Hitachi Content Platform Anywhere Enterprise

v7.6

Disaster Recovery and Business Continuity Guide

With HCP Anywhere Enterprise you can protect and manage for unplanned disruptions, safeguarding your data and enabling users to continue driving your business. This guide describes a BC/DR plan using HCP Anywhere Enterprise.

MK-HCPAE014-01
December 2023

Contents

Preface

About this document

With Hitachi Content Platform Anywhere Enterprise you can protect and manage for unplanned disruptions, safeguarding your data and enabling users to continue driving your business.

This document describes a BC/DR plan using Hitachi Content Platform Anywhere Enterprise.

Document conventions

This document uses the following typographic convention:

Convention	Description
Bold	• Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click **OK**. • Indicates emphasized words in list items.
Italic	Indicates a document title or emphasized words in text.
`Monospace`	Indicates text that is displayed on screen or entered by the user. Example: `pairdisplay -g oradb`

Intended audience

This document is intended for HCP Anywhere Enterprise Edge Filer administrators.

Accessing product downloads

Product software, drivers, and firmware downloads are available on Hitachi Vantara Support Connect: https://support.hitachivantara.com/.

Log in and select Product Downloads to access the most current downloads, including updates that may have been made after the release of the product.

Getting Help

Hitachi Vantara Support Connect is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to Hitachi Vantara Support Connect for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

Hitachi Vantara Community is a global online community for customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Chapter 1. Introduction

With HCP Anywhere Enterprise you can protect and manage for unplanned disruptions, safeguarding your data and enabling users to continue driving your business. The following solutions should be incorporated in to the company business continuity plan.

During normal operations users access their files residing in a HCP Anywhere Enterprise Edge Filer via network drives that map via the SMB protocol. In the background, the HCP Anywhere Enterprise Edge Filer syncs, in near real time, any file changes to the HCP Anywhere Enterprise Portal, creating another identical copy of the data.

Business continuity (BC) is a set of pre-defined plans that dictate how a company will continue to operate during a disruptive event. BC is proactive and generally refers to the processes and procedures an organization must implement to ensure that mission-critical functions can continue during and after a disaster.

Disaster recovery (DR) is a set of pre-defined procedures that dictate how a company plans to recover its IT infrastructure after a disruptive event. DR is reactive and comprises specific steps an organization must take to resume operations following an incident. Disaster recovery actions take place after the incident, and response times can range from seconds to days.

Whereas BC aims to keep operations running during the incident, DR focuses on restoring technology-based systems to the pre-failure state.

Ransomware is a type of cyber attack where malware designed to encrypt files on a device is used, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption.

Throughout this article, the HCP Anywhere Enterprise Portal or HCP Anywhere Enterprise Edge Filer failure refers to failure due to unplanned events, from cyber attacks to human error to a natural disaster.

Automatic Ransomware Protection and Recovering Compromised Content

HCP Anywhere Enterprise Edge Filers from version 7.6 include **HCP Anywhere Enterprise Ransom Protect** to stop any ransomware attack as soon as it is identified. Taking proactive measures against ransomware attacks helps safeguard your data and ensures the continuity of your operations. HCP Anywhere Enterprise Ransom Protect is able to detect and block ransomware attacks within seconds. For details, see the section on ransomware protection in the *Hitachi Content Platform Anywhere Enterprise Edge Filer Administration Guide*.

Once a ransomware attack has been identified, every affected file is listed. You can then go through the list and rollback the affected files to the state immediately prior to the attack using snapshots.

The HCP Anywhere Enterprise Portal retains previous file versions, by using snapshots. Snapshots are read-only copies of files as they were at a particular point-in-time. A new snapshot is created every 30 seconds. The snapshots are saved for a specified period, as defined in the retention

policy, described in the *snapshot retention policy* section for either a global administrator or for a team administrator. You can restore a version prior to the date that the content was compromised, as described in the *managing previous versions* of folders and files section in the *Hitachi Content Platform Anywhere Enterprise Portal Team Administration Guide*.

Note: Storage node vendors also provide ways to protect the data from disasters and ransomeware attacks.

Continuing Operations After a Portal Fails

If the HCP Anywhere Enterprise Portal fails, end users can continue to work on any file that is not a stub file on the HCP Anywhere Enterprise Edge Filer. The changed files will not be synced to the HCP Anywhere Enterprise Portal nor other HCP Anywhere Enterprise Edge Filers connected to the HCP Anywhere Enterprise Portal until the HCP Anywhere Enterprise Portal has been recovered and syncing from the HCP Anywhere Enterprise Edge Filer completed.

To ensure business continuity in case the HCP Anywhere Enterprise Portal fails, you need to back up the HCP Anywhere Enterprise Portal servers and storage. You need to use third-party recovery tools to back up the HCP Anywhere Enterprise Portal servers and storage.

You also need to back up the HCP Anywhere Enterprise Portal database. To restore the HCP Anywhere Enterprise Portal database from a backup requires at least one WAL file as well as the base backup. Hitachi Vantara recommends enabling WAL archiving and keeping the WAL archives and a copy of the base backup at a different physical location to ensure recovery is possible even when the database becomes unusable in the primary location.

You can also use other PostgreSQL tools, or other third-party tools, to back up the HCP Anywhere Enterprise Portal database. For example, you can use the PostgreSQL tool *pg_dump* to back up the PostgreSQL database on the primary database server. pg_dump makes consistent backups even if the database is being used concurrently. pg_dump does not block other users accessing the database (readers or writers). Dumps can be output in script or archive file formats which should be saved to a different location.

- Script dumps are plain-text files containing the SQL commands required to reconstruct the database to the state it was in at the time it was saved. To restore from such a script, feed it to psql. Script files can be used to reconstruct the database even on other machines.
- Archive file formats must be used with *pg_restore* to rebuild the database. When used with the archive file format,

For more details, refer to PostgreSQL documentation.

Note: Using third-party tools can result in a recovery after a disaster not being consistent with the database, with the recovery being either older or newer than the database recovery.
If the HCP Anywhere Enterprise Portal recovery is older than the database, it will be missing some recent blocks. In this situation, you should rollback the database to an earlier point-in-time that matches the latest HCP Anywhere Enterprise Portal recovery.
If the HCP Anywhere Enterprise Portal recovery is newer than the database, since deleted blocks are kept for a minimum of 30 days and these blocks are never modified, as long as the database is no more than 30 days older, there will be no data loss.
Running HCP Anywhere Enterprise FSCK is usually recommended following a disaster recovery. HCP Anywhere Enterprise FSCK must be run only with approval from Hitachi

Vantara support.

Continuing Operations After the HCP Anywhere Enterprise Edge Filer Fails

If the HCP Anywhere Enterprise Edge Filer fails, end users want to continue with minimal downtime and as seamlessly as possible. Hitachi Vantara provides the following options to maintain business continuity when an HCP Anywhere Enterprise Edge Filer fails:

- Using a Second HCP Anywhere Enterprise Edge Filer
  With at least two HCP Anywhere Enterprise Edge Filers you can use the second HCP Anywhere Enterprise Edge Filer as a fail-safe device if the primary HCP Anywhere Enterprise Edge Filer fails. The failover to the second HCP Anywhere Enterprise Edge Filer is achieved automatically using Microsoft DFS. The HCP Anywhere Enterprise Edge Filers must be configured in either caching or sync mode and each HCP Anywhere Enterprise Edge Filer must be connected to the Windows Server running Active Directory with DFS.
  Advantages: Immediate failover to the second HCP Anywhere Enterprise Edge Filer with LAN access.
  Disadvantages: An additional HCP Anywhere Enterprise Edge Filer is required for failover.
- Directly to HCP Anywhere Enterprise Portal
  Until the faulty HCP Anywhere Enterprise Edge Filer is replaced and fully operational, Hitachi Vantara provides end users with access to their files in the HCP Anywhere Enterprise Portal, also via mapped network drives, providing a very similar user experience to the HCP Anywhere Enterprise Edge Filer access the end users are familiar with. Virtually immediate data-access recovery is enabled by diverting end users from the HCP Anywhere Enterprise Edge Filer directly to the HCP Anywhere Enterprise Portal, in order to access their files and folders.
  Advantages: Immediate failover to the HCP Anywhere Enterprise Portal using WebDAV instead of SMB.
  Disadvantages: During the failover period, access is over WAN and not LAN. A Cloud Drive Connect license must be purchased for every HCP Anywhere Enterprise Edge Filer end user.

Chapter 2. Using a Second HCP Anywhere Enterprise Edge Filer

With at least two HCP Anywhere Enterprise Edge Filers you can use the second HCP Anywhere Enterprise Edge Filer as a fail-safe device if the primary HCP Anywhere Enterprise Edge Filer fails. The failover to the second HCP Anywhere Enterprise Edge Filer is achieved automatically using Microsoft DFS. The HCP Anywhere Enterprise Edge Filers must be configured in caching mode and each HCP Anywhere Enterprise Edge Filer must be connected to the Windows Server running Active Directory with DFS.

The metadata from the HCP Anywhere Enterprise Portal is downloaded quickly so the stub files are almost immediately available on the replacement HCP Anywhere Enterprise Edge Filer. Both metadata and data are populated to the replacement HCP Anywhere Enterprise Edge Filer based on priority: When a path is entered to access content, that content receives download priority. This feature is not enabled by default. For details about enabling the feature, contact Hitachi Vantara Support.

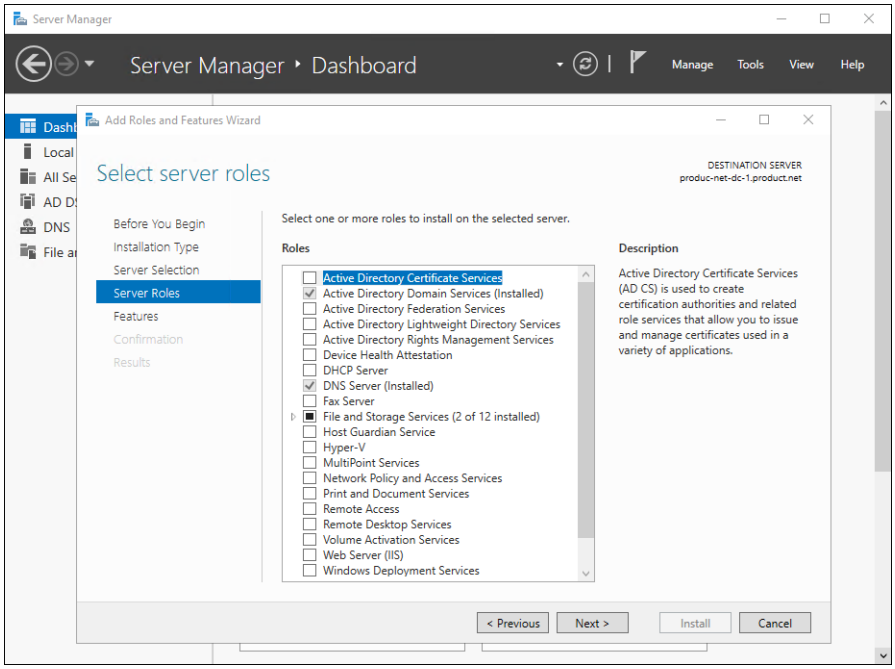
Note: The Windows Server must be Windows Server 2012 R2 or higher.

Installing DFS on the Windows Server:

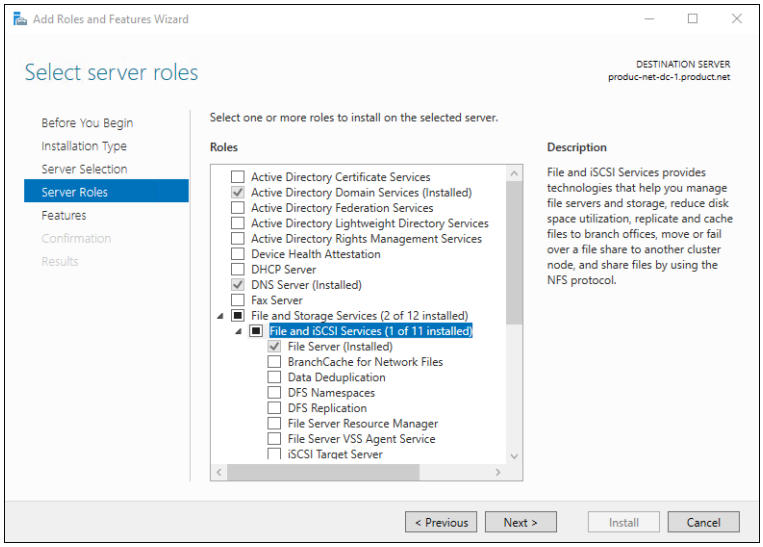
The procedures in this section can vary slightly, depending on the version of Windows Server.

To Install and Configure DFS on the Windows Server:

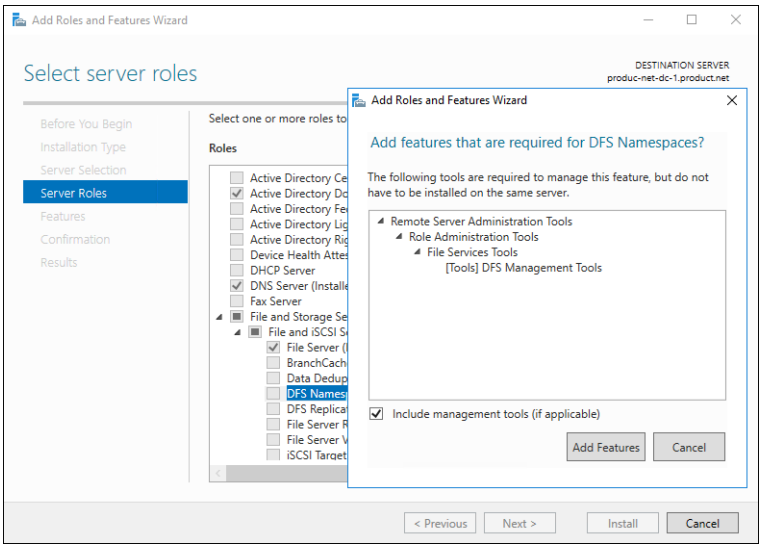
1. On the Windows Server open Server Manager and select Manage > Add Roles and Features.
2. Click Server Selection, select the server and then click Server Roles.



3. Expand **File and Storage Services (x of y installed)** and then expand **File and iSCSI Services (x of y installed)**.



4. Check **DFS Namespaces** and in the **Add Roles and Features Wizard** click **Add Features**.

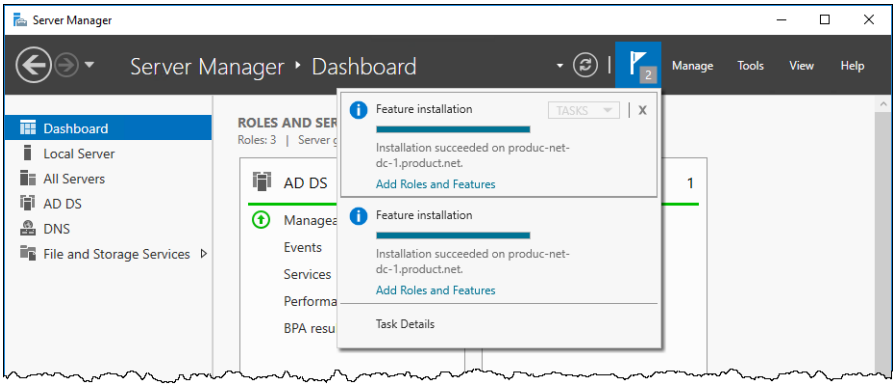


5. Check DFS Replication.

   Note: **DFS Replication** is not used, but must be installed.

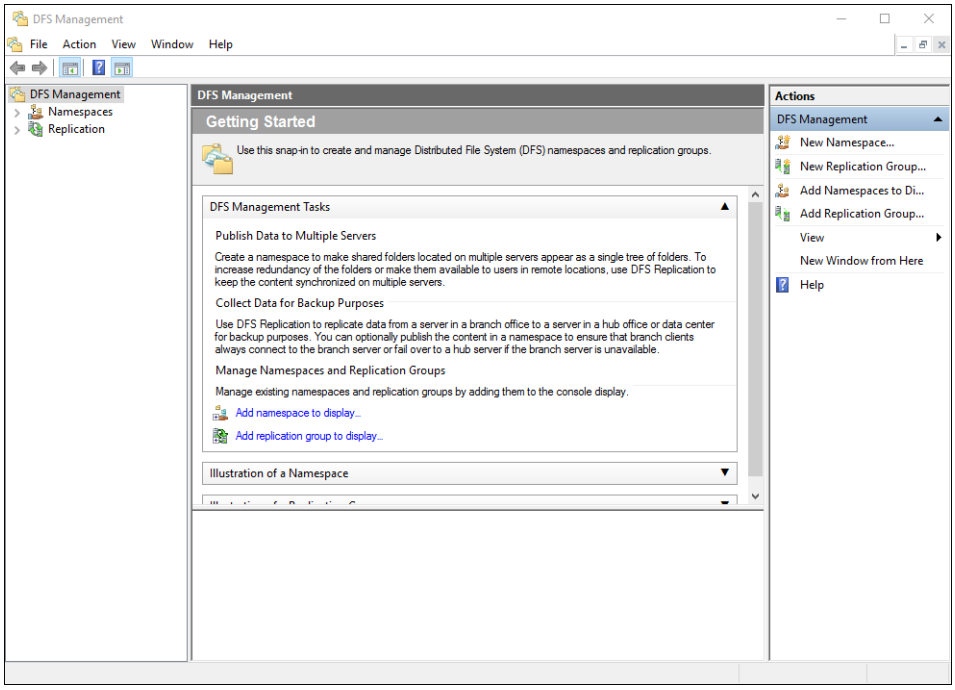
6. Click **Next** until the end of the wizard and then click **Install**.
7. Click **Close**.

The status of the installation can be viewed by clicking the flag at the top right of the Server Manager.



To configure DFS:

1. In Server Manager select Tools > DFS Management.



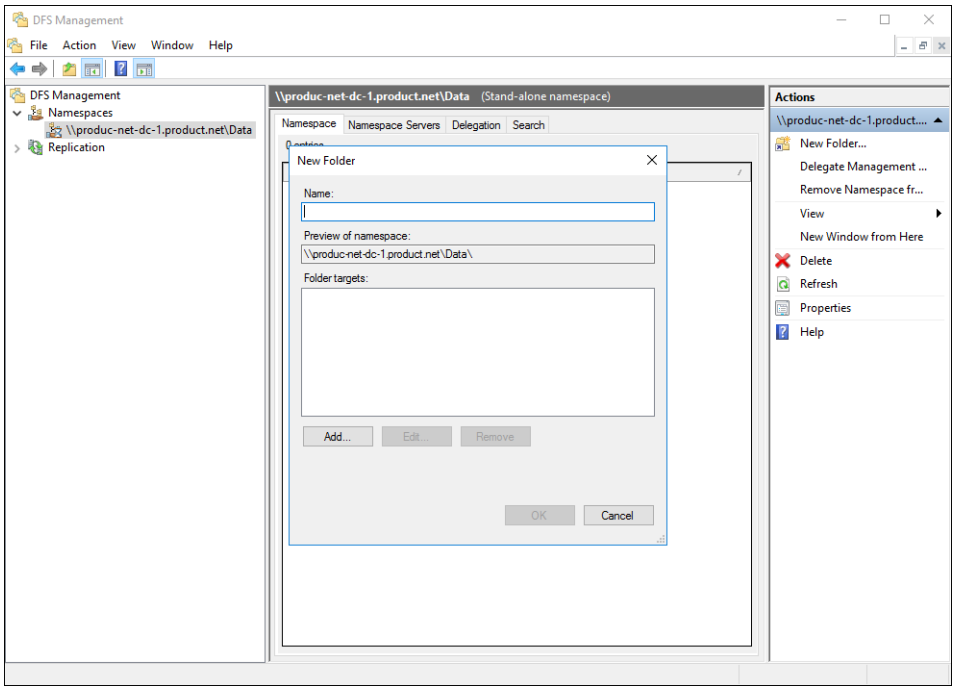
2. Expand **Namespaces** in the navigation pane and if there are no namespaces defined, create a new namespace.
   a) Right-click **Namespaces** in the navigation pane and select **New Namespace**.
   b) Follow the wizard to create the namespace.
   The namespace is the container/folder where the shares will reside. For example, if the namespace is Data the DFS namespace path will be **\domain\data**.
3. Right-click the namespace in the navigation pane, select Properties and then the Referrals tab and set Cache duration to the required value.

   For demos and testing, the Cache duration value should be low. In production the value should be great enough for the HCP Anywhere Enterprise Edge Filer to sync data with the HCP Anywhere Enterprise Portal when it comes back online. For example, if the primary HCP Anywhere Enterprise Edge Filer goes down, DFS will failover to the backup HCP Anywhere

Enterprise Edge Filer. While down users will be changing files on the backup HCP Anywhere Enterprise Edge Filer, which are not being synced to the down HCP Anywhere Enterprise Edge Filer. When the primary HCP Anywhere Enterprise Edge Filer comes back online, you need to allow a period of time for it to sync changed data back down to it.

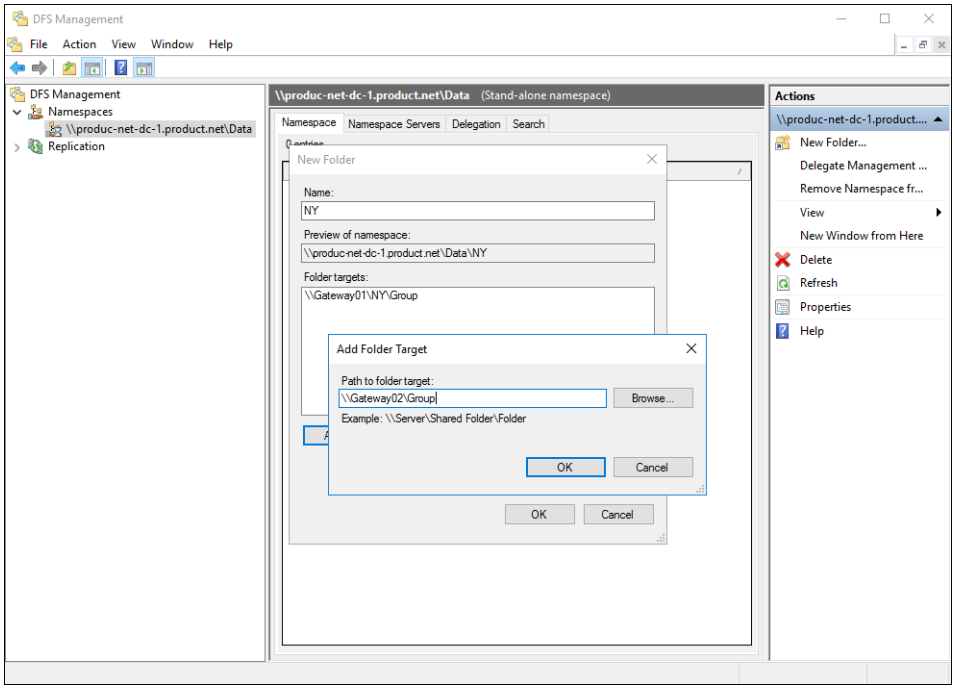
Note: Make sure that Ordering method is Lowest Cost and Clients fail back to preferred targets is checked.

4. Click **OK**.
5. Right-click the namespace in the navigation pane and select **New Folder** and define the folder which will be a share names that users will connect to.



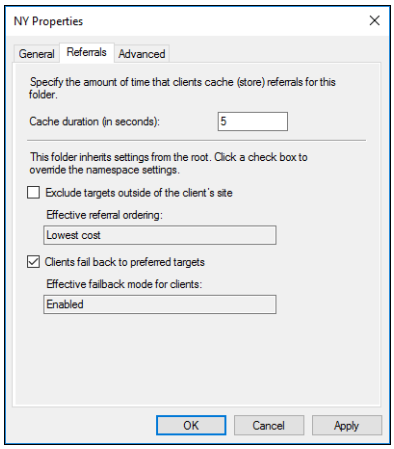
For example, for a folder NY the UNC path is **\domain\data\NY**.

6. Click **Add** to add **Folder Targets** that will be the UNC path of the HCP Anywhere Enterprise Edge Filer shares you want to use.

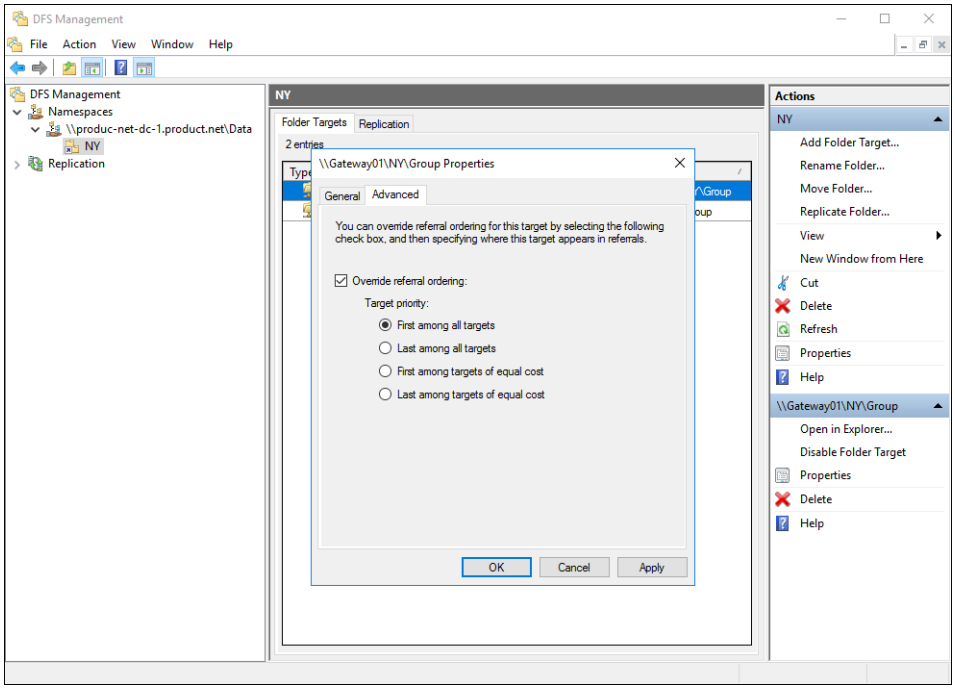


7. Click **OK** to add the folder target and then **OK** to complete the folder addition.
8. Right-click the folder in the navigation pane, select **Properties** and then the **Referrals** tab and set **Cache duration** to the required value.

   For demos and testing, the Cache duration value should be low. In production the value should be great enough for the HCP Anywhere Enterprise Edge Filer to sync data with the HCP Anywhere Enterprise Portal when it comes back online.

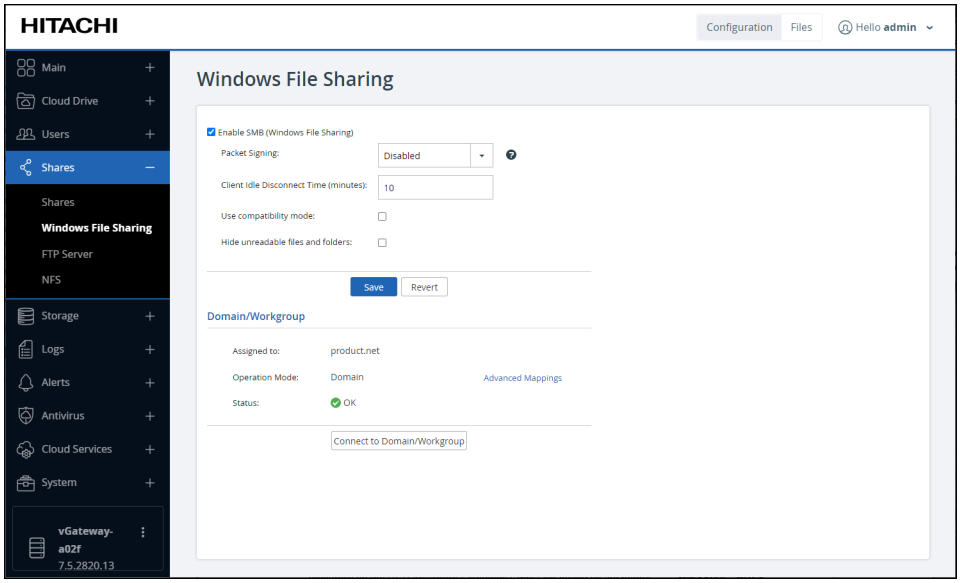


   Note: Make sure that Ordering method is Lowest Cost and Clients fail back to preferred targets is checked.
9. Click **OK**.
10. Double-click the folder in the navigation pane to display it with the folder targets and right-click a folder target, select **Properties** and then the **Advanced** tab.
11. Set the priority for which HCP Anywhere Enterprise Edge Filer will be first and which will be last.



Testing Automatic Edge Filer Disaster Recovery

1. Check which HCP Anywhere Enterprise Edge Filer is recognized by DFS as the primary HCP Anywhere Enterprise Edge Filer. On the primary HCP Anywhere Enterprise Edge Filer, open several files so they are cached locally. On the other HCP Anywhere Enterprise Edge Filer, these files are presented as stub files.
   If the opposite situation occurs, that the stub files are presented on the primary HCP Anywhere Enterprise Edge Filer, reconfigure the DFS Management properties for the folder targets.
2. In Windows Explorer, browse to the DFS namespace to verify that the primary HCP Anywhere Enterprise Edge Filer is displayed.
3. Log on to the primary HCP Anywhere Enterprise Edge Filer as an administrator and navigate to **Shares > Windows File Sharing**. Uncheck **Enable SMB** and **Save**. This will cause the shares on the primary HCP Anywhere Enterprise Edge Filer to be unavailable and DFS should automatically failover to the other HCP Anywhere Enterprise Edge Filer. You should be able to tell this because instead of files, you will see stubs.
4. Log on to the HCP Anywhere Enterprise Edge Filer as an administrator.
5. In the **Configuration** view, select **Share > Windows File Sharing** in the navigation pane.
   The **Windows File Sharing** page is displayed.



6. Uncheck **Enable SMB (Windows File Sharing)** and click **Save**.
7. Check the primary HCP Anywhere Enterprise Edge Filer and the shares should now be unavailable.

   DFS will automatically failover to the secondary HCP Anywhere Enterprise Edge Filer which can be accessed using the same SMB path, for example, **\domain.local\data\NY**, and the files will be available as stubs.
8. Validate failback by re-enabling SMB on the primary HCP Anywhere Enterprise Edge Filer in the HCP Anywhere Enterprise Edge Filer user interface.

Within the cache duration specified, the path will automatically fail back to the primary HCP Anywhere Enterprise Edge Filer, where the share will contain files and not stubs.

Chapter 3. Directly to HCP Anywhere Enterprise Portal

During normal operations end users access their files residing in a HCP Anywhere Enterprise Edge Filer via network drives that map via the SMB protocol. In the background, the HCP Anywhere Enterprise Edge Filer is capable of syncing, in near real time, any file changes to the HCP Anywhere Enterprise Portal, effectively creating another identical copy of the data.

If an HCP Anywhere Enterprise Edge Filer fails, end users want to continue with minimal downtime and as seamlessly as possible. Until the faulty HCP Anywhere Enterprise Edge Filer is replaced and fully operational, HCP Anywhere Enterprise provides end users with access to their files in the HCP Anywhere Enterprise Portal, also via mapped network drives, providing a very similar user experience to the HCP Anywhere Enterprise Edge Filer access the end users are familiar with. Virtually immediate data-access recovery is enabled by diverting end users from the HCP Anywhere Enterprise Edge Filer directly to the HCP Anywhere Enterprise Portal, in order to access their files and folders.

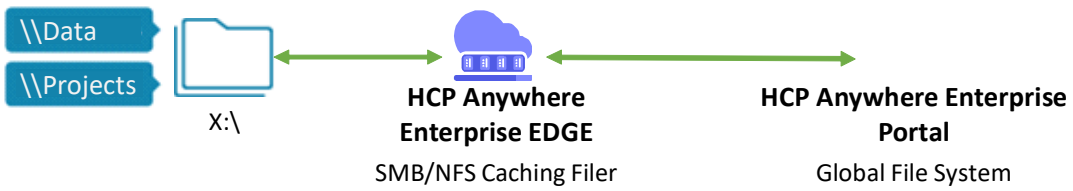
Setting up business continuity to the HCP Anywhere Enterprise Portal is described in the following sections:

Overview

To enable business continuity to a HCP Anywhere Enterprise Portal, customers need to purchase endpoint Cloud Drive Connect licenses for every HCP Anywhere Enterprise Edge Filer end user. A Cloud Drive Connect license provides an end user with access to the files on the HCP Anywhere Enterprise Portal for disaster recover, but excludes file collaboration options.

Note: A Cloud Drive Connect license also enables access to the end user files via the HCP Anywhere Enterprise Portal web browser user interface or a mobile device, such as a tablet or smart phone.

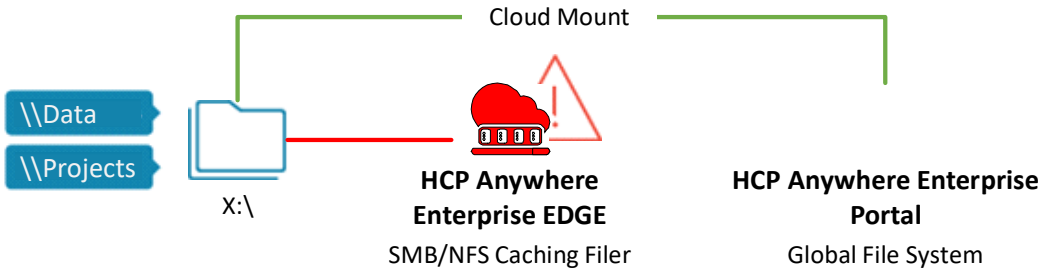
How does it work?



When the HCP Anywhere Enterprise Edge Filer operates normally, workstations have access to it via one or more network drive letters, which are mapped to the HCP Anywhere Enterprise Edge Filer. The mapping is achieved via a mapping policy that is pushed to the workstation by default.

If the HCP Anywhere Enterprise Edge Filer fails, an alternate mapping policy is pushed to the workstation. In this situation the workstation has access to the HCP Anywhere Enterprise Portal via one or more network drive letters to the same data that it had access to with the HCP Anywhere Enterprise Edge Filer.

Folders can be mounted directly from the Portal when an Edge Filer is inaccessible



Note: Each user that will connect directly to the HCP Anywhere Enterprise Portal requires a license to connect to the HCP Anywhere Enterprise Portal.

Setting Up Business Continuity to the HCP Anywhere Enterprise Portal

Business continuity to the HCP Anywhere Enterprise Portal requires setting up the HCP Anywhere Enterprise Edge Filer so that any files written to the HCP Anywhere Enterprise Edge Filer are immediately synced to the HCP Anywhere Enterprise Portal. The HCP Anywhere Enterprise Portal contains a duplicate set of all the files on the HCP Anywhere Enterprise Edge Filer and it is this set of files that can be used if the HCP Anywhere Enterprise Edge Filer fails.

During normal HCP Anywhere Enterprise Edge Filer operations, end users access the HCP Anywhere Enterprise Edge Filer through SMB, via one or more mapped drives. Thus, the end user accesses the folders and files using macOS Finder or Windows File Explorer, in the same way that all folders and files are accessed.

Note: A mapped network drive can also be accessed via a drive letter, using the Windows Map network drive mechanism.

If the HCP Anywhere Enterprise Edge Filer fails, the end users need to maintain access to their data through a similar mechanism, except that the data now originates from the HCP Anywhere Enterprise Portal. Access is provided though WebDAV technology, which allows mapping the same drive letter to the HCP Anywhere Enterprise Portal. The HCP Anywhere Enterprise Portal supports the WebDAV protocol and serves as a WebDAV server.

Access to the HCP Anywhere Enterprise Portal using *HCP Anywhere Enterprise Drive Connect* uses WebDAV to display the content in a file manager.

Hitachi Vantara

Corporate Headquarters 2535 Augustine Drive
Santa Clara, CA 95054 USA www.HitachiVantara.com community.HitachiVantara.com

Regional Contact Information
Americas: +1 866 374 5822 or info@hitachivantara.com
Europe, Middle East and Africa: +44 (0) 1753 618000 or info.emea@hitachivantara.com
Asia Pacific: +852 3189 7900 or info.marketing.apac@hitachivantara.com