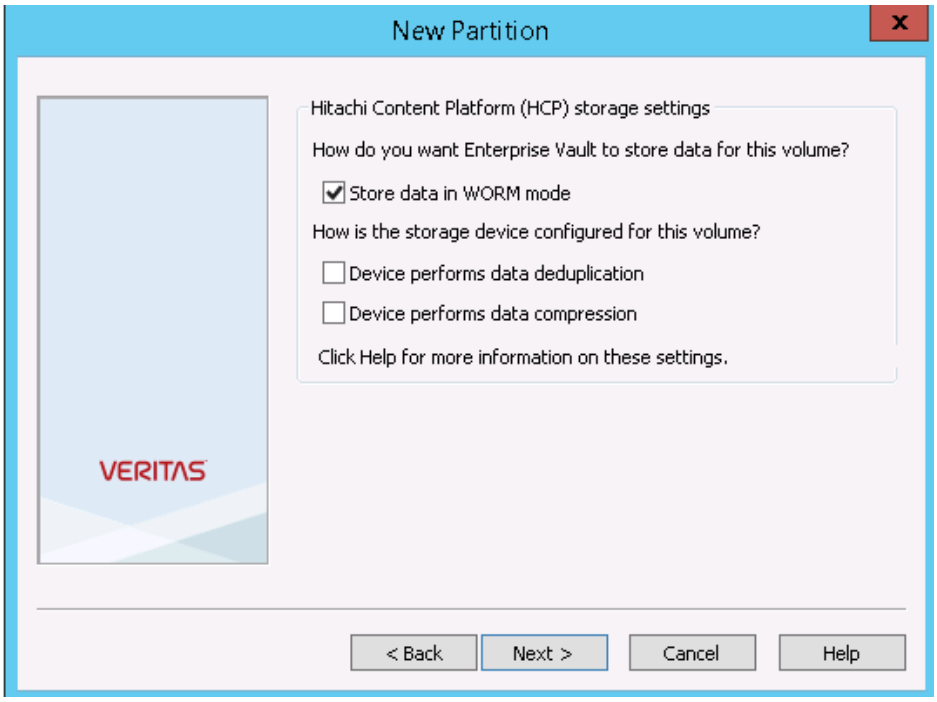


7. Confirm the settings then click on **Test**. The following confirmation message is displayed:



Note: In the above message, **Streamer Version** refers to EV Streamer. **Storage System Version** refers to HCP.

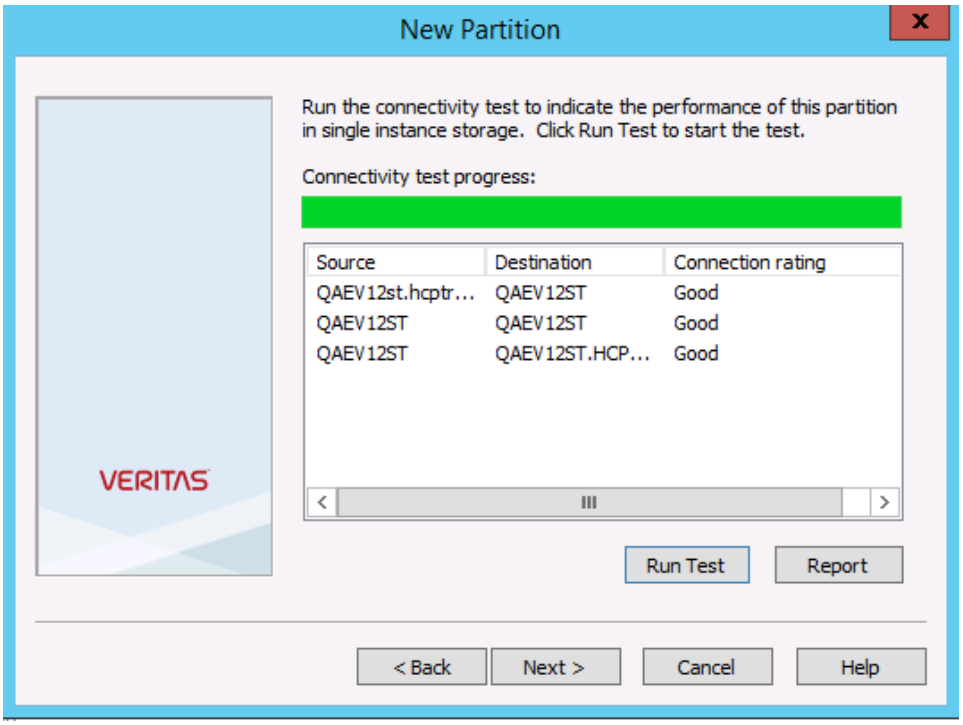
8. Click on **OK** to return to the **New Partition** window.



9. Check the **Store data in WORM mode** checkbox.
10. Uncheck the **Device performs data deduplication** checkbox.

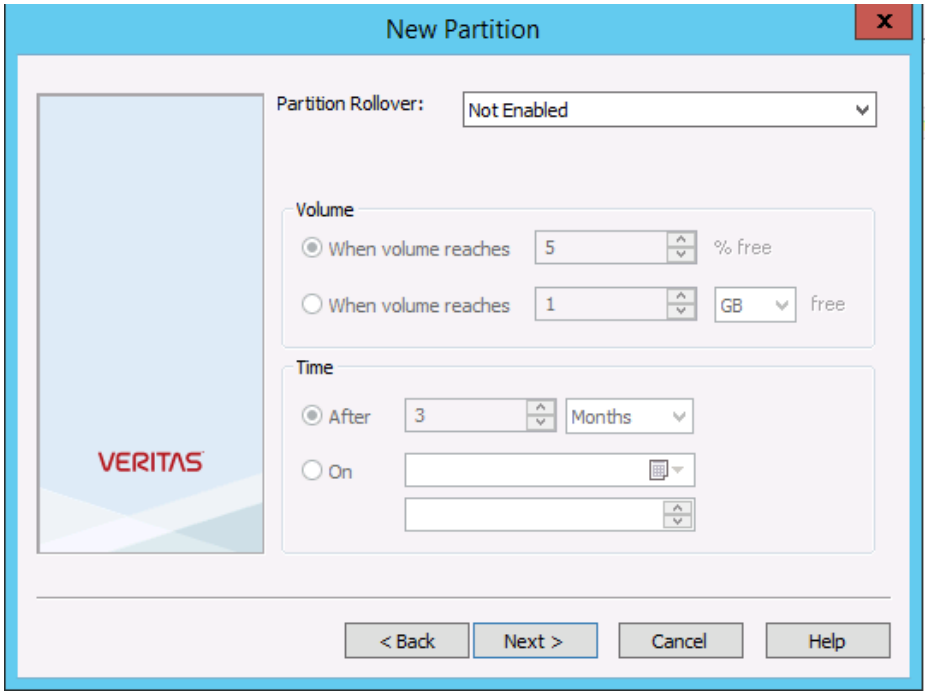
Important: If you do not uncheck this checkbox, EV sends data to HCP in a format that is incompatible with HCP's data deduplication feature.

11. Uncheck the **Device performs data compression** checkbox to allow compression through EV.
12. Click on **Next** to display the **Connectivity Test** window.

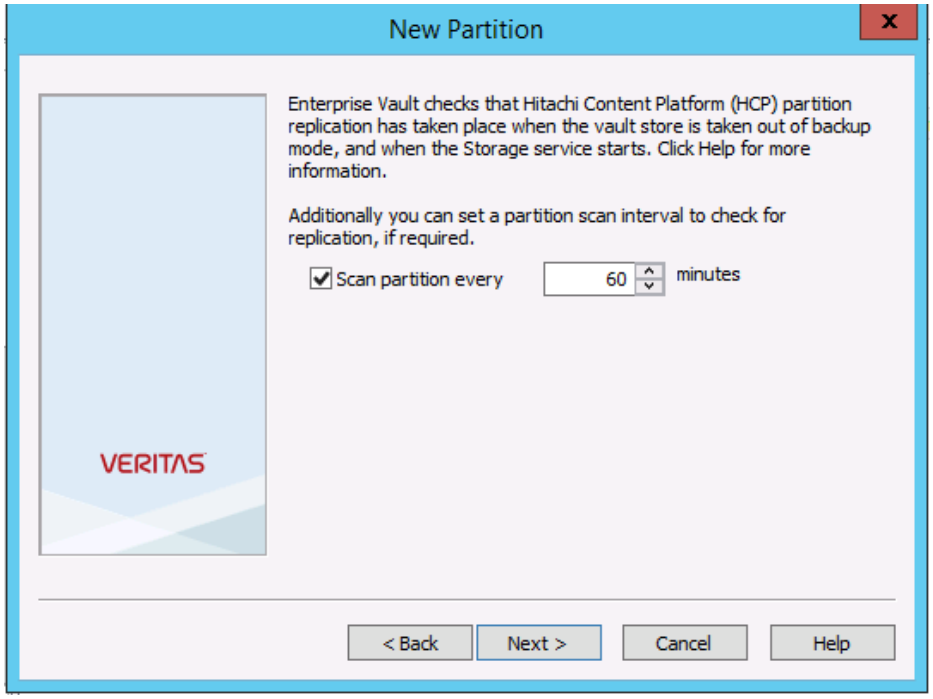


13. Click on **Run Test** to ensure proper connectivity of all EV server components with HCP.

14. Click on **Next** to display the **Partition Rollover Configuration** window. By default, Partition Rollover is not enabled.

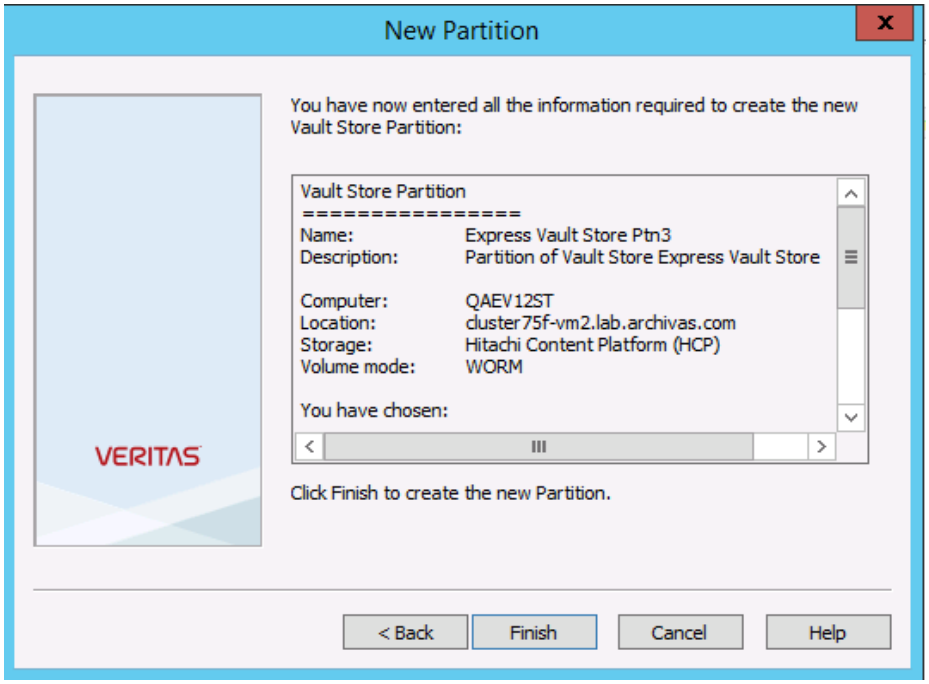


15. Click on **Next** to display the **Scan Frequency** window.



16. Adjust the scan frequency as necessary.

17. Click on **Next** to display the **Final Summary** window.



18. Review the summary of the new Vault Store Partition then click on **Finish** to create the new Partition. If any items in the summary are incorrect, click on **Back** to change a setting or **Cancel** to terminate the process.

19. After you complete the above procedures and return to the EV Administration Console, right-click on **Vault Store Group**.

20. Click on **Properties**.

21. Click on the **Sharing** tab.

22. Click on **Configure Sharing**.

23. In the dropdown menu next to **All Vault Stores configured as**, select **Share within Vault Store**.

    Make sure that **Share within group** is **NOT** selected.

    The default and recommended selection is **Share within Vault Store**.

24. Click on **Next**.

25. Click on **Finish**.

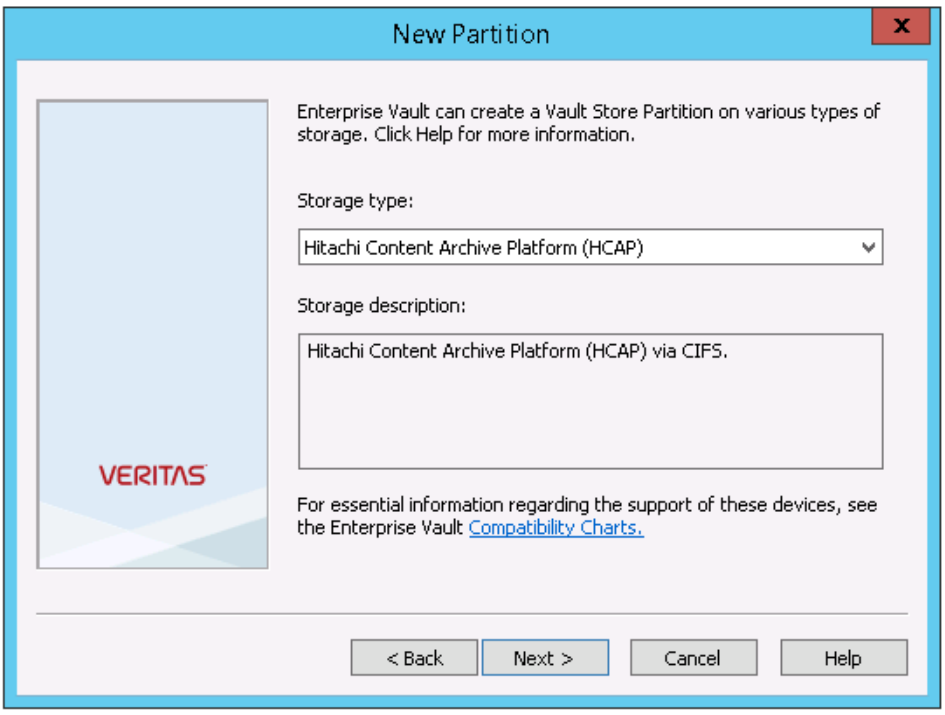
Creating an HCP Vault Store Partition in EV with CIFS

The HCP Vault Store Partition can be created within any existing Vault Store Group and Vault Store within EV. A new Vault Store Group and/or Vault Store may be created for HCP using standard EV techniques. You can also create HCP Vault Store Partitions in EV using the CIFS namespace access protocol.

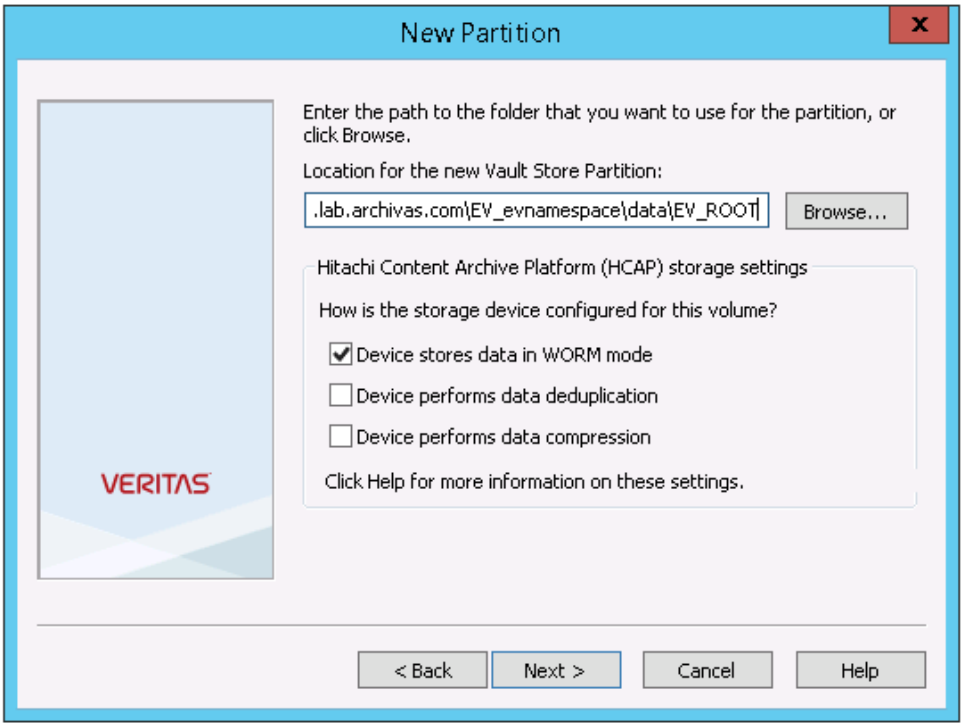
For the procedural steps on creating HCP Vault Store Partitions in EV without using the CIFS protocol, see Creating an HCP Vault Store Partition in EV.

To create an HCP Vault Store Partition in EV using the CIFS protocol:

1. Right-click on the selected Vault Store and select **New Partition**. In the Veritas **New Partition** window, select **Hitachi Content Archive Platform (HCAP)** from the dropdown menu.



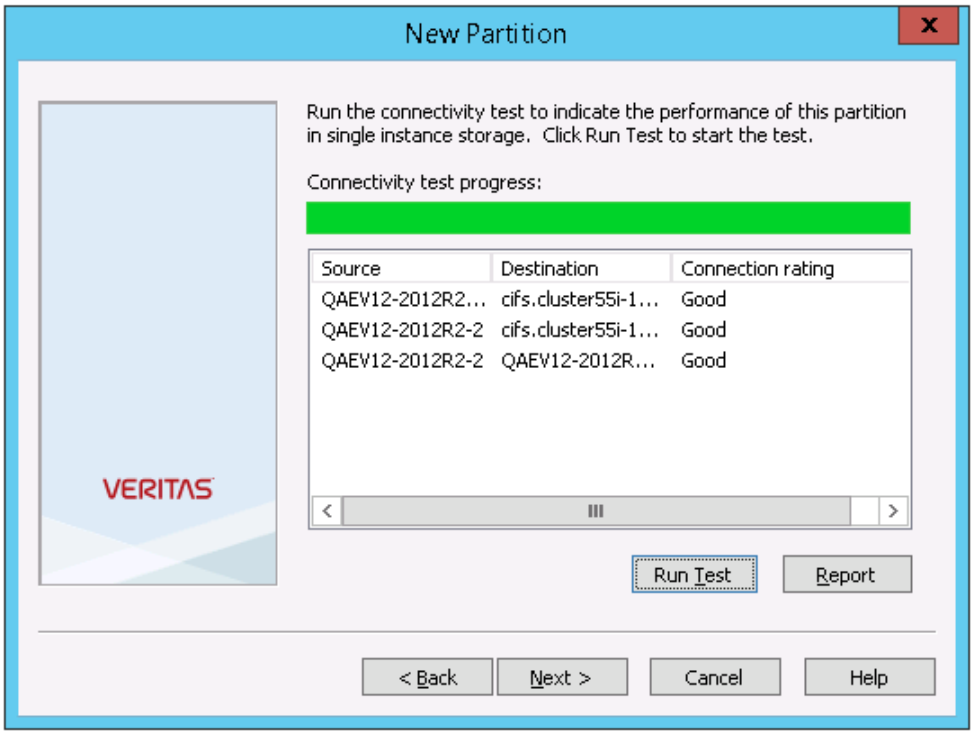
2. In the **Location for the new Vault Store Partition** field, enter the network address of the HCP namespace that you have configured for CIFS. At the end of the address, enter **\data** followed by the name of the top-level directory that you have created in Configuring an HCP namespace for CIFS, as displayed in the following image.



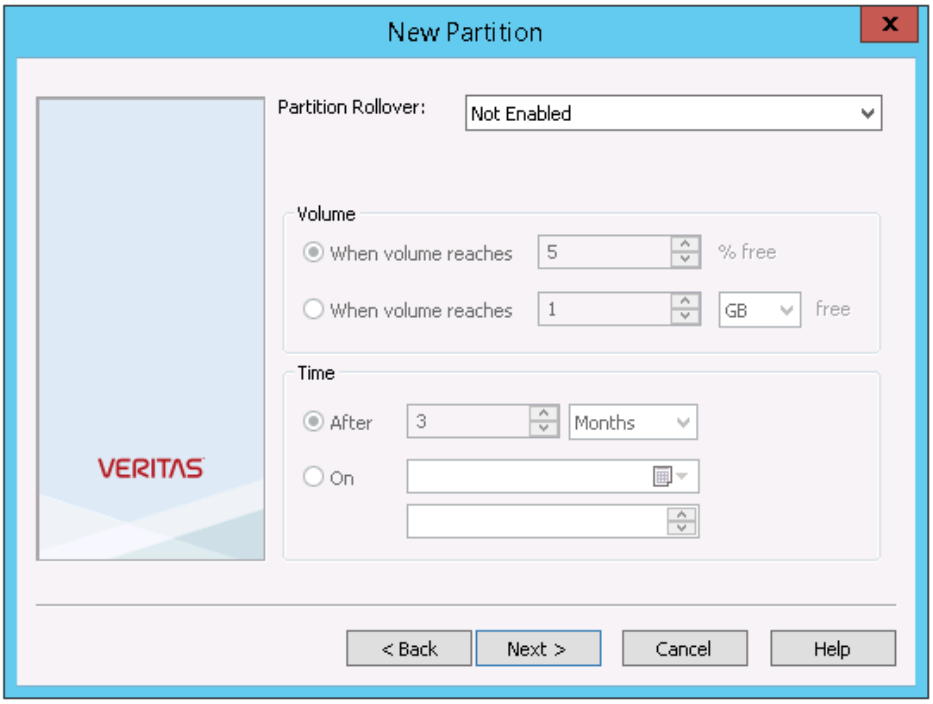
3. Optionally, check the **Device stores data in WORM mode** checkbox.
4. Uncheck the **Device performs data deduplication** checkbox.

Important: If you do not uncheck this checkbox, EV sends data to HCP in a format that is incompatible with HCP's data deduplication feature.

5. Uncheck the **Device performs data compression** checkbox to allow compression through EV.
6. Click on **Next** to display the **Connectivity Test** window.

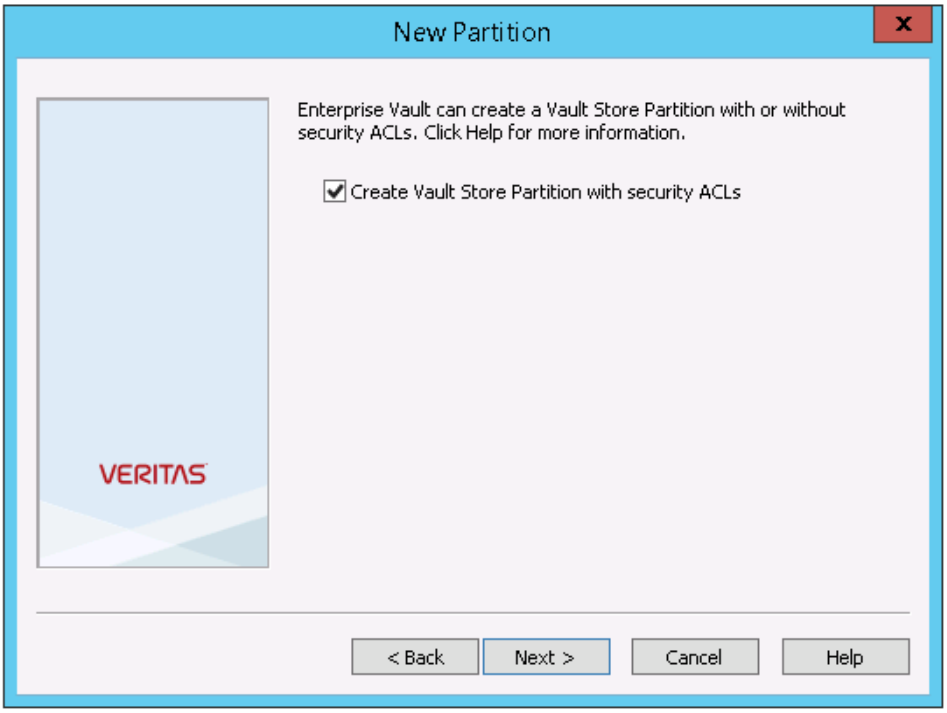


7. Click on **Run Test** to ensure proper connectivity of all EV server components with HCP.
8. Click on **Next** to display the **Partition Rollover Configuration** window. By default, Partition Rollover is not enabled.



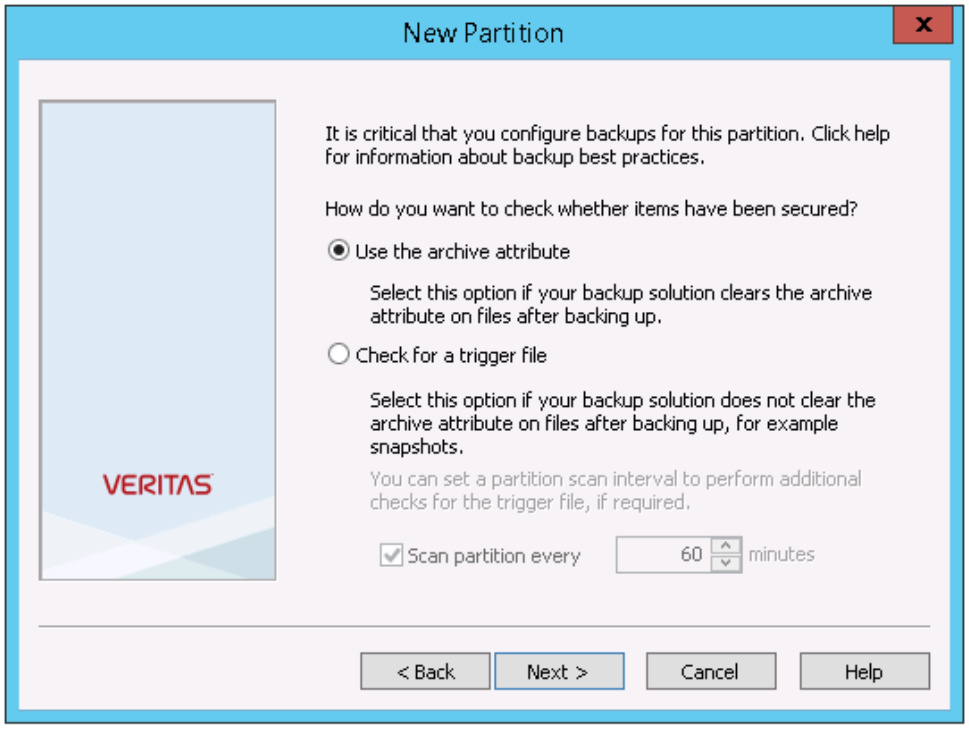
9. Click on **Next**.

10. Optionally, select **Create Vault Store Partition with security ACLs**.

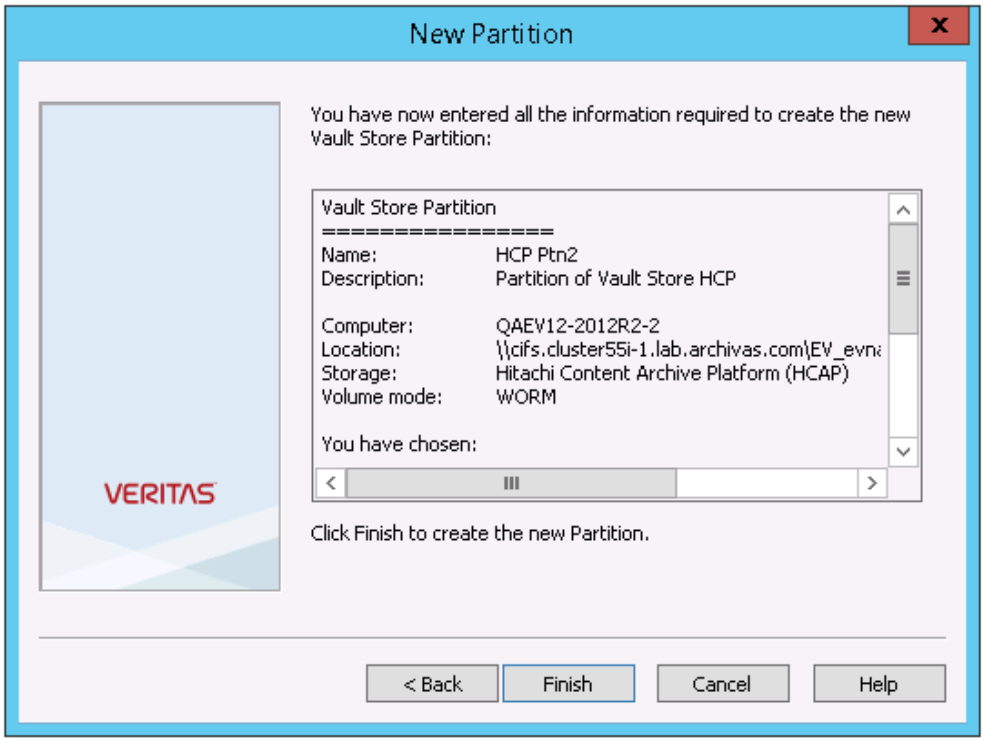


11. Click on **Next**.

12. Select the method for checking whether items have been secured to the HCP Vault Store Partition.



13. Click on **Next** to display the **Final Summary** window.



14. Review the summary of the new Vault Store Partition then click on **Finish** to create the new Partition. If any items in the summary are incorrect, click on **Back** to change a setting or **Cancel** to terminate the process.

15. After you complete the above procedures and return to the EV Administration Console, right-click on **Vault Store Group**.

16. Click on **Properties**.

17. Click on the **Sharing** tab.

18. Click on **Configure Sharing**.

19. In the dropdown menu next to **All Vault Stores configured as**, select **Share within Vault Store**.

    Make sure that **Share within group** is **NOT** selected.

    The default and recommended selection is **Share within Vault Store**.

20. Click on **Next**.

21. Click on **Finish**.

4

Best practices

This chapter provides some best practices to consider while installing, setting up, and configuring EV Streamer. This chapter also provides some information about Enterprise Vault Safety Copies.

- ☐ Best practices
- ☐ About Enterprise Vault Safety Copies

Best practices

Here are some best practices for installing, setting up, and configuring EV Streamer:

- During the Enterprise Vault installation and configuration, consider having storage queue, cache, indexes, and MSMQ on different dedicated physical drives rather than on the system drives.
- Increase the number of threads for the storage archive process to achieve a higher archival rate depending on the workload.
- Use two separate physical servers for EV and SQL Server.
- For SQL Server, allot separate disks for SQL installation, data, and logs. For more information on this, see Enterprise Vault SQL best practices.
- Allot a minimum of 16 GB of RAM for the EV server.
- Follow the network bandwidth guidelines in the Veritas Performance Guide.

About Enterprise Vault Safety Copies

Enterprise Vault can be configured to retain archived items until you back up the vault store partition that contains the items. During the time between archiving and removal, the original items are treated as safety copies by EV. After the vault store partition is backed up, EV removes the safety copies.

The removal of safety copies occurs when the storage service starts and when backup mode is cleared from the vault store. EV also creates shortcuts and placeholders at this time if EV is configured to do so. During the creation of each vault store, you can select from the following options to control how EV manages safety copies:

- **No, remove immediately after archiving**: All safety copies are removed immediately after the items have been archived.
- **Yes, in the original location**: EV keeps the original items until you back up the vault store partition that contains the items.
- **Yes, in the storage queue**: EV keeps safety copies in the storage queue until you back up the vault store partition that contains the items.

The optimal EV safety copies settings are situationally dependent, but selecting **Yes, in the original location** is typically the safest option.

Selecting **Yes, in the storage queue** immediately frees up space on the source but also runs the risk of possible third-party interference.

5

Troubleshooting

This chapter provides some information for troubleshooting EV Streamer.

- ☐ Access to HCP failed
- ☐ Incorrect parameter

Troubleshooting

Access to HCP failed

An access failure leads to a connection test failure. Access Denied to HCP occurs under the following conditions:

- The tenant name is incorrect (for HCP 7.*x* or later)
- The namespace name is incorrect (for HCP 7.*x* or later)
- The user name is incorrect or does not exist
- The password is incorrect

Check the Enterprise Vault event log for more information.

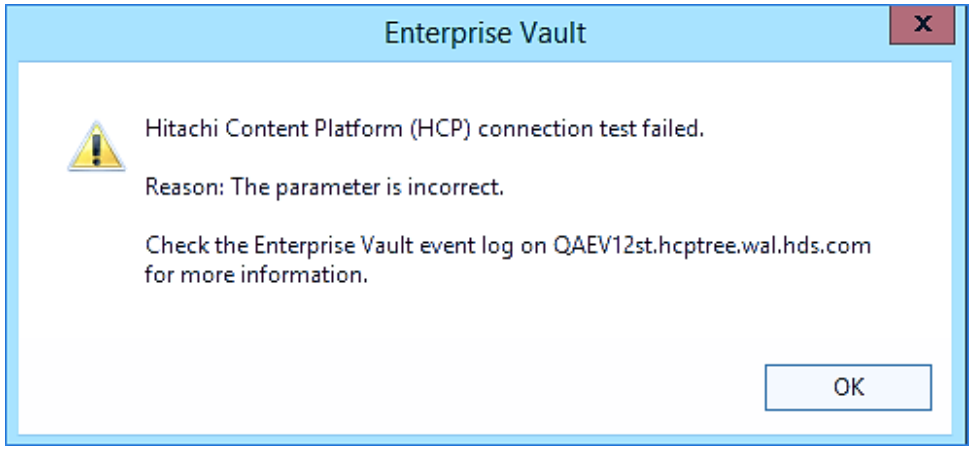
Incorrect parameter

An incorrect parameter leads to a connection test failure. Parameter failures occur under the following conditions:

- The value for remote safety copies (other than zero) is specified with no replica
- The Primary Cluster DNS Name is incorrect

Check the Enterprise Vault event log for more information.

When the parameter is incorrect, Enterprise Vault alerts you that the HCP connection test failed.



Hitachi Vantara

Corporate Headquarters
750 Central Expressway
Santa Clara, California 95050-2627
U.S.A.
Phone: 1 408 970 1000
HitachiVantara.com
info@hitachivantara.com

Asia Pacific and Americas
750 Central Expressway
Santa Clara, California 95050-2627
U.S.A.
Phone: 1 408 970 1000
info@hitachivantara.com

Europe Headquarters
Sefton Park
Stoke Poges
Buckinghamshire SL2 4HD
United Kingdom
Phone: + 44 (0)1753 618000
info.emea@hitachivantara.com