Hitachi Content Platform Gateway Administration Guide

v4.2.0

Windows Only

The objective of this document is to provide details on the configuration and use of the Hitachi Content Platform Gateway with the Hitachi Content Platform (HCP) storage system.

MK- HCPG000-11
April 2022

Table of Contents

Introduction

The objective of the Hitachi Content Platform Gateway (HCP Gateway) is to enable organizations to intelligently manage data which is stored on the Hitachi Content Platform. The HCP Gateway enables applications and user access to cloud/object storage via legacy file systems protocols. The HCP Gateway also helps organizations manage data, protect data and help organizations comply with governance and compliance rules and regulations including immutability, retention, legal hold, data integrity, chain-of-custody, and data disposition.

The HCP Gateway software provides data management with easy access to data for users/applications, independent of what access protocol or storage system is used. By separating the data access from the data storage, HCP Gateway enables IT administrators to manage the data (for example, move data to new storage locations) without impacting user/application access, which provides tremendous flexibility. The Policy engine in HCP Gateway automates processes and reduces IT administration and cost.

The key benefits of HCP Gateway are:

- Help organizations meet compliance and governance requirements
- Meet retention and auditing requirements
- Security and isolation features to keep data safe
- Simplifies file system administration by eliminating backup
- Increases efficiency by using policy-based automation
- Reduces costs by enabling low-cost private cloud storage
- Reduces risk with encryption
- Enables transition from legacy storage to cloud or object storage

HCP Gateway is licensed software and cannot be used without a valid license key from Hitachi Vantara.

This document will cover the administration of HCP Gateway. If there are questions or topics not covered, contact Support.

WARNING: Do not cut and paste text from this document directly into a Windows or Linux HCP Gateway server. It is required to first copy the text to a Windows Notepad to remove any formatting, before copying from the Windows Notepad to the final destination.

Documentation Conventions

The following conventions are used throughout this manual to represent specific types of information.

All images, diagrams, or drawings are listed as Figures in the following format:

Figure X.Y.Z - Description

X = Chapter of document

Y = Sequence number for each Figure in a Chapter

Z = Callouts inside a Figure (these are represented by small numbers inside red circles)

Figure 2.1 - Example

2.1.1 – Select File System Mode

2.1.2 – Read/Write option

2.1.3 – Apply setting to share

2.1.4 – Cancel selection

WARNING: Precautionary note in a box.

Note:

Commentary or additional information need on the topic.

Action Buttons

Below is a list of ACTIONS that can be performed on the GUI page:

Browse to location other than Default location

Login to application

Logout of Application

Start	Start a new process such as Audit
Stop	Stop the current process
Apply	Apply changes to current setting
Cancel	Do not apply changes to current setting
Add	Add something like user or share or storage
TEST	Test connection
	Edit setting
	Delete setting
	Refresh displayed information
ON	Turn a setting ON or OFF

Pre-Installation Planning

HCP Gateway is a software appliance that includes:

1. Virtual File System (filter driver)
2. Operating System (Debian Linux OS or Windows Server – license not included)
3. Database (Maria DB)
4. Management Console (WildFly provides Webserver interface)
5. Core code (C++)

Many of the HCP Gateway features are enabled and tracked using an internal database. It is critical for data protection to backup this database outside of the data storage device. The HCP is the recommended choice for a backup target. The HCP Gateway application includes a database and configuration file backup utility for ease of use. If you want to use a different backup utility/application, contact Support to discuss your plans.

HCP Gateway supports several options for storage including local storage, network storage and cloud storage. Local storage is anything that the host OS can access, which could include local disk, iSCSI, SAN, network drive using a UNC path, etc. HCP Gateway supports NFSv3, NFSv4, SMB, and SFTP access to data. Do not use the cache drive for local storage, add a separate drive for local storage.

HCP Gateway has a default 100GB license key for demo purposes. Any capacity above 100GBs requires a production license key. Starting in HCP Gateway version 4.1.3, the License Key is generated based on a digital fingerprint of the server that is running the HCP Gateway. Make sure that a Fixed IP address is used, otherwise HCP Gateway will not be accessible after a reboot.

Shares cannot be created unless the HCP Gateway system has available Storage configured to hold the content.

Note that the Windows HCP Gateway will auto-negotiate TLS with the storage system starting from 1.2 and if both the Gateway and storage do not support 1.2, then the Gateway will revert to TLS 1.1 and then to TLS 1.0 until both Gateway and storage both support the same version. The Linux HCP Gateway will not auto-negotiate TLS version and is configured for 1.2 in the Linux OS.

If you elect to run HCP Gateway in an environment that is not explicitly supported then your maintenance agreement may be terminated and the support team will only provide limited help.

Deployment Options

The first decision is what access protocols are required for client and user access? The answer will determine what OS configuration will be used:

NFS only – Linux Debian Server 10.x

SMB only – Microsoft Windows Server 2016 and 2019 Standard or higher

If you are unsure about your future requirements for protocol access, consult Hitachi Vantara to discuss the options and requirements.

The HCP Gateway is distributed as either an appliance, VM, or Software only image.

1. **Appliance**

HCP Gateway software is pre-installed on a Hitachi physical server at the Hitachi Distribution Center.

2. **VM**
   HCP Gateway can be installed on a virtual machine (VM). HCP Gateway supports the following VM hosts:
   - VMWare ESXi version 6.5 or higher

Network Ports

> **Note:**
>
> LACP is supported with HCP Gateway networking. Verify that the latest versions of the Intel Chipset and NIC drivers are installed.

Protocol	Port
HTTPS	28443
Wildfly Admin	9990 (internal only)
RDP	3389
MySQL	3306
CIFS	445,137,138,139
NFS	2049 and 111
SFTP/SSH	22
End-User Restore Client	9090

Database Management

Managing the HCP Gateway is easier with a GUI SQL interface. Applications that can be used include: DBeaver, HeidiSQL, or MySQL CLI. The documentation references HeidiSQL by name, but any of the applications listed above can be used. HeidiSQL and DBeaver are not included due to distribution limitations associated with its Open Source license but can be downloaded and installed during Gateway setup. For Linux, you can install the software on a separate Windows client.

Database Replication

Replicating the database to another Gateway(s) provides the ability to access customer data when the primary Gateway is not available. Refer to the Hitachi Content Platform Gateway Multi-Node Replication Guide for details on the features and configurations available. The most common configuration is a 2-node master to master configuration, but only 1 node can be active at a time. If the primary Gateway is not available and files are written to a replica Gateway, contact Hitachi support for assistance when failing back to the primary Gateway. It is recommended to turn off the Windows **SAM VFS** and **Wildfly** services on the non-active node(s).

When using a Server Mode Copy or Tiering policy where the cache is not shared between the Gateways, the file metadata will replicate immediately, but the file content will not be available on the replica Gateway(s) until the file content is written to the storage on the HCP.

Disk Setup and Management

The configuration of disks in the HCP Gateway documentation is written for normal use cases. As a reminder do not delete any folders, or files on the D: and E: drives in Windows and the /archive, /var/lib/mysql and /storage filesystems in Linux.

Do not use the **cache** drive, which is E: drive in Windows or /storage in Linux for additional copies of data on local Gateway storage.

Do not put the Windows page file or the Linux swap file on the **cache** drive (E: drive in Windows or /storage in Linux) or the **database** drive (D: drive in Windows or /var/lib/mysql partition in Linux).

For **Local Gateway Storage**, add another drive, F: drive in Windows or mount another disk in Linux as /storage/local (used for additional copy of the data on HCP Gateway server that is separate from the cache).

WARNING: If you add an additional disk to the HCP Gateway for local storage after copying files to the HCP Gateway, you will need to move the files on the local storage to the new storage. When adding another drive for the local storage, in Windows, create a Storage folder on the additional drive and add that as the Local Storage in Chapter 9. In Linux, mount another disk to /storage/local.

Quotas

Quotas on HCP Gateway are not supported in Windows and Linux. Quotas cannot be enforced on HCP Gateway due to the use of offline files (Size on Disk = 0).

Data Migration

If there is existing data to be migrated to the HCP Gateway there are a few key considerations:

1. Only write to Shares and Exports presented, do not write directly to local drives (such as E:, G: in Windows or /archive or /storage in Linux) on the HCP Gateway.
2. Despite its popularity, Robocopy has known issues working with HCP Gateway that can result in corrupted data, hence we highly discourage the use of Robocopy.
3. We suggest considering these migration tools:
    a. DataTrust Copy2HCPG (C2HCPG)
    b. Quest SecureCopy
    c. GuruSquad RichCopy 360
    d. Hitachi CMT
    e. Hitachi Content Intelligence
4. Pay special attention to permissions management prior to starting the migration. Follow the instructions in the **Access and Permissions Management** section below.
5. If the Share is configured with Retention and data needs to be validated prior to being committed, consider using a longer grace period in the Retention policy, so the files can be hash validated by the migration application and recopied if needed before the files are locked under Retention.

Access and Permissions Management

There are two areas to consider when managing permissions on HCP Gateway. The first is access to the HCP Gateway UI. Typically, this is managed in Active Directory (see Chapters 8 and 27 for details) or users can be configured locally on the HCP Gateway.

The second is the ACLs (only in Windows) and Access Permissions (in Windows and Linux) on the exposed Shares. When using Windows, configure the inheritable ACL permissions at

the top the share before creating any folders or files, by accessing the share on the HCP Gateway in Windows File Explorer using \\localhost\share and then right-clicking in the white space of the share and selecting Properties -> Security. Make sure the inheritable permissions include a Full Control ACL for the user that is configured in the sam.account parameter in C:\SAM\etc\sam\sam.properties and that the SAM VFS service is running as the same user. The default user is the local SYSTEM account. Refer to Step 10 in Chapter 18 HCP Gateway Software Upgrade for more details.

HCP Gateway Logins and Passwords (default):

It is highly recommended that default password for the HCP Gateway UI admin be changed for security reasons. Note that when installing the non-VM software image, the person doing the installation will have to manually reset the default passwords, required by law in the State of California (USA). For Windows, a PowerShell script is provided to assist in this process to reset the HCP Gateway UI admin password. The VM image forces the password reset after the initial login to the Windows Operating System.

HCP Gateway UI / Management Console:

Username: admin

password: admin

Windows OS Administrator:

Username: administrator

password: <set by the person who installed the HCP Gateway>

Linux OS Administrator:

Username: vault

password: 0rgan1c

WildFly Administrator / Console Administrator (for Upgrades and Maintenance – deploy UI war file):

Username: admin

password: 0rgan1c (Linux) or 0rgan1c@HV (Windows)

How to manually reset the HCP Gateway UI admin password

Open a Windows PowerShell prompt running as Administrator and change directory to **C:\SAM\ps** (Figure 3.2.1). Issue the command **.\setRunOnce.ps1** (Figure 3.2.2). Select the Windows Start button and restart the HCP Gateway. After the HCP Gateway reboots, a prompt will appear to change the UI admin password.

Figure 3.2 – Change HCP Gateway UI admin password

Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cd \SAM\ps 1
PS C:\SAM\ps> .\setRunOnce.ps1 2
Changing RunOnce script.
PS C:\SAM\ps> _
```

HCP Gateway Login

Access to the HCP Gateway Management Console is via a web browser over HTTPS. In your browser window, type the IP address or DNS name followed by ":28443/hcpg" (e.g., https://192.168.1.10:28443/hcpg). If logged into the HCP Gateway, there is a shortcut on the desktop for the HCP Gateway UI.

Enter **"admin"** in the username (Figure 4.1.1) and enter the password (Figure 4.1.2), select the Locale (Windows only) (Figure 4.1.3) pulldown and choose the locale that matches the locale setting for your OS, then select **Login** (Figure 4.1.4) or press the enter key. The Linux version of HCP Gateway does not have a Locale (Figure 4.1.3) menu.

Figure 4.1 – Login

NOTE:

For security reasons the system default passwords should be changed, and the new passwords stored securely.

When doing VM deployment, upon first login to the HCP Gateway Windows Operating System, the default HCP Gateway UI admin password will need to be changed, after which the system will reboot.

For non-VM deployments, the default passwords will need to be changed by running the PowerShell script and setting a registry entry, then reboot the HCP Gateway system, and then login to Windows OS as Administrator. Please refer to the Changing the Password section in the next chapter.

To exit the HCP Gateway Management Console, click on **Logout** (4.2.1).

Figure 4.2 - Logout

Getting Started

Summary of the steps required to configure the HCP Gateway system:

1. Changing the UI Admin Password (applies to VM deployment during the first login to the Windows Operating System)
2. Setup and configure HCP and/or HCP for Cloud Scale object storage for use with HCP Gateway
3. Configuration – Verify network interfaces
4. Configuration – Add license key
5. Storage – Add Storage and configure Storage Group
6. Policy – Create policies
7. Shares – Create and configure shares
8. Shares – Make shares active and give access to Users and Applications
9. Operations – Configure backup schedule
10. Configure Antivirus scanning (optional)
11. Configure Windows OS Time zone

HCP Gateway Management Console:

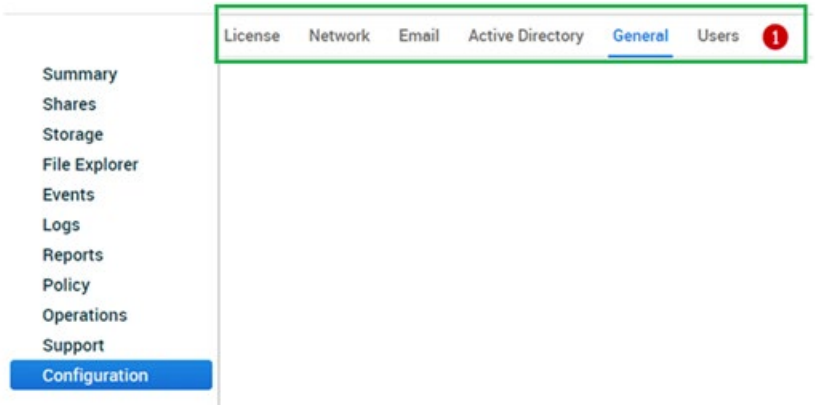
Navigation is achieved by selecting options located in a column on the left side of the page (Figure 5.1). Selecting a topic can be done by using a mouse and clicking on it. The default page is the summary page which displays summary information on Shares and Storage.

1. **Summary** – List of Shares & storage, with statistics
2. **Shares** – Create & manage Shares and settings
3. **Storage** – Add and manage Storage options
4. **File Explorer** – Like MS Explorer, admin view of shares, versioning files, Legal Hold, Privileged Delete, Delete file copy from Local Storage, Copy Files to Cache
5. **Events** – Operational, Warnings and Errors, such as when an internal operation starts or stops
6. **Logs** – Information, Warning or Error messages
7. **Reports** – Run and download reports
8. **Policy** – Create & manage Policies
9. **Operations** – Database Backup & Restore, Delete on Storage
10. **Support** – HCP Gateway version information and contact info
11. **Configuration** – License, networking, users, AD, email alerts and cache management

Figure 513 – Main Menu

The Operations and Configuration web pages contain subsections which are displayed in tabs across the top of the page (Figure 5.2.1).

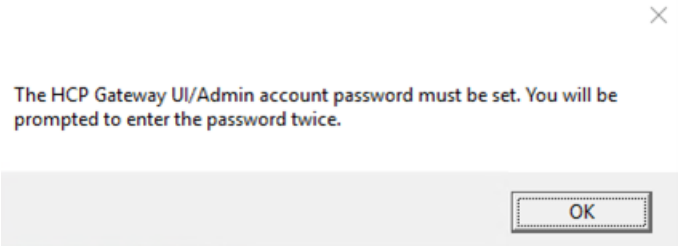
Figure 5.2 – Secondary Menu



Changing the Password (applies to VM deployment during the first login to the Windows Operating System):

Step 1 – A popup window will appear (Figure 5.3) click **OK** to start the process to reset the Gateway UI Admin password.

Figure 5.3 – Reset password

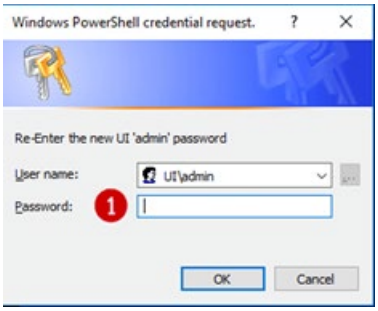


Step 2 – Enter a new UI Admin password (Figure 5.4.1) that will be used to log into the HCP Gateway UI. Then click the **OK** button.

Figure 5.4 – Enter New UI Admin password

Step 3 – Verify the UI password (Figure 5.5.1) by re-entering it. Then click the **OK** button.

Figure 5.5 – Re-Enter New UI Admin password



Note:

If the passwords do not match, the Change password popup screen will not advance. If you do not remember the original password the only way to fix the issue is to log out of the HCP Gateway UI and restart the PowerShell change password process.

WARNING: Secure all passwords. If passwords are forgotten or lost you must contact Hitachi Vantara support for assistance.

HCP Gateway Configurations settings in C:\SAM\etc\sam\sam.properties

This section will explain the parameters used to configure the HCP Gateway UI, internal HCP Gateway UI Backup, MariaDB access and SAM VFS Filter Driver. Do not change any of these parameters unless instructed in the HCP Gateway Software Upgrade, HCP Gateway Database Replication, HCP Gateway Cluster guides or by HCP Gateway Support.

Here is a sample version of the parameters (Figure 5.6)

Figure 5.6 – Sample C:\SAM\etc\sam\sam.properties file

*C:\SAM\etc\sam\sam.properties - Notepad++ [Administrator]

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

sam.properties

```
1  #Thu Feb 18 07:01:54 MST 2021
2  backup.days=10
3  backup.dir=\\localhost\operation$
4  backup.enabled=1
5  backup.password=
6  backup.scheduled=0
7  backup.scheduled.count=0
8  backup.type=network
9  backup.user=
10 binlog.folder="D:\MariaDB\binlog"
11 binlog.name=hcpg-1-bin
12 cluster=0
13 data.folder="D:\MariaDB\data"
14 database.binlog="C:\Program Files\MariaDB 10.4\bin\mysqlbinlog.exe"
15 database.dump="C:\Program Files\MariaDB 10.4\bin\mysqldump.exe"
16 database.ip=localhost
17 database.name=SAM
18 database.password=0gi3vyJNMR+lH8FCWhydEg==
19 database.port=3306
20 database.program="C:\Program Files\MariaDB 10.4\bin\mysql.exe"
21 database.root.password=0gi3vyJNMR+lH8FCWhydEg==
22 database.username=sam
23 letter=E:\
24 registry.shares=yes
25 report.dir=E:\Reports
26 sam.account=SYSTEM
27 server.id=1
28 server.ignore=0
29 server.ip=127.0.0.1
30 thrift.ip=0.0.0.0
31 zip.program="C:\Program Files\7-Zip\7z.exe"
```

The parameters that start with **backup**. (2-9) are updated when the HCP Gateway Backup is configured in the HCP Gateway UI Backup page. Do not change any of these settings in this file unless directed by HCP Gateway Support.

binlog.folder (10) - the location of the binary transaction logs used by the MariaDB database.

binlog.name (11) - the prefix name of the binary transaction logs used by the MariaDB database. When using a set of HCP Gateways with database replication or a clustered set of HCP Gateways, the number in the name will be different on each node.

cluster (12) - When using a clustered set of HCP Gateways, the value will be 1. When using a standalone HCP Gateway or a set of HCP Gateways with database replication, the value will be 0.

data.folder (13) - the location of the HCP Gateway MariaDB database that contains the metadata information for the files on the shares on the HCP Gateway.

database.binlog (14), **database.dump** (15), **database.program** (20) - the location of the MariaDB database programs used by the HCP Gateway.

database.ip (16) - the IP address or FQDN of the location of the MariaDB database.

database.name (17) - the name of the MariaDB database used by the HCP Gateway.

database.password (18) - the encrypted password for the user sam that is used by the SAM VFS service to connect to the MariaDB database used by the HCP Gateway.

database.port (19) - the TCP port used to connect to the MariaDB database.

database.root.password (21) - the encrypted password for the user root that is used by the SAM VFS service to connect to the MariaDB database used by the HCP Gateway.

database.username (22) - the username used by the SAM VFS service to connect to the MariaDB database used by the HCP Gateway.

letter (23) - the drive letter for the cache drive, E:\ for a standalone or an HCP Gateway node in a replication set, G:\ for an HCP Gateway cluster node.

registry.shares (24)

- For a single standalone HCP Gateway, add the line **registry.shares=yes**. This will configure HCP Gateway to look in Windows Registry for the share configuration.
- For a clustered pair of HCP Gateways with a shared cache, add the line **registry.shares=yes** to both nodes of the cluster. This will configure HCP Gateway to look in Windows Registry for the share configuration.
- When using database replication with or without cluster, on the active node, add the line **registry.shares=yes**. On all of the other nodes that do not have a shared cache with the active node, add the line **registry.shares=no**. When using database replication without a shared cache, only 1 node can have this parameter set to **yes**.

IMPORTANT NOTE:

When using more than 1 HCP Gateway with database replication or more than 1 clustered pair of HCP Gateways, when the HCP Gateway active node is not available and the replica node becomes the active node, change the **registry.shares** parameter from **no** to **yes** on the new active node and restart the **SAM VFS** service. When the original active node then becomes available again and is promoted to the active node, change the **registry.shares** parameter from **yes** to **no** on the new passive replica node and restart the **SAM VFS** service.

report.dir (25) - the drive letter for the HCP Gateway reports created in the HCP Gateway UI Reports page.

sam.account (26)

The default setting is to use the local System account, set **sam.account=SYSTEM**.

If there is a domain service account that has access to all of the files on the Gateway, use that account for the **sam.account** parameter in the **C:\SAM\etc\sam\sam.properties** file.

IMPORTANT NOTE:

If the **sam.account** parameter is not added to the **C:\SAM\etc\sam\sam.properties** file, then the **SAM VFS** service will not start and an error **"sam.account setting is missing in configuration file"** will entered into the **C:\SAM\var\log\sam\log-0.txt** file.

server.id (27) - when using database replication with or without cluster, each HCP Gateway node needs to have a unique server.id. Generally In a pair of HCP Gateway nodes in a

replication set, the active node will have **server.id=1**, the passive node will have **server.id=2**. Refer to the HCP Gateway Database Replication and HCP Gateway Cluster Setup Guides for additional information.

server.ignore (28) - when using database replication without cluster, on each HCP Gateway set **server.ignore=0**. When deploying a cluster with a shared cache and only 1 node will be active at a time, set **server.ignore=1** on each HCP Gateway.

server.ip (29)

- The default setting is **127.0.0.1**.
- The valid values are a **valid host IP address**, **localhost** or **127.0.0.1**.
- Used by the HCP Gateway UI and SAM VFS Filter Driver for any local services or sockets. Thrift clients can use this to connect to the local Thrift service. Only need to change from the default when recommended by HCP Gateway Support.

> **NOTE:**
>
> **Only IPv4 addresses are supported. If both IPv6 and IPv4 are enabled on the server, do not use "localhost" for thrift.ip or server.ip.**

thrift.ip (30)

- The default setting is **127.0.0.1.**
- The valid values are a **127.0.0.1**, **valid host IP address** or **localhost**.
- If this value is not set to **0.0.0.0**, then the **server.ip** and **thrift.ip** parameters must have the same value.
- Used internally by the HCP Gateway UI and SAM VFS Filter Driver Thrift Server to listen for requests from the specified IP addresses. Only need to change from the default when recommended by HCP Gateway Support.

> **NOTE:**
>
> **Only IPv4 addresses are supported. If both IPv6 and IPv4 are enabled on the server, do not use "localhost" for thrift.ip or server.ip.**

zip.program (31) - the location of the 7zip compression program used by the HCP Gateway UI Backup.

Recommended Best Practices and HCP / HCP for Cloud Scale Settings

Supported Versions

HCP Supported Versions

1. HCP 8.x
2. HCP 9.1 or later

HCP for Cloud Scale Supported Versions

1. HCP for Cloud Scale 2.3 or later

IMPORTANT NOTE:

When using encryption and/or compression on HCP Gateway, it will not be possible to read the file content directly from the HCP namespace or HCP for Cloud Scale bucket. The only way to read the file content is through the HCP Gateway.

Recommended Best Practices

1. **Server Mode** – use **COPY** policy to ensure data is always stored and protected on HCP system and a copy is kept on the cache of the HCP Gateway.
2. **S3 v4 Payload Signature** – enabling the S3 v4 payload signature will have some performance impact. It is required on the HCP for Cloud Scale but not on the HCP. HCP Gateway can be configured to use the Amazon S3 signature authentication policy when communicating with the HCP storage system.
3. **Encryption with HCP**– please use data encryption in either the HCP Gateway or HCP storage, but not in both. If encryption is needed, we recommend enabling encryption in the HCP storage, since the HCP has more resources than the Gateway. Enable on the Gateway only if using a local Storage and need encryption on the files on the local storage. The Gateway uses the industry standard AES-256 encryption algorithm.
4. **Compression with HCP** – please use data compression in either the HCP Gateway or HCP storage, but not in both. If compression is needed, we recommend enabling compression in HCP Storage, since the HCP has more resources than the Gateway. Enable on the Gateway only if using a local Storage and need compression on the files on the local storage. The Gateway uses the industry standard LZW (Lempel-Ziv-Welch) compression algorithm.
5. **Deduplication with HCP** - the Gateway deduplicates at the share level, the HCP deduplicates at the HCP level. Use Gateway deduplication when using more than one Storage in the Storage Group, otherwise use deduplication on the HCP.
6. **Compression, Encryption and Deduplication (HCP for Cloud Scale)** - If required, enable **Compression, Encryption** and **Deduplication** on the HCP Gateway share, as these settings are not available on the HCP for Cloud Scale buckets. Note that **Deduplication** is not available on a share on the HCP Gateway when the share is configured with an HCP for Cloud Scale storage using **File Path** storage.

NOTE:

Enabling Compression and Encryption at the Gateway level will have a performance impact and will increase the CPU load and RAM usage of the system.

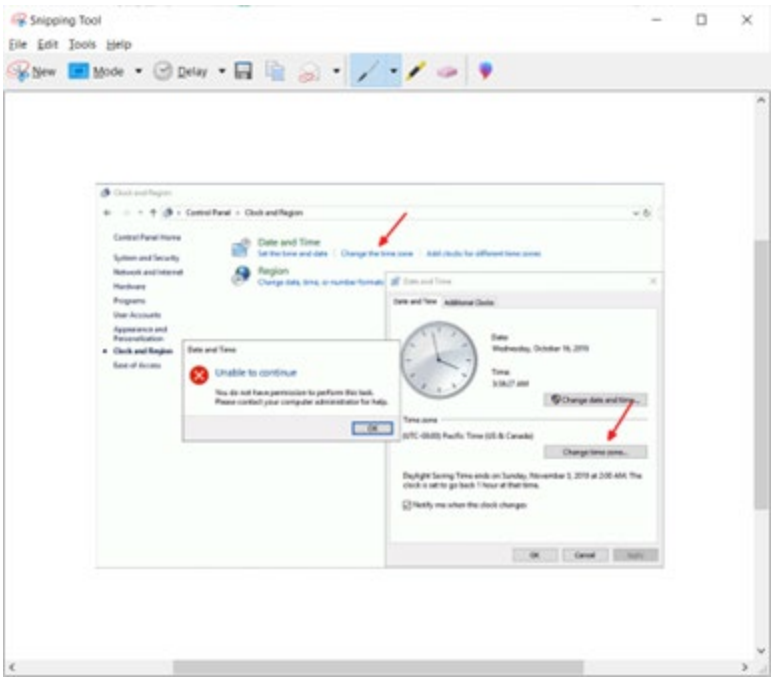
7. **Privileged Delete** - HCP Gateway **Privileged Delete** is **NOT** supported with HCP for Cloud Scale buckets since the HCP for Cloud Scale Retention is in Compliance mode and the HCP for Cloud Scale is not able to delete files until the Retention Period on the file expires. HCP Gateway **Privileged Delete** is supported with HCP namespaces.
8. **Metadata Replication** – use HCP Gateway Database Replication
9. **Data replication** – For HCP, use HCP Active/Active replication. For HCP for Cloud Scale, use HCP Gateway Storage Group to write to multiple HCP for Cloud Scale clusters.
10. **GPT format for database D:, cache E: and local storage F: drives** – please use GPT format for the D:, E: and F: drives to permit the Microsoft Windows file system to be larger than 2TB on those drives.
11. **Active Directory Setup**
    HCP Gateway can integrate with one Microsoft Active Directory server to utilize AD users, groups, and permissions. The HCP Gateway UI is used to configure AD access for the Management Console UI only.

    Separately, you will need to use the Windows File Explorer to configure AD access for the shares, folders, and files.

    Local users and Active Directory users cannot be used at the same time in the HCP Gateway UI. If using Active Directory users, only the local admin user will remain enabled in the HCP Gateway UI, which can be used to access the HCP Gateway UI in case the Active Directory server is not accessible.

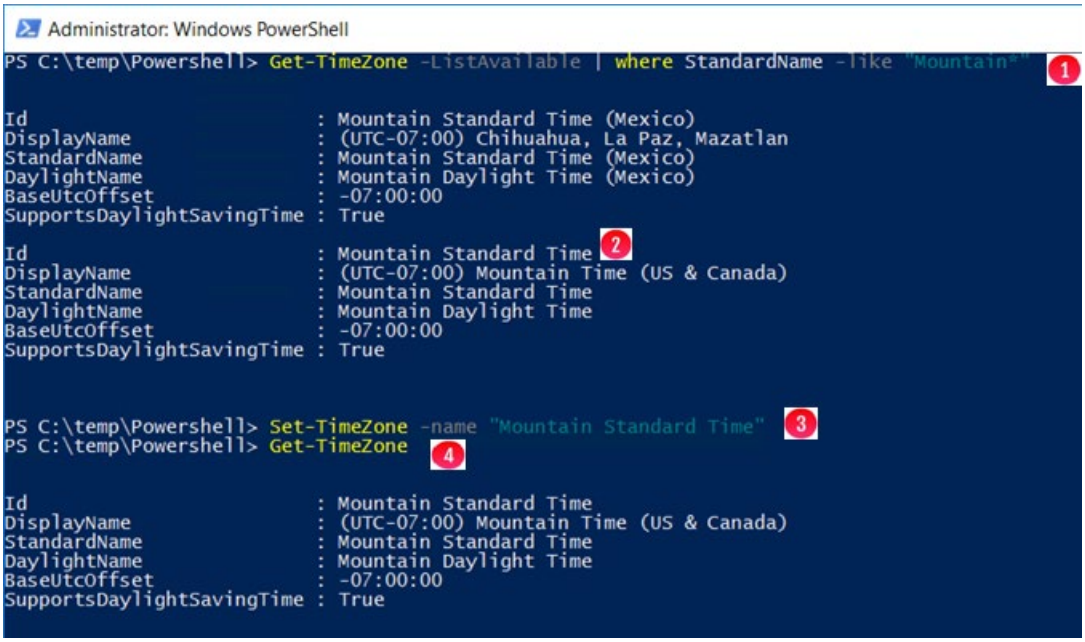
12. **Configure Share Permissions**
    The ACLs and Access Permissions on the exposed Shares are managed in Windows File Explorer. When using Windows, configure the inheritable ACL permissions at the top the share before creating any folders or files, by accessing the share on the HP Gateway in Windows File Explorer using \\localhost\share and then right-clicking in the white space of the share and selecting Properties -> Security. In Linux, manage the Share permissions in the Shares page of the HCP Gateway UI.
13. In Windows Server 2019, when setting the Time Zone, if you receive this error Unable to continue (Figure 6.1), then open a Windows PowerShell running as Administrator and for this example, set the time zone to US Mountain Standard Time.

Figure 6.1 – Windows error setting time zone



In PowerShell, enter the command **Get-TimeZone -ListAvailable | where StandardName -like "Mountain*"** (Figure 6.2.1). Locate the time zone **Mountain Standard Time** (Figure 6.2.2). Enter the command **Set-TimeZone -name "Mountain Standard Time"** (Figure 6.2.3). Verify the time zone was set correctly by entering the command **Get-TimeZone** (Figure 6.2.4).

Figure 6.2 – PowerShell set time zone



HCP Settings

Best Practices

1. **Encryption** – only enable on HCP Storage
2. **Compression** – only enable on HCP Storage
3. **Deduplication** – enable on both HCP Gateway and HCP storage
4. **Metadata Replication** – use HCP Gateway DB replication
5. **Data Replication** – use HCP Active/Active Replication for data
6. **Payload Signature** – Recommend using S3 V4 signature with HCP storage

Configuring HCP Tenant and Namespace Settings

In the HCP Tenant Management Console, create an HCP Tenant and Namespace that will be used by the HCP Gateway to store the data and backups.

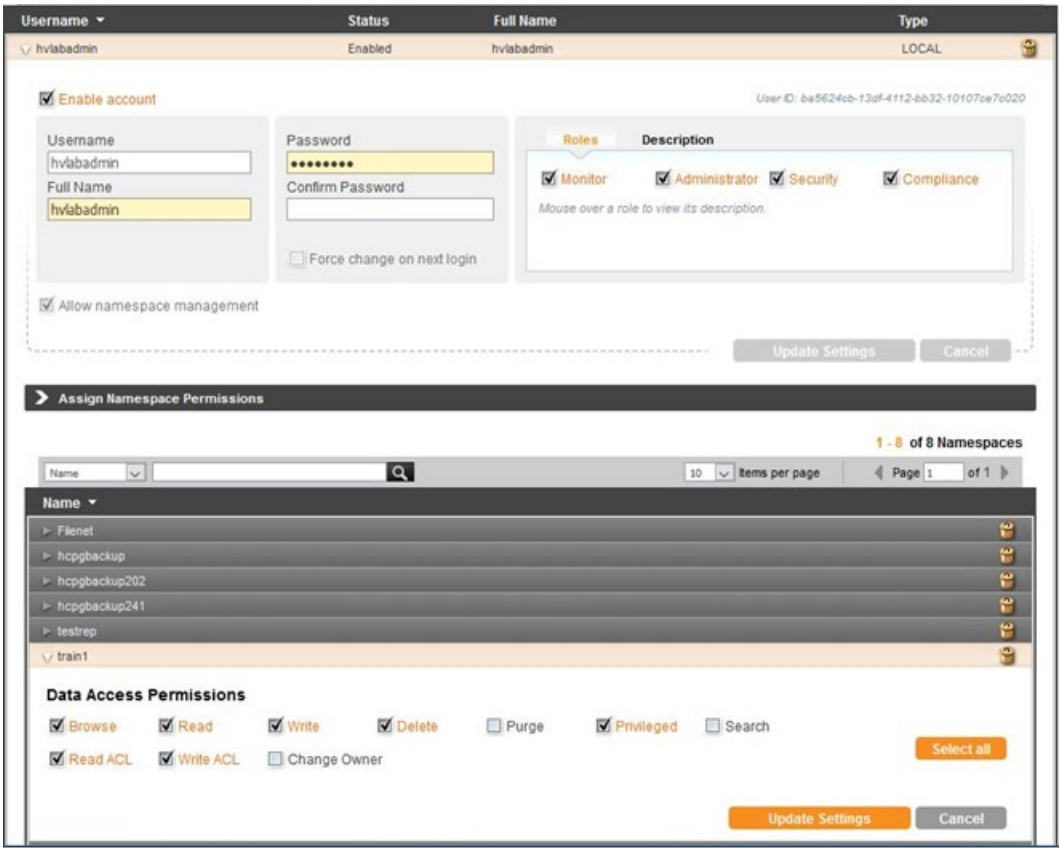
HCP S3 Payload Signature Settings

1. HCP 9.x supports both S3 v4 signed and unsigned payload.
2. HCP 8.x supports both S3 v4 signed and unsigned payload.

HCP Tenant Settings

1. **Authentication Types** – Enable both Local and Active Directory Authentication
2. **Configuration -> Namespace Defaults** – Enable Versioning
3. **Security –> MAPI** – Enable the management API
4. **Security –> Users** – Assign Data Access Permissions to the user that owns the Namespace: Browse, Read, Write, Delete, Read ACL, Write ACL, and Privileged (Figure 6.3)

Figure 6.3 – Tenant Security for Users

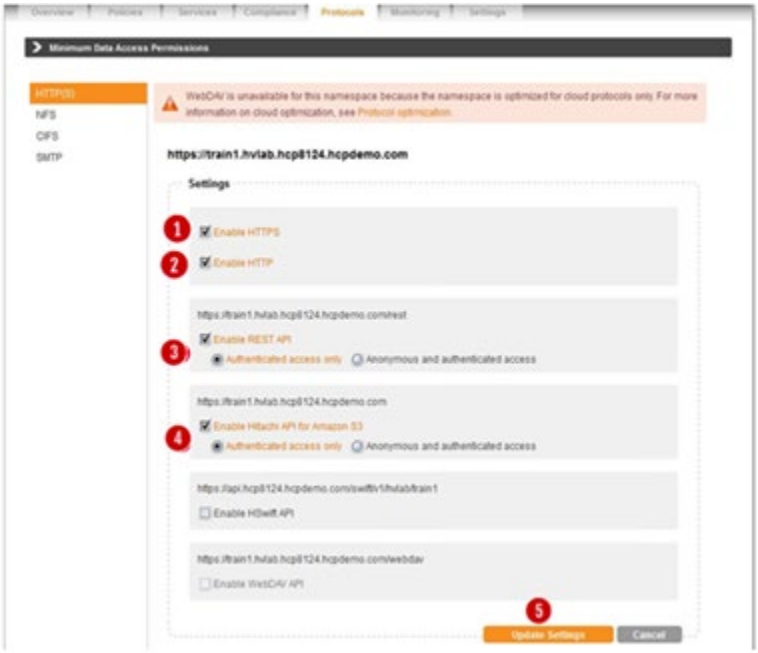


HCP Namespace Settings

1. **Assign Owner** to HCP Namespace (Figure 6.4.1)
2. **Versioning** – Enable versioning for ALL HCP Namespaces including data and database backup.
3. **Retention** – Do **not** set retention (HCP Gateway will pass the retention settings for each file)
4. **MPU** (supported on HCP 8.x or higher) – Enable
5. **Settings** –> **ACLs** – Enable ACLs and Enforce ACLs
6. **Settings** –> **Optimization** – Enable Optimized for Cloud protocols only
7. **Protocols –> HTTP(S)** – Enable HTTPS (Figure 6.5.1)
8. **Protocols –> HTTP(S)** – Enable HTTP (Figure 6.5.2)
9. **Protocols –> HTTP(S)** – Enable REST API (Figure 6.5.3)
    a. Select authenticated access only
    b. Enable Active Directory single sign-on (if needed)
10. **Protocols –> HTTP(S)** – Enable Hitachi API for Amazon S3 (Figure 6.5.4)
    a. Select Authenticated access only
    b. Enable Active Directory single sign-on (if needed)
11. Remember to click **Update Settings** (Figure 6.5.5) on each screen to save the changes.

Figure 6.4 - Namespace Assign Owner

Figure 6.5 - Namespace Protocol Settings



Configure the pruning settings on HCP to meet customer requirements for how long they want to keep the files on HCP after they are deleted on the HCP Gateway. When a file is deleted from the share on the HCP Gateway and the Delete on Storage runs to delete that file off the HCP, the pruning setting will determine how long the file will remain on HCP

before they are removed by the HCP garbage collection. Also, please make sure that HCP replication is configured so that when the Delete on Storage deletes the file off the primary HCP cluster, the HCP replication will delete the file off the replica HCP cluster.

HCP for Cloud Scale Settings

Best Practices

1. **Encryption** – only use on HCP for Cloud Scale
2. **Compression** – only use on HCP Gateway
3. **Metadata Replication** – use HCP Gateway DB replication
4. **Data Replication** – use HCP Gateway Storage policy to write data to multiple Cloud Scale clusters (from single Gateway)
5. **Payload Signature** – must enable and use S3 V4 signature with HCP for Cloud Scale
6. **HTTPS** – must enable HTTPS for all communication to HCP for Cloud Scale (cannot use HTTP)
7. **Deduplication** – use on HCP Gateway only if using "UUID" method for S3 Object ID
8. If using **"File Path"** method for S3 Object ID please see note below.

IMPORTANT NOTE:

When using the "File Path" (no name mangling) setting for S3 Object ID creation (in the HCP Gateway Storage Policy and Share Configuration), the following are required:

1. Disable all deduplication to avoid Data Loss
2. A separate S3 bucket must be created on an HCP for Cloud Scale for each share on all of the HCP Gateways at the customer site. Every bucket on HCP for Cloud Scale at the customer site must have a unique name. Every share on each HCP Gateway at the customer site must have a unique Storage defined in the Storage page on the HCP Gateway that will read from and write to the HCP for Cloud Scale bucket created for this HCP Gateway share. Failure to follow these recommendations may result in data loss if a user writes a file with the same file system path and name and different content to more than 1 share on the HCP Gateway.
3. Do not enable compression or encryption on the HCP Gateway share using HCP for Cloud Scale storage because the user will not be able to read the file content directly from the HCP for Cloud Scale bucket.

HCP for Cloud Scale Settings

1. Only generate the credentials once on the HCP for Cloud Scale, as each time the credentials are generated, the old credentials are invalidated.
2. When using a share on the HCP Gateway with Retention, enable **Object Lock** on the HCP for Cloud Scale bucket in order for the HCP Gateway to lock files under Retention and Legal Hold.

3. When using a share on the HCP Gateway without Retention, enable **Object Lock** on the HCP for Cloud Scale bucket in order for a Legal Hold to be placed on a file.
4. Do not enable any settings in the **Expiration Lifecycle** for any HCP for Cloud Scale buckets except, it is supported to enable the **Delete incomplete multi-part uploads** and configure the number of days until the upload is aborted, the default is 7.
5. Do not set retention on HCP for Cloud Scale buckets, the HCP Gateway will handle setting the file retention and then removal after the file retention expires.
6. Use HCP Gateway database replication to replicate the file metadata on the files in the HCP Gateway shares to a secondary HCP Gateway.
7. To write to multiple HCP for Cloud Scale clusters from a single HCP Gateway, in the HCP Gateway UI **Storage** page, add a **Storage** for each bucket on each HCP for Cloud Scale and then combine up to 3 Storages into a **Storage Group** on the HCP Gateway Storage page. Then use this **Storage Group** when creating the share on the HCP Gateway.
8. HCP for Cloud Scale bucket names cannot have upper case letters.

IMPORTANT NOTE:

When using an HCP Gateway share with retention, the **Privileged Delete** feature in the HCP Gateway is not available because it will not be able to delete a file off the HCP for Cloud Scale bucket because the HCP for Cloud Scale uses Compliance mode for retention.

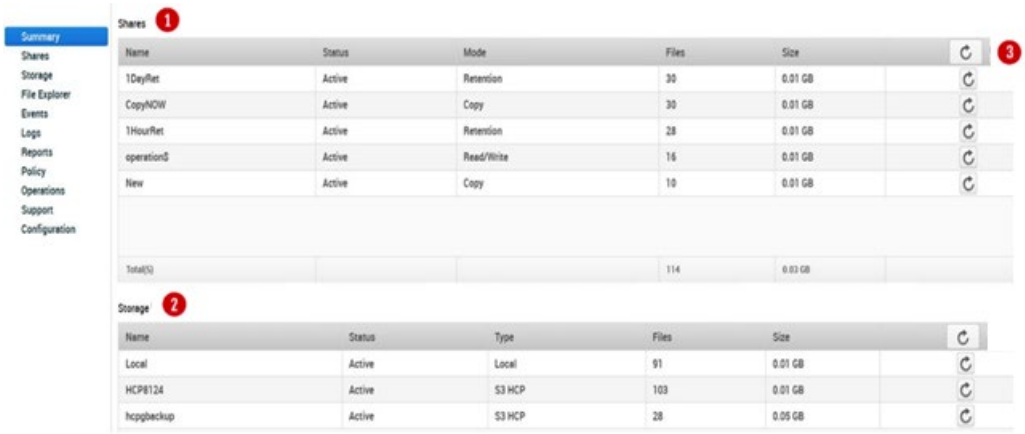
HCP for Cloud Scale Payload Signature Settings

1. HCP for Cloud Scale 2.3 only supports S3 v4 signed payload.

HCP Gateway Summary Page

The Summary page is the default starting point or landing page for the HCP Gateway application. The Summary page consists of two sections: Shares and Storage (Figure 7.1). Prior to configuring and using HCP Gateway these sections will be blank. Once HCP Gateway is operational the objective of the Summary page is to provide a status on each Share (Figure 7.1.1) and backend storage (Figure 7.1.2). To most effectively utilize system resources the status page is not dynamic. To update the status on all of the Shares or Storage select the refresh button (Figure 7.1.3) at the top of each section.

Figure 7.1 – Summary Page



Shares

This section lists the Shares that have been configured in HCP Gateway. Each row contains the information related to one Share. The first column contains the Name of the Share (Figure 7.2.1). The second column reports the Status of the Share (Figure 7.2.2). The Status will be either “Active” or “Off Line.” Status is Active when the Share is accessible to Users or Applications. The Status is Off Line when the Share is not visible or accessible to Users or Applications.

Figure 7.2 – Share Summary

The third column provides info on the Mode (Figure 7.2.3) of the Share. The options are: Read-Only, Read/Write, Copy, Tiering and Retention. In Read Only Mode files managed by the Share are accessible via read operations, but no file updates or new files can be created. In Read/Write Mode the files in the Share can be read, or overwritten, or deleted and new files can be written. Copy and Tiering modes allow the files to remain in the HCP Gateway

cache for fast access and can be read, modified, deleted and new files can be written. In Retention Mode, files in the Share can be read and new files can be written. However, files cannot be changed or deleted if the Retention time has not been passed. The fourth column provides info on the File count in the Share (Figure 7.2.4). The fifth column contains information on file Size or capacity in the Share (Figure 7.2.5). The minimum size displayed in the GUI is 0.01 GBs. If the total of all the files in a Share are below this value the GUI will display 0.01 GBs. Note this does not apply to licensed capacity just GUI display. The sixth column contains the refresh button which updates the info for the Shares. To update the info for all Shares, select the refresh button from the column header (Figure 7.2.6). To update info for a select Share, select the Refresh button (Figure 7.2.7) for a specific Share. The Total line (Figure 7.2.8) will show the total number of files and the total capacity used for all the Shares.

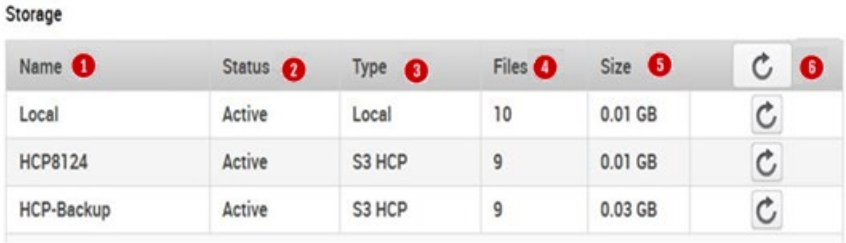
WARNING: The File and Size data are NOT dynamically updated. The Refresh button must be selected to update the metrics.

Storage

This section lists the Storage that is available for the Shares on the HCP Gateway. Each row contains the information related to one Storage option.

1. Name (7.3.1) – The name assigned to the storage device
2. Status (7.3.2) – Active or Not active
3. Type (7.3.3) – Type of storage device, Local, S3 HCP, etc.
4. File (7.3.4) – The total number of files on that storage device
5. Size (7.3.5) – Amount of space used on that storage device
6. Refresh (7.3.6) – Used to refresh all Storage information using the refresh button on the Header line or only information for a specific Storage using the refresh button on that line

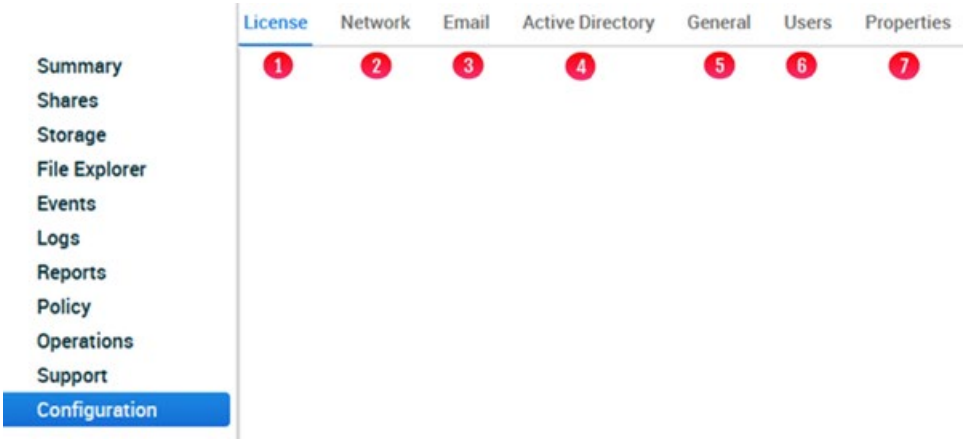
Figure 7.3 – Storage Summary



HCP Gateway Configuration

The Configuration section (Figure 8.1 - Configuration) is composed of 7 topics. To select a topic simply select the desired topic name and it will turn blue and load in the work area.

Figure 8.1 - Configuration



Below is a list of topics and a brief description of what can be done in each.

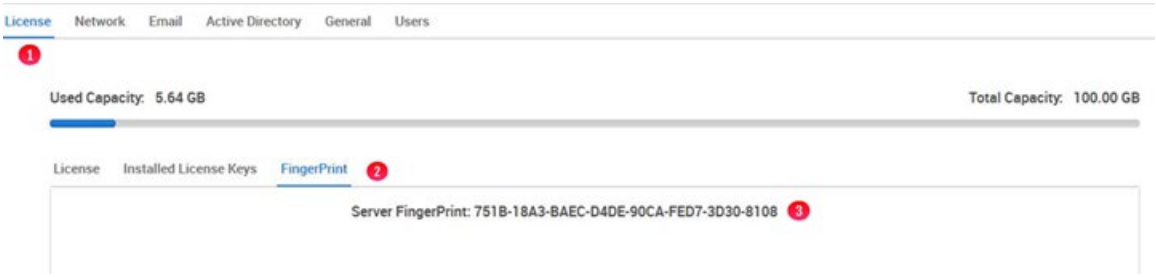
1. License – EULA, Add License Key (Figure 8.1.1)
2. Network – Interfaces (required to be static IP and MAC addresses) (Figure 8.1.2)
3. Email – required to enable alerts to be sent to Admins or Users (Figure 8.1.3)
4. Active Directory – Add, configure (Figure 8.1.4)
5. General – Cache Management and Unit settings (GBs or TBs) (Figure 8.1.5)
6. Users – add and manage users (Figure 8.1.6)
7. Properties - configure HCP Gateway properties (Figure 8.1.7)

Some Configuration topics such as License and Network are mandatory, the remaining are optional. Each topic will now be covered.

8.1 License

The HCP Gateway is licensed by managed capacity. All HCP Gateway Software License keys are generated for a specific server and tied to a digital fingerprint of the server. On the License page (Figure 8.2.1) select **Fingerprint** (Figure 8.2.2) to generate the digital fingerprint (Figure 8.2.3) for the server. Send the digital fingerprint and total license capacity purchased to Hitachi Support so they can generate the license key.

Figure 8.2 – Digital fingerprint

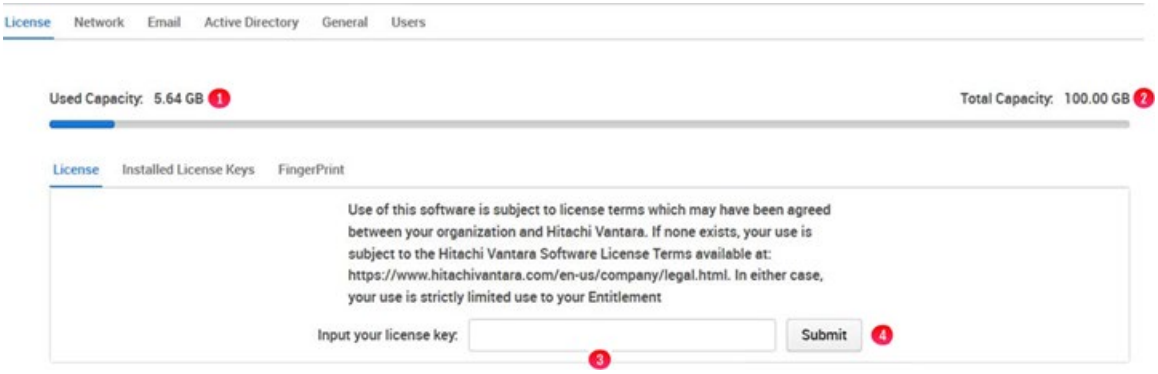


The License page will display both the **Used Capacity** (Figure 8.3.1) and **Total Capacity** (Figure 8.3.2) licensed. Type or paste the HCP Gateway License key into the box (Figure 8.3.3). Next the **Submit** button (Figure 8.3.4) must be selected to enter the information into HCP Gateway. If the License key is valid, it will add the key to the installed keys and adjust the total License capacities.

NOTE:

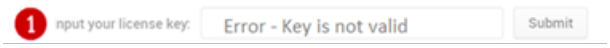
If a “License Key invalid” error appears, verify that the Locale in the HCP Gateway UI login page matches the Locale of the HCP Gateway Windows server.

Figure 8.3 - License



If the License key is not valid an error will be displayed (Figure 8.4.1).

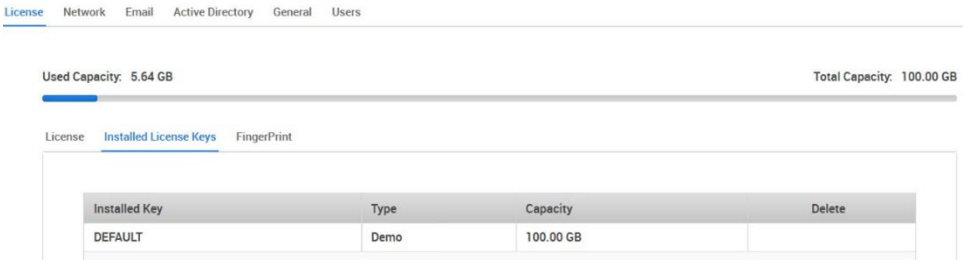
Figure 8.4 -Error License Key



Installed License Keys

All License keys are displayed and entered on the Installed License Key page (Figure 8.5). For demonstration and basic functional testing purposes a 100 GB default license is provided. As the Used License capacity approaches the License capacity an administrative alert is generated. File access will not be impacted when the licensed capacity has been reached.

Figure 8.5 - Installed License Keys



8.2 Network

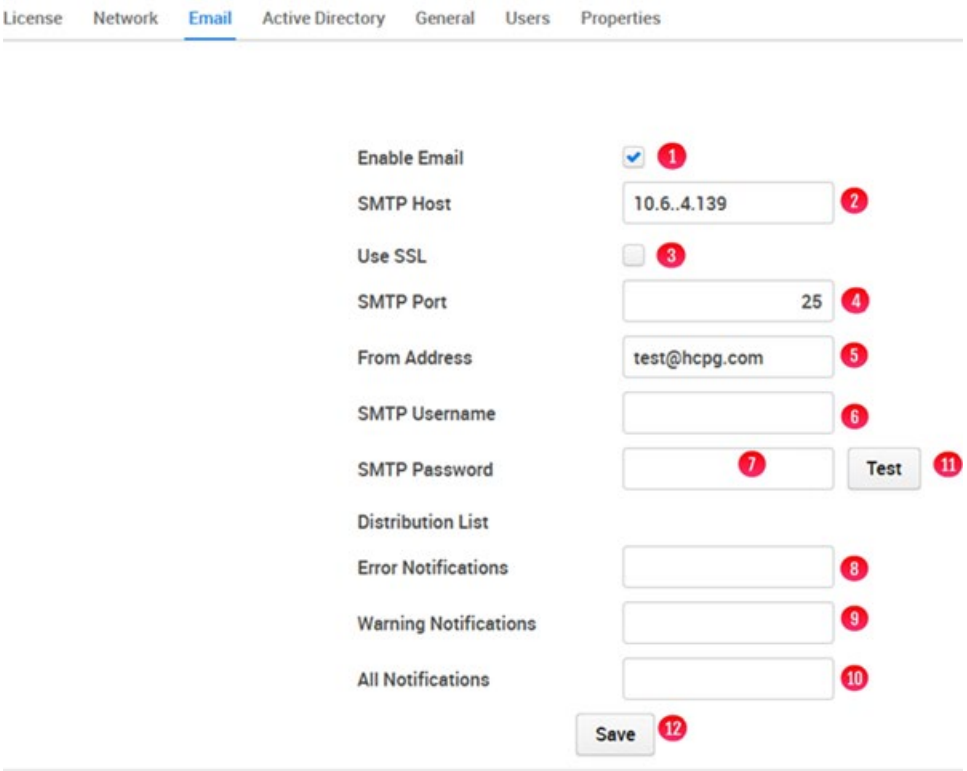
Before the HCP Gateway License Key can be entered the network interfaces must be configured. Installed Network Interfaces will be displayed in the table (Figure 8.6.1). Make sure that a Fixed IP address is used, otherwise HCP Gateway will not be accessible after a reboot.

Figure 8.6 Network

8.3 Email

Email must be enabled and configured for HCP Gateway to send information or alerts to Users or Administrators. From the email tab select the check box **Enable Email** (Figure 8.7.1). Then fill out the remainder of form and select the **Save** button.

Figure 8.7 - Email



SMTP Host - The hostname or IP address of the SMTP server that HCP Gateway should use for sending alert emails (Figure 8.7.2).

Use SSL - Check this box if the SMTP host is configured for TLS/SSL (Figure 8.7.3).

SMTP Port - Default port is 25 for unencrypted communication or 465 for TLS/SSL, but check with your email administrator to verify what port is appropriate for your organization (Figure 8.7.4).

From Address - When HCP Gateway sends an alert email it will use this as it's "From address". It is generally a good idea to create a unique email address to assist in filtering HCP Gateway alerts from other mail (Figure 8.7.5).

SMTP Username - If the SMTP host requires authentication, provide a username here, otherwise leave this field blank (Figure 8.7.6).

SMTP User Password – If the SMTP host requires authentication, provide the password for the username here, otherwise leave this field blank (Figure 8.7.7).

Distribution List Error Notifications – Valid email address and/or distribution list address to receive Error level event emails. Multiple email addresses can be entered, separated by commas (Figure 8.7.8).

Distribution List Warning Notifications – Valid email address and/or distribution list address to receive Warning and Error level event emails. Multiple email addresses can be entered, separated by commas (Figure 8.7.9).

Distribution List All Notifications – Valid email address and/or distribution list address to receive Operational, Warning and Error level event emails. Multiple email addresses can be entered, separated by commas (Figure 8.7.10).

Test - Send a test email to the Distribution List(s) Notification fields with valid email addresses (Figure 8.7.11).

Save - Save the configuration and will send a test email to the Distribution List(s) Notification fields with valid email addresses (Figure 8.7.12).

NOTE:

The first time the test email is sent, if it is not received within a few minutes, check the SPAM folder of the user the email was sent to and select report the email as not SPAM so that future emails will be received in the user's Inbox.

8.4 Active Directory setup for Management Console Users

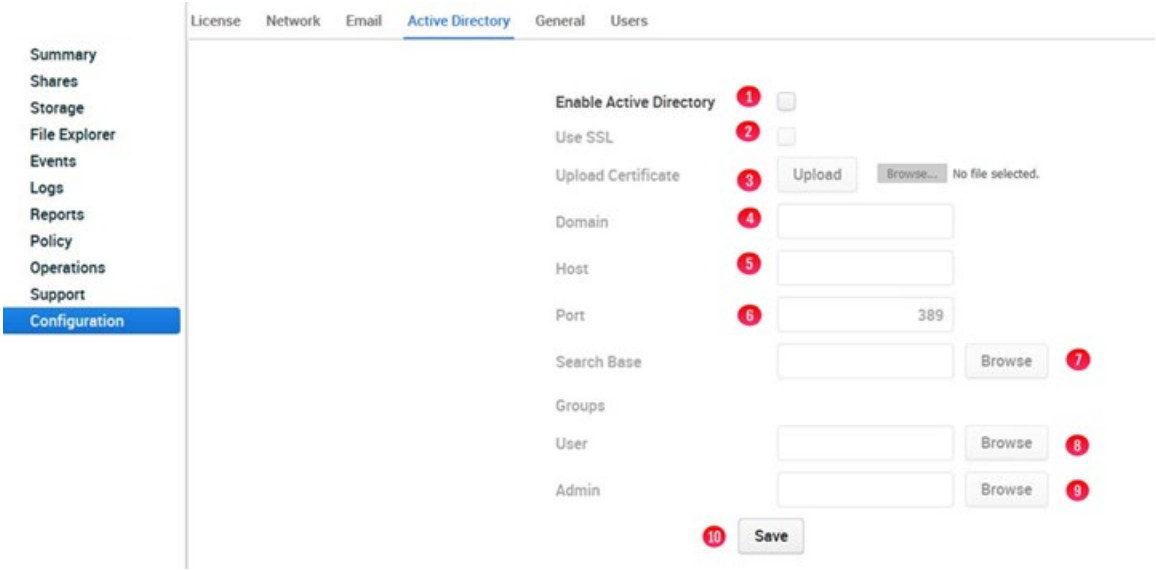
HCP Gateway can integrate with one Microsoft Active Directory server to utilize AD users, groups, and permissions. Active Directory 2012, 2016 and 2019 are supported. This page in the HCP Gateway UI is used to configure AD access for the Management Console UI only.

Separately, you will need to use Windows File Explorer to configure AD access for the shares, folders, and files.

Local users and Active Directory users cannot be used at the same time in the HCP Gateway UI. If using Active Directory users, only the local admin user will remain enabled in the HCP Gateway UI, which can be used to access the HCP Gateway UI in case the Active Directory server is not accessible.

To join Active Directory, select the **Enable Active Directory** check box (Figure 8.8.1).

Figure 8.8 - Active Directory



WARNING: AD can be confusing if you are not familiar with it. Contact your AD administrator and get their assistance with getting the correct user, group or service account and credentials. If you are part of a large organization also request which Search Base to use.

IMPORTANT NOTE:

The HCP Gateway AD configuration will only use objects that are in the level immediately below the Search Base.

Use SSL	Select this box to use secure Active Directory (Figure 8.8.2). Refer to **LDAP authentication to Active Directory via SSL certificate** chapter for more information about how to configure Active Directory with SSL.
Upload certificate	Only use this option if the **Use SSL** box is selected. Browse to the location where the secure client certificate is located, highlight the certificate, and select the **Upload** button (Figure 8.8.3).
Domain	The name of the Active Directory domain you wish to join. Depending on the version of Windows AD server you are using this may need to be the short name, i.e., domain name, or long name, i.e., domainname.com or domainname.local (Figure 8.8.4).
Host **Port**	The IP address or host name of the AD server (Figure 8.8.5). The port used to connect to Active Directory. For non-SSL the default port is 389, 0 can also be used and should find the appropriate port. For SSL, port 636 is the default (Figure 8.8.6).

Search base	The path that contains the Active Directory users and groups. Be sure to set the correct **Port** (Figure 8.8.6) before selecting the **Browse** button. Select the **Browse** button (Figure 8.8.7) to open the **Select search base** screen (Figure 8.9). Enter an administrator username in the **User** field (Figure 8.9.1) and password in the **Password** field (Figure 8.9.2), then select the **Connect** button (Figure 8.9.3) to access the AD search base. It is advisable to create a special user for this task as this user is allowed access to the Active Directory Administrator group. This user only requires read-only privileges; the user will be used by HCP Gateway to validate login requests and access to the HCP Gateway UI. Each OU has a Common Name (CN). Both the Groups and the users in the Groups for user and admin level access must be located immediately under the Search Base OU. You will select the CN entry for the OU where the User and Admin groups are located. Search Base OU (CN=Users, DC=dtschdmz,DC=com) • Group for user level access (CN=Domain Users, CN=Users, DC=dtschdmz,DC=com) • Group for admin level access (CN=Domain Admins, CN=Users, DC=dtschdmz,DC=com)

IMPORTANT NOTE:

For this example, the users Administrator and Andy Thomson are members of the Domain Admins group (Figure 8.11). The Domain Admins Group and CN's for Administrator and Andy Thomson are all in the level immediately below the Search Base (Figure 8.11).

Gateway AD User	After selecting the **Connect** button (Figure 8.9.3) various domain and configuration information should be displayed in the left pane. Select the CN entry that lists the OU where the User and Admin Groups are located (Figure 8.9.4), then select **Apply** (Figure 8.9.5). The user level privilege will not have access to modify the HCP Gateway UI Configuration page and won't be able to access the download, versioning and show deleted files features in the HCP Gateway UI File Explorer page.
Gateway AD Admin	To add a group with user level access from AD, select the **Browse** button (Figure 8.8.8). Select the **Connect** button (Figure 8.10.1) to access the AD search. Under the **Search Base OU**, select the CN

	entry for the group that you want to provide user level privileges (Figure 8.10.2 and 8.10.3). Select the **Apply** button (Figure 8.10.4) to save the setting. To add a group with admin level access from AD, select the **Browse** button (Figure 8.8.9). Select the **Connect** button (Figure 8.11.1) to access the AD search. Under the **Search Base** OU, select the CN for the group that you want to provide admin level privileges (Figure 8.11.2 and 8.11.3). Select the **Apply** button (Figure 8.11.4) to save the setting. Select the **Save** button (Figure 8.8.10) to save the AD configuration.

Figure 8.9 - Search Base

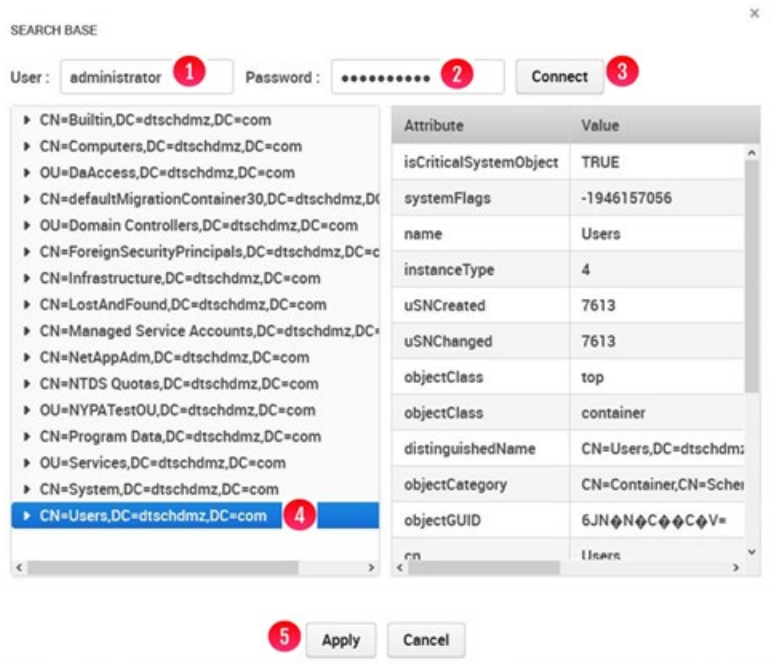


Figure 8.10 - AD User Group

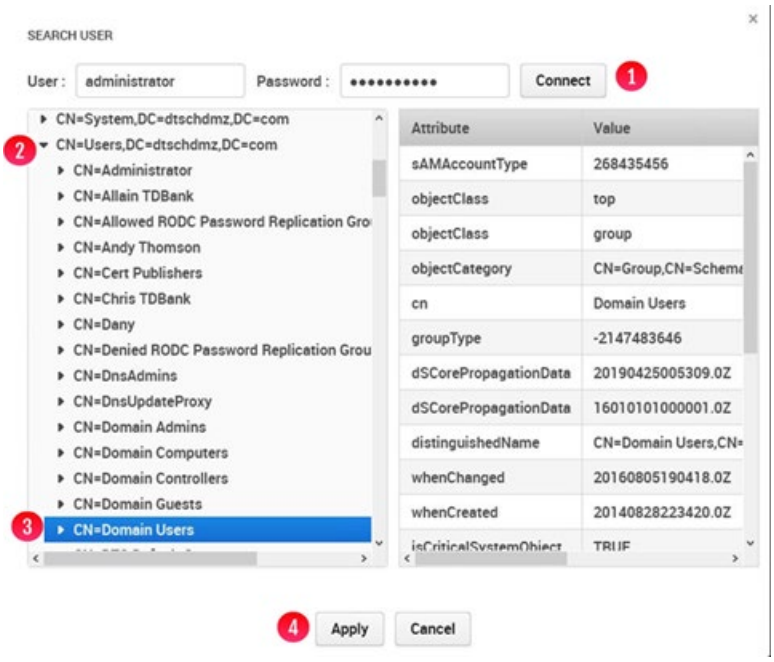
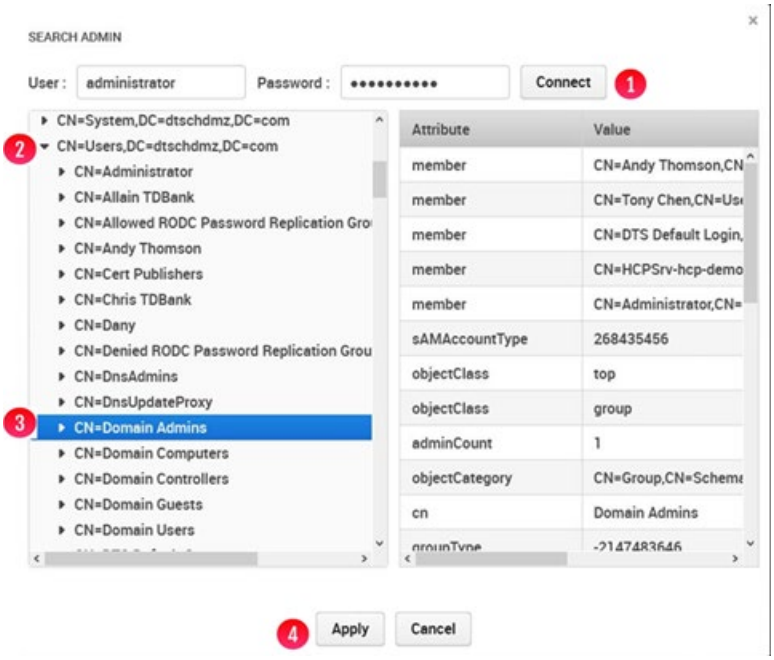


Figure 8.11 - AD Admin Group



8.5 Cache Management (General Tab)

HCP Gateway has some configuration parameters that are important to its functioning. On ingest the HCP Gateway saves files to a local cache. All Shares write data into this common cache. To prevent the cache from getting full and rendering the HCP Gateway server unusable it is important to reserve some space and this is done by setting the **Cache Limit** (Figure 8.12.1). The default setting is 90% and can be set to any value between 20% and 95%. Once this value is reached the Shares are put into Read Only mode.

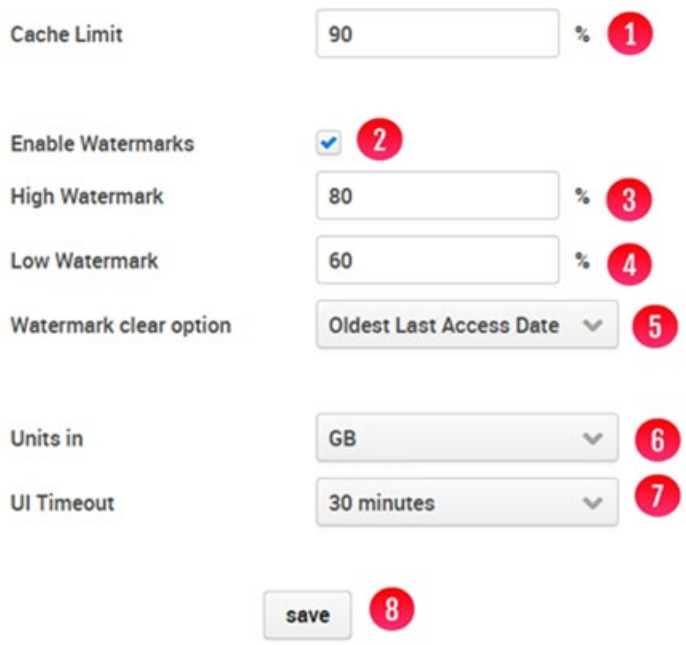
To avoid reaching this threshold and putting the Shares into Read Only mode, the Watermarks feature can be enabled (Figure 8.12.2). The role of the **High Watermark** (Figure 8.12.3) is to release the file content, which is stored on the Storage(s) in the Storage Group(s), from the local cache to avoid reaching the **Cache Limit**. The default setting is 85% and can be set to any value between 20% and 95%. The **High Watermark** needs to be lower than the **Cache Limit** and higher than the **Low Watermark**. How much lower is dependent upon how much data is ingested during peak time. If the peak write rate is 10MB/sec and the Gateway holds files in cache for 3 minutes or 180 seconds, the minimum gap needs to be 180 * 10MB/sec or 1.8GBs. Better safe than sorry so multiple that by a factor of 2-3.

The role of the **Low Watermark** (Figure 8.12.4) is to stop the draining of the Cache. The default setting is 60% and can be set to any value between 20% and 95%. The **Low Watermark** must be lower than the **High Watermark**. If the environment is very active with lots of writes, then the safe route is to set the **Low Watermark** at 10-15% below the **High Watermark**. Deleting files from Cache is an expensive operation so smaller gaps will have less impact to writes than larger gaps. The **Watermark Clear** option (Figure 8.12.5) is used to select which files to release from cache and can be set to "Oldest Create Date", “Oldest Modification Date” or "Oldest Last Access Date".

Some organizations have lots of data and others do not, therefore there is the option to report metrics in **Units** of TBs or GBs (Figure 8.12.6). This metric option can be changed at any time. A GB is calculated as 1024x1024x1024 bytes. Units are traced to two decimal points, so round up at 0.51. This impacts any metric on Summary Pages, Shares, Storage and Reports.

The final parameter is the administrative **UI Timeout** (Figure 8.12.7). Select the **save** button (Figure 8.12.8) to save any changes.

Figure 8.12 - General

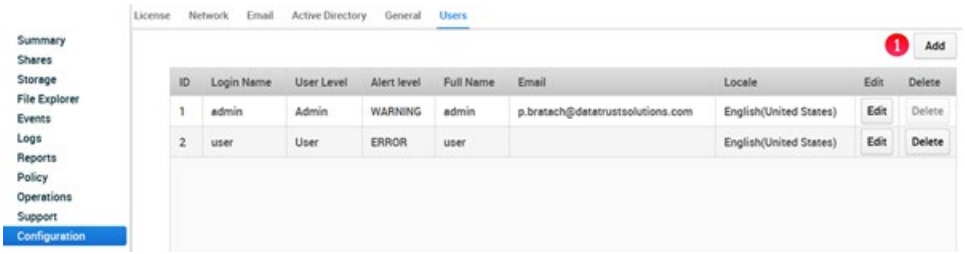


8.6 Users

HCP Gateway supports the role-based access to “administer” and to “view” the system. The roles categories are administrator or general user. A user can view information but not configure, start, or stop any processes. The administrator role (admin) has full control of the HCP Gateway configuration and operation.

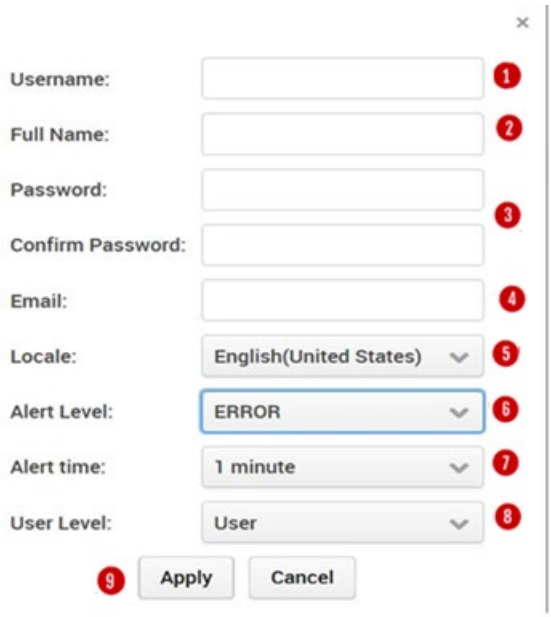
An Admin can add users by selecting the **Add** button (Figure 8.13.1).

Figure 8.13 - Manage Users



This action displays a form (Figure 8.14) that needs to be filled out. The mandatory items are: Username, Password/confirmation, and User level. The remaining fields are optional.

Figure 8.14 - Add Users



The requirements for each info box are:

Username – Must be a minimum of 3 and maximum of 256 alpha numeric characters excluding special characters (Figure 8.14.1).

Full name – If provided it must be a minimum of 3 and maximum of 256 alpha numeric characters excluding special characters (Figure 8.14.2).

Password – Must be a minimum of 3 and maximum of 256 alpha numeric characters excluding special characters (Figure 8.14.3).

Confirm password – Enter the password again for confirmation that you entered it correctly (Figure 8.14.3).

Email – Email address or SMS address can be entered here (Figure 8.14.4)

Locale – Default is English, select from pull down (Figure 8.14.5)

Alert level – Select Alert Level from list: Off, Error, Warning, Operational (Figure 8.14.6). For a list of Alerts see description in next section below.

Alert time – Select how often to receive this alert if the issue is recurring (Figure 8.14.7).

User level – Select from the options in pull down menu. The default option is User (Figure 8.14.8).

To save the information entered select the **Apply** button (8.14.9)

Alerts levels from most severe to least are: Error, Warning, Operational and Off. The user will receive alerts of the selected level as well as all levels above the selected level. For example, if the user requests Warning alerts they will also get Error alerts. A description of each is provided in the table below:

ERROR

Indicates a serious error that occurred during a scheduled operation and that the process was not able to continue. Possible causes include:

- Target does not exist
- I/O error
- database error

WARNING

Indicates an error that does not immediately impact the operation of the system, but may need attention. Possible causes include retrying a file save to target storage.

OPERATIONAL

Details about the normal operation of the system. Includes:

- Updates to schedules
- Updates to settings
- Operation start/stop times

OFF

When this level is selected, the user does not receive any alerts.

8.7 Properties

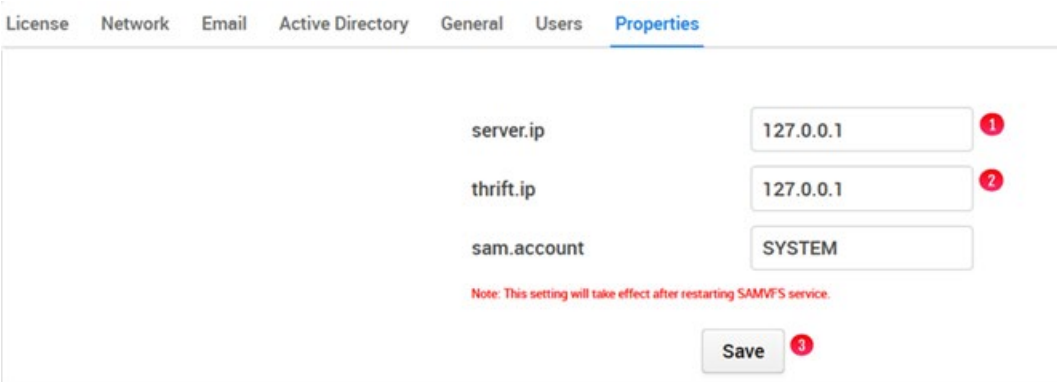
HCP Gateway has some configuration parameters that are important to its functioning. Refer to **Chapter 5** Section **HCP Gateway Configurations settings in C:\SAM\etc\sam\sam.properties** for a detailed description of these parameters (Figure 8.15).

NOTE:

Do not change the **server.ip** (Figure 8.15.1) or **thrift.ip** (Figure 8.15.2) unless instructed by HCP Gateway Support. All of these fields must have a value before selecting **Save**

(Figure 8.15.3). The SAM VFS service in Windows services must be restarted after changing any of these parameters.

Figure 8.15 - Properties

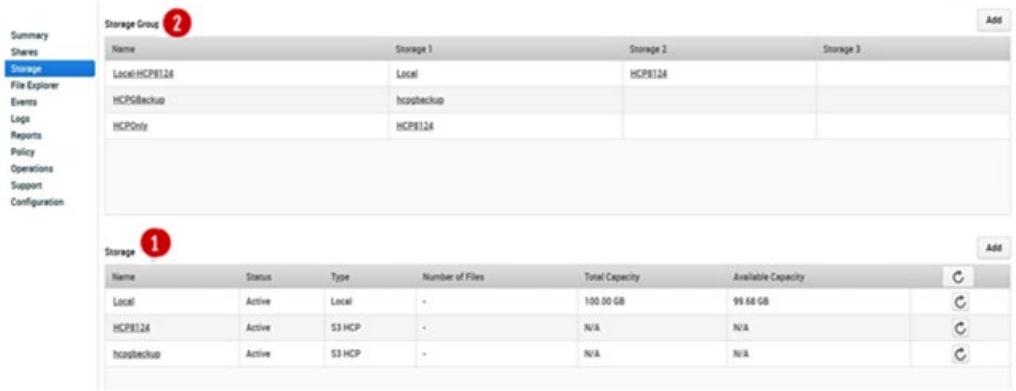


HCP Gateway Storage

HCP Gateway can manage data on local, network attached, public cloud storage and private cloud storage like the Hitachi Content Platform (HCP) or HCP for Cloud Scale. Before an administrator can create a Share there must be a place to save the data.

The Storage (Figure 9.1) page is divided into two sections: Storage (Figure 9.1.1) and Storage Group (Figure 9.1.2). The Storage section is where physical or virtual devices are added to the HCP Gateway system and ultimately where the data will reside. Storage devices are not exposed to Shares. Shares are configured to interact with Storage Groups, which consist of one or more Storage devices.

Figure 9.1 – Storage Tab (menu)



Note a Storage device provides storage capacity to the HCP Gateway. A Storage device can be used by one or more Storage Groups. Similarly, Storage Groups can be used by more than one Share.

Figure 9.2 – Storage Target

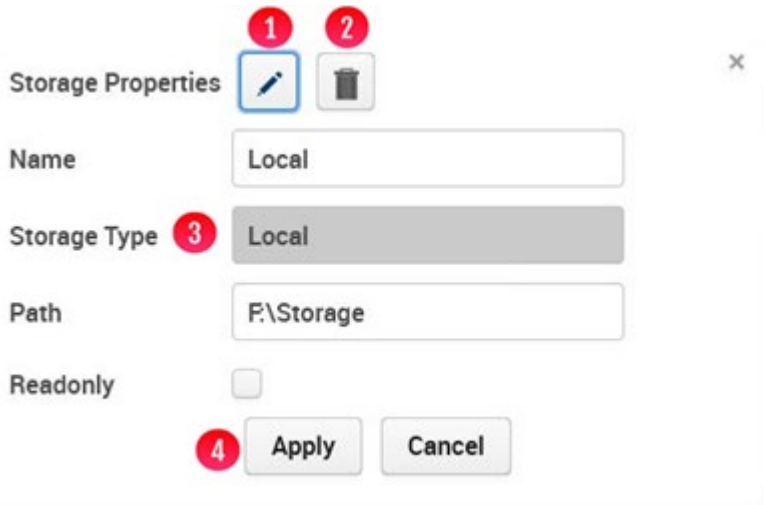
The Storage table (Figure 9.2) provides an overview of available Storage devices. Each Storage device has attributes and metrics. The metrics include number of files, total capacity, and available capacity. The metric information is displayed from a point in time. To get the most current metrics for a specific Storage device, select the refresh button (Figure 9.2.2). Alternatively select the refresh button in the header (Figure 9.2.3) to refresh the metrics for all Storage devices. The Status of Storage can be Active or Inactive. Active indicates that the Storage is ready and can be used. Inactive implies that the Storage is not available for use.

9.1 Edit/Delete Storage

The Storage configuration has only a few settings that can be edited once it has been used by a Share. Stopping the Share will not change which fields can be edited.

To edit an existing storage configuration, select the storage name (Figure 9.2.1). A popup form (Figure 9.3) will appear with the current configuration information displayed. To edit the storage information, select the **Edit settings (pencil icon)** (Figure 9.3.1). If the storage has not been used in a share, you can delete the storage by selecting the trash can icon (Figure 9.3.2). The Storage Type is not editable (Figure 9.3.3). Select the **Apply** button (Figure 9.3.4) to save the changes.

Figure 9.3 – Edit Storage



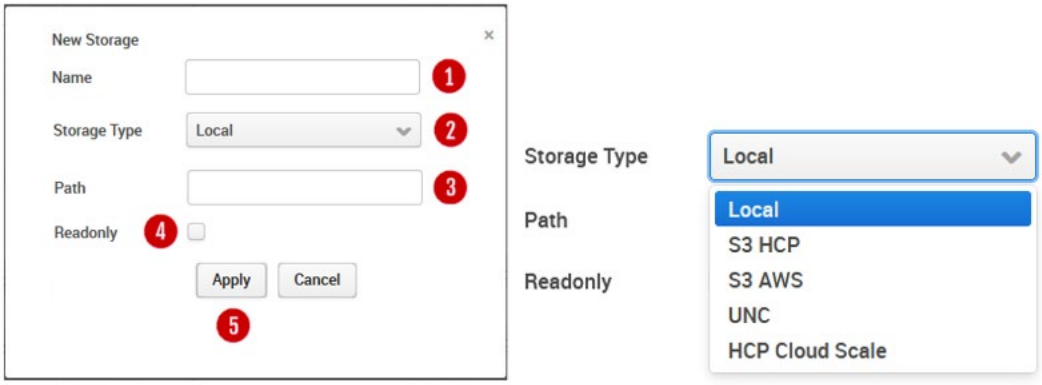
9.2 Add Storage

To make additional storage available to HCP Gateway, select the **Add** button for Storage (Figure 9.6.1). This will open up a pop-up form (Figure 9.4) that must be completed and saved by selecting the **Apply** button (Figure 9.4.5).

Each storage option must have a **Name** (Figure 9.4.1). A name must be a minimum of 3 characters and less than or equal to 256 characters. The Type of storage can be selected from the drop-down menu (Figure 9.4.2). The supported storage type options include: Local, S3 HCP, S3 AWS, UNC, and HCP for Cloud Scale.

If you are using local storage, enter the path to the storage in the input area (Figure 9.4.3). The default local path in Windows is recommended to be **"F:\Storage"**. The default local path is Linux is recommended to be **/storage/local**. To enable the new storage, select the **Apply** button (Figure 9.4.5) or to discard the information in the form select **Cancel**.

Figure 9.4 – Add Storage



WARNING: Do not use the cache drive for local storage, add another disk to the Gateway for local storage. In Windows, do not use the cache drive, the E: drive, for local storage. In Linux, ensure that /storage/local is not on the same drive as the cache, /storage/sam.

9.3 Local Storage

Figure 9.5 depicts the dialogue box for configuring Local Storage as a storage source. The Name must be a minimum of 3 characters and less than or equal to 256 characters. The Storage Type will already be filled in as Local.

In Windows the Path is typically a drive letter followed by a colon and then the backwards slash followed by the name and is recommended to be: **F:\Storage** (Figure 9.5W). The path must exist before you can add it into HCP Gateway.

In Linux the recommended path is: **/storage/local** (Figure 9.5L).

Figure 9.5W – Windows - Local Storage

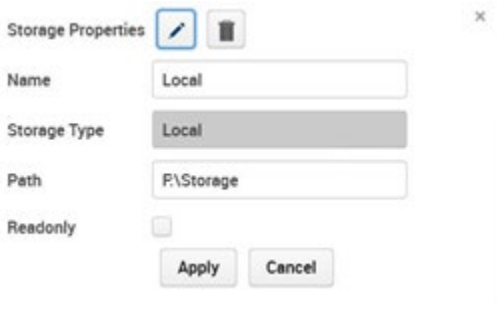
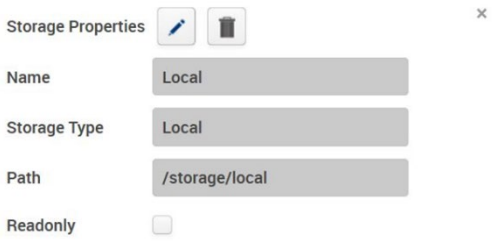


Figure 9.5L – Linux - Local Storage



WARNING: When using the Linux version of HCP Gateway, the Storage Name should be all lower case and not use spaces or any invalid characters. Windows versions of HCP Gateway can have spaces in the Storage Name.

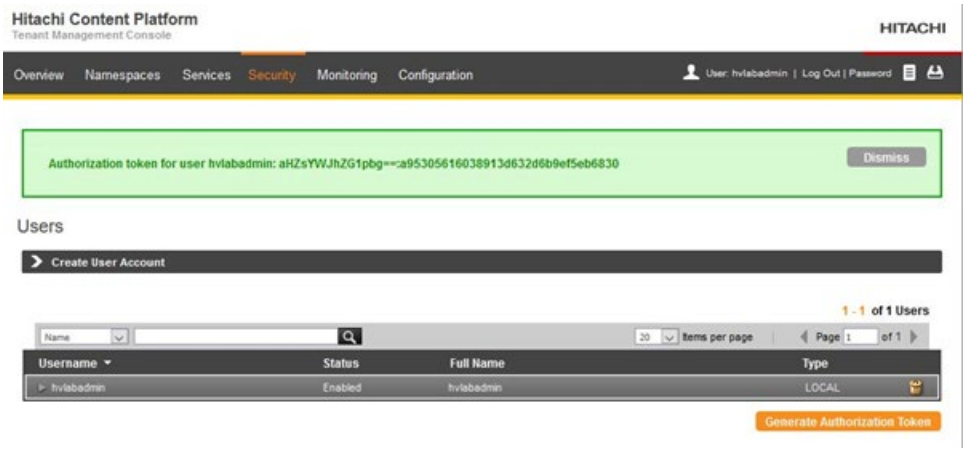
9.4 Add HCP Storage

Now create the Storage on the HCP Gateway that will use the namespace on the HCP as the location to store the files.

WARNING: The HCP must be configured prior to adding it as Storage on the HCP Gateway. Meet with the HCP Administrator and discuss Tenants, Data Namespaces, Backup Namespaces, and the form in Figure 9.8. In addition, the HCP **"tenant.hostname"** and **"namespace.tenant.hostname"** name and IP address information must be entered in either DNS or the local **"hosts"** file located in the **"C:\Windows\System32\drivers\etc"** folder on the HCP Gateway Windows and **"/etc/hosts"** in HCP Gateway Linux.

In addition, the HCP needs to have the following configuration parameters set (refer to the **HCP Settings** chapter for details on the HCP configuration settings):

1. Generate Authorization Token for the owner of the namespace that will provide the Access and Secret keys to be entered in the Add Storage page, you will find the "Generate Authentication Token" button in the Security -> Users page of the Tenant on the HCP. In the Authorization Token, all the text before the ":" is the S3 access key, all the text after the ":" is the S3 secret key that you will enter in the Storage page on the HCP Gateway.



2. Assign an owner to the HCP Namespace
3. Enable ACLs – Enforce ACLs
4. Enable "Optimized for Cloud protocols only"
5. Enable Multipart Upload if using for large files
6. Enable Protocols – HTTP (optional), HTTPS, REST API, and Hitachi API for Amazon S3
7. Enable Versioning (NEW)
8. In Tenant/Configuration/Namespace Defaults - Enable Versioning
9. In Tenant/Security - Enable MAPI
10. In Tenant/Security - Assign Data Access Permissions to the user that owns the Namespace: Browse, Read, Write, Delete, Read ACL, Write ACL, and Privileged

In the HCP Gateway UI, navigate to the Storage page (Figure 9.6.1). Select **Add** (Figure 9.6.2) in the Storage section of the page.

Figure 9.6 – Add Storage

In the “New Storage” window, enter **Name** (Figure 9.7.1) and select **S3 HCP** (Figure 9.7.2) from the “Storage Type” drop down menu. The options vary in the Windows and Linux versions of HCP Gateway.

Figure 9.7 – Storage Types in Windows

The description about each field in the Add Storage page is listed below.

Name – The name for the HCP storage (Figure 9.8.1).

S3 Protocol – Enter the S3 Protocol, HTTP or HTTPS used to connect to the HCP namespace (Figure 9.8.2).

S3 Host 1 – Enter the FQDN of the first “tenant.hostname” used to connect to the HCP namespace (Figure 9.8.3).

S3 Host 2 – Enter the FQDN of the second “tenant.hostname” used to connect to the HCP namespace (Figure 9.8.4).

S3 Access – Enter the Base64-encoded username for the HCP user account that owns HCP namespace for this storage (Figure 9.8.5).

S3 Secret – Enter the MD5-hashed password for the HCP user account that owns the HCP namespace for this storage (Figure 9.8.6).

S3 Bucket – Enter the name of the namespace on the HCP for this storage (Figure 9.8.7).

S3 Request Timeout – Number of seconds to wait before an S3 Request will time out (Figure 9.8.8).

WARNING: The **S3 Request Timeout** default is 300 seconds. This will handle a multi-part upload of a large file in most cases, it’s been tested with 900GB files. However, if you receive **“Fail to migrate”** warnings in the **C:\SAM\var\log\log-#.txt** log in Windows or **/var/log/sam/log-#.txt** in Linux, then you may need to increase the timeout.

Multipart Upload – Uploads multiple chunks of a file to the object storage in parallel for faster writes (Figure 9.8.9). Recommended to leave this enabled unless otherwise directed by HCP Gateway support.

Signed Payload – Enable or disable the S3 v4 signed payload (Figure 9.8.10) which will have some performance impact when enabled. Recommended to leave this enabled unless otherwise directed by HCP Gateway support.

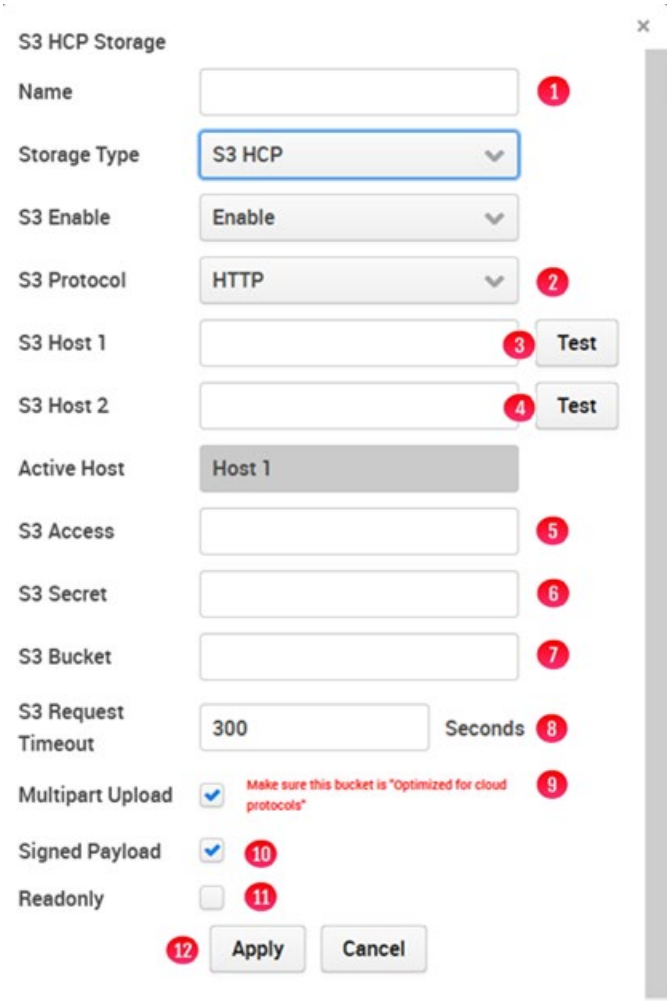
Readonly – Enable only if access to the storage is needed to be read-only (Figure 9.8.11)

Select the **Test** button (Figure 9.8.3) to ensure there is network connectivity to the HCP storage device. If the Test button returns **"Storage inactive"**, then check the network and HCP configuration and resolve any connectivity issues. Once the **Test** button returns **"Storage Active"**, select **Apply** (Figure 9.8.12) to save the settings or to discard the information in the form select **Cancel**. The **Apply** button will not allow you to save the Storage if the **Test** button returns **"Storage inactive"**.

NOTE:

Ensure that there is an entry in the local hosts file on the HCP Gateway or a DNS entry for the "namespace.tenant.host".

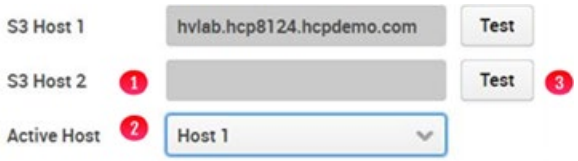
Figure 9.8 – Add HCP Storage



In Figure 9.8 the **S3 Host 2** field (Figure 9.8.4) was skipped so it can be addressed appropriately. The primary HCP information was entered as **S3 Host 1**. If the primary HCP is not available and the HCP replicates data to a second HCP system, adding an **S3 Host 2** entry will make the HCP Gateway aware of the second HCP for reading and writing files when the primary HCP is not available. When you enter a value in the **S3 Host 2** field, you can then define the **Active Host** (Figure 9.9.2) as the primary HCP for reads and writes.You can test the S3 Host 2 connectivity by selecting the **Test** button (Figure 9.9.3).

WARNING: If the **Active Host** is **S3 Host 1** and **S3 Host 1** fails to communicate with the HCP Gateway, the HCP Gateway will automatically fail the **Active Host** to **S3 Host 2**. When the **S3 Host 1** comes back online, the HCP Gateway will not automatically fail back the **Active Host** to **S3 Host 1**. When **S3 Host 1** is back online, manually change the **Active Host** to **S3 Host 1**.

Figure 9.9 – DR HCP



9.5 Add HCP for Cloud Scale Storage (Windows only)

IMPORTANT NOTE:

When using the **Use File Path** (no name mangling) setting when creating an HCP Gateway Storage using an HCP for Cloud Scale bucket, a bucket must be created on an HCP for Cloud Scale for each share on all of the HCP Gateways at the customer site. Every bucket on every HCP for Cloud Scale at the customer site must have a unique name. Every share on each HCP Gateway at the customer site must have a unique Storage defined in the Storage page on the HCP Gateway that will read from and write to the HCP for Cloud Scale bucket created for this HCP Gateway share. Failure to follow these recommendations may result in data loss if a user writes a file with the same file system path and name and different content to more than 1 share on the HCP Gateway.

WARNING: The HCP for Cloud Scale must be configured prior to adding it as Storage on the HCP Gateway. Meet with the HCP for Cloud Scale Administrator and discuss Data Buckets, Backup Buckets, and the form in Figure 9.12. In addition, the HCP for Cloud Scale **"hostname"** name and IP address information must be entered in either DNS or the local **"hosts"** file located in the **"C:\Windows\System32\drivers\etc"** folder on the HCP Gateway Windows and **"/etc/hosts"** in HCP Gateway Linux.

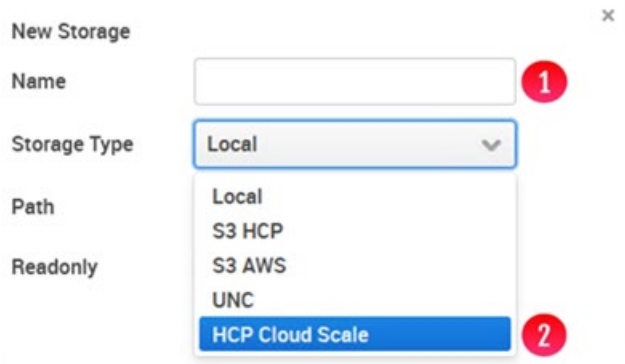
In addition, the HCP for Cloud Scale and HCP for Cloud Scale buckets need to have the parameters set as described in the **HCP and HCP for Cloud Scale Settings** chapter.

In the HCP Gateway UI, navigate to the Storage page (Figure 9.10.1). Select **Add** (Figure 9.10.2) in the Storage section of the page.

Figure 9.10 – Add Storage

In the "New Storage" window, enter **Name** (9.11.1) and select **HCP for Cloud Scale** (9.11.2) from the "Storage Type" drop down menu. The options vary in the Windows and Linux versions of HCP Gateway.

Figure 9.11 – Storage Types in Windows



The description about each field in the Add Storage page is listed below.

Name – The name for the HCP for Cloud Scale storage (Figure 9.12.1).

S3 Protocol – It is required to enter HTTPS as the S3 Protocol used to connect to the HCP for Cloud Scale bucket (Figure 9.12.2).

S3 Host 1 – Enter the FQDN of the "hostname" used to connect to the HCP for Cloud Scale bucket (Figure 9.12.3). Note that the **S3 Host 2** and **Active Host** are greyed out, because the S3 access and S3 secret keys are unique on each HCP for Cloud Scale, so it is not possible to have 2 Cloud Scale hosts in one HCP Gateway Storage. If the HCP Gateway needs to read and write to more than one HCP for Cloud Scale bucket, create a Storage in the HCP Gateway for each HCP for Cloud Scale bucket, and add them both to a Storage Group.

S3 Access – Enter the Base64-encoded username for the HCP for Cloud Scale user account that owns the Cloud Scale bucket for this storage (Figure 9.12.4).

S3 Secret – Enter the MD5-hashed password for the HCP for Cloud Scale user account that owns the HCP for Cloud Scale bucket for this storage (Figure 9.12.5).

S3 Bucket – Enter the name of the bucket on the HCP for Cloud Scale for this storage (Figure 9.12.6).

S3 Request Timeout – Number of seconds to wait before an S3 Request will time out (Figure 9.12.7).

WARNING: The **S3 Request Timeout** default is 300 seconds. This will handle a multi-part upload of a large file in most cases, it's been tested with 900GB files. However, if there are **"Fail to migrate"** warnings in the **C:\SAM\var\log\log-#.txt** log in Windows or **/var/log/sam/log-#.txt** in Linux, then it may be necessary to increase the timeout.

Multipart Upload – Uploads multiple chunks of a file to the HCP for Cloud Scale bucket in parallel for faster writes (Figure 9.12.8). Recommended to leave this enabled unless otherwise directed by HCP Gateway support.

Signed Payload – It is required to enable the S3 v4 signed payload (Figure 9.12.9).

Readonly – Enable only if access to the storage is needed to be read-only (Figure 9.12.10)

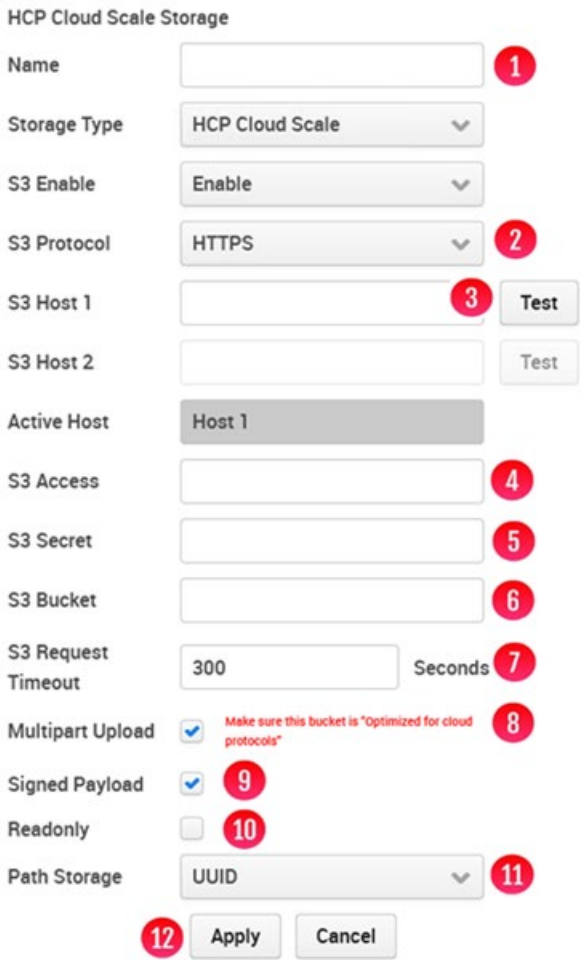
Path Storage – Select **UUID** to store the objects on the HCP for Cloud Scale bucket using a generated UUID, as is used with HCP storage. Select **Use file path** to store the files on the HCP for Cloud Scale bucket with their existing file paths (Figure 9.12.11). Please read and understand the **IMPORTANT NOTE** at the beginning of this section (Section 9.5) before enabling the **Use file path** setting.

Select the **Test** button (Figure 9.12.3) to ensure there is network connectivity to the HCP for Cloud Scale storage device. If the **Test** button returns **"Storage inactive"**, then check the network and HCP for Cloud Scale configuration and resolve any connectivity issues. Once the **Test** button returns **"Storage Active"**, select **Apply** (Figure 9.12.12) to save the settings or to discard the information in the form select **Cancel**. The Apply button will not allow you to save the Storage if the **Test** button returns **"Storage inactive"**.

NOTE:

Ensure that there is an entry in the local hosts file on the HCP Gateway or a DNS entry for the FQDN "hostname".

Figure 9.12 – Cloud Scale Storage



9.6 Add UNC Storage (Windows only)

In order to add a UNC Storage, select Add Storage (Figure 9.6.2) then select the **UNC** option from the Storage Type pull-down menu (Figure 9.7.2).

Name – Enter the name for the UNC storage (Figure 9.13.1).

UNC Path – Enter the UNC path with the syntax \\IPaddress\share (Figure 9.13.2).

Use Alias – This must be selected to use the UNC storage (Figure 9.13.3). The HCP Gateway will add an alias to the local Windows hosts file C:\Windows\System32\drivers\etc\hosts. Do not make any changes to this alias.

Username – Enter the username to connect to the UNC path (Figure 9.13.4).

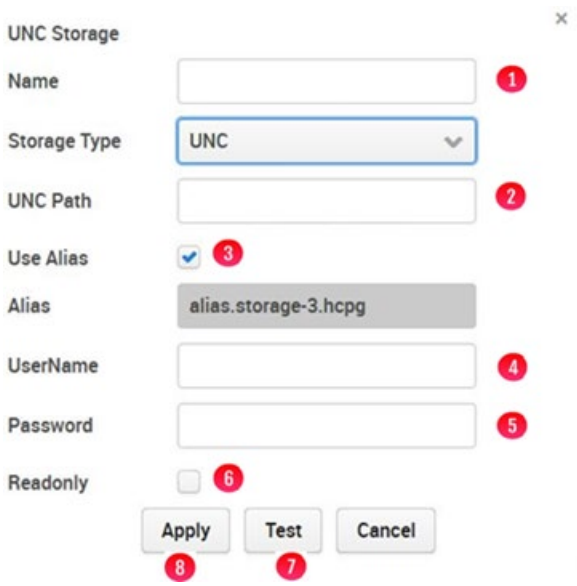
Password – Enter the password for the user to connect to the UNC path (Figure 9.13.5).

Readonly – Select this option if you want to only enable read access to the files on the UNC storage (Figure 9.13.6).

Test – Select the button to test the connectivity to the UNC share (Figure 9.13.7). Note that if the **Test** button returns "Storage inactive", check the network and UNC configuration settings and resolve any issues until the **Test** button returns "Storage active".

To enable the new storage, select the **Apply** button (Figure 9.13.8) or to discard the information in the form select Cancel. The **Apply** button will not allow you to save the Storage if the **Test** button returns "Storage inactive".

Figure 9.13 – UNC Storage



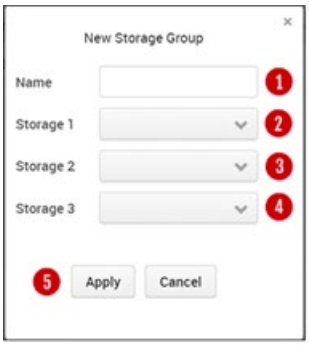
9.7 Storage Groups

After the HCP or other storage has been added in the Storage page, it is time to create a Storage Group. Storage Group allows the HCP Gateway to write to one, two or three storage targets. You will add the Storage Group to a share when you create a share. A file is written to the storage targets in the order they are listed in the Storage Group. On the top part of the Storage UI page, select **Add** (Figure 9.14.1).

Figure 9.14 – Add Storage Group

Enter a **Name** (Figure 9.15.1) in the form, it must be 3 characters or longer and less than 255 characters. Then select the down arrow (Figure 9.15.2) in the “Storage 1” box to see available Storage options. If you want to add a second Storage location, select the down arrow in the Storage 2 box (Figure 9.15.3), then select a storage from the available Storage options. If you want to add a third Storage location (Figure 9.15.4), select the down arrow then select a storage from the available Storage options. Then select **Apply** (Figure 9.15.5) to save the setting.

Figure 9.15 – Add Storage Group



HCP Gateway Shares

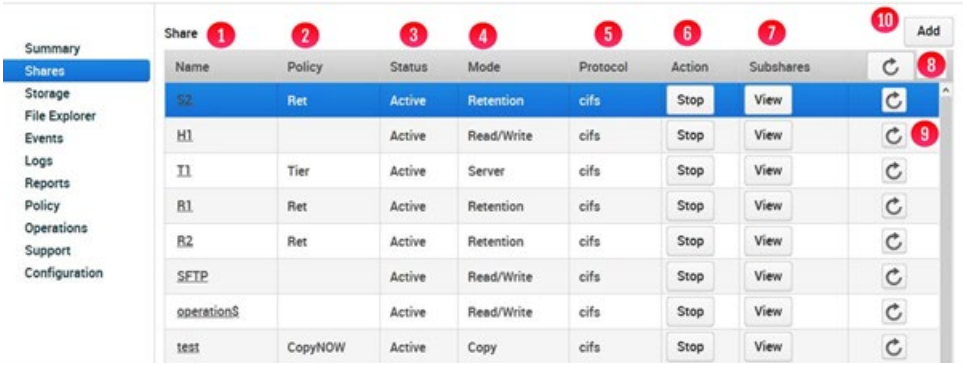
The Shares are the most critical aspect of the HCP Gateway system and time should be taken to review the user and application requirements before configuring a Share. Note that once files are written to a Share, the Share cannot be deleted until all the files, folders and the file history records are deleted from the database. If the Share is configured with a Server Mode Policy or is Read/Write, all the data in the Share can be deleted.

WARNING: Do not use the Windows or Linux sharing to share any of the HCP Gateway. All sharing of the shares MUST be handled by the HCP Gateway application.

10.1 Shares Menu Page

The Share landing page contains a summary of all the Shares listed in the order they were created (Figure 10.1). The information related to each Share is in a row. In the example below the share has one retention policy, is active and uses the CIFS.

Figure 10.1 – Shares



Name – must be a minimum of 3 characters and not more than 256 characters and review the list in section 10.2 for special characters (Figure 10.1.1) that are not allowed.

Policy – list applied Policies (Figure 10.1.2)

Status – is either Active or Off Line (Figure 10.1.3)

Mode – examples of the mode can be: Read/Write, Read Only, or a Policy type (Figure 10.1.4)

Protocol – is either CIFS or NFS (Figure 10.1.5)

Action – Start or Stop the Share (Figure 10.1.6).

Subshares (Windows only) – View Name, Path, and Access information about Subshares inside a Share (Figure 10.1.7).

Refresh – Gray button  (Figure 10.1.8) refreshes all shares, otherwise each share can be refreshed by selecting the refresh button in the appropriate row (Figure 10.1.9).

To view the settings of a Share simply select the “Name of the Share” (e.g., HCP) and a form will pop-up with the current settings. Some Share settings can be modified and saved, others cannot. For instance, you can disable the Share, or change the Hash, Compression, Encryption, Deduplication and Replication settings.

WARNING: Changes to settings of a Share only apply to new data; changes are not applied to existing data.

10.2 Add / Configure a Share

To add a Share to HCP Gateway, select the **Add** button (Figure 10.1.10). This will open a form in a pop-up window (Figure 10.2W for Windows and Figure 10.2L for Linux). Check the appropriate Windows or Linux figures when viewing the settings, as not all the settings are the same in Windows and Linux and are pointed out below. In this form are the default settings. To change them simply select the pull-down menu and select a different option.

Figure 10.2W – Add Share (Windows)

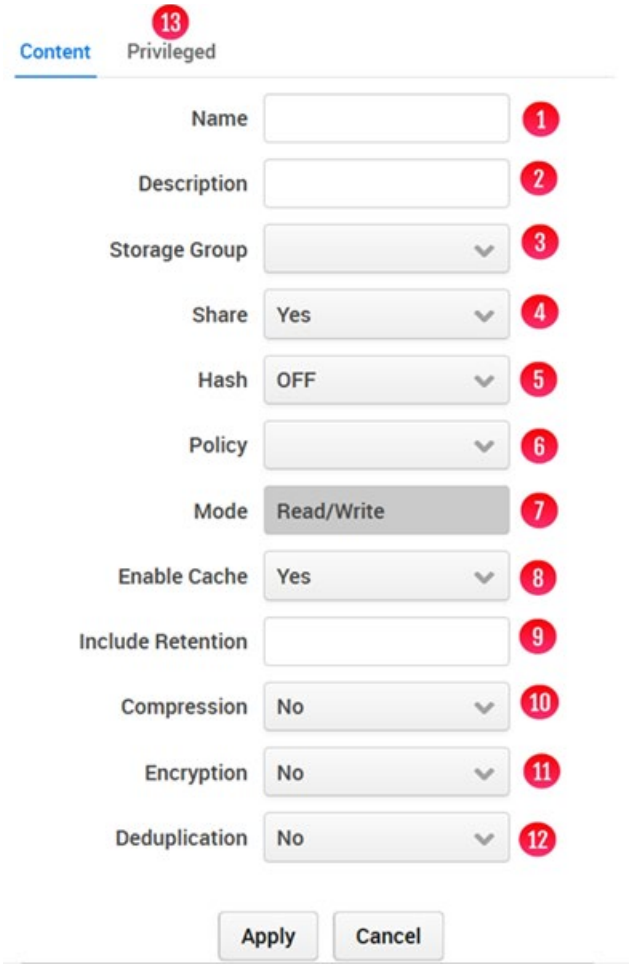
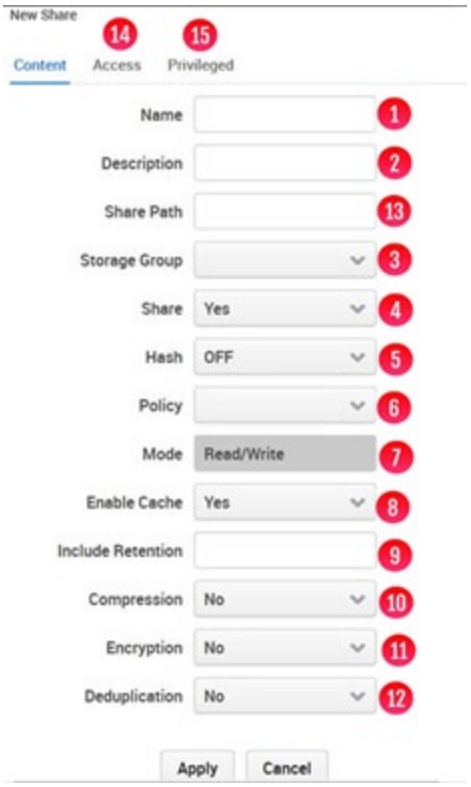


Figure 10.2L – Add Share (Linux)



Name – This will be the Share name. It must be a minimum of 3 characters and not more than 256 characters and may not use any special characters listed below (Figure 10.2W/L.1)

WARNING: In Windows, the name of the Share will be what users see as the exposed Share name on the network. Enter a valid Windows Name in the field (Figure 10.2W/L.1) and an optional description (Figure 10.2W/L.2).

The following are special characters cannot be used in a Windows share name:

* (asterisk)

< (less than)

> (greater than)

: (colon)

“ (double quote)

/ (forward slash)

\ (backslash)

| (vertical bar or pipe)

? (question mark)

The following share names are invalid:

CON, PRN, AUX, NUL, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8, and LPT9.

Description – optional text description for the Share (Figure 10.2W/L.2) (e.g., Image scans of Reseller agreements).

(Linux only) Share Path – Enter the NFS mount point, for this example, **sharepath**. The HCP Gateway will add "/archive" to the beginning of the path, for example "/archive/sharepath" (Figure 10.2L.13). The "/archive/sharepath" will be the NFS export for the share.

Storage Group – Select from the list of previously defined Storage Groups. (Figure 10.2W/L.3).

Share – the default option **Yes** sets a Share as accessible to users and applications. The alternative is **No** and this can be used when setting up the Share before publishing it or for maintenance reasons (Figure 10.2W/L.4).

Hash – content based cryptographic hashes are used to create a digital fingerprint for a file that the HCP Gateway can use to verify its integrity over time (Figure 10.2W/L.5). The options are MD-5 (128 bit), SHA-1 (160 bit) and SHA-256 (256 bit). The higher the bit count the less likely collisions exist.

Policy – a list of previously defined policies will be displayed on a pull-down list and one can be selected. If no policies have been created the list will be empty. If the policy field is left blank, the share will be in read/write Archive mode. Note multiple policies can be combined during the Policy configuration, but not here (Figure 10.2W/L.6). Refer to the HCP Gateway Policy chapter for more details.

Mode – the mode is automatically set based upon the policy, the options are Read/Write, Read-Only or a Policy type (Figure 10.2W/L.7).

Enable Cache – options are **Yes** or **No** (Figure 10.2W/L.8). This option is **not** available with a Server Mode Copy, Directory Copy or Combine policy because the Enable Cache setting is set to Yes automatically and cannot be changed. Setting this option to **Yes** (the default) will keep the files in the cache after writing them to HCP storage. It will also keep files in local cache after reading them from HCP storage. This provides faster read performance for future access. If the **Cache High Watermark** causes the file to be released from the cache, then when the file is read again, it will remain in the cache until the cache high watermark releases it from the cache again. Note that you must **Enable Watermarks** in the **Configuration -> General page** in order for this feature to work, so that when the cache capacity reaches the **High Watermark**, files will be released from the cache based on the **Watermark clear option** (see the **HCP Gateway Configuration** chapter Section 5 for the details). Setting this option to **No** will maintain the current behavior, where files will be released from the cache for a share in Archive mode and when the Tiering time is reached in a Server Mode Tiering Policy, after writing the file to the storage, and will leave a pointer to the file content on the share.

Include Retention – a list of **previously defined include retention policies** will be displayed, select the include retention policies you want to apply to this share (Figure 10.2W/L.9).

Compression – can be enabled or not. Compression works well with some content types, such as text and is not effective with other types (Figure 10.2W/L.10), such as zip files.

Encryption – to enable encryption, select the **Yes** option. HCP Gateway encrypts each file with a unique key. Keys need to be backed up, so configure the integrated backup in the Operations page or use a 3rd party backup tool to back up the database (Figure 10.2W/L.11).

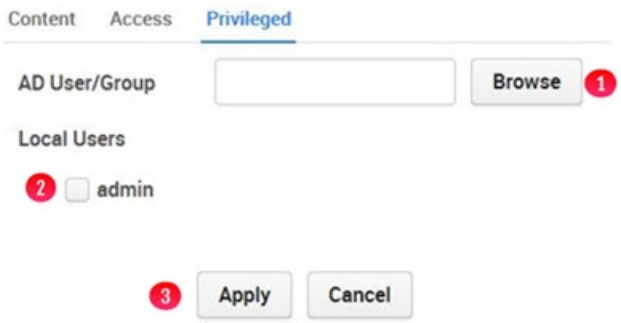
Deduplication – Deduplication is limited to the contents of a Share (Figure 10.2W/L.12). If deduplication is set to **Yes** then HCP Gateway will compare the hash of a newly ingested

file/object to existing files/objects to determine if the file/object exists. If the file/object exists then a pointer to the original file/object will be saved but not the content. Deduplication is done at a file/object level, and this is sometimes also referred to a single instancing. When you enable Deduplication, you will need to select a **Hash** option (Figure 10.2W/L.5).

> **Note:**
>
> When using Compression, Encryption and Deduplication together on a share, the order of operations on a file is Deduplication, Compression then Encryption. If a file with the same content is written to the share again, the Compression and Encryption operations will not run once the HCP Gateway determines the file is a duplicate.

Privileged – When logged into the HCP Gateway UI as an **admin** level user, select the **Privileged** (Figure 10.2W13/10.2.L.15) option to enable the users who will be able to use the **Privileged Delete** (see the **Administrator Privileged Delete** chapter for the details) and the **Delete File Copy off Local Storage** (see the **Delete File Copy off Local Storage** chapter for the details) features. If assigning an Active Directory user/group for the UI **Privileged Delete** permission, select **Browse** (Figure 10.3.1) to select the Active Directory User/Group that will be given the **Privileged Delete** permission, which also permits that User/Group to delete a file copy off local storage. If assigning local users for the UI **Privileged Delete** permission, select the local user(s) (Figure 10.3.2) that will be given the **Privileged Delete** permission, which also permits that user(s) to **Delete a File Copy Off Local Storage**. Select **Apply** (Figure 10.3.3) to save the settings.

Figure 10.3 – Enable Privileged Delete Permissions



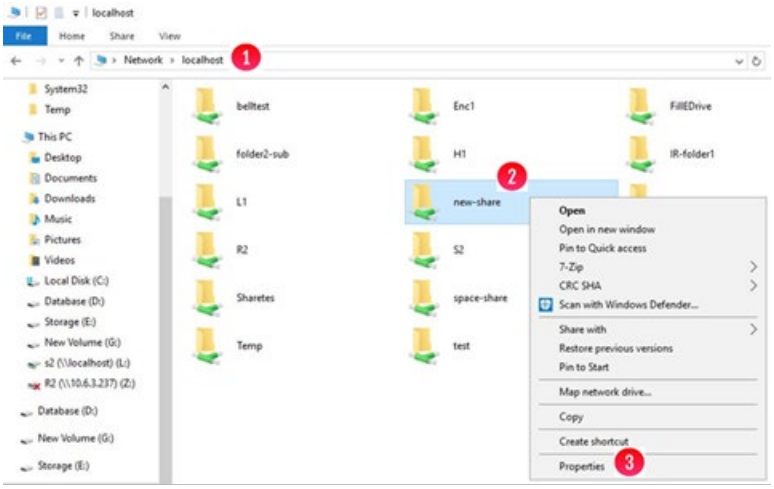
Once all the settings for the Share and Privileged have been entered, the **Apply** button (Figure 10.2W/L) must be selected to create the Share. Note that if any of the Storage devices in the Storage Group are not active, you will not be able to create the Share until all the Storage devices in the Storage Group are active.

WARNING: Do not use the Windows or Linux sharing to share any of the HCP Gateway shares. All configuration of the shares MUST be handled by the HCP Gateway UI. However, creating, editing, or deleting a Subshare inside an HCP Gateway share is performed in Windows File Explorer.

Windows: After creating the share in the HCP Gateway UI, configure the Share Access Permissions in Windows File Explorer. Refer to **Step 10** in the **HCP Gateway Software Upgrade** chapter for details on the **registry.shares** parameter. By default, Windows sets the

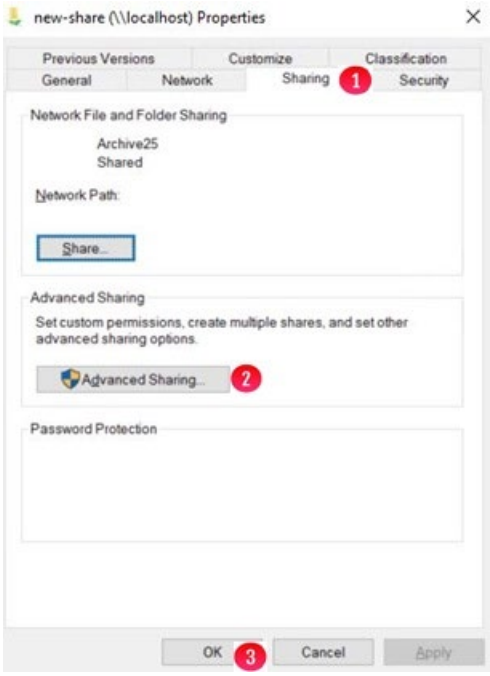
Share Access Permissions to Everyone - Full Control. To configure the Share Access Permissions, in Windows File Explorer on the HCP Gateway navigate to \\localhost (Figure 10.4W.1), right-click on the Share name (Figure 10.4W.2) and select **Properties** (Figure 10.4W.3).

Figure 10.4W – Windows Share Properties



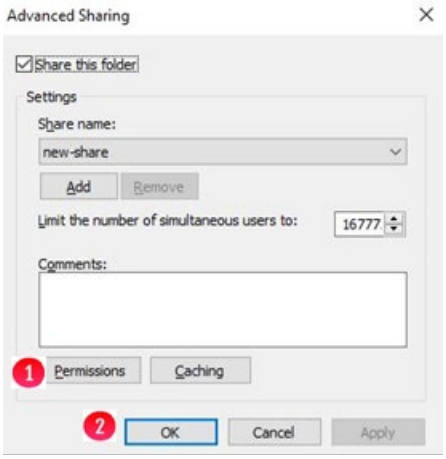
Select the **Sharing** tab (Figure 10.5W.1) and select **Advanced Sharing** (Figure 10.5W.2).

Figure 10.5W – Windows Share Properties



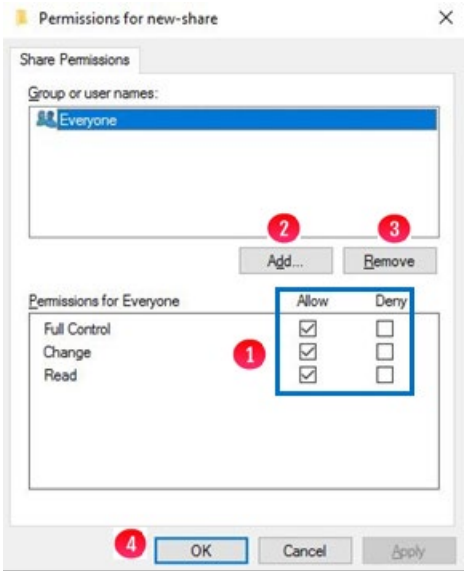
Select **Permissions** (Figure 10.6W.1).

Figure 10.6W – Windows Advanced Sharing



If necessary, edit the settings for Everyone (Figure 10.7W.1). Select **Add** (Figure 10.7W.2) to add permissions for other users or groups, select **Remove** (Figure 10.7W.3) to remove permissions for a user or group. Select **OK** (Figure 10.7W.4) to save the settings. Select **OK** (Figure 10.6W.2) to close the Advanced Sharing window. Select **OK** (Figure 10.5W.3) to close the share Properties window.

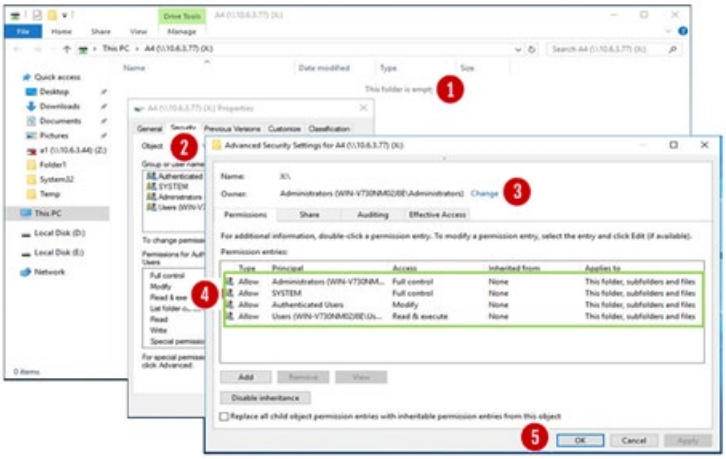
Figure 10.7W – Windows Share Permissions



Windows: After creating the share and setting the Share Access Permissions and before creating any folders or files in the share, set any additional Inheritable NTFS Permissions that are needed for the folders and files on the share. Make sure the inheritable permissions include the user that is configured in the sam.account parameter in C:\SAM\etc\sam\sam.properties and that the SAM VFS service is running as the same user. The default user is the local SYSTEM account. In Windows File Explorer, map a drive to the share and right-click in the white space (Figure 10.8W.1) and select **Properties**. In the Properties window, select **Security** (Figure 10.8W.2) then **Advanced**. If necessary, change the Owner (Figure 10.8W.3). If necessary, change the Permission entries (Figure 10.8W.4). Select OK (Figure 10.8W.5) to continue. Select **OK** in the Properties window to save the

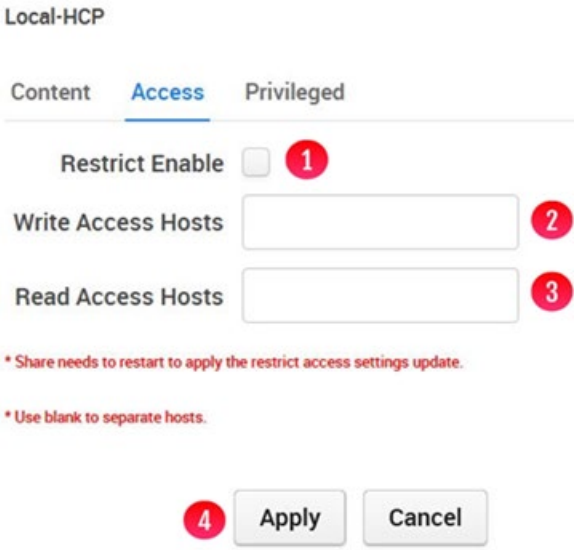
settings. Note that if there are already folders and files in the Share, this process may take some time to apply the new permissions to all the folders and files.

Figure 10.8W – Windows - Set NTFS Permissions



Linux: To restrict the access to the share, set the Share Access Permissions by selecting **Access** (Figure 10.2L.14). Select **Restrict Enable** (Figure 10.9L1). For hosts with Read and Write access to the share, enter the names of the hosts, separated by a space (Figure 10.9L.2). For hosts with Read Only access to the share, enter the names of the hosts, separated by a space (Figure 10.9L.3). Select **Apply** to save the changes (Figure 10.9L.4). Stop and restart the share for the access changes to take effect.

Figure 10.9L – Linux - Restrict Share Access Permissions



Linux: After creating the share, set any additional Linux Permissions that are needed for the folders and files on the share using the **chown** and/or **chmod** commands.

10.3 Modify a Share

The process to modify a share varies based on the type of policy being used by the share. In the Shares page in the HCP Gateway UI, select the name of the share. Generally, you can edit the **Description** (Figure 10.2W/L.2), **Share** (Figure 10.2W/L.4), **Hash** (Figure 10.2W/L.5), **Enable Cache** (Figure 10.2W.8), **Include/Exclude Retention** (Figure 10.2W/L.9), **Compression** (Figure 10.2W/L.10), **Encryption** (Figure 10.2W/L.11) and **Deduplication** (Figure 10.2W/L.12) fields. In addition, you can edit the Share Access permissions by selecting the **Access** (Figure 10.2L.14) (Linux only) or **Privileged** tabs (Figure 10.2W13/10.2.L.15).

10.4 Delete a Share

The process to delete a share varies based on if retention policy is being used or not. If no retention policy is used, complete steps 1 and 2, otherwise complete steps 1 and 3.

Step 1: Delete all the files and folders in the share

Step 2: If the Share is configured with a Server Mode Copy policy or in Archive Mode without a Retention policy the process is:

1. Go to the **Operations -> Delete on Storage** page in the UI
2. Turn the **Status** button to **On** for the share you want to delete
3. Select the **Settings** button for the share you want to delete
4. In the Deleted file versions section, select **"Delete all versions"**
5. In the File history record, select **"Remove all deleted files records"**
6. Select the **"Start Now"** button to run the **Delete on Storage** for the share you want to delete
7. Once the Delete on Storage finishes (you can check the **Events** page in the UI to check the completion status), then go to the Shares page, select the Share, and select the Delete button.

Step 3: If the Share is configured in Archive Mode with a Retention policy, there is one additional setting you need to enable in the Delete on Storage settings.

1. Go to the **Operations -> Delete** on Storage page in the UI
2. Turn the **Status** button to **On** for the share you want to delete
3. Select the **Settings** button for the share you want to delete
4. In the Deleted file versions section, select **"Delete all versions"**
5. In the Expired retention files section, select **"Delete"** (this is the additional setting when using a Retention policy)
6. In the File history record, select **"Remove all deleted files records"**
7. Select the **"Start Now"** button to run the **Delete on Storage** for the share you want to delete
8. Once the Delete on Storage finishes (you can check the **Events** page in the UI to check the completion status), you go to the Shares page, select the Share, and select the Delete button.
9. When the share is deleted, any reports that were configured are removed from the UI Reports page and Windows scheduler. However, any report output files will remain in the E:\Reports folder and will need to be manually deleted.

10.5 Rename a Share

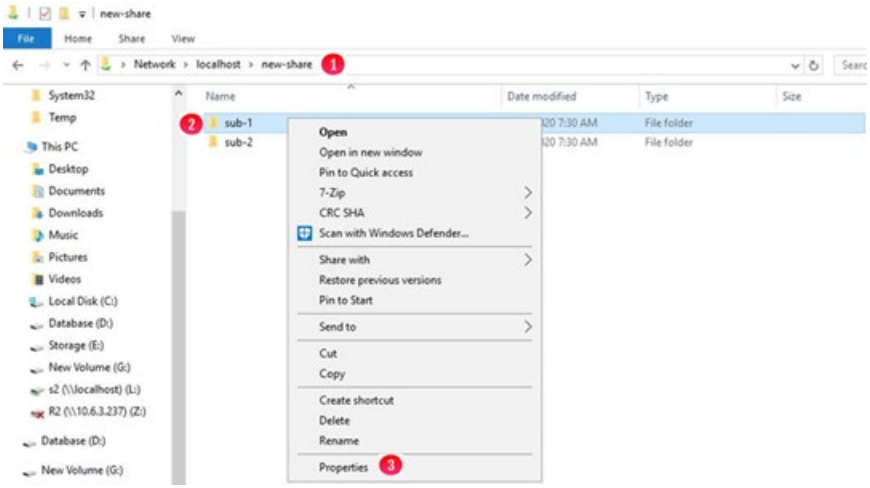
Contact Hitachi Vantara support if you want to rename a share in the HCP Gateway.

10.6 Add a Subshare (Windows only)

The HCP Gateway Subshare feature allows creating a share inside of an HCP Gateway share at any level of the share folder tree. This feature is currently only available in Windows.

To add a subshare when using an HCP Gateway with Microsoft Failover Cluster, refer to the **HCP Gateway Windows Cluster Setup Guide Chapter 14.** The **registry.shares** parameter needs to be in the **C:\SAM\etc\sam\sam.properties** file for the Subshare feature to operate. Refer to **Chapter 18 HCP Gateway Software Upgrade Chapter** Step 10 for details on this parameter. In Windows File Explorer on a standalone HCP Gateway, navigate to the HCP Gateway share, for this example **\\localhost\new-share** (Figure 10.10.1) then create a folder that will become the Subshare, for this example, sub-1 (Figure 10.10.2). Right-click on the Subshare folder (Figure 10.10.2) and select **Properties** (Figure 10.10.3).

Figure 10.10 - Create Subshare

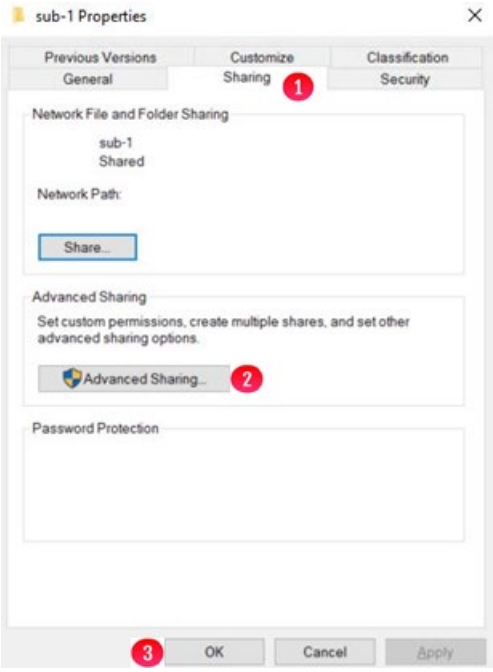


IMPORTANT NOTE:

It may take a few minutes after creating the Subshare folder before the Sharing tab is available. You can Refresh or close and open the Windows File Explorer that contains the Subshare folder to reduce the amount of time to wait to see the Sharing tab.

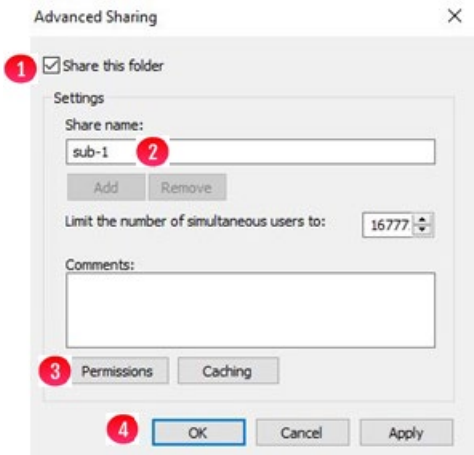
Select **Sharing** (Figure 10.11.1), then select **Advanced Sharing** (Figure 10.11.2).

Figure 10.11 - Share Subshare



Select **Share this folder** (Figure 10.12.1), if necessary, edit the **Share name** (Figure 10.12.2), select **Permissions** (Figure 10.12.3) to configure the Subshare Access Permissions. Select the Security tab in Figure 10.11 to configure the Inheritable NTFS Permissions. Follow the steps in the **Chapter 10 Section 2 Add / Configure a Share** section for configuring Share Access and Inheritable NTFS Permissions. Select **OK** (Figure 10.12.4) to save the Subshare settings. Select **Close** in the Subshare Properties window (Figure 10.11.3). Stop and restart the share in the HCP Gateway Shares page for the Subshare configuration to be saved in the Gateway database. Refer to Section **10.1 Shares Menu Page** for details on stopping and starting a share.

Figure 10.12 – Subshare Advanced Sharing



10.7 Edit a Subshare (Windows only)

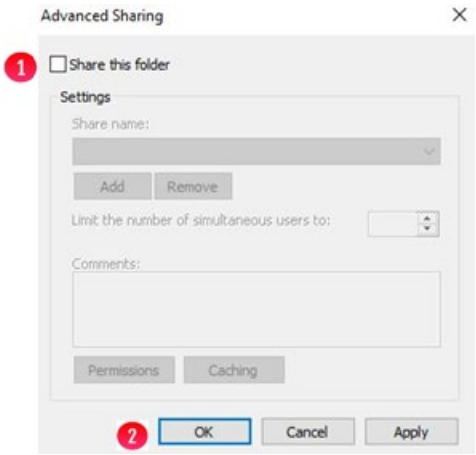
To edit a subshare when using an HCP Gateway with Microsoft Failover Cluster, refer to the **HCP Gateway Windows Cluster Setup Guide Chapter 14**. To edit a Subshare on a

standalone HCP Gateway, in Windows File Explorer, navigate to the HCP Gateway share, for this example **\\localhost\new-share** (Figure 10.10.1) then right-click on the Subshare folder (Figure 10.10.2) and select **Properties** (Figure 10.10.3). Select **Sharing** (Figure 10.11.1), select **Advanced Sharing** (Figure 10.11.2). Enable/Disable the Subshare (Figure 10.12.1), edit the **Share name** (Figure 10.12.2), select **Permissions** (Figure 10.12.3) to configure the Subshare Access Permissions. Select the Security tab in Figure 10.11 to configure the Inheritable NTFS Permissions. Follow the steps in the **Add / Configure a Share** section above for configuring Share Access and Inheritable NTFS Permissions. Select **OK** (Figure 10.12.4) to save the Subshare settings. Select **Close** in the Subshare Properties window. Stop and restart the share in the HCP Gateway Shares page for the Subshare configuration to be saved in the Gateway database. Refer to Section **10.1 Shares Menu Page** for details on stopping and starting a share.

10.8 Delete a Subshare (Windows only)

To delete a subshare when using an HCP Gateway with Microsoft Failover Cluster, refer to the **HCP Gateway Windows Cluster Setup Guide Chapter 14.** To delete a Subshare on a standalone HCP Gateway, in Windows File Explorer, navigate to the HCP Gateway share, for this example **\\localhost\new-share** (Figure 10.10.1) then right-click on the Subshare folder (Figure 10.10.2) and select **Properties** (Figure 10.10.3). Select **Sharing** (Figure 10.11.1), select **Advanced Sharing** (Figure 10.11.2). Unselect **Share this folder** (Figure 10.13.1), then select **OK** (Figure 10.13.2) to remove the Subshare. Select **Close** in the Subshare Properties window (Figure 10.11.3). Stop and restart the share in the HCP Gateway Shares page for the Subshare configuration to be saved in the Gateway database. Refer to Section **10.1 Shares Menu Page** for details on stopping and starting a share.

Figure 10.13 - Remove Subshare



HCP Gateway Policy

Policies can be applied to data when it is ingested into the share (e.g., set retention) or when data is at rest (e.g., legal hold). Policies are defined independent of a Share and can be applied to more than one Share. A Policy must be defined before it can be applied to any Share. Therefore, if data in a Share needs to be retained for 5 years, then a Policy must be configured with 5-year retention prior to creating the Share. If the Policy was applied to the Share after data had been ingested the existing data would not be retroactively subject to that 5-year Retention Policy. Only data ingested after the 5 Year Retention Policy is applied to the Share would be subject to Retention.

Policies fall into two categories: Server (NAS like mode) and Archive. Archive mode includes all Policies related to Compliance or Governance. Server mode covers all other Policy types. Unlike Archive mode, files in Server mode can be edited or deleted.

Policies cannot be deleted because they need to be kept around for auditing purposes and for files that still exist that were created with a policy.

You can disable a policy that you no longer need, but any files that were assigned the policy already need to have the policy information available.

Policies in **Archive** mode:

1. Retention
2. Include Retention
3. Exclude Retention
4. Legal Hold
5. Read Only
6. SnapLock

Policies for **Server** mode:

1. Combine
2. Copy
3. Directory Copy
4. Tiering
5. Exclude Tiering

11.1 Archive Mode and Retention Policies:

1. **Retention** – A Policy applied at a Share level that does not allow a user or administrator to delete or modify data until after a specified time has elapsed. The Retention Units can be defined in seconds, days, months or years, with the maximum of a 100-year retention period allowed. Associated with the Retention Period is a Grace Period. The Grace Period allows a predefined window of time after file is ingested prior to the setting of the Retention Policy. During the Grace Period a file can be modified or deleted by a user or administrator. Note that you can't use an Include Retention policy with a Share level Retention policy. When the retention expires on a file, the file will be left in read-only mode. The user can choose to change the file properties to read-write to modify the file.
2. **Include Retention** – A Policy to enforce Retention at a Directory or File level versus at Share level. This Policy enables different Retention periods to be set on one or more directories or files in a Share with the maximum of a 100-year retention period allowed. Note that you can't use an Include Retention policy with a Share level Retention policy.
3. **Exclude Retention** – A Policy applied to a directory in a Share where Retention has been applied at the Share level. The designated directory or directories would be

excluded from the Share Retention Policy. This Policy can be applied to files in addition to directories. Typically, this policy is used with content management systems that have temporary directories for work-in-process files or annotations. When you add the Share with a Share level Retention policy, you can select the Exclude Retention policy.

4. **Legal Hold** – A Policy applied to data at rest that does not allow a user or administrator to delete or modify data for the length of time the file is under the Legal Hold.
5. **Read-Only** – A Policy that is applied at a Share level (e.g., all files in the Share) that restricts user and administrator privileges to only enable reading of files. No files can be ingested, modified, or deleted. This is typically used for a Cold share or archive or for remote offices document distribution by the corporate office (e.g., policies, procedures, forms, etc.)
6. **SnapLock** – A Policy applied at a Share level that uses a per file meta data value to set the Retention Period of that file. If the “Access Time” file meta data value is set to a future time then HCP Gateway will place the file under Retention and not allow the file to be deleted or modified until after the Access Time date has been passed.

Syntax: The following syntax must be followed.

Directories use **“d:”** as a prefix (lowercase).

Files use **“f:”** as a prefix (lowercase).

File extensions use **“e:”** as a prefix and must begin with a ”.” (lowercase).

For multiple items use the “|” bar as a separator with no spaces added.

Characters “*” and “?” can be used as a wildcard in a filename or directory name.

VERY IMPORTANT: In Windows, use the backslash “\” character around folder names, in Linux use the forward slash “/” character around folder names.

Windows Directory Examples:

d:folder1 – select all files and folders in the directory folder1

d:Florida\|d:Alabama – select files and folders located in the directory named Florida or Alabama

d:New* – select files and folders located in directories that start with "New" like New Jersey, New York, etc.

d:\State\Colorado – select files and folders in the directory \State\Colorado that starts at the root of the share

Linux Directory Examples:

d:folder1/ – select all files and folders in the directory folder1

d:Florida/|d:Alabama/ – select files and folders located in the directory named Florida or Alabama

d:New*/ – select files and folders located in directories that start with "New" like New Jersey, New York, etc.

d:/State/Colorado/ – select files and folders in the directory /State/Colorado that starts at the root of the share

File Examples:

f:*.* – select all files and folders in the Share

f:filename.txt – select files named filename.txt

f:anno*.txt – select all files whose names that start with “anno” and end in “.txt”

Extension Examples:

e:.conf – select all files with a .conf extension

e:.temp|e:.mp3|e:.txt – select all files with .temp or .mp3 or .txt extension

Windows Combined Examples:

d:Florida\|f:*KatyPerry*.*|e:.mp3" – select all the files in the Florida folder that have KatyPerry in the name and have the extension .mp3

d:FolderA\|f:xyz*.*|e:.log – select all the files in Folder A that start with xyz in their name and have the extension .log

Linux Combined Examples:

d:Florida/|f:*KatyPerry*.*|e:.mp3" – select all the files in the Florida folder that have KatyPerry in the name and have the extension .mp3

d:FolderA/|f:xyz*.*|e:.log – select all the files in FolderA that start with xyz in their name and have the extension .log

Retention Policy Rules:

1. **Include Retention**
    a. The first character in the Include filter can only be lowercase. Uppercase characters are **not** allowed. Select the blue “i” icon for help.
    b. Asterisk ‘*’ character is allowed, but an include filter of “d:*\” does **not** protect the files in the ROOT directory. It does protect files in subdirectories.
    c. If you need to protect all files, including those in the ROOT directory, use the include filter “f:*.*”.
    d. Retention is applied on both the Gateway and HCP systems.
2. **Setting Retention and keeping a cache copy of files in addition to HCP Storage**
    a. Use Archive mode
    b. Create a Storage Group with 1 storage device, the HCP Namespace.
    c. Enable the **Cache Watermark**, set the **High** and **Low Watermarks**.
    d. When creating the share, set **Enable Cache** to **Yes** to keep a copy of the file in cache until it is released from cache by the **Cache High Watermark**.
    e. When creating the share, select the desired retention policy.
    f. Retention will be applied only on the objects on the HCP.
    g. Cached copy of file is useful for fast reads.
3. **Retention on a Subfolder**
    When retention is set on a subfolder (e.g. in Windows, retention is set on Colorado subfolder in the following path **“H:\abc\sales\usa\Colorado”** or Linux **/mnt/abc/sales/usa/Colorado**), the path before the subfolder becomes fixed and cannot be deleted, renamed or in any way modified.
4. **Legal Hold and Retention Scheduler**
    There is a scheduler in place that handles legal hold and retention. The scheduler runs every 10 minutes, so it can take up to 20 minutes before a legal hold is placed

or removed from a file or retention is set on a file on the HCP. This also impacts the **Grace Period** being used to set Retention on an object.

Below are some examples of using Archive Mode Policies:

Example 1: A Share called Keep was created and a One Year Retention Policy was applied at inception. Six months later the CIO informs the HCP Gateway Administrator that the data in the Keep Share needs to be placed on 3 Year retention. The HCP Gateway administrator creates a new Retention Policy called 3Year. They then go to the Policy menu and disable the One Year Retention Policy and then add the new 3Year Policy. All the existing files will retain the One Year Retention, but all new files will get the 3 Year Retention. Then if other Shares are using the One Year Retention Policy go back to the Policy menu and make it active.

Example 2: A Bank uses ApplicationXtender to manage documents. They need to retain the documents for 5 years. However, ApplicationXtender uses a folder called \anno to save the annotation file for the data file. Unfortunately, there is a single anno file for each data file, so the anno file needs to be able to change. The HCP Gateway Administrator sets up a Share called Documents and applies a 5 Year Retention Policy. They also set up a Policy to exclude retention on the \anno directory in the Document Share.

11.2 Server Mode Policies (all data remains Read/Write):

1. **Combine** – Sometimes more than one Policy is needed, and the "Combine Policy" is used to apply two or more Policies at one time. Just select the check boxes for desired Policies to the applied (Figure 11.1).

WARNING: Listed below are the restrictions when using a Combine policy.

- Users are **not** able to combine a Copy policy and an Include Retention policy.
- Users are **not** able to combine a Retention policy and a Snaplock policy.
- Users are **not** able to combine a Retention policy and an Include Retention policy.
- Users are **not** able to combine a Snaplock policy and an Include Retention policy.
- Users are **not** able to combine more than 1 Retention policy.
- Users are **not** able to combine more than 1 Snaplock policy.

Figure 11.1 – Combine Policy

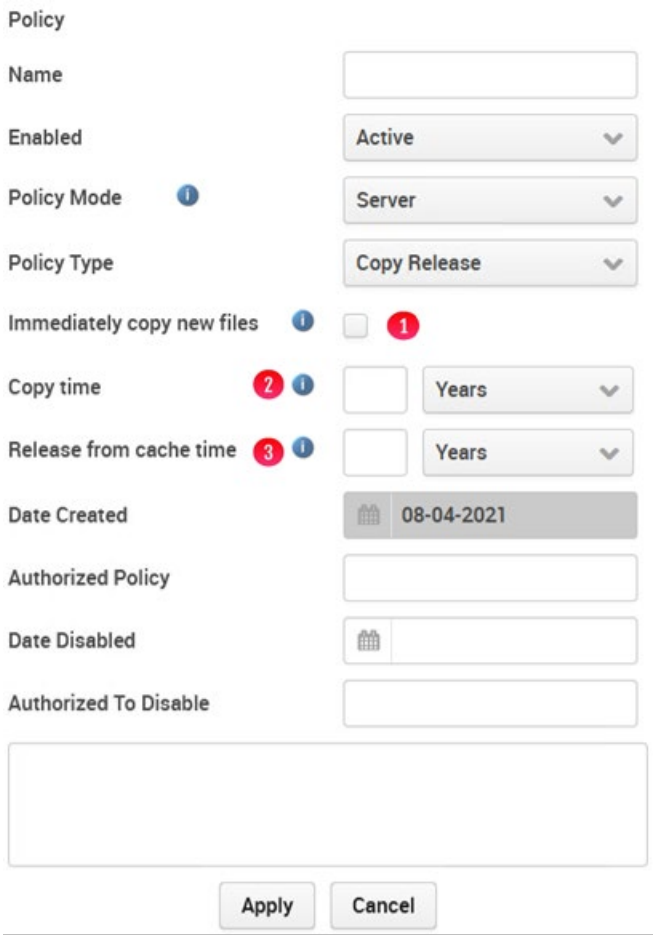
2. **Copy** – This Policy works at a Share level. It determines when a file is written to the storage location(s) defined in a Storage Group. The options are: immediate, seconds, minutes, hours, months, and years. The file is stored in cache until the time value is met, the file is then written to the storage device(s) and will remain in cache if the Cache Watermarks are enabled, until the **Cache High Watermark** is reached. When a file is read in a share and the file content is not in the cache, usually because the cache high watermark was reached which caused the file content to be

released from the cache, the file content will be restored to the file in the cache and the file content will remain in the cache until the **Cache High Watermark** is reached and releases the file content from the cache. The **Enable Cache** setting is not available in a Share when you select a Copy policy.

WARNING: Do **not** combine “Server Mode” policy and “Include Retention” policy. This is **not** supported.

3. **Copy Release (Cache Release)** – This Policy works at a Share level. It determines when a file is written to the storage location(s) defined in a Storage Group. The **Enable Cache** setting is not available in a Share when you select a Copy Release policy. The 'Release' action of the Copy Release Policy will only be applied if a file is new or modified. If a file is deleted before the file was saved to the Storage Group, the file is permanently deleted. The options are:
    - **Immediately copy new files** (Figure 11.2.1) will immediately copy a newly written file to the Storage Group.
    - **Copy time** (Figure 11.2.2) options are immediately, seconds, minutes, hours, days, months, and years. When a file is modified or the Immediately copy new files is not enabled, the file will be copied to the Storage Group when this time is reached, and the file will remain in cache until the Release from cache time is reached.
    - **Release from cache time** (Figure 11.2.3) options are immediately, seconds, minutes, hours, days, months, and years. The file is stored in cache until this time value is met (Figure 11.2.3). If the file is modified, the modified file is written to the Storage Group and will be released from the cache when this time value is met after the file was modified. When a file is read that is not in the cache, the file will remain in the cache, and if the Cache Watermarks are enabled, until the **Cache High Watermark** is reached. If the **Release from cache time** is less than the **Copy time**, the file will be released from cache shortly after it is written to storage.

Figure 11.2 – Copy Release (Cache Release) Policy



NOTE:

If the UI File Explorer is used to version a file before the release time is reached, then the file will remain in cache, and if the Cache Watermarks are enabled, until the Cache High Watermark is reached.

4. **Directory Copy** – This Policy is similar to Copy Policy in that it makes a copy at a specified time to the storage location(s) and the cache also behaves the same. However, it only works on specific directories or folders versus at the Share level like the Copy Policy.
5. **Tiering** – This is an aging Policy to keep a file in cache for fast retrieval. Upon reaching the time constraint in the Tiering policy, the files are copied to the storage location(s) specified in the Storage Group. If the **Enable Cache** setting is set to **Yes** on the share, the file will remain in the cache until it is released from cache by the **Cache High Watermark**. If the **Enable Cache** setting is set to **No** on the share, the file will be released from the cache after it is copied to the storage location(s) specified in the Storage Group. Note that prior to reaching the tiering date/time the data is **not** stored and protected in the storage location(s) specified in the Storage Group (for example the HCP system), there is just a single copy in the local cache on the Gateway. If the file is read and is not in cache, then if the **Enable Cache** setting is set to **Yes** on the share and the **Cache Watermarks** are enabled, the file will

remain in the cache until it is released from cache by the **Cache High Watermark**. Note that files under a Tiering policy are editable in place both before and after reaching the time constraint in the Tiering policy.

6. **Exclude Tiering** – The Exclude Tiering policy is combined with a Tiering policy in a Combine policy to exclude files from following the rules of the Tiering policy. Files under an Exclude Tiering policy will follow the rules of an Archive Mode policy without Retention where the file will be protected in the storage location(s) specified in the Storage Group (for example the HCP system), within a couple minutes of being written to the share. These files cannot be edited in place but can be overwritten.

Below are some examples of using a Server Mode Policy:

Example 1: A remote office wants to simplify their operations and replace Windows servers with HCP Gateway. A Share called Users is created and a Copy Policy is applied to this share. The result is data is written to the HCP Gateway cache for fast access. And the Copy Policy makes an immediate copy to a central HCP, thus effectively making a real time backup of the User data.

Example 2: The Sales team in the same remote office creates monthly deals that the Sales Reps can uses to close business that month. The Sales Manager wants fast access to the deals data which changes for a month. The HCP Gateway Administrator sets up a Share called Deals for the Sales Manager. He then applies a Tiering Policy that keeps the data only in local cache for 30 days and then writes a copy to HCP for long term storage. Then based on the Enable Cache setting for the share, the file will remain in cache (Enable Cache=Yes) or be released from cache (Enable Cache=No).

Example 3: The Central IT department is instructed by the CIO to keep all user web browsing logs for 30 days in cache for fast retrieval, but the HTML files are to be written to storage immediately since they will rarely be accessed. The HCP Gateway Administrator creates a Tiering policy for 30 days and creates an Exclude Tiering policy for all files with an ".html" extension. The Administrator then creates a Combine policy that includes the Tiering and Exclude Tiering policies. Then the Administrator creates a Share called Tracking with the Combine policy. The web browsing logs will remain only in local cache for 30 days and then the logs will be copied to the HCP. The HTML files will be immediately copied to the HCP. Then based on the Enable Cache setting for the share, the files will remain in cache (Enable Cache=Yes) or be released from cache (Enable Cache=No).

Example 4: The same remote office users want fast access to a project folder. IT knows from experience that most users do not look at files after 60 days. Use the Copy Policy to do two things. First, keep the files in local cache for fast access. Second, make an immediate copy of the files to HCP storage. Additionally, use the Cache Watermark setting to delete the older files from local cache over time.

WARNING: If using Copy or Tiering Policy that is not immediately writing the data to HCP, then the data is only on local cache disk on the Gateway and not protected from system failures.

11.3 Policy Menu Page

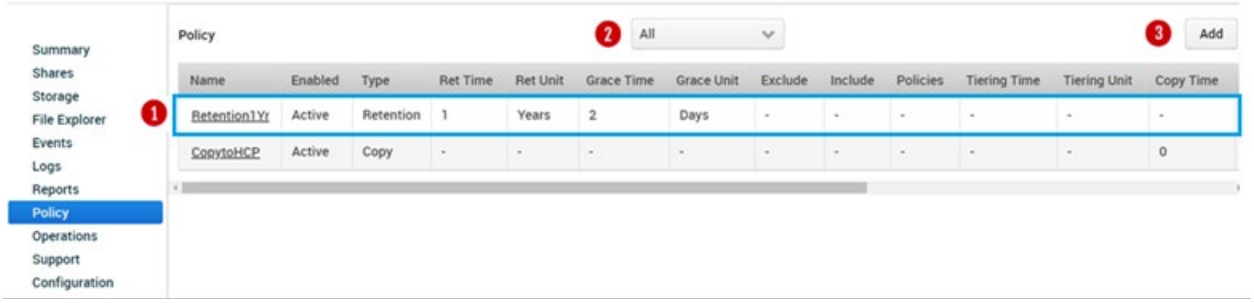
The Policy menu page provides a list of all existing Policies (Figure 11.3). The details of each Policy are listed in a row (Figure 11.3.1). The Policy is applied to a Share can be changed as needed. However, a Policy set on a Share cannot be deleted. Optionally a new Policy can be applied, and it will only impact data after it was applied.

Example: 2 Year Retention Policy applied to Share ABC. After 6 months 2 Year Retention Policy is removed from Share ABC so data can be R/W. Existing data will continue to be under retention for remaining time. Eighteen months for data written in the first day the Policy

was set and 2 years for data written in minutes before Policy was removed. If another Policy called 90-day retention is applied to Share ABC then new data will only be under retention for 90 days but all existing data will be under retention until two years from the file create date.

In cases where there are many Policies the “All” button can be selected (Figure 11.3.2) and the displayed Policies can be narrowed down by selecting a Policy Type (e.g., Legal Hold) from the pull-down menu.

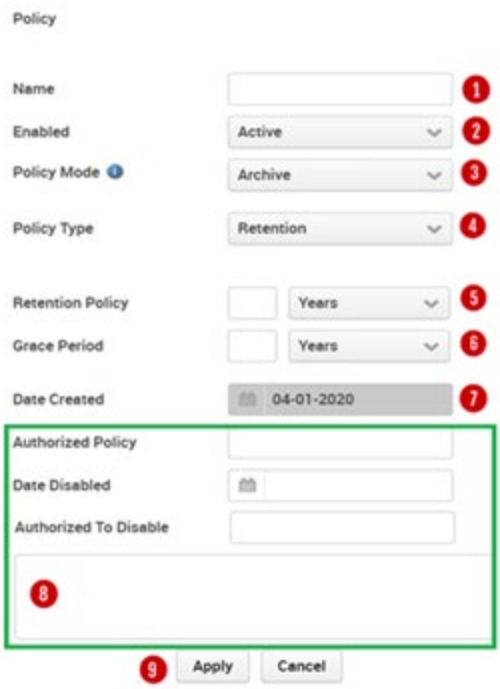
Figure 11.3 – Policy Menu



11.4 Add Policy

To Add or create a new Policy select the **Add** button (Figure 11.3.3). Then the Policy form to be filled out appears as a pop-up window (Figure 11.4). Form items number 1-6 are mandatory, however the items in the green box (Figure 11.4) are optional. Each Policy Type requires specific information for it to be configured, thus the selection from the pull-down menu (Figure 11.4.4) will determine the items in the green box. In this example the items in the green box are optional for a Retention Policy. After filling out the Policy form select the **Apply** button (Figure 11.4.9) to save. If you leave this page without selecting Apply the information entered will not be saved in the form for future use.

Figure 11.4 - Add Policy



Name – Every policy must have a unique name (Figure 11.4.1) consisting of a minimum of 3 alpha numeric characters and less than 255 alpha numeric characters. Do not use special characters or emoji.

Enabled – The default setting for a Policy is “Active.” To disable a Policy after creation, select “Disable” from the pull-down menu (Figure 11.4.2).

Policy Mode – Either Server or Archive (Figure 11.4.3).

Policy Type – The default Policy Type in Archive Mode is “Retention” as seen in (Figure 11.4.4). Additional Policy Types are listed in the pull-down menu and can be selected by highlighting them. Each Policy Type will result in different items being listed (Figures 11.4. 5-8).

Retention Policy – The units of time available for setting a Retention Policy are Years, Months, Days, Hours, Minutes, and seconds (Figure 11.4.5). The default setting is “Years.” The other options are available via the pull-down menu. Note only integers may be entered, other values are invalid.

Grace Period – The units of time from when a file is ingested and can be modified or deleted by a user or administrator prior to being subject to the Retention Policy. An integer value must be entered (Figure 11.4.6).

Date Created – The Date the administrator created the Policy (Figure 11.4.7).

Authorized Policy – Optional field to capture the name of the person authorizing the disabling of the Policy.

Date Disabled – The Date the administrator elected to disable the Policy.

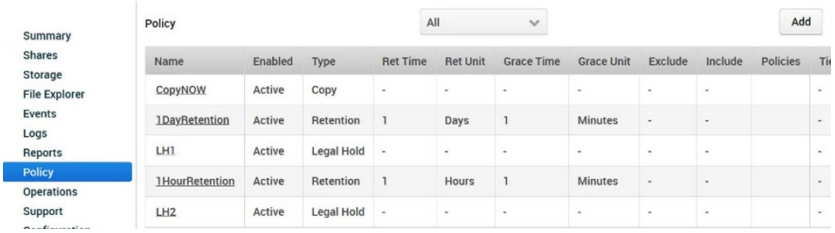
Authorized to Disable – Optional field to capture the name of the person authorizing the disabling of the Policy.

Note Box – Optional field to enter comments and save (Figure 11.4.8) for future reference.

11.5 Update Policy

To update a Policy, select the Policy Name (Figure 11.5).

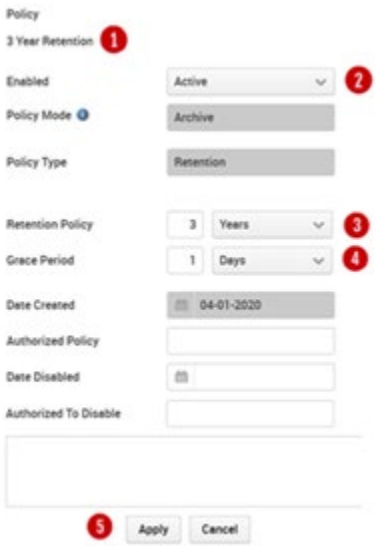
Figure 11.5 – Update Policy



Name	Enabled	Type	Ret Time	Ret Unit	Grace Time	Grace Unit	Exclude	Include	Policies	Ti
CopyNOW	Active	Copy	-	-	-	-	-	-		-
1DayRetention	Active	Retention	1	Days	1	Minutes	-	-		-
LH1	Active	Legal Hold	-	-	-	-	-	-		-
1HourRetention	Active	Retention	1	Hours	1	Minutes	-	-		-
LH2	Active	Legal Hold	-	-	-	-	-	-		-

This will pull up the Policy form with the existing data in the fields (Figure 11.6). The selected Policy is identified by the Policy name (Figure 11.6.1). The Name and Policy Type fields are NOT editable. An “Active” Policy (Figure 11.6.2) can be “Disabled” by using the pull-down menu and selecting the “Disabled” option, then eventually selecting the **Apply** button (Figure 11.6.5). The Retention Policy can be extended but NOT SHORTENED (Figure 11.6.3). The Grace Period can be extended or shortened (Figure 11.6.4). The Date Created will be updated by HCP Gateway to the current date. All the text fields can be updated. The Date Disabled should only be updated if the choice is to stop using the Policy. If you change a policy, the existing files retain the old policy settings, all new files added to the Share will have the updated policy settings.

Figure 11.6 – Update Policy



WARNING: Policies may be applied to more than one Share. Disabling or Updating a Policy will impact all Shares using the Policy.

HCP Gateway File Explorer

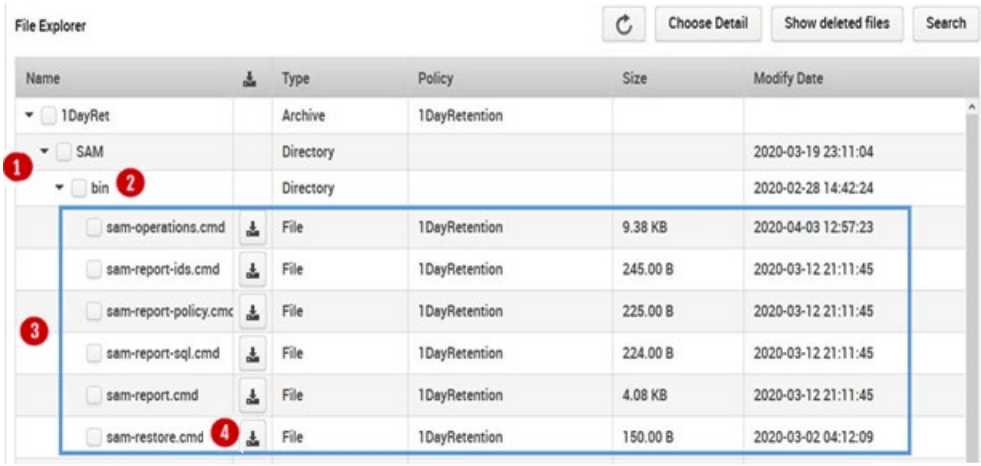
The File Explorer allows authorized users, auditors, or administrators to search or manually explore the contents of a Share, apply or remove Legal Hold Policies, version or download files when allowed by file level permissions, privileged delete files under retention, delete file copies from local storage and copy files from storage to cache.

Each Share is listed under the Name column (Figure 12.1.1) in a row. The download icon (Figure 12.1.2) can be used to download a file, it does not work at the share or folder levels. The Share (Figure 12.1.3) type is either Server or Archive. If any Policies are applied at a Share level, they are listed in the Policy column (Figure 12.1.4). Values in the Size column (Figure 12.1.5) are only displayed at a file level. The Modify Date (Figure 12.1.6) applies to Folders and Files inside the Share. The Refresh (Figure 12.1.7) is used to refresh the File Explorer page. The **Choose Detail** (Figure 12.1.8) will be covered in section 12.1. The **Show deleted files** (Figure 12.1.9) button enables files that were deleted to be displayed in File Explorer or not. This topic will be covered in the Chapter **"Recover Previous Versions and Deleted Files"**. The **Search** option (Figure 12.1.10) is just what you think it is and will be covered in section 12.3 below.

Figure 12.1 - File Explorer Menu

To drill down into a Share, click on the triangle (Figure 12.2.1) to the left of the Share and folder names. In the example below the Share named **1DayRet** has a folder named **SAM**. Drilling down into the SAM folder reveals a **bin** folder (Figure 12.2.2) which contains 6 files and their attributes (Figure 12.2.3). To download a file, click on the download icon (Figure 12.2.4). Note you must be authorized to read the file to download it.

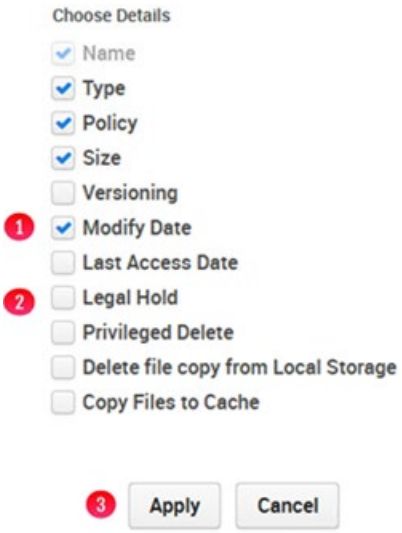
Figure 12.2 - Drilling Down



12.1 Chose Details

The **Choose Details** menu button (12.1.8) will bring up the columns that will be displayed in the File Explorer. The default is all items are displayed except Versioning, Last Access Date, Legal Hold, Privileged Delete, Delete file copy from Local Storage and Copy Files to Cache. Name is mandatory, all others are optional. To remove an item from the file Explorer display, uncheck the box (Figure 12.3.1) by the item to disable that selection in the UI File Explorer. To add an item that is not already selected, select the box (Figure 12.3.2) to enable that item in the UI File Explorer, then select **Apply** (Figure 12.3.3) to enable the selected settings. Note that you need to make these selections every time you open File Explorer.

Figure 12.3 – Choose Detail

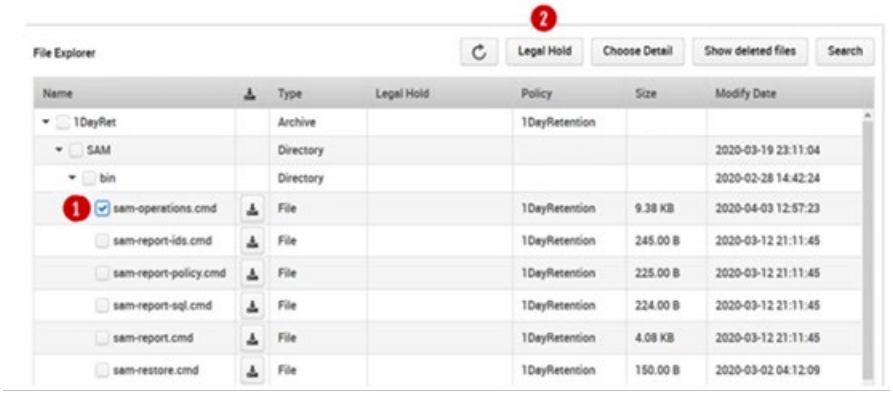


12.2 Legal Hold Policy

If any Policies have been applied to a Share, they will be displayed in the Policy column (Figure 12.1.4). To view or configure a Legal Hold, select the **Legal Hold** box in the **Choose Details** (Figure 12.3.2) menu and select **Apply** (Figure 12.3.3). A Hold Policy is applied to a share, folder(s), or file(s). To apply a Legal Hold Policy the Admin must expand the Share down to the folder or files or use the search feature. Note that Legal Hold Policies must be created using the Policy menu option before they can be applied to files.

To select a share, folder(s), or file(s) to apply a Legal Hold Policy select the box in front of the name (Figure 12.4.1). This will highlight the box blue and add a checkbox. Now that a file has been selected, select **Legal Hold** (Figure 12.4.2).

Figure 12.4 – Legal Hold Policy

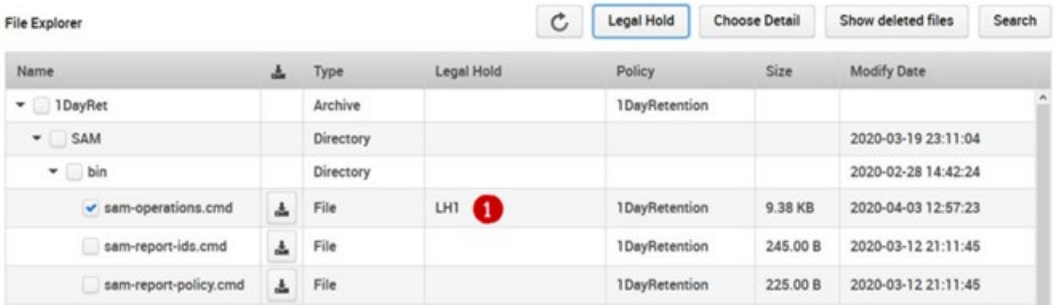


A pop-up box will appear on the top of the screen (Figure 12.5.1). Select the down arrow and a list of Legal Hold Policies will be displayed (Figure 12.5.2). Select a Legal Hold Policy to select it and notice that it is displayed in the **Policy** field (Figure 12.5.3). Finally, select **Apply** (Figure 12.5.4) to set the file on the Legal Hold. The process to apply a Legal Hold runs on a schedule, so it may take up to 20 minutes before the Legal Hold is applied on the file on the HCP storage.

Figure 12.5 - Applying Hold Policy to a file

After selecting the Apply button the UI is updated and the **LH1** Policy (Figure 12.6.1) is now applied to the file.

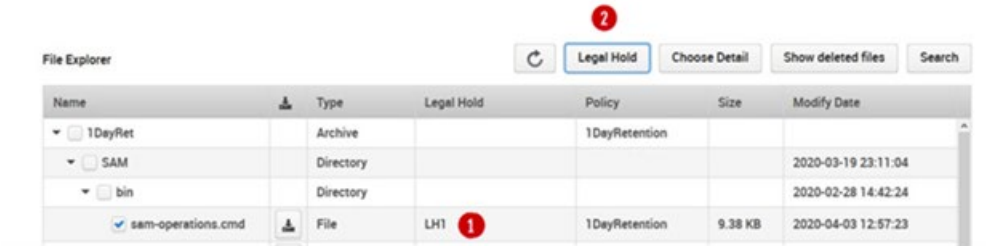
Figure 12.6 – Legal Hold Policy Applied



The process to remove a Legal Hold Policy is very similar to the process of applying the Legal Hold. To remove a Legal Hold, select the **Legal Hold** box (Figure 12.3.2) in the **Choose Details** (Figure 12.3) menu and select **Apply** (Figure 12.3.3).

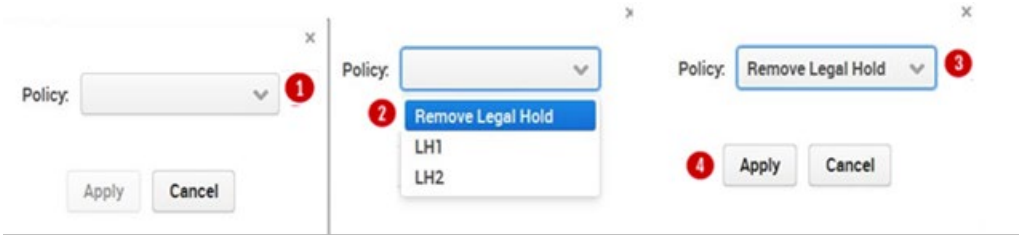
To select a share, folder(s), or file(s) to remove from a Legal Hold Policy select the box in front of the name (Figure 12.7.1). This will highlight the box blue and add a checkbox. Now that a file has been selected, select **Legal Hold** (Figure 12.7.2).

Figure 12.7 – Remove Legal Hold 1



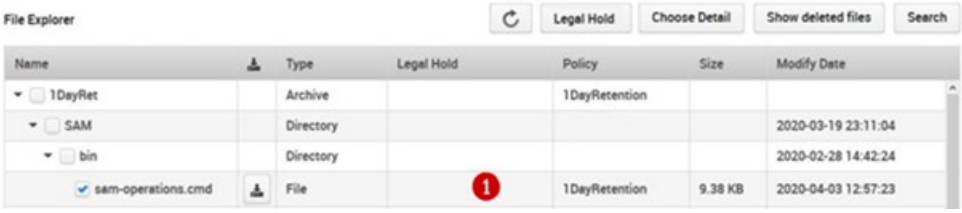
A pop-up box will appear on the top of the screen (Figure 12.8.1). Select the down arrow and a list of Legal Hold Policies will be displayed (Figure 12.8.2). Select the **Remove Legal Hold** Policy and notice that it is displayed in the **Policy** field (Figure 12.8.3). Finally, select **Apply** (Figure 12.8.4) to set the Legal Hold on the file. The process to remove a Legal Hold runs on a schedule, so it may take up to 20 minutes before the Legal Hold is removed from the file on the HCP storage.

Figure 12.8 - Removing Hold Policy to a file



After selecting the Apply button the UI is updated and the **LH1** Policy (Figure 12.9.1) is now removed from the file.

Figure 12.9 – Legal Hold Policy Removed



12.3 Search

To enable the Search functionality, select **Search** (Figure 12.10.1) from the File Explorer menu. Search is performed at a Share level, not a system level. Therefore, the first task is to select the Share menu (Figure 12.11.1), then select the Share to search from the list displayed in the pull-down menu (Figure 12.11.2).

Figure 12.10 – Search

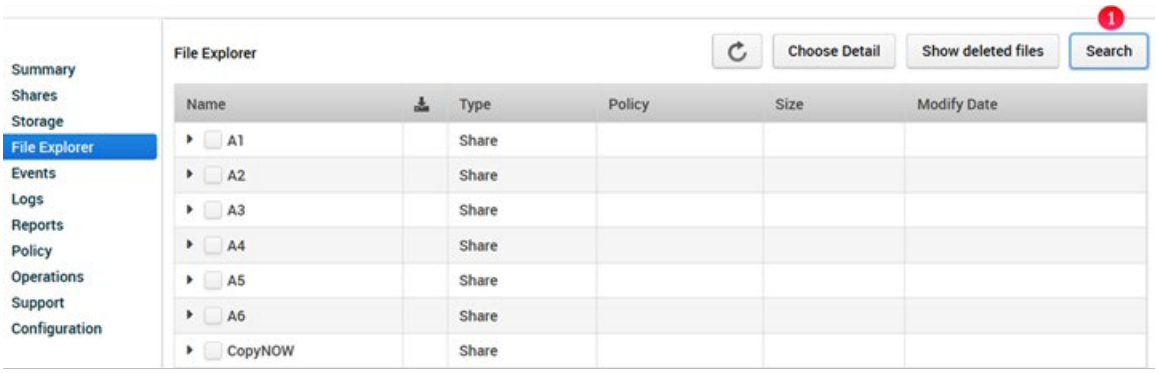
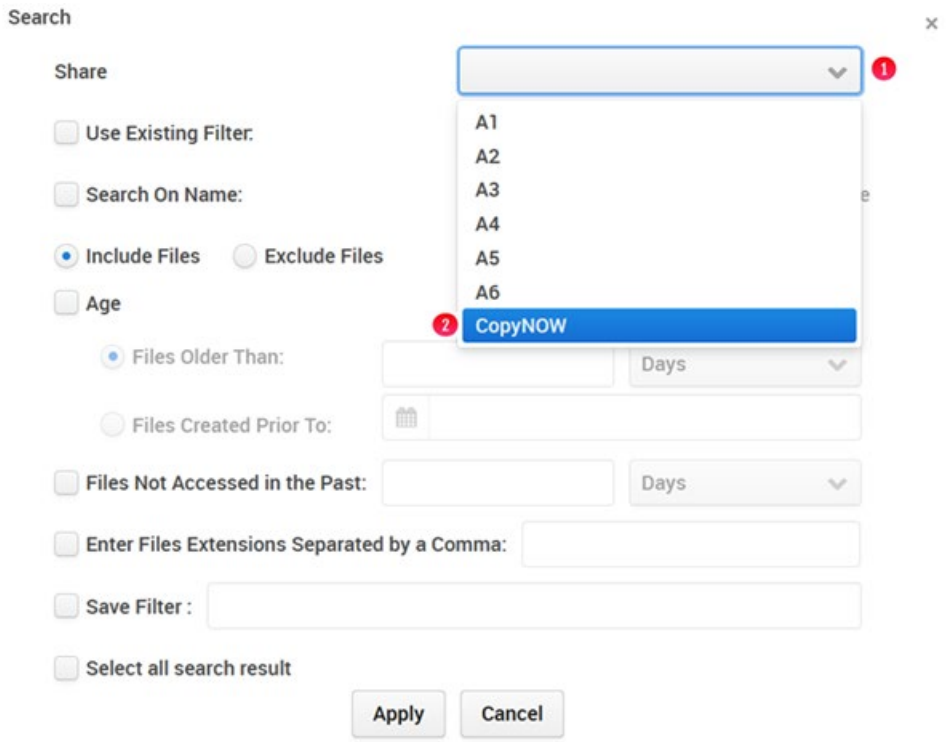
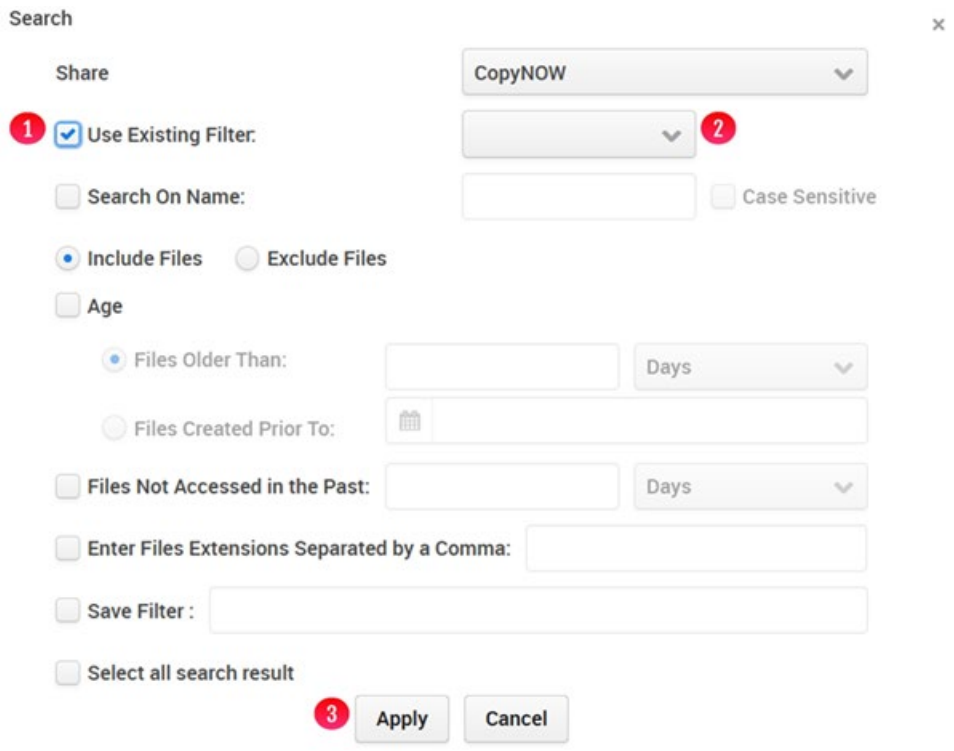


Figure 12.11 – Search Share



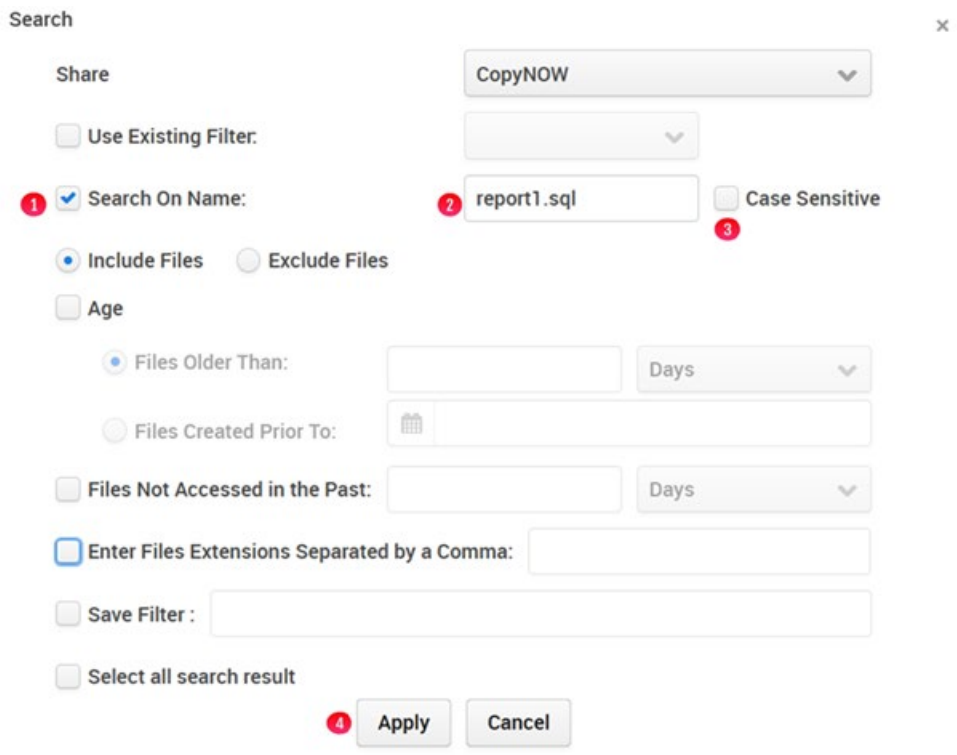
If you plan to run a Search with the HCP Gateway settings multiple times it may be time efficient to save the Search parameters, also called a Filter. If you have previously saved a Filter, it can be selected by checking the box called **Use Existing Filter** (Figure 12.12.1), selecting the appropriate filter name from the pull-down menu (Figure 12.12.2), then select **Apply** (Figure 12.12.3).

Figure 12.12 – Search Filters



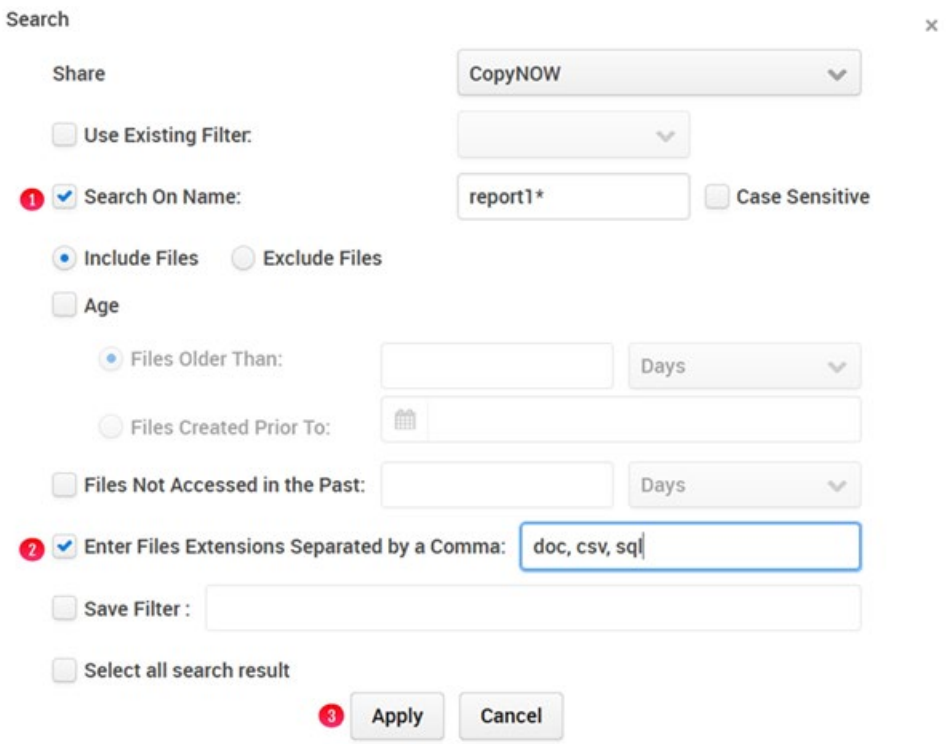
Alternatively, a Search for a known file can be run by selecting the **Search on Name** box (12.13.1) and then entering the file name in the data entry box (Figure 12.13.2). If the Share supports NFS access (Linux only) and you know the “case”, the **Case Sensitive** box (Figure 12.13.3) can be selected. Note CIFS or Windows Shares are not case sensitive so selecting this option will not matter. Finally select **Apply** (Figure 12.13.4) to start the search.

Figure 12.13 – Search for a Known File Name



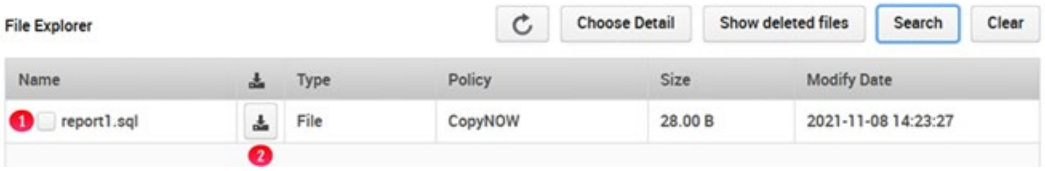
In the first example the file name of report1.sql was known. However, sometimes the type of file is not known. Was the report a Word document or a csv file? By selecting the **Search on Name** (Figure 12.14.1), enter a name with an "*" and without an extension (e.g., report1*) in the data entry box (Figure 12.14.1) then skip down and enter several file extensions (e.g., .doc, csv, sql) in the data entry box (Figure 12.14.2). In this example we were not sure if the file name was report1.sql or report1.doc or report1.csv so we entered the three extensions. Select **Apply** (Figure 12.14.3) to start the search. Note the extensions can be entered with or without the period, so "sql" or ".sql" would have been acceptable.

Figure 12.14 – Search for File Name with Unknown Extension/Type



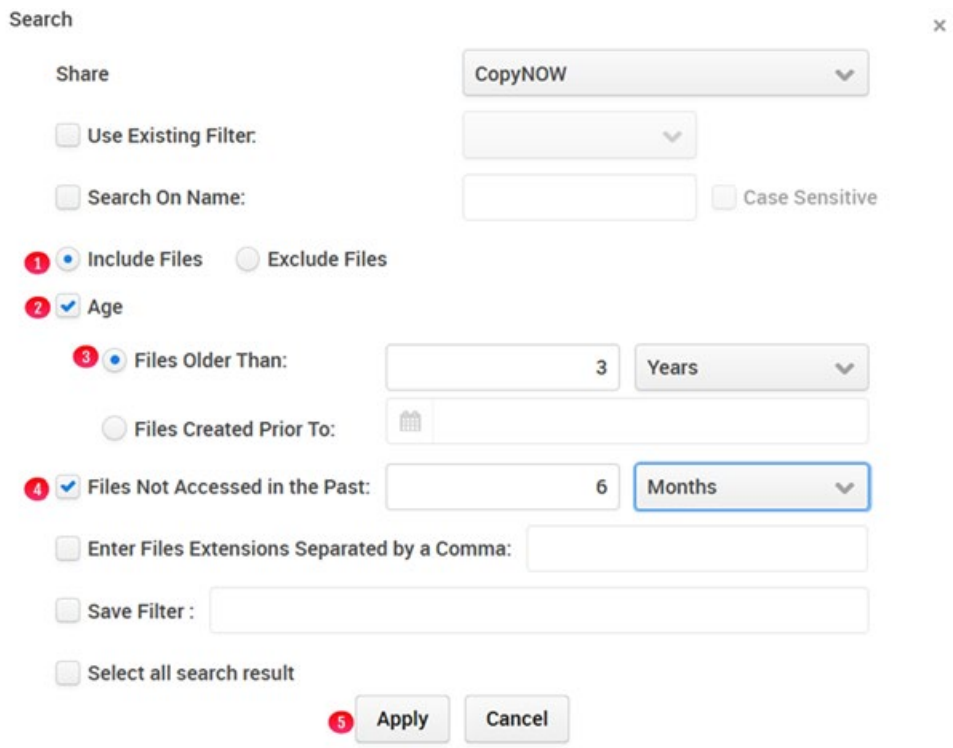
In this example the Search results provided us with a single file named report1.sql (Figure 12.15.1). If the user/admin/auditor running the Search has permissions they could download the file by selecting the box after the file name (Figure 12.15.1) and then selecting the download icon (Figure 12.15.2).

Figure 12.15 – Search for File Name with Unknown Extension/Type



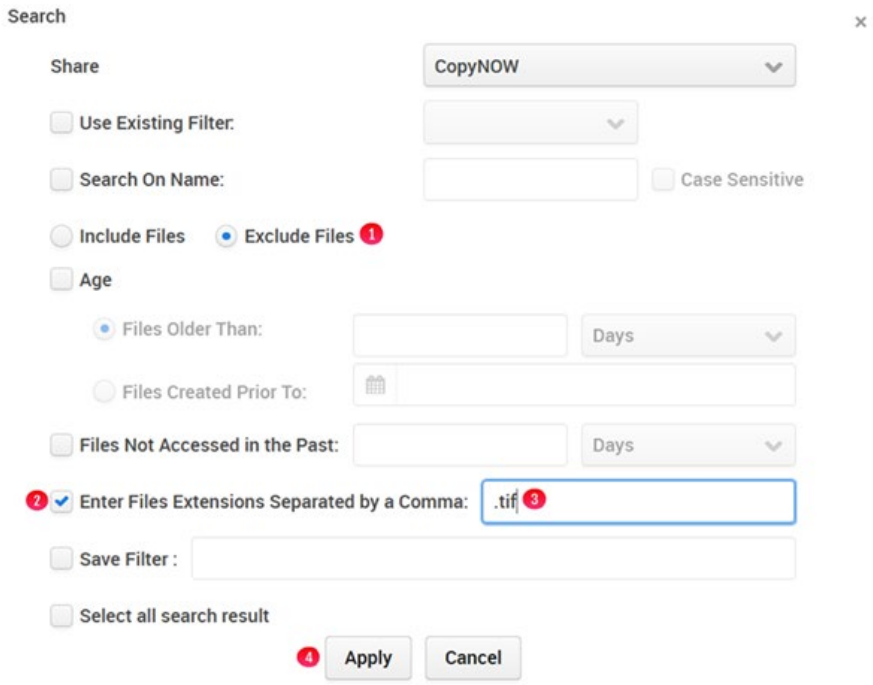
In the previous examples the Search criteria was simple. HCP Gateway has the ability to do compound or complex searches. What if you want to find a list of files (Figure 12.16.1) that are 3 years or older (Figure 12.16.2 and 12.16.3) AND have not been accessed in the past 6 months (Figure 12.16.4), then select **Apply** (12.16.5).

Figure 12.16 – Compound Search



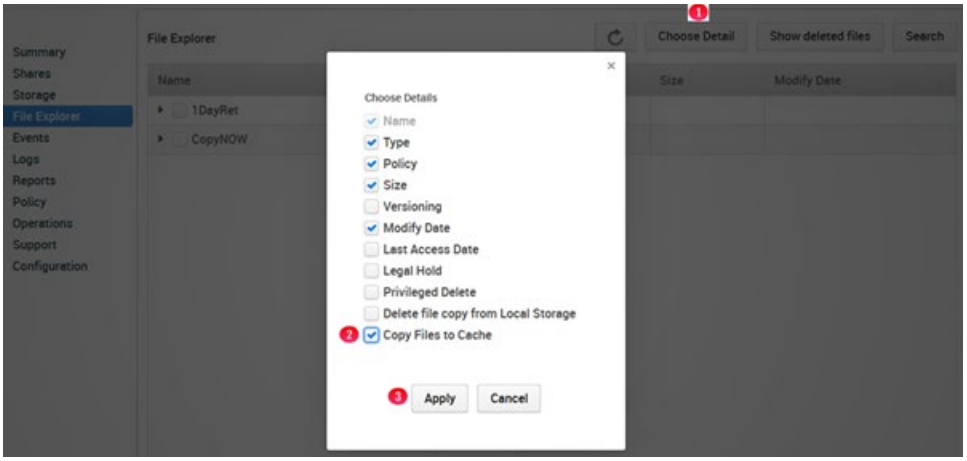
Searches can also be exclusive. Suppose you want a list of all files but you do not want (Figure 12.17.1) to include TIFF files (Figure 12.17.2 and 12.17.3)? Select **Apply** (Figure 12.17.4) to make this selection.

Figure 12.17 – Exclude Files from Search



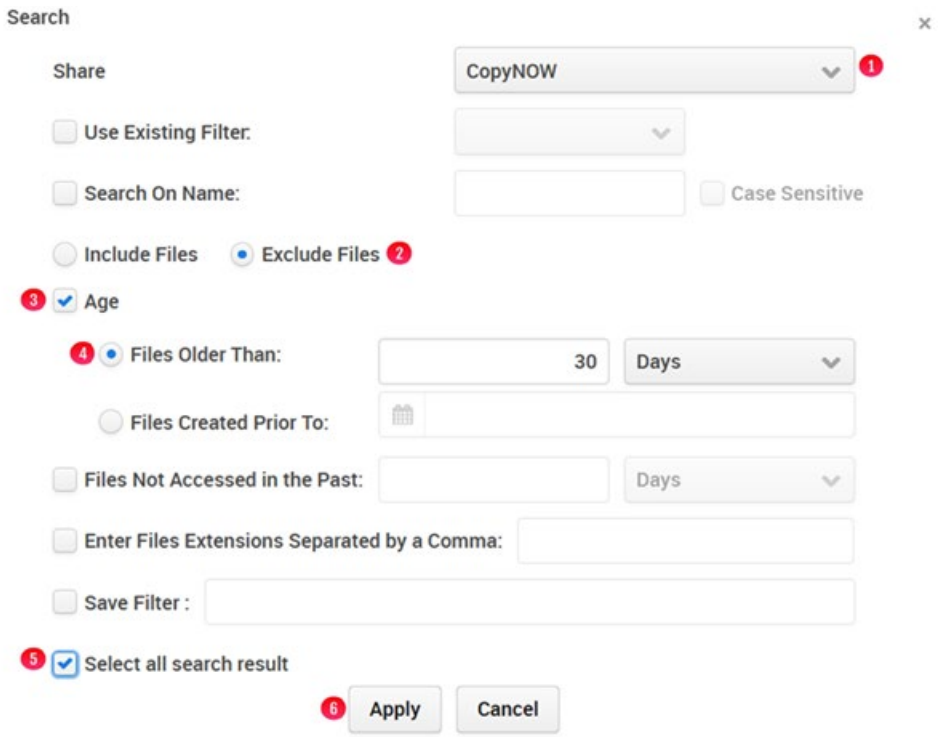
Finally, what happens if files were released from the HCP Gateway cache by the cache high watermark and you want to be sure that all files modified in the last 30 days are still in the cache? In the UI File Explorer, select Choose Detail (Figure 12.18.1), then select **Copy Files to Cache** (Figure 12.18.2), then select **Apply** (Figure 12.18.3).

Figure 12.18 – Select Choose Detail then select Copy Files to Cache



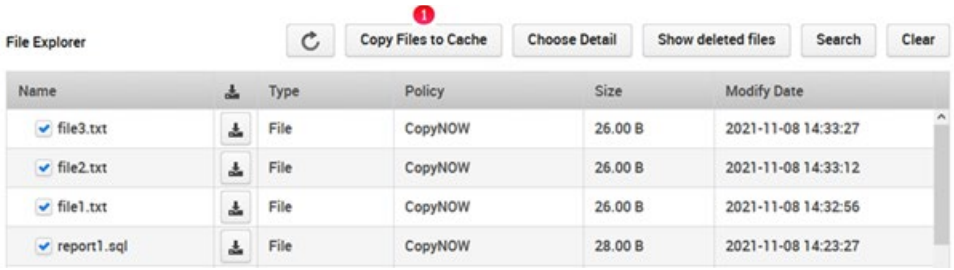
Next, select **Search** (Figure 12.10.1), select the Share (Figure 12.19.1), then select **Exclude Files** (Figure 12.9.2), then select all files by **Age** (Figure 12.19.3) older than 30 days (Figure 12.19.4). These files can be automatically selected by the **Select all search result** (Figure 12.19.5), then select **Apply** (Figure 12.19.6) to generate the list of files.

Figure 12.19 – Select files to Copy to Cache



Select **Copy Files to Cache** (Figure 12.20.1).

Figure 12.20 – Copy Files to Cache



Confirm whether to **Copy Files to Cache** (Figure 12.21.1).

Figure 12.21 – Confirm Copy Files to Cache

HCP Gateway Logs

The Logs page (Figure 13.1) from the main menu is used to view various log files associated with the HCP Gateway application. Under normal circumstances a user or administrator should never need to access any of the log files. These are primarily generated so Hitachi Vantara can review the state of the HCP Gateway processes and provide Support.

NOTE:

The HCP Gateway also logs Operational, Warning and Error events in the Microsoft Windows Event Viewer Application logs.

HCP Gateway has the following logs:

1. **GUI** (Wildfly application) – Log records for the HCP Gateway UI web interface events and activity

   In Windows - **C:\opt\wildfly-18.0.1.Final\standalone\log**

In Linux - **/opt/wildfly/standalone/log**

Audit - log records for access and authentication events for the Wildfly management interface.

Server - log records for all hosted application events on the Wildfly server

Service - log records for the Wildfly Windows Service event

wildfly-stdout - log records for all console messages related to wildfly, i.e., output one would expect to see if the service was run from a command window

2. **Database** – **Maria DB**

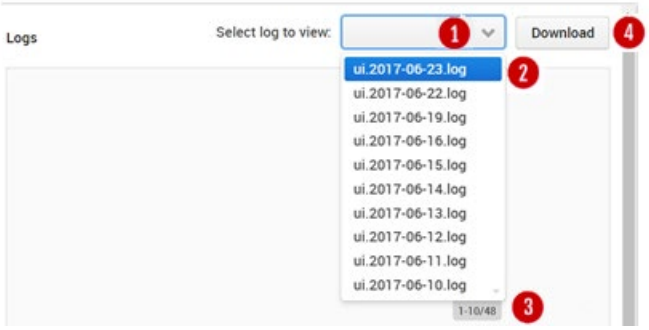
   In Windows - **D:\MariaDB\data*.err**

   In Linux - **/var/log/mysql/*.err**

   Error file - log records for all events related to the operation of the database engine

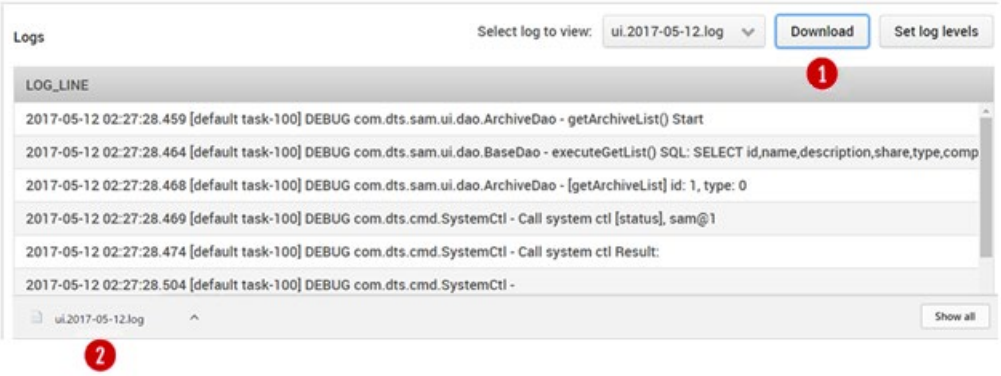
3. **HCP Gateway Application**
   In Windows - **C:\SAM\var\log**
   In Linux - **/var/log/sam**
   log-n.txt - Where n = index to the share in the database. Log records of all activity for share <n>.
   To view a specific log, use the pull-down box for **Select log to view** (Figure 13.1.1) and select the desired log (Figure 13.1.2). Note logs are ordered with the most recent at the top. The total number of Logs is visible in (Figure 13.1.3). Logs can be downloaded to a zip file for sending to Support by selecting the **Download** button (Figure 13.1.4).

Figure 13.1 – Logs



Use the **Download** button (Figure 13.2.1) to generate a log file (Figure 13.2.2).

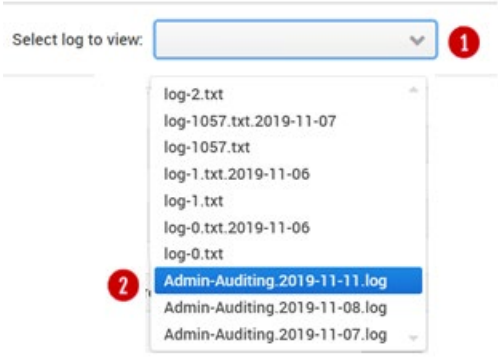
Figure 13.2 Download Logs



Administrative Audit Logs

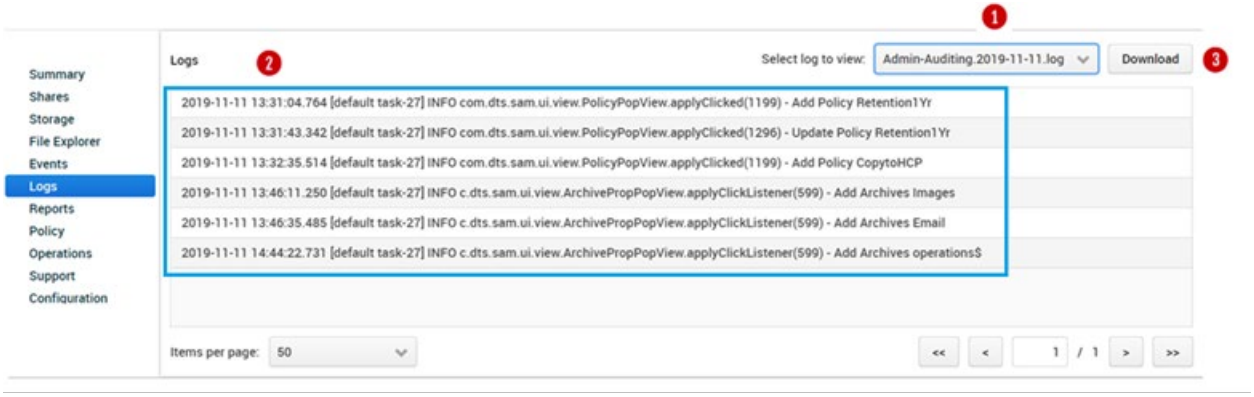
All Administrator actions are logged and available to be viewed or downloaded. Select the **down arrow** (Figure 13.3.1) from the **Select Log to View** box. A list of available logs will be displayed. Scroll down the list until logs named “Admin-Auditing” are displayed. They will be organized by date. Select the desired date (Figure 13.3.2).

Figure 13.3 Administrator Audit Logs



The selected log label will then be displayed in the **Select Log to View** box (Figure 13.4.1). The body of the page will then display the log of the Administrator for that day (Figure 13.4.2). This log can be downloaded by selecting the **Download** button (Figure 13.4.3).

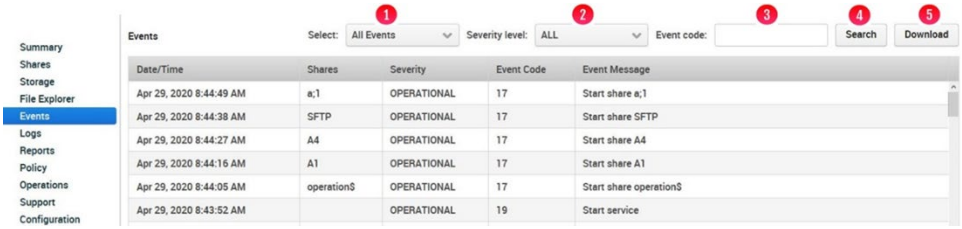
Figure 13.4 Administrator Audit Logs



Events Log

The Events log is accessed from the Events tab in the HCP Gateway UI. This log contains information about processes and operations in the HCP Gateway, such as starting/stopping a share, starting/stopping the HCP Gateway services, running a backup or restore (Figure 13.5). You can select a specific set of Events using the **Select** (Figure 13.5.1) drop down menu, **Severity Level** (Figure 13.5.2) drop down menu and/or enter an **Event Code** (Figure 13.5.3) then select **Search** (Figure 13.5.4). You can also download the Events by selecting the **Download** button (Figure 13.5.5).

Figure 13.5 Events



Events and Alerts have 3 levels of Severity:

Operational	Operation of task is successful running
Warning	Task or action failed, HCPG will automatically retry in most cases. Otherwise manually restart task
Error	HCPG has a critical issue that cannot be automatically fixed. Data may be lost or a process has crashed/exited.

List of HCP Gateway Event codes in Windows Event Viewer. Currently the Events in the HCP Gateway UI Events page and Events in the Windows Event Viewer are different:

Level	Event ID	Event Message
Error	2200	Error 2200, Failed to initialize the COM library, error code = xxx
	2201	Error 2201, Failed to register COM security and set the default security values, error code = xxx
	2202	Error 2202, Failed to get property 'letter' setting from C:\SAM\etc\sam\sam.properties.
	2203	Error 2203, Cache disk is not available:DeviceDosName
	2204	Error 2204, Failed to open a new connection to a communication server port that is created by the file system minifilter, error code= xxx
	2205	Error 2205, Failed to create an input/output (I/O) completion port, error code=xxx
	2206	Error 2206, Failed to allocate minifilter message buffer, exception code=xxx
	2207	Error 2207, Failed to get a message from a kernel-mode minifilter, error code=xxx
	2208	Error 2208, Failed to attempt to dequeue an I/O completion packet, error code=xxx
	2209	Error 2209, Failed to reply to a message from a kernel-mode minifilter. error code=xxx
	2210	Error 2210, Failed to get a message from a kernel-mode minifilter, error code=xxx
	2211	Error 2211, Failed to retrieve information about MS-DOS device DeviceDosName + ErrorCode
	2212	Error 2212, Failed to get shared object
	2213	Error 2213, Failed to attach minifilter instance to the volume xxx, return code=xxx
	2214	Error 2214, Failed to initialize database connection pool.
	2215	Error 2215, Create Database/table failed!

	2216	Error 2216, Setting is invalid in configuration file C:\SAM\etc\sam\sam.properties
	2217	Error 2217, Cannot find configuration file C:\SAM\etc\sam\sam.properties
	2218	Error 2218, Failed to get file FilePath
	2219	Error 2219, Failed to open file FilePath
	2220	Error 2220, Failed to get last write time of (SourcePath)
	2221	Error 2221, Cache Limit has been reached, no available space.
	2222	Error 2222, Failed to copy file: ("SourcePath") to ("TargetPath")
	2223	Error 2223, Property 'sam.account' setting is missing in configuration file C:\SAM\etc\sam\sam.properties
Warn	2100	Warning 2100, Failed to create share for archive ShareName
Info	2001	Stop SAM VFS service
	2000	Start SAM VFS service

HCP Gateway Reports

The Reports page is divided into two sections. The top portion of the page contains the available Reports (Figure 14.1.1) that can be run. The bottom half of the page contains the Configured Reports (Figure 14.1.2). Reports are exported to a csv file delimited by a '|' (pipe) that can be downloaded and opened. The Reports run in the background, so other UI activities can be performed while the report is running.

IMPORTANT WARNING: The HCP Gateway reports use the same database tables that the Gateway uses to maintain the information about the files. When there are a large number of files on a share, running a report will impact and may even bring a share Offline while the report runs. Be very careful when running reports when there is a large number of files on a share.

NOTE:

The HCP Gateway has no way to know the maximum size of a report that can be attached to an email at a customer site. If a report is too large to send over email, the Gateway will not send any alert, it will just not send the report.

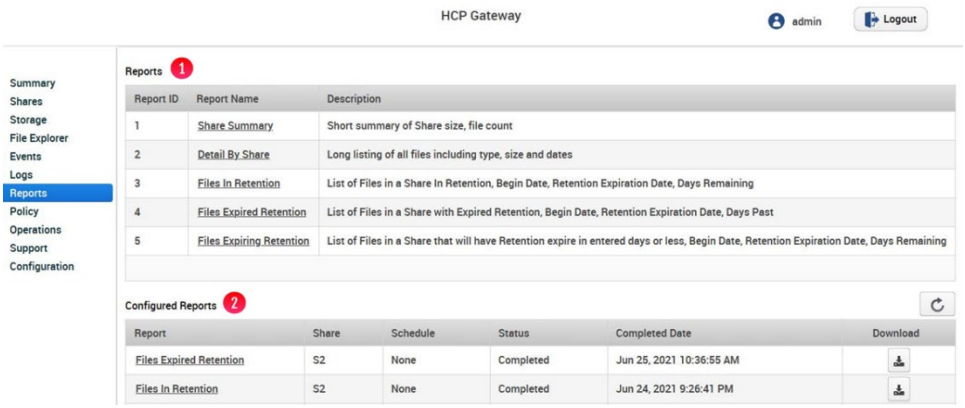
Note:

A comma is a valid character for a file name in Linux, so HCP Gateway uses a PIPE character as the field separator because a PIPE can't be used in a file name in Windows or Linux.

To display the report in Excel, you just need to open Excel and select **New file**, select **Data**, select **From Text**, select the csv file, select **Import**, select **Delimited**, select **My data has headers**, select **Next**, unselect **Tab**, select **Other** and enter the **'|'** (pipe) as the Delimiter, select **Next**, optionally configure the Column data formats, select **Finish**.

Select **OK** to import the data.

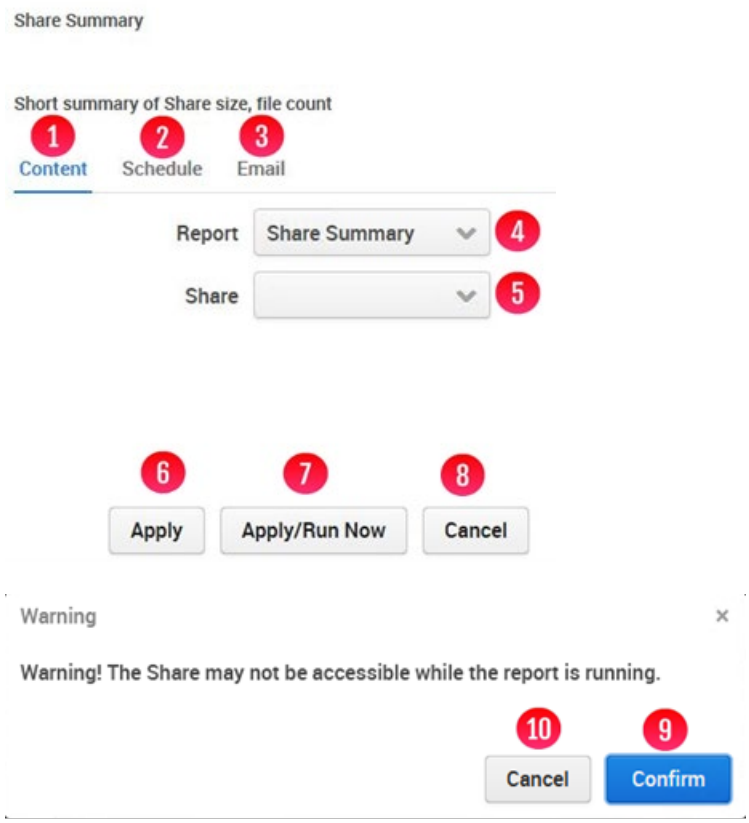
Figure 14.1 - Reports



The default Reports are:

1. Share Summary – only contains Share Size in bytes and number of files
2. Detail by Share – detailed listing of all files with meta-data
3. Files In Retention – detailed listing of files under a Retention Policy and associated dates
4. Files Expired Retention – detailed listing of files with no Retention Policy. Note that the report compares the time a file expires against the current date, so the report won't contain the files with expired retention until the day after they expire. Also note that when running this report against a share that is not using a Retention Policy, all files in this share will appear in the report since they are not under retention.
5. Files Expiring Retention – detailed listing of files with retention expiring in the selected Span (days) or less

Figure 14.2 – Run report



To run a report select the **Report Name**. A popup will appear (Figure 14.2) with the **Content** window (Figure 14.2.1) that contains menus with the selected Report and the menu to select the Share to run the report on. Optionally select another Report to run (Figure 14.2.4). Select the Share name (Figure 14.2.5). Then select **Apply/Run** (Figure 14.2.7) to start the report generation process. Optionally, select **Apply** (Figure 14.2.6) to create the Report template without running the report. Select **Cancel** (Figure 14.2.8) to exit the Report Content menu without creating the report.

When the report is run, a warning will appear that the share may not be accessible while the report is running. Select **Confirm** (Figure 14.2.9) to run the report or **Cancel** (Figure 14.2.10) to return to the previous menu without running the report.

To edit the configuration of an existing report, select the Report Name to make changes.

The Configured Reports table will be updated with a new row for the report that was created and/or run.

The **Report** column (Figure 14.3.1) shows the name of the report and if selected, is used for editing the Report configuration.

The **Share** column (Figure 14.3.2) shows the name of the Share that the report was run on.

The **Schedule** column (Figure 14.3.3) indicates the schedule the report is configured for and will be described below.

The **Status** of the report will show Running (Figure 14.3.4) until completed, then the Status will show Completed. A **Status** of Defined indicates the report was created but has not yet run. The **Completed Date** column (Figure 14.3.5) shows the most recent time the report was generated.

The Download button in the **Download** column (Figure 14.3.6) is used to download the report output to a csv file on the system that is running the HCP Gateway UI.

The **Refresh** button (Figure 14.3.7) is used to refresh the Configured Reports information.

By default, the most recent Reports will be at the top of the list. The Configured Reports can be sorted by clicking on any of the column headers (Figures 14.3.1 to 14.3.5).

Figure 14.3 – Pending Status on Report

Select **Schedule** (Figure 14.4.1) and the Schedule window will appear. Select **Frequency** (Figure 14.4.2) and the **Report Frequency** (Figure 14.4.3) options for running the reports will be displayed, they are:

1. None – the report will never run
2. Daily (Figure 14.5.1) – the report will run at the selected time (Figure 14.5.2) every day
3. Weekdays (Figure 14.6.1) – the report will run at the selected time every weekday (Monday through Friday) (Figure 14.6.2)
4. Weekly (Figure 14.7.1) - the report will run on the selected day (Figure 14.7.2) at the selected time (Figure 14.7.3) of every week
5. Monthly (Figure 14.8.1) - the report will run on the selected day (Figure 14.8.2) at the selected time (Figure 14.8.3) of every month. Select **Last** for the last day of the month or the number of the day in the month (Figure 14.8.2)
6. Monthly first week (Figure 14.9.1) - the report will run on the selected day (Figure 14.9.2) at the selected time (Figure 14.9.3) of the first week of every month

7. Monthly second week (Figure 14.10.1) - the report will run on the selected day (Figure 14.10.2) at the selected time (Figure 14.10.3) of the second week of every month
8. Monthly third week (Figure 14.11.1) - the report will run on the selected day (Figure 14.11.2) at the selected time (Figure 14.11.3) of the third week of every month
9. Monthly fourth week (Figure 14.12.1) - the report will run on the selected day (Figure 14.12.2) at the selected time (Figure 14.12.3) of the fourth week of every month

After configuring the Content, Report Schedule and Email, select **Apply** (Figure 14.5.3) to save the configured report to run at the scheduled time, or select **Apply/Run Now** (Figure 14.5.4) to save the configured report and run it now, or select **Cancel** (Figure 14.5.5) to return to the previous page without saving the configured report.

When the report is run, a warning will appear that the share may not be accessible while the report is running. Select **Confirm** (Figure 14.2.9) to run the report or **Cancel** (Figure 14.2.10) to return to the previous menu without running the report.

Figure 14.4 – Report Frequency

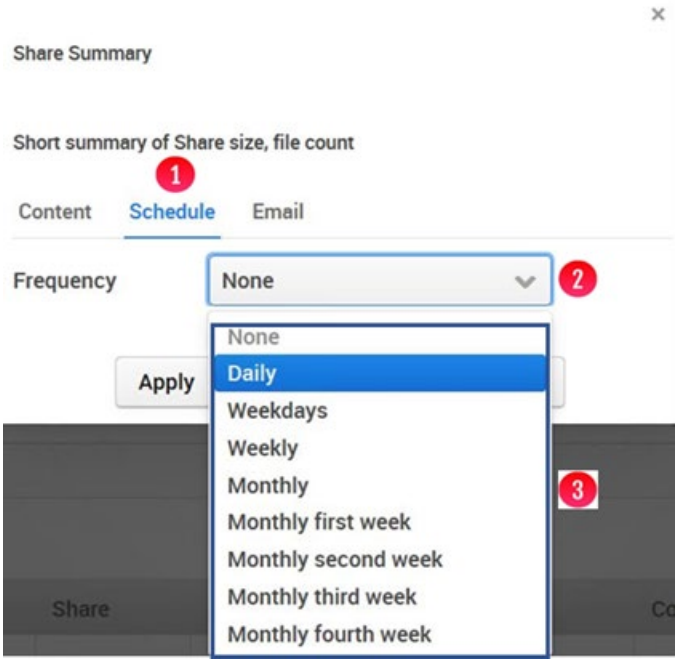


Figure 14.5 – Report Frequency Daily

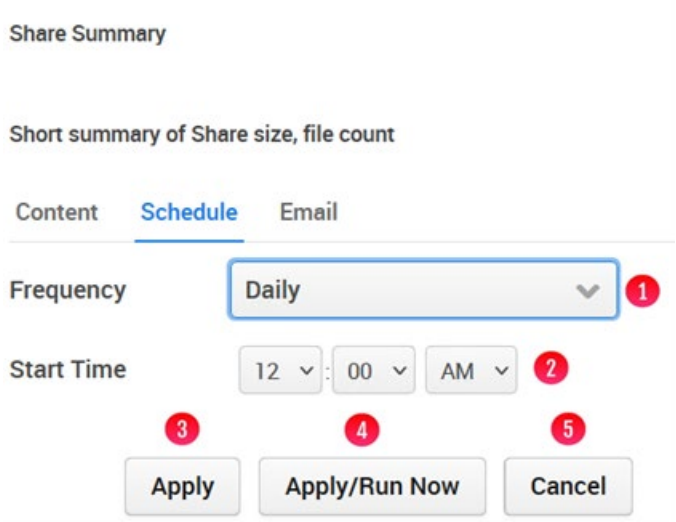


Figure 14.6 – Report Frequency Weekdays

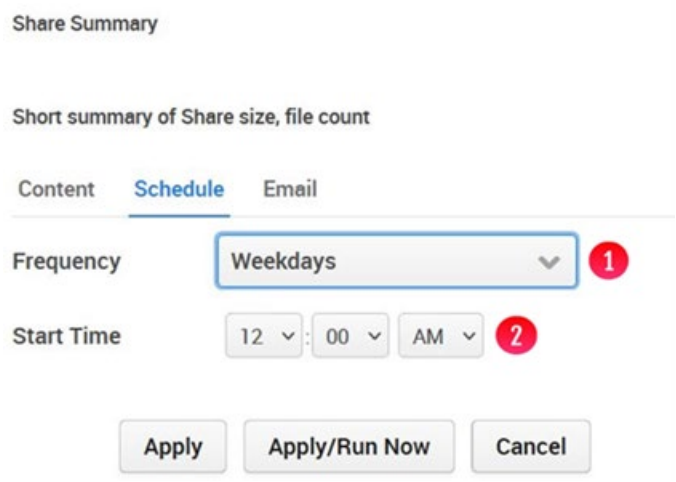


Figure 14.7 – Report Frequency Weekly

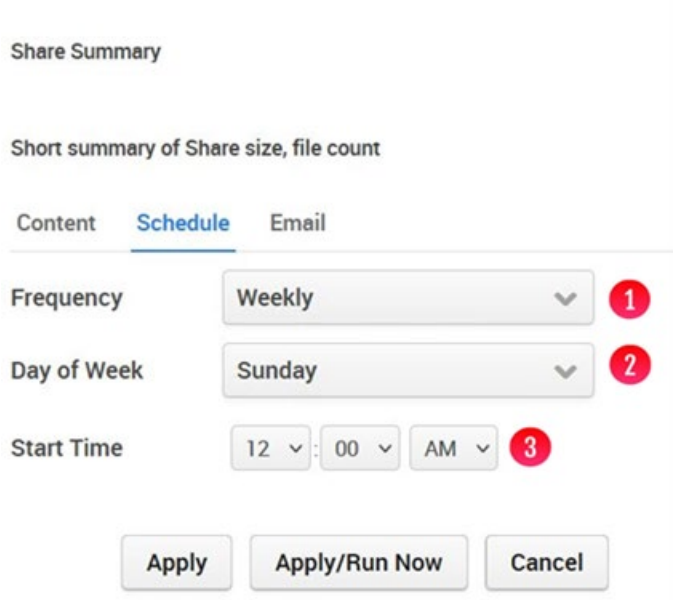


Figure 14.8 – Report Frequency Monthly

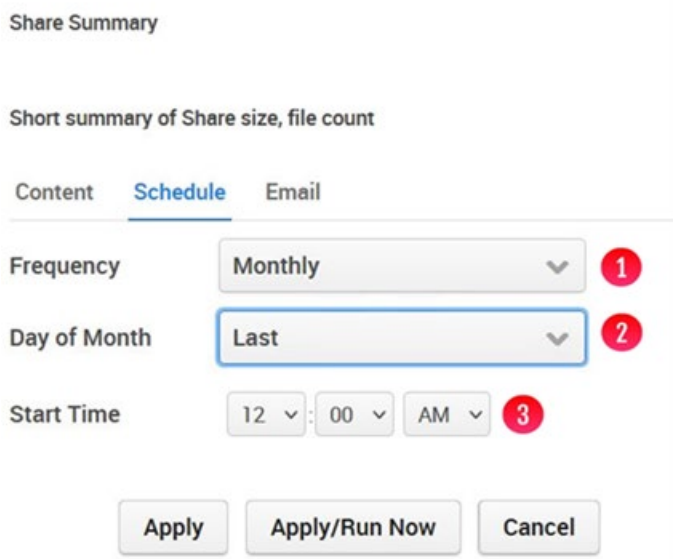


Figure 14.9 – Report Frequency Monthly first week

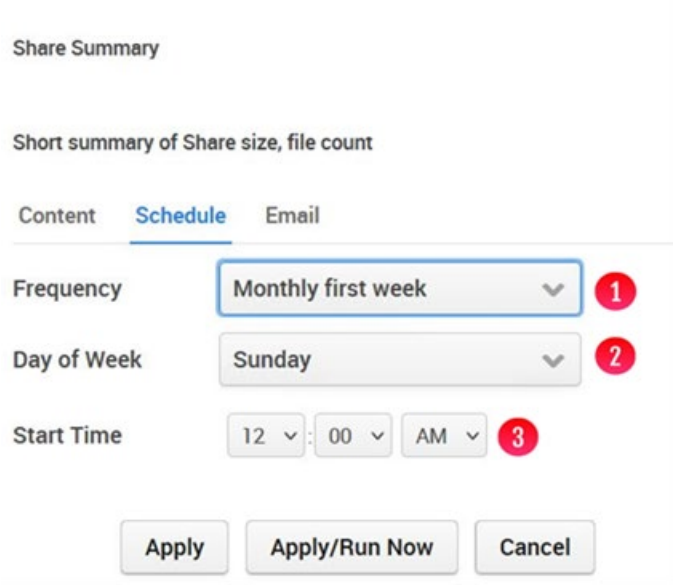


Figure 14.10 – Report Frequency Monthly second week

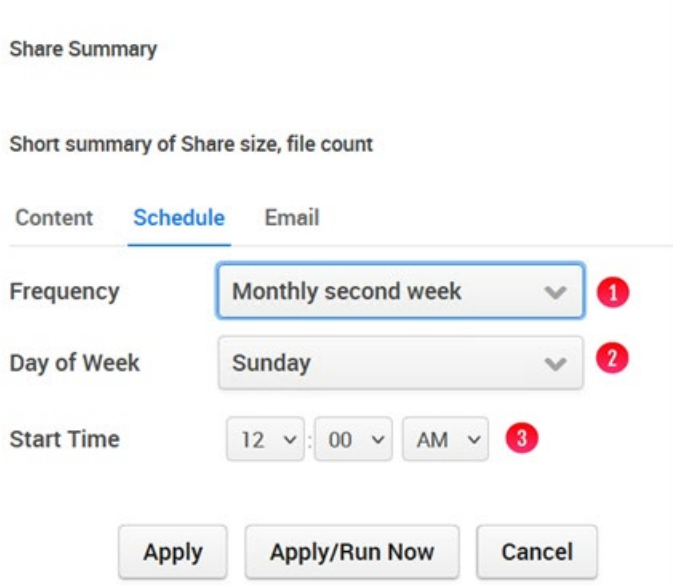


Figure 14.11 – Report Frequency Monthly third week

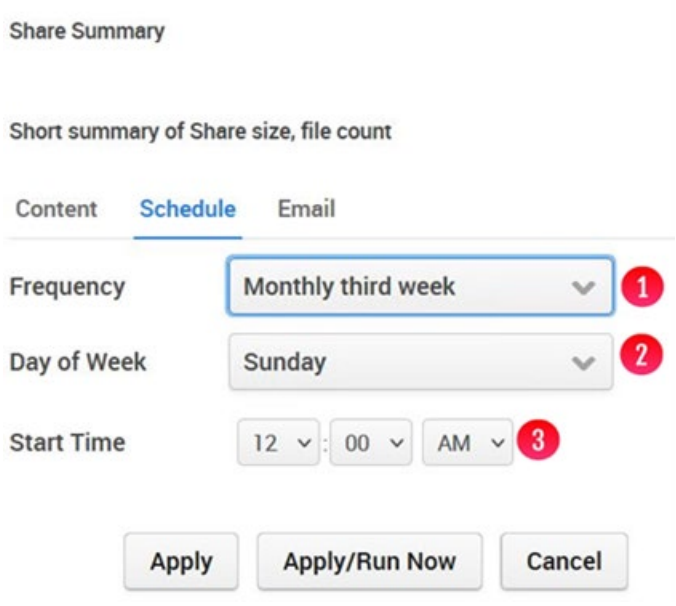
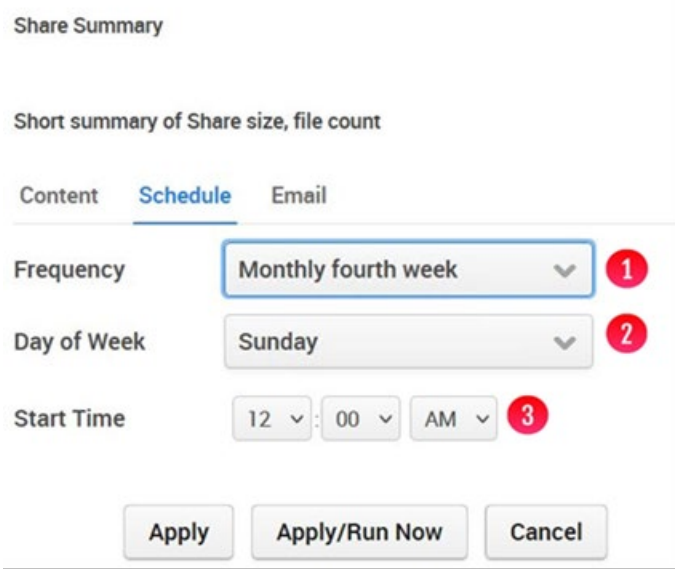
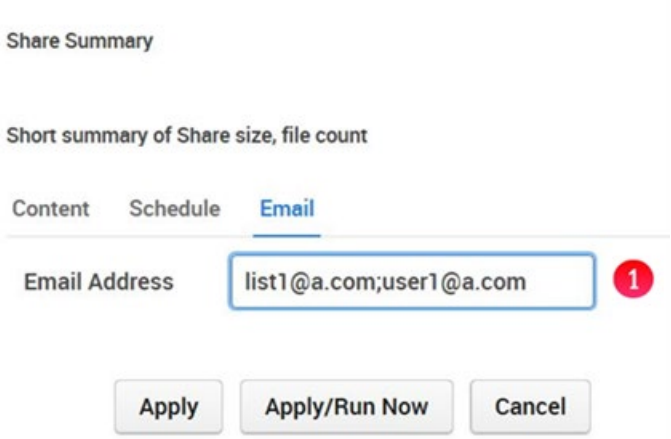


Figure 14.12 – Report Frequency Monthly fourth week



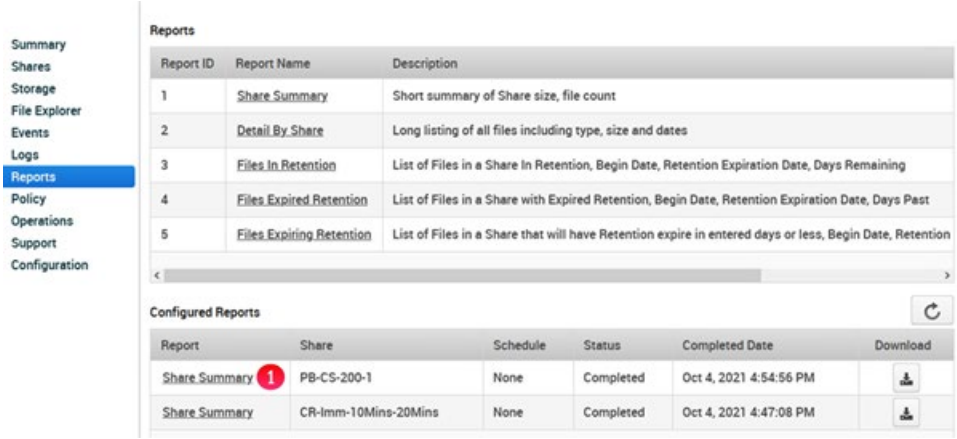
To have the report output sent over email after the report runs, select **Email** (Figure 14.2.3). Enter individual email addresses and/or email distributions lists separated by a ";" (semi-colon) (Figure 14.13.1).

Figure 14.13 – Report Email



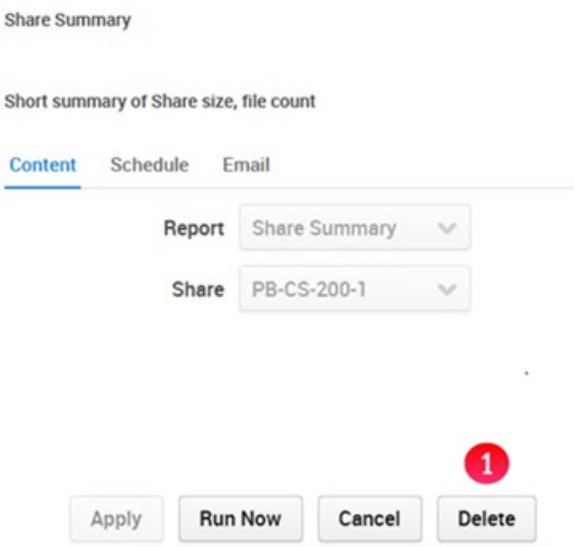
To delete a report and its output files, select the Report Name, for this example, **Share Summary** (Figure 14.14.1).

Figure 14.14 – Select Report to Delete



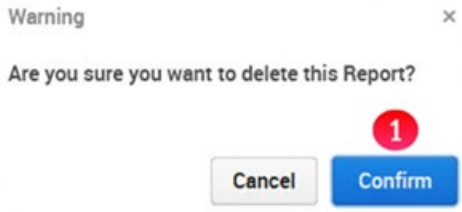
Select Delete (Figure 14.15.1).

Figure 14.15 – Select Delete



Select **Confirm** (Figure 14.16.1) to confirm deletion of the report and its output files.

Figure 14.16 – Confirm Delete



HCP Gateway Operations

It is imperative that the internal database of HCP Gateway be protected by backing it up to an external storage location. The Backup tab of the Operations section will utilize internal processes to perform this database and configuration backup. If a different process is to be used to back up HCP Gateway, contact Support for assistance.

15.1 Backup to HCP Storage

Object Storage based upon a dispersion algorithm provides a higher level of data protection versus local storage or even network storage. Therefore, it is required to save the HCP Gateway backups to the object storage. To do this, create a bucket/namespace on the object storage called for example “HCP Gateway Backups” (follow the Add Storage and Add Storage Groups processes in the **HCP Gateway Storage** chapter). If you are planning to use the Restore feature of HCP Gateway, then it is required for the backup location namespace be created with versioning enabled on the HCP. Also do not share this HCP namespace with another server, as the backup files are stored on the HCP with their Windows file names, not as an object id.

Now select **Share** from the main menu. To create a Share, click on the **Add Share** button (Figure 10.1.7 in the **HCP Gateway Share** chapter). The Add Share form will appear (Figure 15.1W/L). Remember the Share name is the exposed share name. For backing up HCP Gateway, we require **operation$** for the **Name** field (Figure 15.1W.1) in Windows. In Linux, we require the **Name** (Figure 15.1L.1) and **Share Path** to be **.operation** (Figure 15.1L.2). The **“$”** at the end of the Windows share name makes it invisible to Windows clients. The “.” at the beginning of the Linux share name makes it a special share. Select a **Storage Group** that was previously created (Figure 15.1W.2 for Windows and Figure 15.1L.3 for Linux) with HCP Storage that contains a namespace with Versioning enabled. Do not share this HCP namespace with another server, as the backup files are stored on the HCP with their Windows file names, not as an object id. If you are planning to use the Restore feature of HCP Gateway, then it is required for the backup location to be Network using a share named **operation$** in Windows and **.operation in Linux**. Leave the **Policy** field blank (Figure 15.1W.3 for Windows and 15.1L.4 for Linux) so the share will be Read/Write and the backup files will be released from the cache after they are written to the HCP. Then select the **Apply** button at the bottom of the form to create the share.

IMPORTANT NOTE:

Do not use an Archive Mode Retention, Include Retention, Snaplock or Legal Hold policy with the Windows **operation$** or the Linux **.operation** share. Also, compression and encryption are not used with the Windows **operation$** or the Linux **.operation** share, even when selected in the Add or Edit Share menu.

Figure 15.1W – Windows - Add operation$ Share

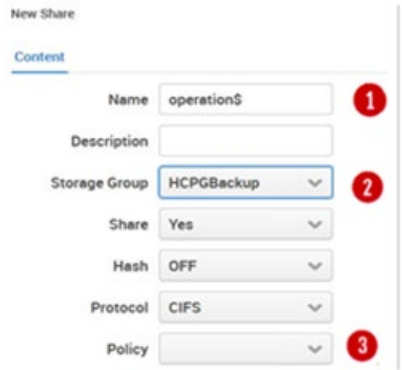
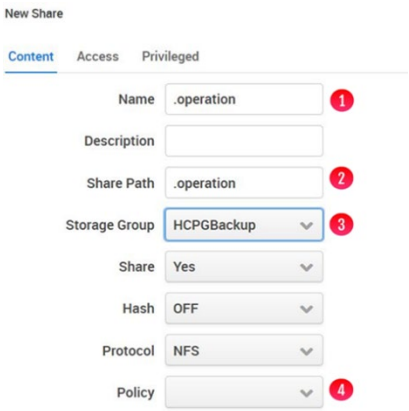


Figure 15.1L – Linux - Add .operation Share



Next select **Shares** from the main menu. In Windows, the **operation$** share is now visible on the Share summary page (Figure 15.2W.1) and in Linux, the **.operation** share is now visible on the Share summary page (Figure 15.2L.1).

Figure 15.2W – Windows - Operation$ share added

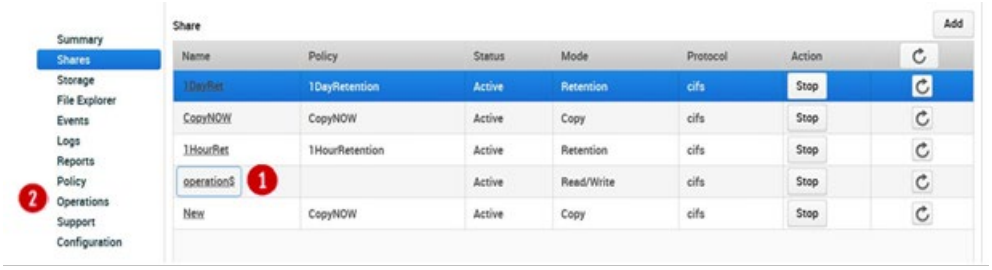
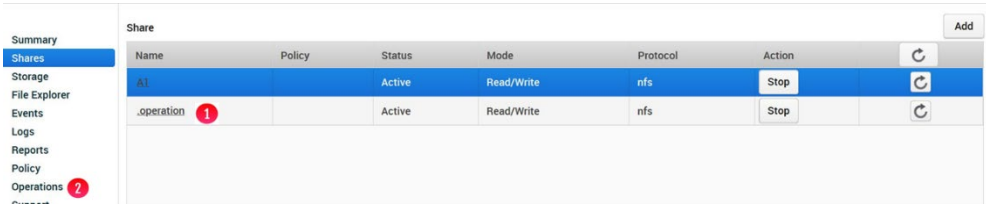


Figure 15.2L – Linux - Backup (.operation) share added



Select **Operations** (Figure 15.2W.2 in Windows or Figure 15.2L.2 in Linux) from the main menu to return to the **Operations** tab to continue with setting up the backup location (Figure 15.3W in Windows or Figure 15.3L for Linux).

In Windows, select the **Network** checkbox (Figure 15.3W.1) as the System Backup Location. Then enter **"\\localhost\operation$"** into the **UNC Path** text box (Figure 15.3W.2). Enter the **User Name** (Figure 15.3W.3) and **Password** (Figure 15.3W.4) for the UNC path. Select **Test** (Figure 15.3W.5) to test the connection. Finally, select **Apply** at the bottom of the page to save the settings. Now all backups will be written to the HCP Object Storage through the **operation$** share, which can be viewed with MS Explorer (Figure 15.4W).

NOTE:

On a Windows Cluster node, set the backup location to \\<cluster-name-or-ip-address>\operation$.

In Linux, the default backup location is **/archive/.operation** (Figure 15.3L). It is not recommended, but if you need to change the location, select the **Edit setting (Pencil)** icon. Select **Apply** at the bottom of the page to save the settings. Now all backups will be written to the HCP Object Storage through the **operation$** share, which can be viewed from the Linux command line (Figure 15.4L).

Figure 15.3W – Windows operation$ share

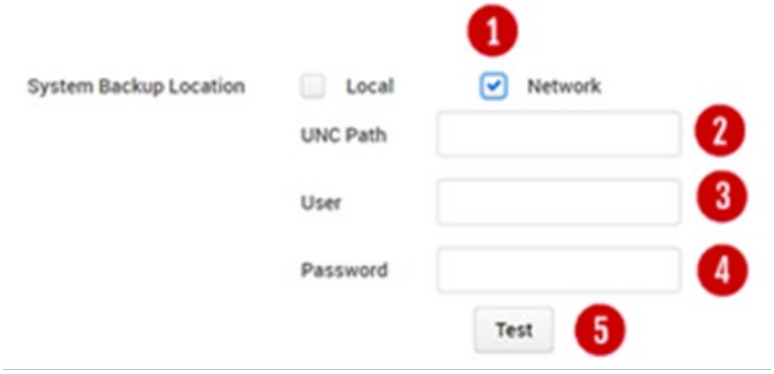


Figure 15.3L – Linux Backup (.operation) share

Figure 15.4W – Windows \\localhost\operation$

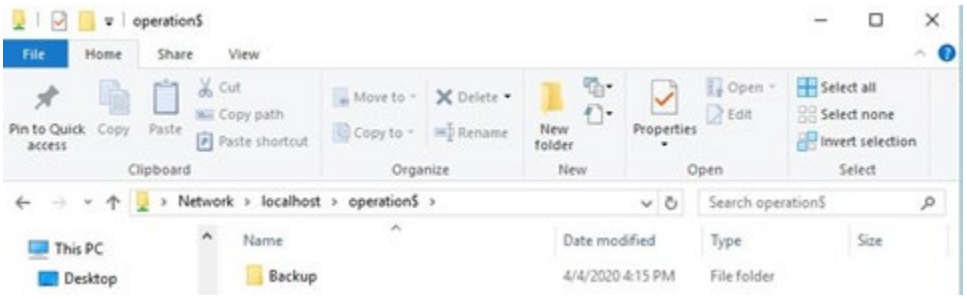
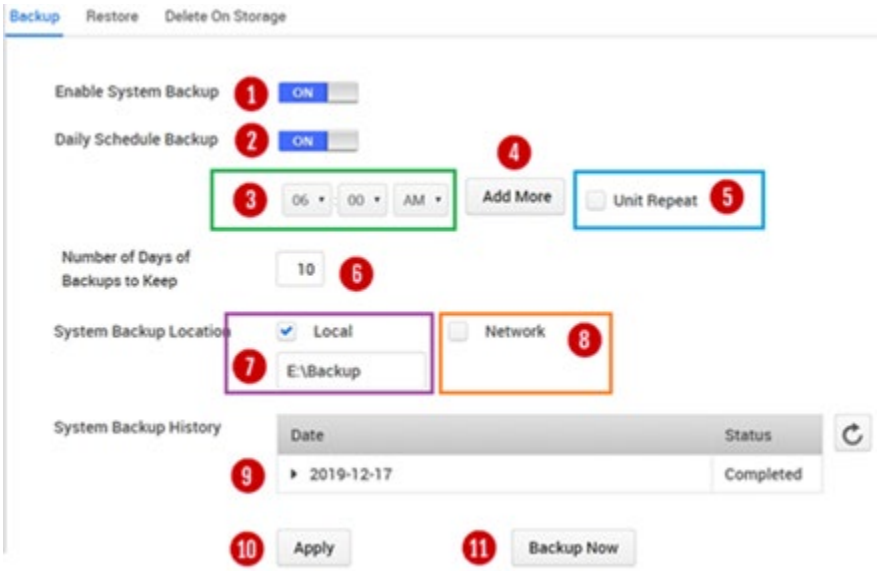


Figure 15.4L – Linux - /archive/.operation

```
vault@hcpg-linux-1:~$ ls -l /archive/.operation
total 0
drwxrwxr-x 1 vault vault 0 Sep 28 15:43 Backup
vault@hcpg-linux-1:~$
```

Toggle the **Enable System Backup to ON** (Figure 15.5.1) to enable backups. Then toggle the **Daily Schedule Backup** button (Figure 15.5.2) to **ON** and then set a starting time (Figure 15.5.3). Use this option if you want to run one backup per day. If you want to run more than one backup a day select **Add More** (15.5.4) and enter another fixed time. Alternatively, select the **Unit Repeat** check box (Figure 15.5.5) to set a frequency, such as run every 6 hours. Note that every backup process is a full backup and will run until complete. Note the frequency will not start until after the time of the Daily Schedule. If you want to do a backup immediately select **Back Up Now** (Figure 15.5.11).

Figure 15.5 - HCP Gateway Backup



Next enter the **Number of Days of Backups to Keep** (Figure 15.5.6). The number must be between 1 and 999. If you run multiple backups per day, Gateway will store that number times the number of days of backups. If the backup location is set to Local, Figure 15.5.7 displays the Local location, otherwise Figure 15.5.8 displays the Network location.

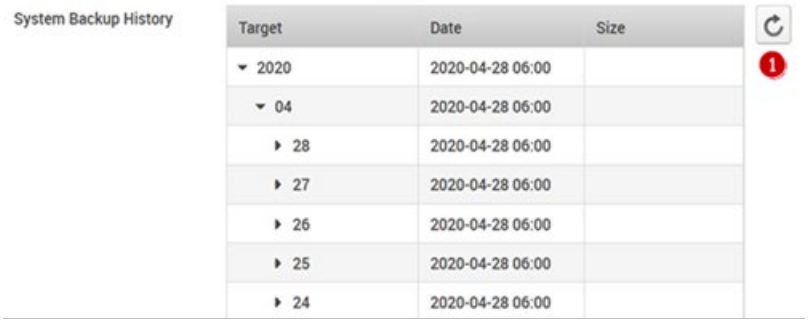
IMPORTANT NOTE:

The HCP Gateway will delete the oldest backup from the share once the Number of Days of Backups to Keep is reached. In order to reclaim the space on the HCP from the oldest backup that was deleted, configure the Delete on Storage to delete the backup from the HCP namespace. Refer to Section 15.3 Delete on Storage for additional information. Note that the deleted objects from the backup will not be deleted off the HCP namespace until the Garbage Collection runs on the HCP namespace.

HCP Gateway provides a Backup history (Figure 15.5.9) of backups. The list is organized in chronological order from newest to oldest. Each Backup has a status of “Completed” if it ran correctly. The status will be “failed” if backup was not successful.

If at any time the **Backup now** button is selected, a message in blue letters will appear on the screen for a few seconds indicating the Backup started. If you remain on the Backup page, another message in blue letters will appear on the screen for a few seconds when the Backup completes. Also, selecting the refresh icon (Figure 15.6.1) will update the status of completed backups. A third way to check the status of a backup is the Events page in the UI (refer to Chapter 13 HCP Gateway Logs).

Figure 15.6 – Backup History



To see the details of a backup, select the triangle located to the left of the date. This will display the database and configuration backup file (Figure 15.7.1) and database binary log files (Figure 15.7.2). Both files are required to perform a restore or system recovery operation.

Figure 15.7 - Database Backup

15.2 Restore

The HCP Gateway allows the administrator to recover the system from backups and this is covered in **Chapter 17 Recover from Backup**.

15.3 Delete on Storage

The Delete on Storage option allows backend storage space to be recovered and manages the number of file versions on the HCP Gateway. This is desirable when a file under retention has passed its retention date or if the User or Admin manually deletes the file from the front-end file system. The second scenario is when HCP Gateway is in Server or NAS mode and the front-end file system is set to Read/Write and a Copy Policy issued to make a copy to a storage location like a cloud or object storage system. This setting allows the copies on the storage locations to be deleted, thus avoiding orphan files consuming capacity when not needed.

Select the **Delete on Storage** tab from the Operations submenu. A popup will appear with a table containing a list of the Share names (Figure 15.8.1). Next to each Share Name is a Status toggle (Figure 15.8.2) that with the default setting set to off. Slide the toggle to the right to turn it on. Then select **Settings** (Figure 15.8.3) to configure the settings for that Share.

Figure 15.8 – Delete on Storage

Delete on Storage also needs to appropriately handle file versions and the configuration options are selected in the Settings popup (Figure 15.9).

Active Files are files with at least one version on HCP Gateway and the current version of the file is visible in the share (Figure 15.9.1). NOTE that only one of these settings can be configured per share.

Keep all versions will keep every version of the file.

Keep versions for * days – select this option to configure the number of days to keep in the **Number of days to keep** (Figure 15.9.3) field.

Keep * versions for each file – select this option to configure the number of versions of this file to keep in the **Number of versions to keep** (Figure 15.9.2) field. The number of versions does not include the active file in the share, it only counts the number of times the file was modified or overwritten. If the number of versions is set to 5, when the 7th version of a file is written, the Gateway will remove the oldest version of the file, so there will be 1 active file and 5 old versions.

Deleted Files are files with no active versions visible in the share (Figure 15.9.4). NOTE that only one of these settings can be configured per share.

Delete all versions will delete every version of the file.

Do not delete any will keep every version of the file.

Keep versions for * days – select this option to configure the number of days to keep in the **Number of days to keep** (Figure 15.9.3) field.

Keep * versions for each file – select this option to configure the number of versions of this file to keep in the **Number of versions to keep** (Figure 15.9.5) field. Set this to 0 if you want to delete every version of the file.

The **Expired retention files** option (Figure 15.9.6) configures whether to **Keep** or automatically **Delete** files when their retention period expires.

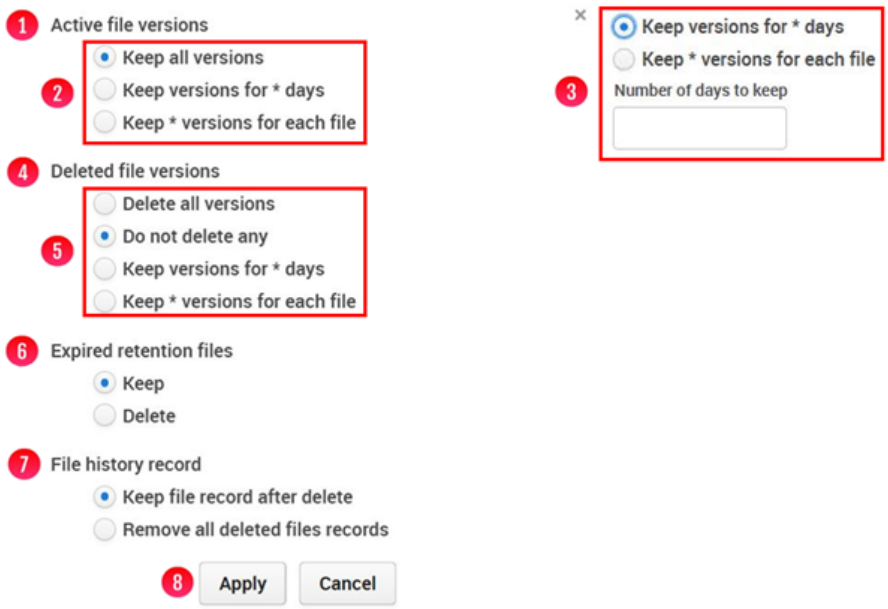
IMPORTANT NOTE:

In order to automatically delete files with expired retention from the share and the storage, when selecting **Delete** in the **Expired retention files** option (Figure 15.9.6), it is required to also select **Delete all versions** in the **Deleted Files** option (Figure 15.9.4). Then the **Delete on Storage** must be run to delete the files off the storage. Refer to the **HCP Gateway Operations** chapter for the details on **Delete on Storage**.

The **File History** option (Figure 15.9.7) configures how to keep track of the file metadata history in the HCP Gateway database. For Compliance reasons it may be necessary to keep track of deleted versions, in this case select **Keep file record after delete**. Alternatively, the metadata can be deleted, and space recovered in the database, in this case, select **Remove all deleted files records**. Note that before a share can be deleted, all the metadata for the files must be deleted from the HCP Gateway database.

Select **Apply** (Figure 15.9.8) to save the configuration.

Figure 15.9 – Delete on Storage Settings

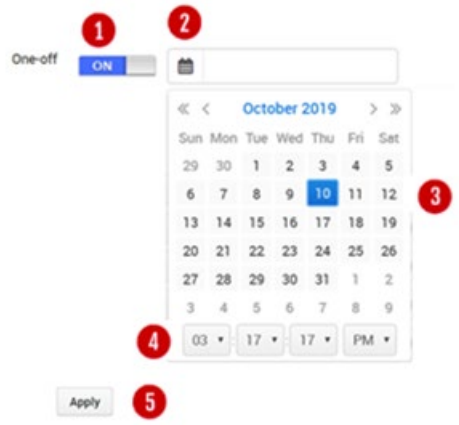


Note that the Delete on storage process can be resource intensive, therefore we recommend that you run in low use periods like evenings or weekends. The next step is to schedule the process. To immediately run the Delete on Storage process select **Start Now** (Figure 15.10.1) otherwise to run at a different time slide the toggle to the right to turn on one of the other options (Figure 15.10.2).

Figure 15.10 – Delete on Storage Settings

To run the delete process just once, select the **One-Off** toggle (Figure 15.11.1) and slide to the right. Then select the calendar icon (Figure 15.11.2). Once the calendar appears select the appropriate month, date (Figure 15.11.3) and then set the time (Figure 15.11.4). The select **Apply** (Figure 15.11.5) to finish the scheduled delete process.

Figure 15.11 –Schedule One-Off Time



To run the Delete on Storage daily, slide the daily toggle to **ON** (Figure 15.12.1). Select the options for setting a starting time (Figure 15.12.2) and an ending time (Figure 15.12.3). Then select **Apply** to save the daily schedule.

Figure 15.12 –Schedule Daily

To run the Delete on Storage weekly, slide the daily toggle to **ON** (Figure 15.13.1). Then select the desired days (Figure 15.13.2) by selecting the appropriate box. Next use the arrows to set the start and ending times (Figure 15.13.3) for each day of the week. Finally, select **Apply** (Figure 15.13.4) to save the settings.

Figure 15.13 –Schedule Weekly

WARNING: Using the Delete on Storage will result in the files selected being deleted off the HCP Gateway and HCP storage. Be very careful using this feature.

Recover Previous Versions and Deleted Files

HCP Gateway supports file versioning at a file level. This means the whole file is versioned, not just the changed blocks of the file.

WARNING: In Server mode in order to recover from a previous version or promote an older version to current version there must be a copy on a storage location, such as the HCP.

IMPORTANT NOTE:

You will need to wait for the file to be completely processed, about 3-5 minutes, before you can version a file in the HCP Gateway UI File Explorer.

The HCP Gateway administrator can use the File Explorer to download a previous version or promote a previous version to the current version. Alternatively, Users can install the HCP Gateway End User Restore application on their Windows computer.

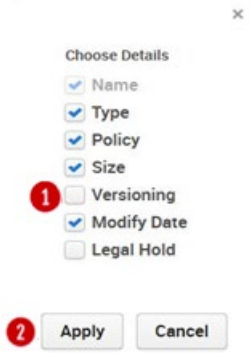
16.1 Version Recovery by Administrator

From the HCP Gateway UI the administrator selects **File Explorer** (Figure 16.1.1) from the main menu. The select the **Choose Detail** button (Figure 16.1.2).

Figure 16.1 – Versions

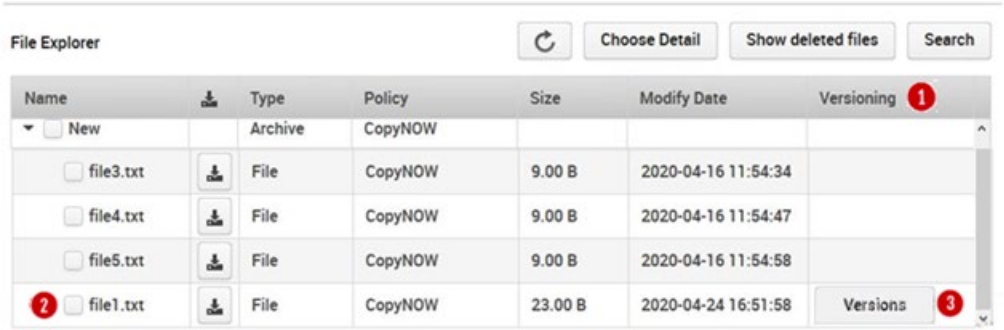
By default, versioning info is not displayed in the File Explorer menu. To include versioning info, click the **Versioning** checkbox (Figure 16.2.1) in the popup form. Then click the **Apply** button (Figure 16.2.2).

Figure 16.2 – Show Versioning Details



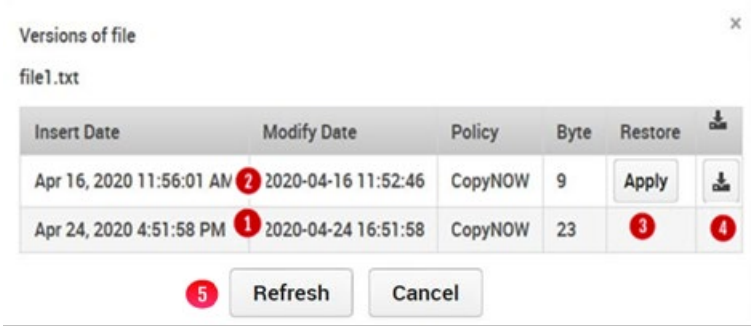
After applying the changes, the File Explorer menu has changed and now has a column called Versioning (Figure 16.3.1). To view the file versions, select the **checkbox** (Figure 16.3.2) for the file and then click on the **Versions** button (Figure 16.3.3).

Figure 16.3 – Check for Versions



In Figure 16.4 there are two versions of the file file1.txt. The current version was saved 2020-04-24 16:51:58 (Figure 16.4.1). The previous version was saved at 2020-04-16 11:52:46 (Figure 16.4.2). The files are listed in order of last modification time, the “current” version, in this example, is the most recent file.

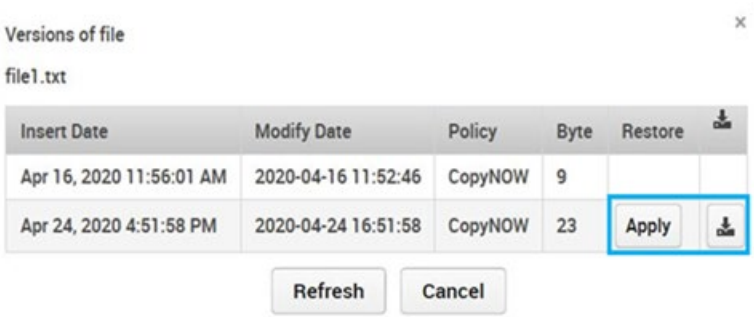
Figure 16.4 – Show File Version



The original version can be promoted by selecting the **Apply** button (Figure 16.4.3). The original version can also be downloaded by clicking the **Download** icon (Figure 16.4.4). The Refresh button (Figure 16.4.5) is used to show the updated status of the files. Note that it will take a minute or 2 for the status to be updated before the Refresh button will show the changes.

After deciding that the original version should be promoted and made the current version by selecting the **Apply** button (Figure 16.4.3) the UI is refreshed and now displays that the older file is the current version (Figure 16.5).

Figure 16.5 – Current Version changed



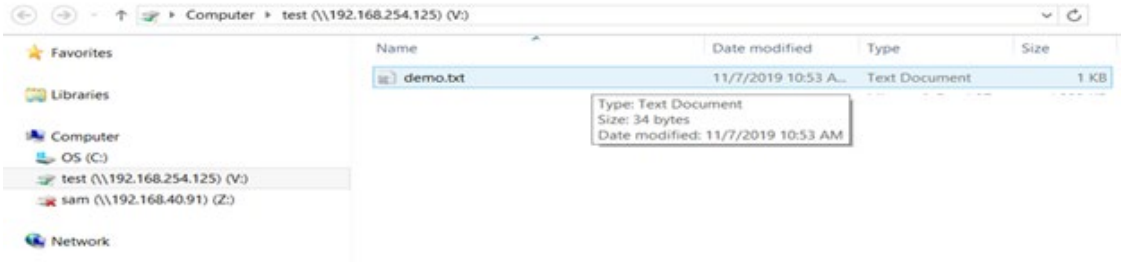
16.2 User Recovery of Previous Version (Windows Only)

In order for a user to recover a previous version of a file from their Windows computer they must have the HCP Gateway End User Restore application installed that matches the version of the HCP Gateway. Download the HCPGUserRestore-X.X.X.msi file to the User's system. Double click on the name to start the Microsoft installer of the application. Take the default options until finished. Make sure TCP Port 9090 is open between the end-user system and the HCP Gateway. If Windows Firewall is enabled on the HCP Gateway, make sure TCP port 9090 inbound is allowed. See Application note with detailed instructions for application installation.

Figure 16.6 – Application Installer

The HCP Gateway is presenting a Share named test to user. The user saves a file named demo.txt at 10:46AM. At 10:53AM the user updates the file (Figure 16.7) and saves it. The file updated at 10:53AM is the current version and visible in the Test Share presented by the HCP Gateway. The version created at 10:46 is not visible in the Test Share.

Figure 16.7 – User View of Test Share

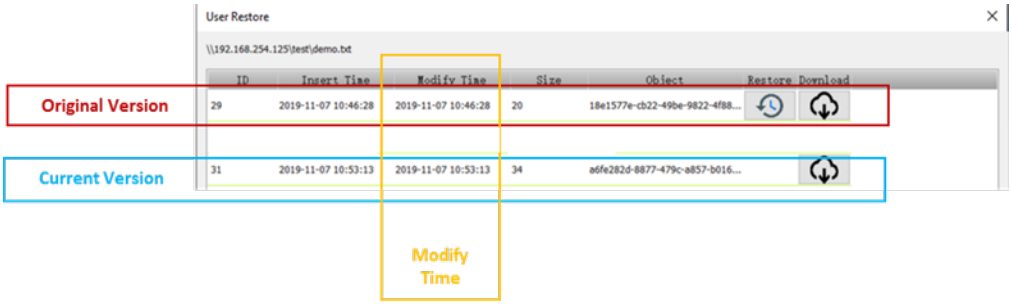


To start the User Restore process the user puts their mouse on the file name and right clicks the mouse. The File Explorer tool menu pops up (Figure 16.8). Find HCPG on the menu and to the right click on the “>” sign (Figure 16.8.1). The menu will then show the HCPG User Restore option (Figure 16.8.2)

Figure 16.8 – Explorer tools

The Version table (Figure 16.9) for the selected file is displayed. In the example there are two versions of the file demo.txt. The current version can be determined by looking at the modify time or the one without the “turn back clock” icon The user can elect to download any version by selecting the cloud download icon This will save the selected file to the download folder of the local system. Alternatively, the user can select the “turn back clock” icon and this file will be promoted to the current version. Click the X in the popup to close the application.

Figure 16.9 – Versions



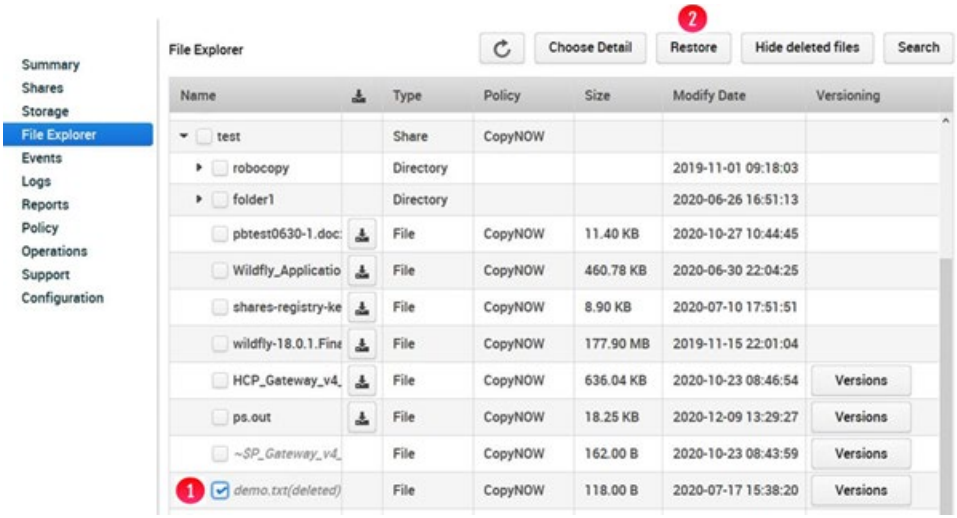
16.3 Recovery of Deleted Files by Administrator

The Gateway Administrator can see and recover deleted files in the File Explorer menu. The **Show deleted files** (Figure 16.10.1) button needs to be checked in the File Explorer to enable the Administrator to recover deleted files.

Figure 16.10 – Select Show deleted files

Deleted files are displayed in gray italic text versus black. To restore a single deleted file, select the file by clicking the box to the left of the file name (Figure 16.11.1) then click the **Restore** button (Figure 16.11.2).

Figure 16.11 – Select Deleted File



The recovered file is now available again in the HCP Gateway File Explorer (Figure 16.12.1) and Windows File Explorer (Figure 16.13).

Figure 16.12 – Deleted File Recovered in HCP Gateway

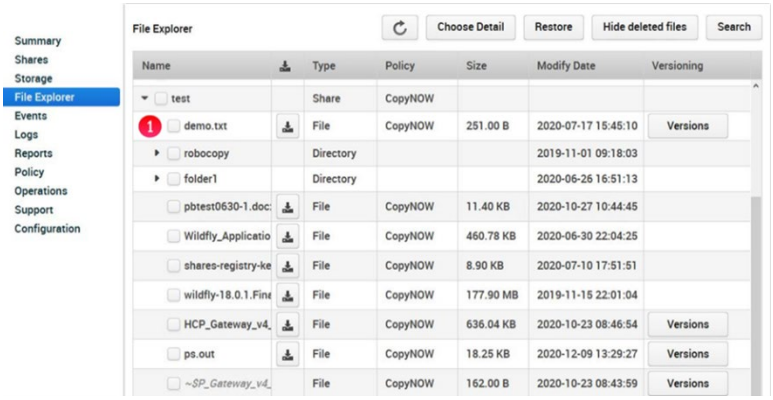
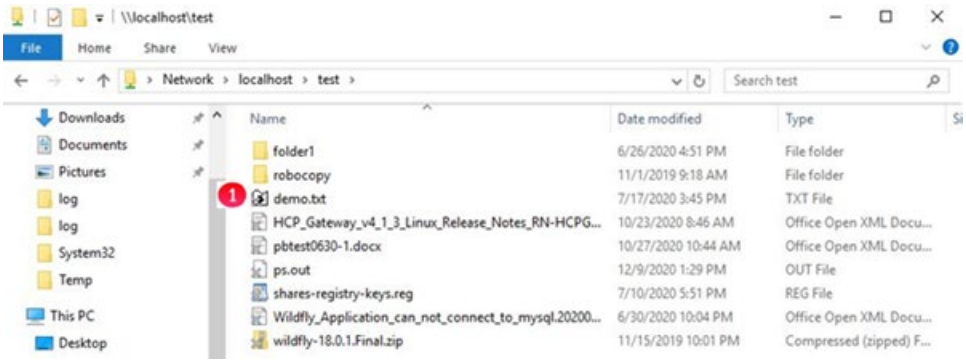
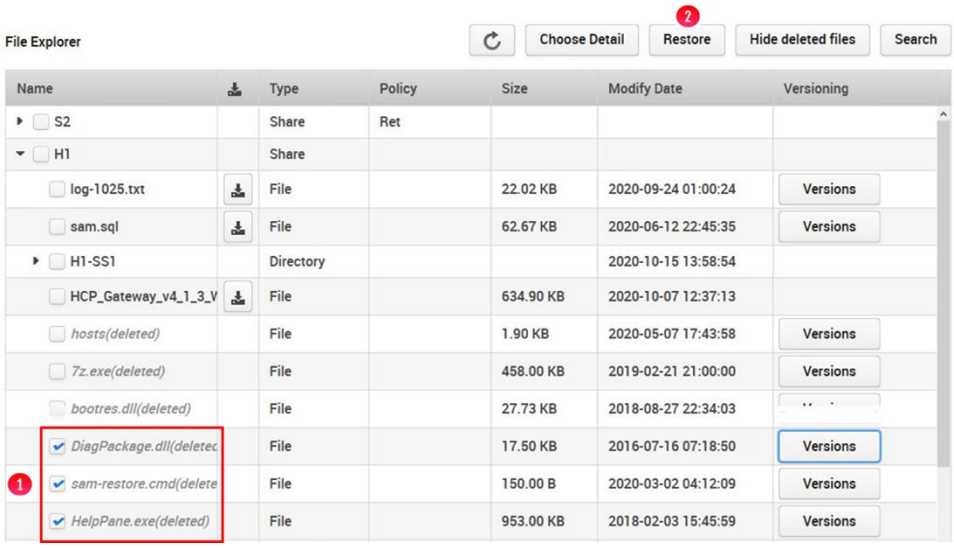


Figure 16.13 – Deleted File Recovered in Windows File Explorer



To restore multiple deleted files, select the files by clicking the box to the left of the file names (Figure 16.14.1) then click the **Restore** button (Figure 16.14.2). If the files are not restored in a few minutes, select the Events page (refer to Chapter 13 HCP Gateway Logs) for more information.

Figure 16.14 – Select Deleted Files



The recovered files are now available again in the HCP Gateway File Explorer (Figure 16.15.1) and Windows File Explorer (Figure 16.16).

Figure 16.15 – Deleted File Recovered in HCP Gateway

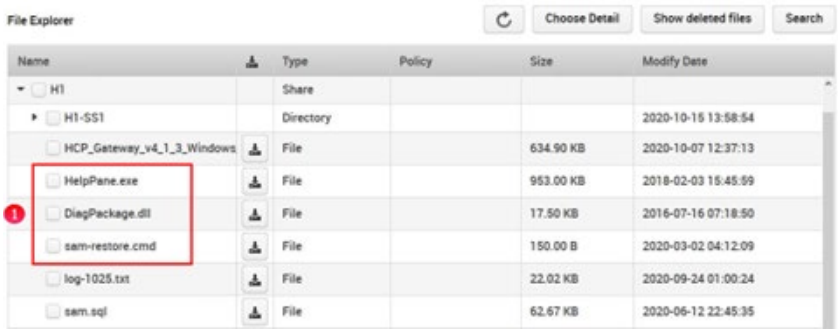
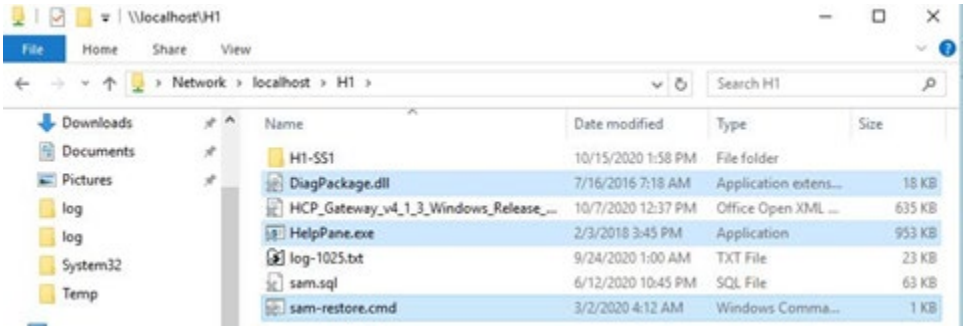


Figure 16.16 – Deleted Files Recovered in Windows File Explorer



Recover from Backup

In this chapter we will cover the process to use the HCP Gateway backup files to recover data on a single HCP Gateway system using the built-in Restore feature in the HCP Gateway UI Operations tab. This feature will work on either a single share or on all shares.

Prerequisites:

1. You need a location to store the backup, it is recommended to use an HCP Namespace. In this example create an “hcpgbackup” namespace. Also, you need to add the Storage for the “hcpgbackup” namespace and a Storage group in the HCP Gateway. The “hcgpgbackup” namespace requires Versioning enabled on the HCP Namespace because the **.bin** files get updated. Do not share this HCP namespace with another server, as the backup files are stored on the HCP with their Windows file names, not as an object id. If you need assistance with these tasks, review the **HCP Gateway Administration Guide Storage** and **Shares** chapters.
2. Next, you need to create a share that will store the HCP Gateway backups in the “hcpgbackup” namespace on the HCP. We **REQUIRE** naming the share **“operation$”** in Windows or **“.operation”** in Linux, so that the share is hidden from users. Leave the **Policy** field blank when creating share so the share will be Read/Write and the backup files will be released from the cache after they are written to the HCP. Next, in the HCP Gateway UI **Operations -> Backup** tab, make sure the **System Backup Location** is set to **Network** and the **UNC Path** is set to the **\\localhost\operation$** in Windows or **/archive/.operation** share in Linux. If you need assistance with this task, review the **HCP Gateway Administration Guide Operations** section.

   NOTE:

   On a Windows Cluster node, set the backup location to \\<cluster-name-or-ip-address>\operation$.

   IMPORTANT NOTE:

   Do not use an Archive Mode Retention, Include Retention, Snaplock or Legal Hold policy with the Windows **operation$** or the Linux **.operation** share. Also, compression and encryption are not used with the Windows **operation$** or the Linux **.operation** share, even when selected in the Add or Edit Share menu.

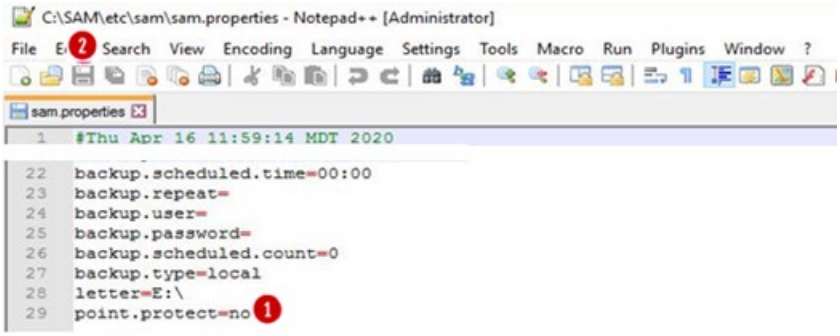
3. If an HCP Gateway backup has not been completed, then in the HCP Gateway UI, go to **Operations -> Backup** tab and click on the **Backup Now** button.

WARNING: If a customer is using a Copy or Tiering Policy and the data is on local disk and an HCP namespace, and there is limited local disk space for the restore from backup, some data from the local disk cache location might need to be deleted (data that is already protected in HCP). Refer to the **HCP Gateway Administration Guide Delete File Copy Off Local Storage** chapter for the steps to delete files off the local storage to free up space in the cache.

Gateway – Backup Recovery Process:

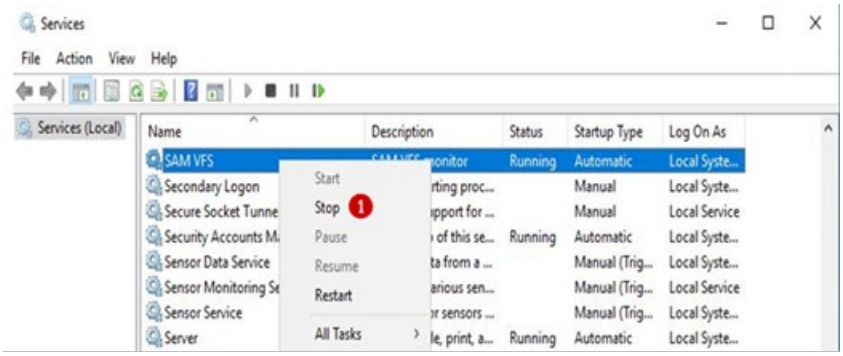
Step 1 – (Windows only) During the restore process, the HCP Gateway cache folder will be renamed so the cache will match the restored database information, which requires a configuration parameter change. Use Notepad++ on the HCP Gateway to edit the file **C:\SAM\etc\sam\sam.properties** and configure the parameter **"point.protect=no"** (Figure 17.1.1). Be sure to save the file by clicking the blue disk icon (Figure 17.1.2) before closing the Notepad++ application.

Figure 17.1 – Edit sam.properties file



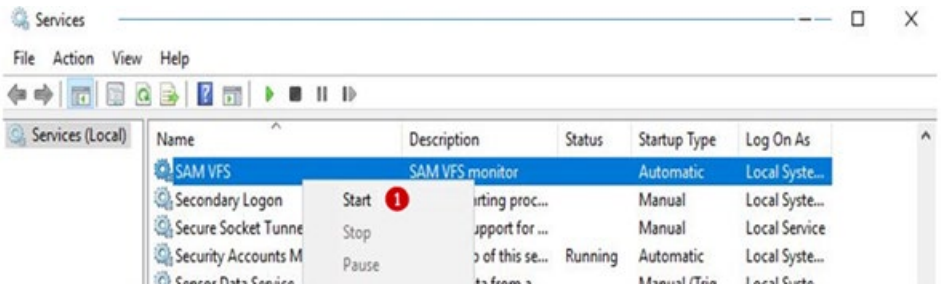
Step 2 - (Windows only) Stop the "SAM VFS" service. It is recommended to wait at least 5 minutes from the time the last file is ingested into HCP Gateway before stopping the "SAM VFS" service. Click on the Windows Start Menu located at the bottom left of the screen. Select the "Services" option. Navigate to the "SAM VFS" service, right-click on it and select **"Stop"** (Figure 17.2.1).

Figure 17.2 – Stop SAM VFS Service



Step 3 – (Windows only) Start the "SAM VFS" service. In the Windows "Services", navigate to the "SAM VFS" service, right-click on it and select **"Start"** (Figure 17.3.1).

Figure 17.3 – Start SAM VFS Service

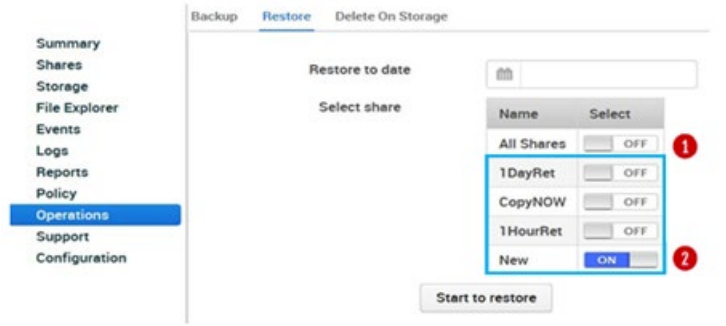


Step 4 – (Windows and Linux) If you have more than 1 share and the shares contain many files, it may take a few minutes before the shares show an **Active** Status. Once all the shares show an **Active** Status, then click the **Stop** button (Figure 17.4.1) of the share you want to restore. If you want to restore **All** shares, you will need to stop all of the customer data shares. **DO NOT STOP THE operation$ (Windows)** or **.operation (Linux) share**, as that is where the restore will be accessing the backup file from.

Figure 17.4 – Stop Share

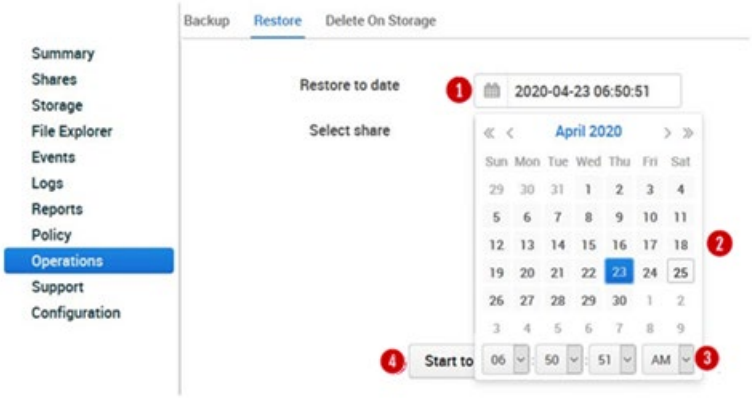
Step 5 – (Windows and Linux) In the HCP Gateway UI, navigate to the **Operations -> Restore** tab (Figure 17.5). Here you can enable the restore of **All** shares by turning on the **All Shares** option (Figure 17.5.1) or select **One** of the shares by turning on the option for that share (Figure 17.5.2).

Figure 17.5 – Operations > Restore



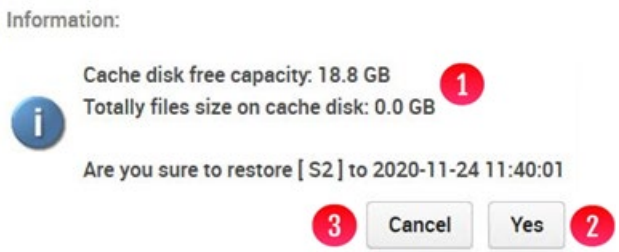
Step 6 – (Windows and Linux) Click the calendar icon in the **Restore to date** (Figure 17.6.1) so you can select the date (Figure 17.6.2) and the time (Figure 17.6.3) to restore to. Check the System Backup History (Figure 15.6) for a list of the available backups to restore from. If you don't pick the exact time the backup was completed, then the restore will use the last backup that was taken before the date and time you enter. The restore may not find the backup from a previous day, so pick the time on a day that a backup was run and completed. Click the **Start** button (Figure 17.6.4) to start the restore.

Figure 17.6 – Select Restore Date and Time



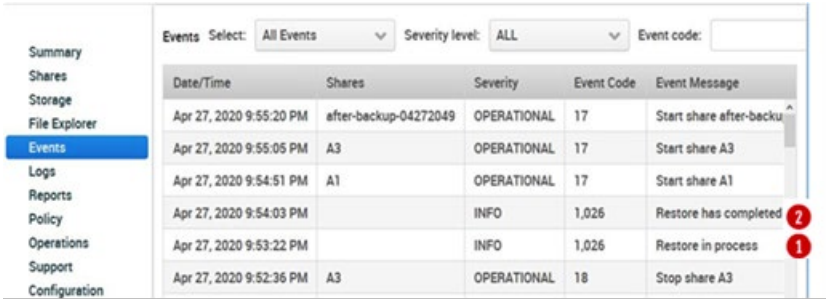
Step 7 – (Windows and Linux) Verify there is enough space in the cache for the restore to complete (Figure 17.7.1). Click the **Yes** button (Figure 17.7.2) to start the restore. Click the **Cancel** button (17.7.3) to cancel the restore.

Figure 17.7 – Confirm Starting Restore



Step 8 – (Windows and Linux) Depending on how many files are on the HCP Gateway share(s) will determine how long the restore process will take. You can monitor the status of the restore by checking the **Events** tab in the HCP Gateway UI (Figure 17.8). You will see an Event posted when the **Restore started** (Figure 17.8.1) and when the **Restore completed** (Figure 17.8.2).

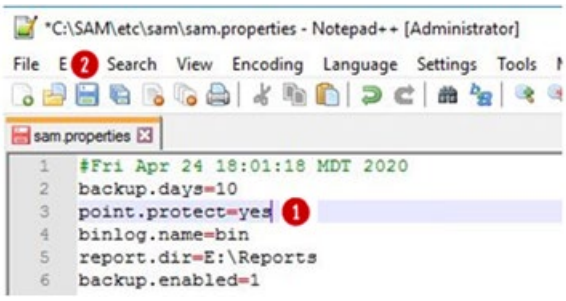
Figure 17.8 – Restore Events



Step 9 – (Windows only) With the restore process complete and the HCP Gateway cache folder renamed, use Notepad++ to edit the file **C:\SAM\etc\sam.properties** and configure the parameter **"point.protect=yes"** (Figure 17.9.1) to set the cache folder so it cannot be

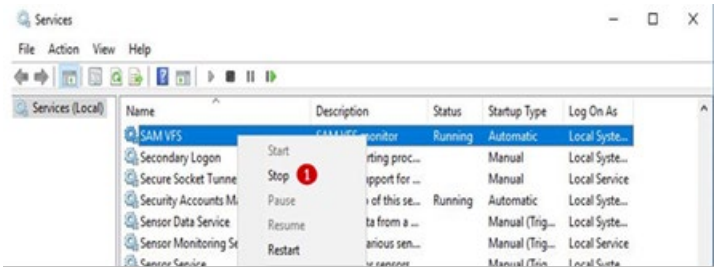
renamed, or you can remove the whole line that contains **"point.protect"**. Be sure to save the file by clicking the blue disk icon (Figure 17.9.2) before closing the Notepad++ application.

Figure 17.9 – Edit sam.properties file



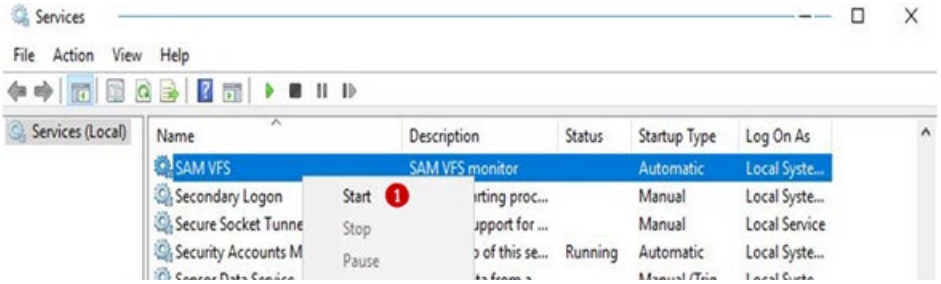
Step 10 - (Windows only) Stop the "SAM VFS" service. It is recommended to wait at least 5 minutes from the time the last file is ingested into HCP Gateway before stopping the "SAM VFS" service. Click on the Windows Start Menu located at the bottom left of the screen. Select the "Services" option. Navigate to the "SAM VFS" service, right-click on it and select **"Stop"** (Figure 17.10.1).

Figure 17.10 – Stop SAM VFS Service



Step 11 – (Windows only) Start the "SAM VFS" service. In the Windows "Services", navigate to the "SAM VFS" service, right-click on it and select **"Start"** (Figure 17.11.1).

Figure 17.11 – Start SAM VFS Service



Step 12 – In the HCP Gateway UI, navigate to the Shares tab. If you have more than 1 share and many files in the shares, it may take a few minutes before the shares that were not restored to show an **Active** Status. Once all the shares, except the share(s) that was/were restored, show an **Active** Status (Figure 17.12.1), then click the **Start** button (Figure 17.12.2) to start the share(s) that was/were restored.

Figure 17.12 – Start Share

WARNINGS:

1. Since the cache was renamed during the restore process, all of the file content is now only on the storage, for example, the HCP. Files will be recalled to the local cache based on the policy. All files are immediately readable. There is a brief 3-5 minute settling period after the file is recalled to the local cache if you are using a Server Mode Copy or Tiering Policy. During this period, to modify or overwrite an existing file will require using “Save As”. As an alternative, in Windows File Explorer, select all the files and folders at the top of the share(s) that was/were restored, right-click and select “Properties” so Windows will read the metadata for each file and start the 3-5 minute settling period. For Linux, the Linux NFS client caches the information about the folders and files on the client. In order to see the current state of the folders and files on a Linux share, you need to unmount (**umount**) and then remount (**mount**) the HCP Gateway share on the Linux NFS client.
2. Starting in HCP Gateway Windows version 4.1.3, when a file is read that is not stored in the cache, if the **Enable Cache** setting is enabled in the share, the file will remain in the cache until the **Cache High Watermark** setting is reached and the file is released from the cache. In addition, there is a new feature **Copy Files to Cache** in the HCP Gateway UI File Explorer that can be used to select all the files or a subset of files in the share from HCP Storage to Cache. See the **Copy Files to Cache** chapter for the details.

Each time the restore process is run, a copy of the cache folder is made on the **E: drive** (Windows) or **/storage/sam** (Linux). If available space on the drive becomes low, you can remove the renamed cache folders. Make sure you only remove the cache folders with a date and timestamp after the name. See Figures 17.13.1W, 17.13.2W and 17.13.3W for Windows and 17.13.1L for Linux examples.

Figure 17.13W – (Windows) Renamed cache folders

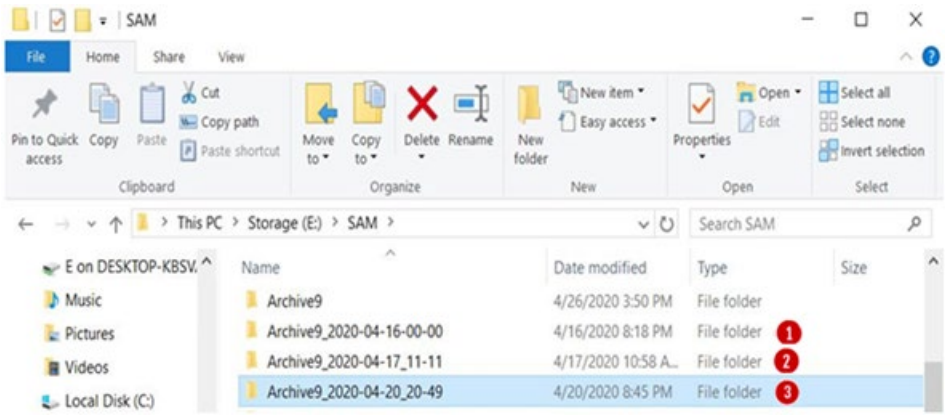


Figure 17.13L – (Linux) Renamed cache folders

```
vault@hcpg-linux-1:~$ ls -l /storage/sam
total 0
drwxrwxr-x 4 root  vault 27 Sep 15 15:19 archive1
drwxrwxr-x 3 root  vault 18 Sep 17 13:45 archive11
drwxrwxr-x 3 root  root  18 Sep 18 13:32 archive13
drwxrwxr-x 4 root  vault 27 Sep 18 09:49 archive13_2020-09-18_13-31 1
drwxrwxr-x 4 root  vault 27 Sep 16 11:07 archive3
drwxrwxr-x 4 root  vault 27 Sep 17 10:37 archive5
drwxrwxr-x 3 root  vault 18 Sep 16 11:27 archive7
drwxrwxr-x 4 root  vault 27 Sep 16 16:24 archive9
drwxrwxr-x 2 vault vault  6 Nov 20  2019 version
vault@hcpg-linux-1:~$
```

HCP Gateway Software Upgrade

These software upgrade steps do not apply for Linux.

18.1 Windows Upgrade Process

This section will cover the process to upgrade the HCP Gateway Windows software from any 4.1.x or later version to 4.2.0.7. Please contact Hitachi support if upgrading from a version before 4.1.4.

You will need to be logged into the HCP Gateway server as a local administrator to perform these steps. Generally, an upgrade is composed of 2 pieces of software, the UI which is in the file named **"hcpg-windows-ui-4.2.0_2022-01-30_02-47-01.war"** and the filter driver, also known as the **SAM VFS** service, which is in the file named **"HCPG-signed-4.2.0.msi"**. There will also be an updated copy of the **C:\SAM** folder in the folder named **"C_Drive_Files"** in the upgrade zip file. In addition, for the 4.2.0 upgrade, the MariaDB and Wildfly software must be upgraded.

There are database table changes in the 4.2.0 release that will cause the shares to take longer to start after the upgrade. How long depends on how many files are stored on the HCP Gateway, the more files on the Gateway, the longer the database updates will take. For perspective, the QA team experienced about 12 minutes for the database updates to take place on a share with 25 million files. Contact Hitachi Support for assistance running the database update scripts after upgrading the MariaDB database application to reduce the time for the shares to start after the upgrade.

A new license key will need to be generated and installed after upgrading to version 4.2.0. After the upgrade, please contact Hitachi Support to generate a new license key.

Occasionally there may be additional steps required to upgrade the HCP Gateway. The additional steps will be documented in the Release Notes for that release. Read the upgrade instructions in the Release Notes and use them in combination with the instructions in this chapter of the Administration Guide, as they may have additional steps to take at specific points of the upgrade.

NOTE:

After upgrading a single standalone HCP Gateway, manually start all of the shares in the HCP Gateway UI.

When upgrading a set HCP Gateways using database replication, it is recommended to upgrade the DR Gateway first, then manually start all of the shares in the Gateway UI on the DR Gateway. Then stop the shares in the DR Gateway. Then upgrade the primary Gateway and manually start all of the shares in the Gateway UI primary Gateway.

When upgrading a clustered pair of HCP Gateways, it is recommended to upgrade the non-active node (node 2) of the

cluster first. Then after the upgrade of node 2 is complete, failover the cluster from the active node (node 1) to the non-active node (node 2), stop and then start all of the shares in the Gateway UI on node2 and then upgrade node1. Then after the upgrade of node1 is complete, fail the cluster back from node 2 to node 1, then manually stop and start all of the shares in the Gateway UI on node1. On a 4-node cluster, upgrade the HCP Gateways at the DR site first, then repeat these steps with the 2 nodes in the cluster at the Primary site.

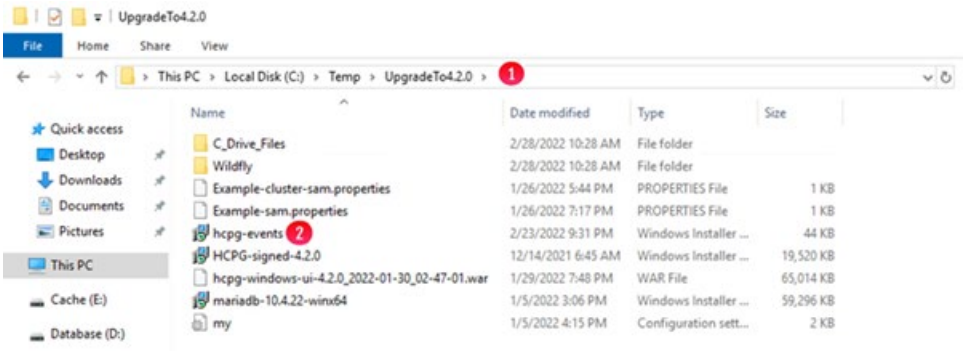
IMPORTANT WARNING: If upgrading from a version prior to 4.1.7, if there were access denied errors accessing files on the HCP Gateway shares, the Windows ICACLS command will need to be run on every folder and file on every share with access denied permissions on the HCP Gateway to add Full Control permissions for an account. The default account to add the permissions on is the local SYSTEM account, so that the HCP Gateway can properly access and process every file on the HCP Gateway regardless of the user permissions that are on the file. It is recommended to perform this action when the shares are not active, so this will cause a longer outage than usual to upgrade to this version.

IMPORTANT NOTE:

The Wildfly version 19 application supports TLS versions 1.2 and 1.3. Microsoft Internet Explorer does not support TLS version 1.3, so it cannot be used to access the HCP Gateway UI. Starting with HCP Gateway version 4.2.0, use a web browser such as Firefox to access the HCP Gateway UI.

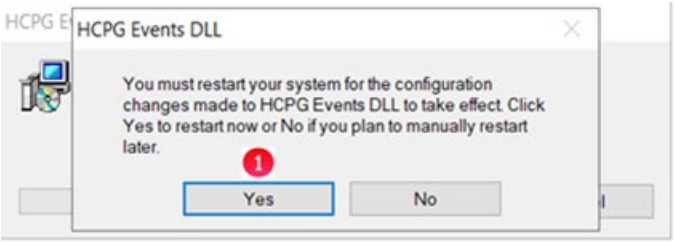
Step 1 – Logon to the HCP Gateway as a local Administrator. Copy the upgrade software zip file to the **C:\Temp** folder on the HCP Gateway server and unzip the file. If the **C:\Temp** folder does not exist, please create the folder, and copy the upgrade software zip file to it. Open a Windows File Explorer and navigate to the folder where the upgrade zip file was unzipped, **C:\Temp\UpgradeTo4.2.0** (Figure 18.1.1). Install the HCP Events add-on package by double-clicking on the **hcpg-events.msi** file (Figure 18.1.2).

Figure 18.1 – HCP Gateway Events Installer



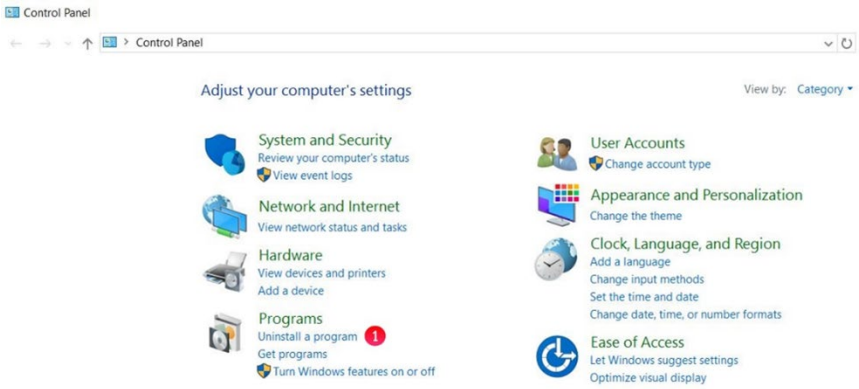
Step 2 – When prompted to restart the system, select **Yes** (Figure 18.2.1).

Figure 18.2 – HCP Gateway Events Installer Restart



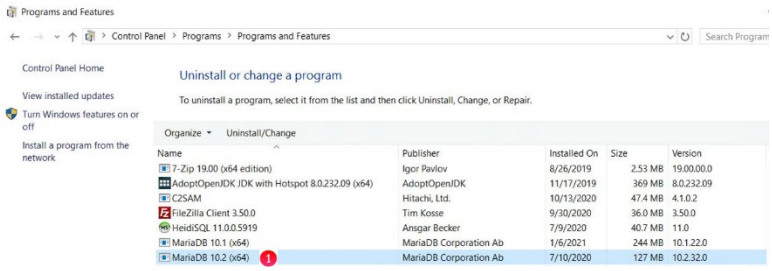
Step 3 – Logon to the HCP Gateway as a local Administrator. Check the version of MariaDB installed, it is required to be MariaDB version 10.4.22. If MariaDB 10.4.22 is not installed, then an upgrade to MariaDB 10.4.22 is required. Open Windows Control Panel, select **Uninstall a program** (Figure 18.3.1).

Figure 18.3 – Windows Control Panel



Step 4 – If MariaDB 10.2 is installed (Figure 18.4.1), it is required to follow the directions in **Chapter 30 Upgrade MariaDB 10.2 to 10.4** in this document to upgrade the MariaDB software. If MariaDB 10.4.21 or a lower version of MariaDB 10.4 is installed, it is required to follow the directions in **Chapter 31 Upgrade MariaDB 10.4.X to 10.4.22** in this document to upgrade the MariaDB software. After upgrading MariaDB to version 10.4.22 or if MariaDB 10.4.22 is already installed, continue with the next step, Step 5.

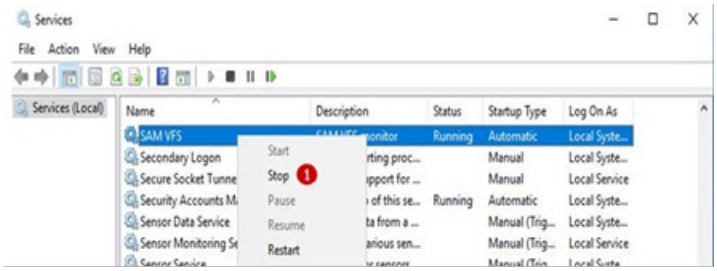
Figure 18.4 – MariaDB Version



Step 5 - Stop the “SAM VFS” service. It is recommended to wait at least 5 minutes from the time the last file is ingested into HCP Gateway before stopping the “SAM VFS” service. Select the Windows Start Menu located at the bottom left of the screen. Select the

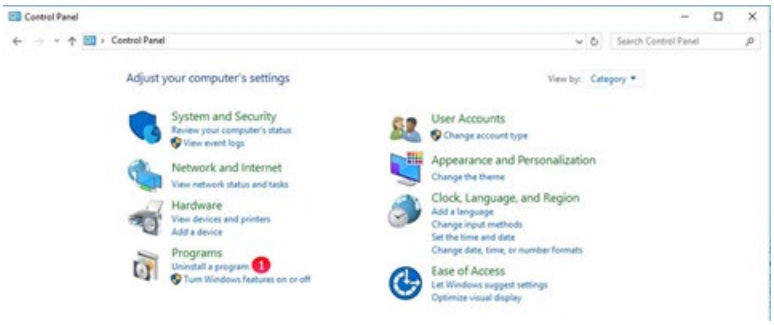
“Services” option. Navigate to the “SAM VFS” service, right-click on it and select **“Stop”** (Figure 18.5.1). Then close the Windows “Services” window.

Figure 18.5 – Stop SAM VFS Service



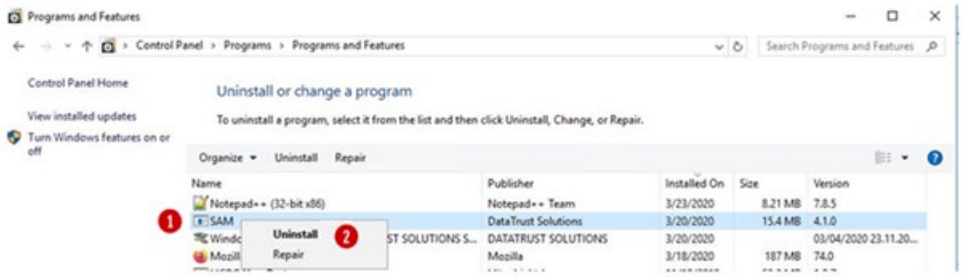
Step 6 - Now the old version of the **“SAM”** program needs to be uninstalled, for this example version 4.1.0. Select the Windows Start Menu located at the bottom left of the screen. Select the “Control Panel” icon. In the “Control Panel” window, under the “Programs” section, select **“Uninstall a program”** (Figure 18.6.1).

Figure 18.6 – Control Panel



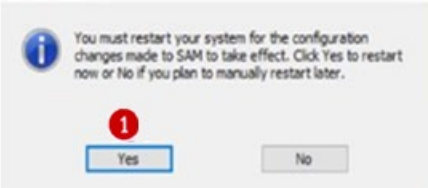
Step 7 – In the “Program and Features” window, right-click the **“SAM”** program (Figure 18.7.1) and select **“Uninstall”** (Figure 18.7.2).

Figure 18.7 – Uninstall Program



Step 8 – In the “Program and Features” window, select **“Yes”** to uninstall “SAM”. Close any other open windows except the “SAM” window. In the “SAM” window, when prompted to restart your system, select **“Yes”** (Figure 18.8.1).

Figure 18.8 – Restart Window



Step 9 – After the HCP Gateway reboots, log into the Windows OS as a local administrator user.

IMPORTANT STEP: In Windows File Explorer, rename the **C:\SAM\bin to C:\SAM\bin.<YYYY-MM-DD>**, the **C:\SAM\lib to C:\SAM\lib.<YYYY-MM-DD>**, the **C:\SAM\ps** to **C:\SAM\ps.<YYYY-MM-DD>** and the **C:\SAM\restore** folder to **C:\SAM\restore.<YYYY-MM-DD**.

NOTE:

If you receive an error that the **C:\SAM\lib** folder does not exist, just continue on with the rest of the instructions.

NOTE:

If you receive an error that the **C:\SAM** folder is open in another program, then stop the **Wildfly** service in Windows Services.

If you are installing from a software release upgrade package, then copy the folders from the release upgrade package in the **C:\Temp\UpgradeTo4.2.0\C_Drive_Files\SAM** folder to the **C:\SAM** folder on the HCP Gateway. Make sure to replace the existing files in the destination when doing the copy. If you stopped the Wildfly service at the beginning of this step, then start the **Wildfly** service in Windows Services.

Step 10 – Compare the contents of the **C:\SAM\etc\sam\sam.properties** file with the **"Example–sam.properties"** file in the folder that has the upgrade files to see if any new parameters were added to this version. If so, copy the new parameters from the **Example-sam.properties** to the **C:\SAM\etc\sam\sam.properties** file as described below.

When upgrading from a version before HCP Gateway Version 4.1.4 there is a new **registry.shares** parameter that needs to be added to the **C:\SAM\etc\sam\sam.properties** file.

- For a single standalone HCP Gateway, add the line **registry.shares=yes**. This will configure HCP Gateway to look in Windows Registry for the share configuration.
- For a clustered pair of HCP Gateways with a shared cache, add the line **registry.shares=yes** to both nodes of the cluster. This will configure HCP Gateway to look in Windows Registry for the share configuration.
- When using database replication with or without cluster, on the active node, add the line **registry.shares=yes**. On all of the other nodes that do not have a shared cache with the active node, add the line **registry.shares=no**. When using database replication without a shared cache, only 1 node can have this parameter set to **yes**.

IMPORTANT NOTE:

When using more than 1 HCP Gateway with database replication or more than 1 clustered pair of HCP Gateways, when the HCP Gateway active node is not available and the replica node becomes the active node, change the **registry.shares** parameter from **no** to **yes** on the new active node and restart the **SAM VFS** service. When the original active node then becomes available again and is promoted to the active node, change the **registry.shares** parameter from **yes** to **no** on the new passive replica node and restart the **SAM VFS** service.

When upgrading from a version before HCP Gateway Version 4.1.7 there is a new **sam.account** parameter that needs to be added to the **C:\SAM\etc\sam\sam.properties** file.

The default setting is to use the local System account, set **sam.account=SYSTEM**.

If there is a domain service account that has read/write access to all of the files on the Gateway, use that account for the **sam.account** parameter in the **C:\SAM\etc\sam\sam.properties** file.

IMPORTANT NOTE:

If the **sam.account** parameter is not added to the **C:\SAM\etc\sam\sam.properties** file, then the **SAM VFS** service will not start and an error **"sam.account setting is missing in configuration file"** will be entered into the **C:\SAM\var\log\sam\log-0.txt** file.

When upgrading from a version before HCP Gateway Version 4.1.9 there are 2 new parameters that can optionally be added to the **C:\SAM\etc\sam\sam.properties** file when directed by HCP Gateway support.

- **server.ip:**
  - This is used for any local services, sockets, it can be set to localhost, 127.0.0.1, or any valid IP address. Thrift clients can use this to connect to the local Thrift service.
  - Default value is 127.0.0.1

- **thrift.ip:**
  - This is used for the Thrift Server, it listens on the IP address, this can be localhost only 127.0.0.1 (default), a single IP, or a named interfaced like localhost.
  - Default value is 127.0.0.1

Make sure the changes are saved in the **C:\SAM\etc\sam\sam.properties** file.

NOTE:

Only IPv4 addresses are supported. If both IPv6 and IPv4 are enabled on the server, do not use "localhost" for

thrift.ip or server.ip. If thrift.ip is not set to 0.0.0.0, then thrift.ip MUST be the same as the server.ip. For example, thrift.ip=127.0.0.1 and server.ip=127.0.0.1.

When upgrading from a version before HCP Gateway Version 4.1.9 there is one modification and 2 new parameters that must be added to the **D:\MariaDB\data\my.ini** file. Please make the modification near the top of the file and add these parameters in the section with the other **replicate-wild-ignore-table** entries and save the changed file.

At the top of the file, change the section named **[mysqld]** to **[mariadb]**.

[client]

port=3306

plugin-dir=C:/Program Files/MariaDB 10.4/lib/plugin

[mysqld] **<= CHANGE THIS LINE to =>** [mariadb]

There are 4 options for updating the replication settings when upgrading a single HCP Gateway or a set of replication or clustered HCP Gateways.

Option 1) If upgrading a single HCP Gateway or in all configurations of HCP Gateway replication, when NOT using a cluster or a shared cache, add these 2 lines (Figures 18.9.1 and 18.9.2).

replicate-wild-ignore-table = SAM.archive_state

replicate-wild-ignore-table = sam.archive_state

Figure 18.9 – MariaDB my.ini file

```
replicate-wild-ignore-table = SAM.%event
replicate-wild-ignore-table = SAM.license
replicate-wild-ignore-table = SAM.archive_state  1

replicate-wild-ignore-table = sam.%event
replicate-wild-ignore-table = sam.license
replicate-wild-ignore-table = sam.archive_state  2
```

NOTE:

When upgrading a set HCP Gateways using database replication that are not in a clustered pair, it is recommended to upgrade the DR Gateway first, then after it reboots, manually start all of the shares in the Gateway UI on the DR Gateway. Note that you may need to open Windows Services and start the **SAM VFS** and **Wildfly** services if they were set to Startup Type Manual during the upgrade before you can login to the HCP Gateway UI and manually start all of the shares. Then stop all of the shares in the DR Gateway. Then upgrade the primary Gateway and after the primary Gateway reboots, manually start all of the shares in the Gateway UI on the primary Gateway.

Option 2) When using a pair of clustered Gateways with a shared cache, comment out any lines that include **archive_state** by adding the **#** character at the beginning of the line. Check the Database Replication Guide for additional information about tables to ignore from replication.

#replicate-wild-ignore-table = SAM.archive_state

#replicate-wild-ignore-table = sam.archive_state

Option 3) When using a pair of clustered Gateways with a shared cache in site A and a single Gateway in site B. Check the Database Replication Guide for additional information about tables to ignore from replication.

Add the following lines to the node1 in site A

node3.replicate-wild-ignore-table = SAM.archive_state

node3.replicate-wild-ignore-table = sam.archive_state

Add the following lines to the node2 in site A

node3.replicate-wild-ignore-table = SAM.archive_state

node3.replicate-wild-ignore-table = sam.archive_state

Add the following lines to the node3 in site B

node1.replicate-wild-ignore-table = SAM.archive_state

node2.replicate-wild-ignore-table = SAM.archive_state

node1.replicate-wild-ignore-table = sam.archive_state

node2.replicate-wild-ignore-table = sam.archive_state

NOTE:

When upgrading a clustered pair of HCP Gateways in Site A and a single HCP Gateway in Site B, it is recommended to upgrade the node is Site B first, then manually start and then stop all the shares. When upgrading the clustered pair of HCP Gateways in Site A, it is recommended to upgrade the non-active node (node 2) of the cluster first then manually start (or if the shares are already started, restart) all of the shares. Then after the upgrade of node 2 is complete, failover the cluster from the active node (node 1) to the non-active node (node 2) and then upgrade node1. Then after the upgrade of node1 is complete and node1 was rebooted, fail the cluster back from node 2 to node 1, then manually start (or if the shares are already started, restart) all of the shares in the Gateway UI on node1.

Option 4) When using a clustered set of 2 HCP Gateways in Site A and 2 HCP Gateways in Site B with database replication. Check the Database Replication Guide for additional information about tables to ignore from replication.

Add these 4 lines to the 2 cluster nodes, node1 and node2in the primary site A. Check the Database Replication Guide for additional information about tables to ignore from replication.

node3.replicate-wild-ignore-table = SAM.archive_state

node4.replicate-wild-ignore-table = SAM.archive_state

node3.replicate-wild-ignore-table = sam.archive_state

node4.replicate-wild-ignore-table = sam.archive_state

Add these 4 lines to the 2 cluster nodes, node3 and node4 in the DR site B

node1.replicate-wild-ignore-table = SAM.archive_state

node2.replicate-wild-ignore-table = SAM.archive_state

node1.replicate-wild-ignore-table = sam.archive_state

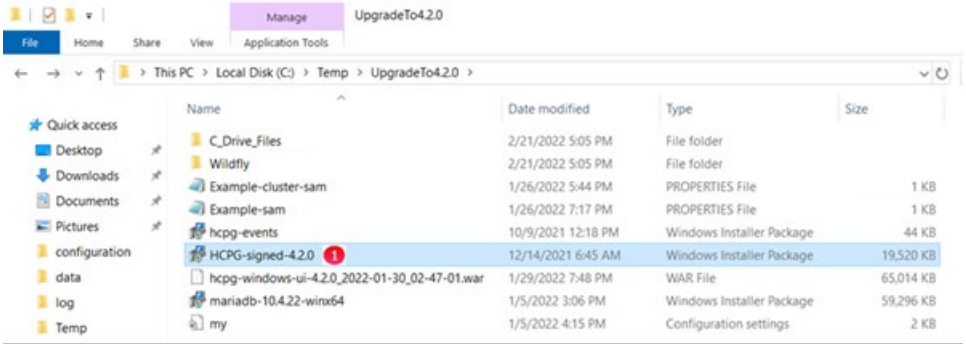
node2.replicate-wild-ignore-table = sam.archive_state

NOTE:

When upgrading a clustered pair of HCP Gateways, options 2 and 4 above, it is recommended to upgrade the non-active node (node 2) of the cluster first then manually start (or if the shares are already started, restart) all of the shares on node2. Then after the upgrade of node 2 is complete, failover the cluster from the active node (node 1) to the non-active node (node 2) and then upgrade node1. Then after the upgrade of node1 is complete and node1 was rebooted, fail the cluster back from node 2 to node 1, then manually start (or if the shares are already started, restart) all of the shares in the Gateway UI on node1. On a 4-node cluster, upgrade the HCP Gateways at the DR site first, then repeat these steps with the 2 nodes in the cluster at the Primary site.

Step 11 – In the Windows File Explorer where you downloaded the new version of the HCP Gateway software, double-click on the MSI file, for this example, **"HCPG-signed-4.2.0.msi"** file (Figure 18.10.1).

Figure 18.10 – Start MSI Installation

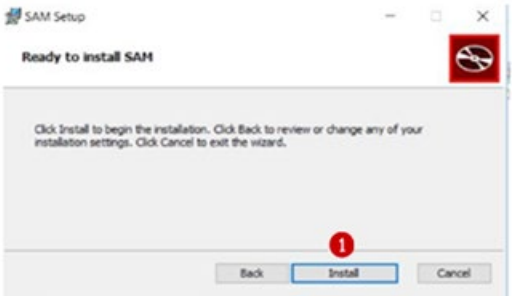


Step 12 – In the "SAM Setup" window select **"Next"** (Figure 18.11.1). In the "SAM Setup End-User License Agreement" window, select the box to accept the terms of the License Agreement then select **"Next"**. In the "SAM Setup Destination Folder" window, accept the default location "**C:\Program Files\SAM**" and select "**Next**".

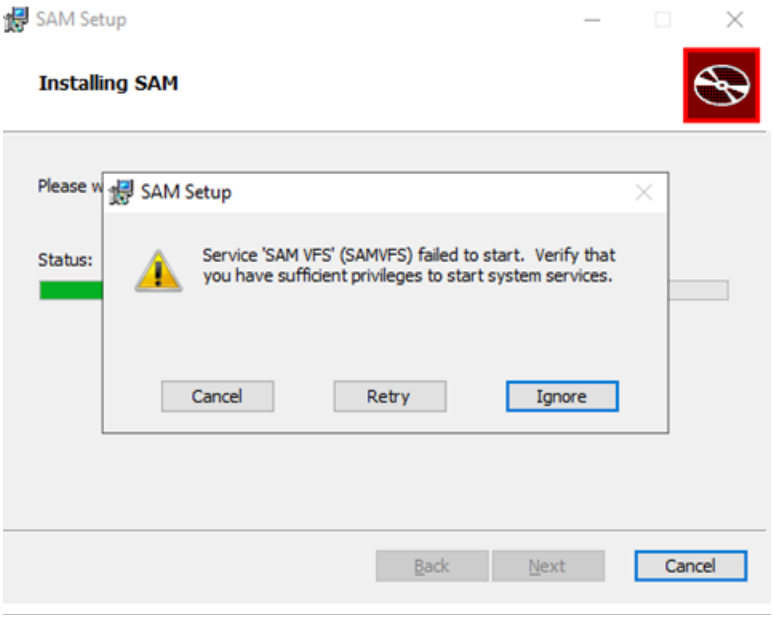
Figure 18.11 – SAM Setup

Step 13 – In the "SAM Setup Ready to Install SAM" window select **"Install"** (Figure 18.12.1).

Figure 18.12 – Ready to Install SAM

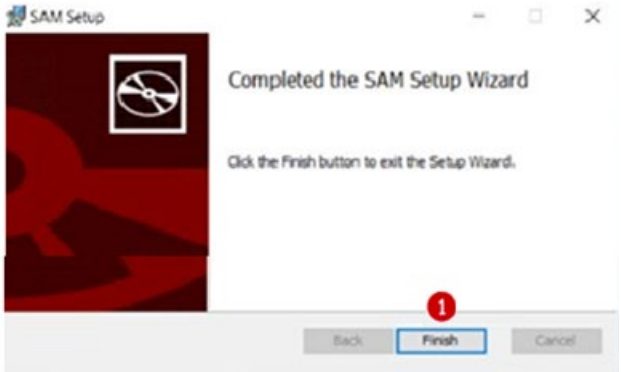


WARNING: If the following error is encountered, check that the sam.account parameter was added to the C:\SAM\etc\sam.properties file in Step 10. Note that if setting the sam.account parameter to something other than SYSTEM, then you will need to set it to SYSTEM during the upgrade and then change it back to the desired setting during Step 17.



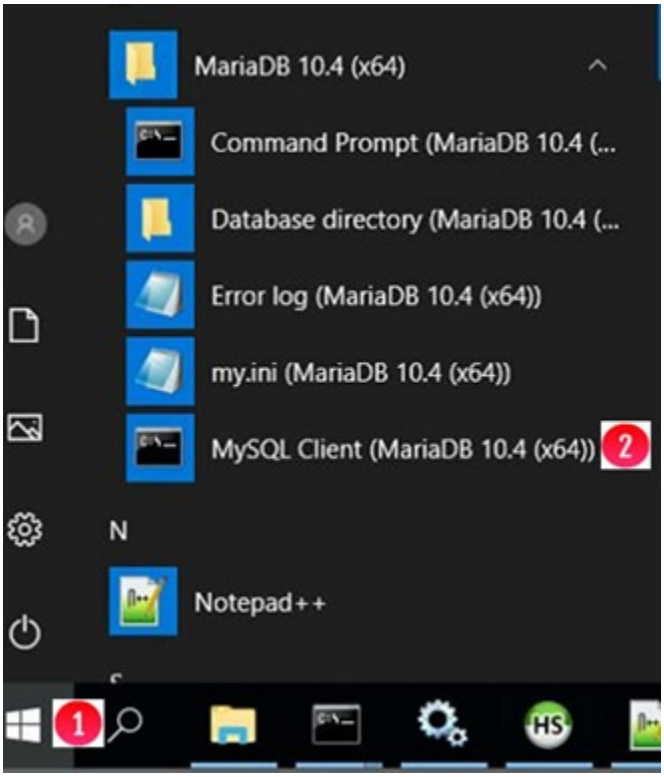
Step 14 – In the "SAM Setup Completed the SAM Setup Wizard" window select "**Finish**" (Figure 18.13.1). When prompted to reboot the server, do not select either **Yes** or **No** at this time. You will answer that prompt to reboot the server after the next few steps.

Figure 18.13 – Completed Install



Step 15 – When upgrading from a version before HCP Gateway Version 4.1.5, select the **Windows Start button** (Figure 18.14.1), then select **MySQL Client (MariaDB 10.X (x64))** (Figure 18.14.2). Otherwise, skip to Step 17.

Figure 18.14 – Open MySQL Client



Step 16 – This step is required to update the reports in the SAM database.

> **NOTE:**
>
> This step will delete any reports that were already generated. It will not delete the .csv files that contain the output of the reports that were already created and saved in the default location **E:\Reports**. Please check the parameter **report.dir** in the **C:\SAM\etc\sam\sam.properties** file for the actual location of the report output files.

When prompted, enter the database root password (Figure 18.15.1). Issue the command "**drop table SAM.report, SAM.report_status**;" (Figure 18.15.2). Issue the command "**exit**;" to close the MySQL Client (Figure 18.15.3). Close the **MySQL Client** window.

Figure 18.15 – Drop Table SAM.report

```
Administrator: MySQL Client (MariaDB 10.4 (x64))
Enter password: ********  1
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 12
Server version: 10.4.14-MariaDB-log mariadb.org binary distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> drop table SAM.report, SAM.report_status;  2
Query OK, 0 rows affected (0.121 sec)

MariaDB [(none)]> exit;  3
Bye

C:\Program Files\MariaDB 10.4\bin>_
```

Step 17 – Open the **Windows Services** panel, right-click on the **SAM VFS** service (if Windows services is already open, you may need to refresh the window to see the **SAM VFS** service) select **Properties** and set the **Startup Type** (Figure 18.16.1) to **Automatic (Delayed Start)**. This will delay the start of the **SAM VFS** service until all of the other Windows services start. Select **OK** (Figure 18.16.2) to save the configuration.

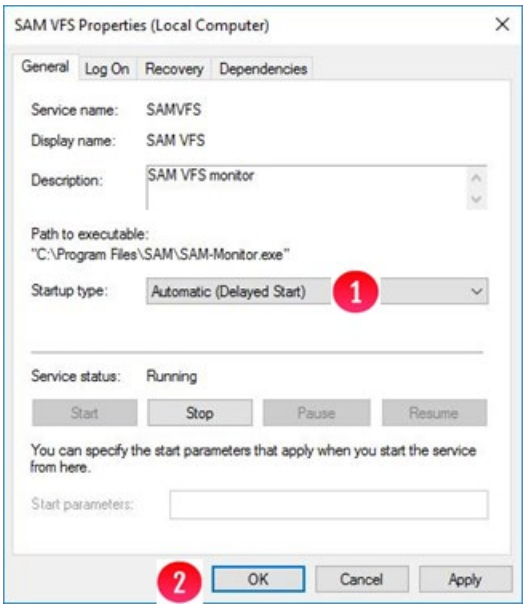
NOTE:

When upgrading an HCP Gateway cluster node, set the **SAM VFS Startup Type** to **Manual**.

NOTE:

When upgrading a set of HCP Gateways with database replication, it is recommended to set the Windows **SAM VFS** and **Wildfly** services **Startup type** on the non-active node(s) to **Manual** so they won't start when the Gateway is rebooted.

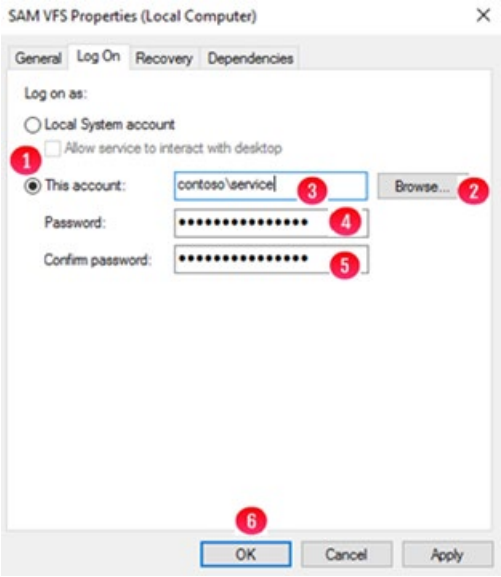
Figure 18.16 – Windows Services SAM VFS Properties



In the **Windows Services** panel, right-click on the **SAM VFS** service, select **Properties**, then select **Log On** and select or enter the account that will run the SAM VFS service. This account must match the **sam.account** parameter entered in the **C:\SAM\etc\sam\sam.properties** file in Step 10 above. The default is the **Local System** account (Figure 18.17.1) and should be used for most use cases. Select **OK** (Figure 18.17.2) to save the configuration and go to the next step. If using a domain service account that has access permissions to all of the files, select **This account** (Figure 18.18.1) and use **Browse** (Figure 18.18.2) or enter the account name (Figure 18.18.3) and enter the password (Figure 18.18.4) and confirm the password (Figure 18.18.5). Select **OK** (Figure 18.18.6) to save the configuration.

Figure 18.17 – Windows Services SAM VFS System Account Log On

Figure 18.18 – Windows Services SAM VFS Domain Account Log On



Step 18 – If you received access denied errors on folders and files on shares on the HCP Gateway, when upgrading from a HCP Gateway version before 4.1.7, open a Windows Command Prompt as Administrator and set the permissions for the user running the **SAM VFS** service on the files on the HCP Gateway. When using the default account **SYSTEM**, issue the following Windows commands. At the end of each command, the expected end result is listed below the command for this example.

> **NOTE:**
>
> If this is a Windows Cluster node, only on the active node, in the Failover Cluster Manager, stop the SAM VFS role and replace the E:\ with G:\ in the ICACLS commands below. **You do not need to run the ICACLS commands on both nodes, just the active node**. After the ICACLS commands complete, start the SAM VFS role on the active node.

ICACLS \\?\E:\ /GRANT SYSTEM:(CI)(OI)F

processed file: E:\

Successfully processed 1 files; Failed processing 0 files

ICACLS \\?\E:\SAM /GRANT SYSTEM:(CI)(OI)F /T

Successfully processed 8794 files; Failed processing 0 files

ICACLS \\?\E:\SAM_LINK /GRANT SYSTEM:(CI)(OI)F /T

Successfully processed 34 files; Failed processing 0 files

When using the a domain account, for example **contoso\service**, issue the following Windows commands (note that if this is a Windows Cluster node, replace the **E:** with **G:**). At the end of each command, the expected end result is listed below the command for this example.

ICACLS \\?\E:\ /GRANT contoso\service:(CI)(OI)F

processed file: E:\

Successfully processed 1 files; Failed processing 0 files

ICACLS \\?\E:\SAM /GRANT contoso\service:(CI)(OI)F /T

Successfully processed 8794 files; Failed processing 0 files

ICACLS \\?\E:\SAM_LINK /GRANT contoso\service:(CI)(OI)F /T

Successfully processed 34 files; Failed processing 0 files

NOTE:

If ICACLS returns access denied errors, then open a Windows Powershell as Administrator and issue the following command (replace E:\SAM with the name of the folder that had the access denied errors)

takeown /a /r /d Y /f E:\SAM

Step 19 – If there were additional steps to run after the upgrade in the Release Notes, follow those instructions now. Make sure all other windows, like Windows File Explorer, Windows Services, Control Panel, etc. are closed. In the **"SAM Setup"** window from Step 14, when prompted to restart your system, select **"Yes"** (Figure 18.19.1) to restart the HCP Gateway server.

Figure 18.19 – Windows Restart

Step 20 – **IMPORTANT NOTE:** The upgrade to HCP Gateway version 4.2.0 requires upgrading the Wildfly application to version 19. It is **required** to follow the instructions in **Chapter 32 Upgrade Wildfly to Version 19** to upgrade the Wildfly application.

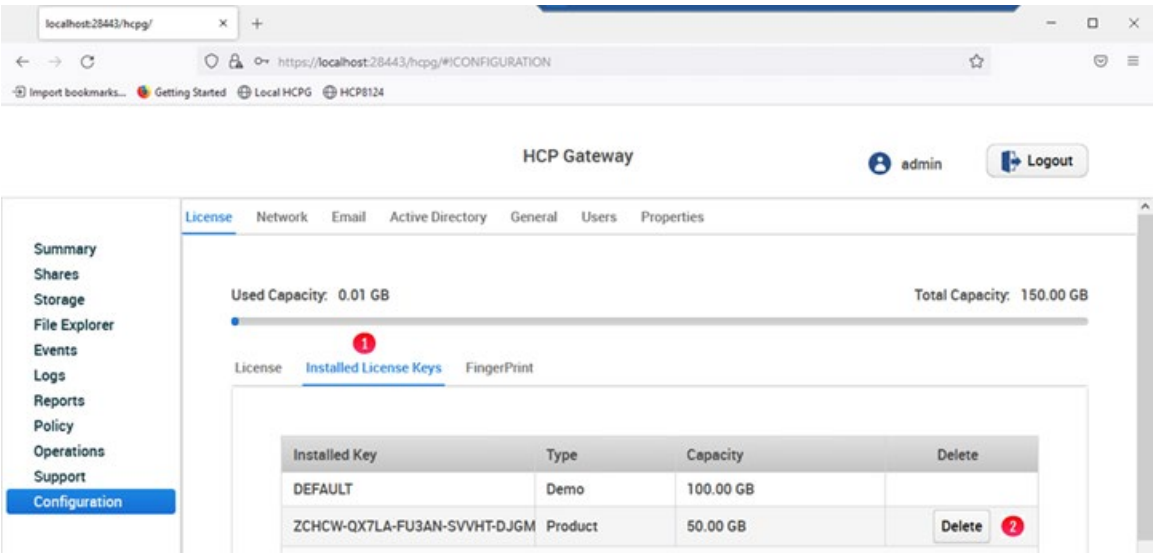
Step 21 – After upgrading a single standalone HCP Gateway, manually start all of the shares in the HCP Gateway UI Shares page. Note that with the Wildfly service set to delayed start, it will take a couple minutes for the HCP Gateway UI to become available. Please refer to Step 10 above for instructions when to manually start all of the shares in the HCP Gateway UI when upgrading a replication or clustered set of HCP Gateways.

Step 22 – After upgrading the Wildfly application to version 19, open a web browser such as Firefox, navigate to the **Configuration -> Installed License Keys** page (Figure 18.20.1) and delete the license key (Figure 18.20.2).

IMPORTANT NOTE:

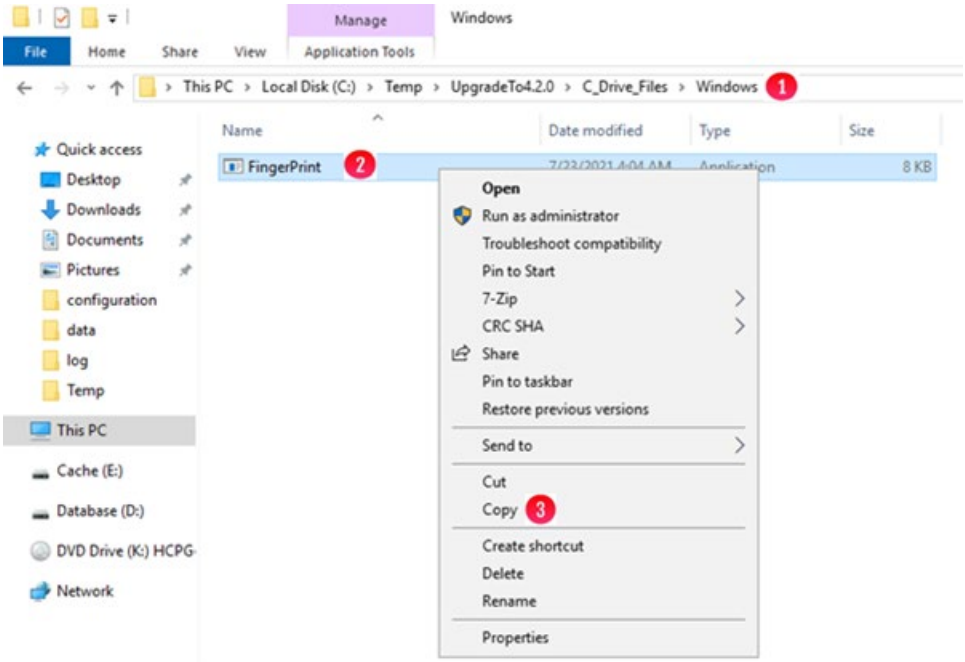
Close all web browsers to make sure nothing is cached in a web browser when the Digital Fingerprint is calculated in Step 25.

Figure 18.20 – Delete License Key



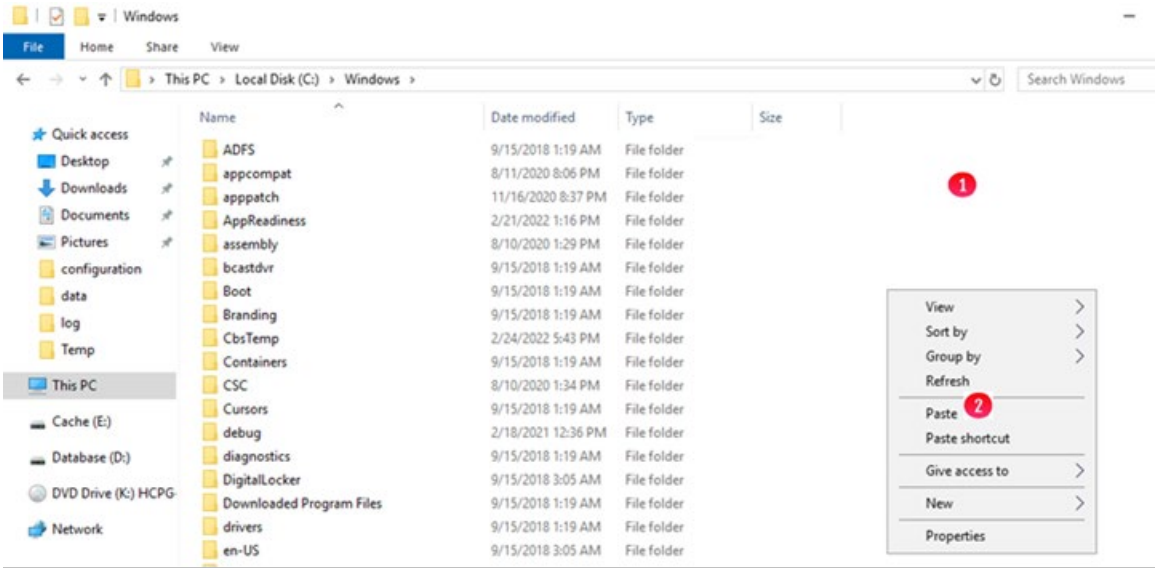
Step 23 – Open a Windows File Explorer and navigate to the **C_Drive_Files\Windows** in the folder where the upgrade zip file was unzipped, for this example, **C:\Temp\UpgradeTo4.2.0\C_Drive_Files\Windows** (Figure 18.21.1) right-click on the file **FingerPrint.exe** (Figure 18.21.2) and select **Copy** (Figure 18.21.3).

Figure 18.21 – Copy FingerPrint.exe File



Step 24 – In the Windows File Explorer, navigate to the **C:\Windows** folder and in the white space to the right of the folder names, right-click and select **Paste** (Figure 18.22.1). When prompted, select **Replace the file in the destination**. Open Windows Services and stop the **SAM VFS** service and then start the **SAM VFS** service.

Figure 18.22 – Paste FingerPrint.exe File



Step 25 – Open a web browser such as Firefox, navigate to the **Configuration -> License -> FingerPrint** page (Figure 18.23.1) and send the **Server FingerPrint** (Figure 18.23.2) to Hitachi support so they can generate a new license key. Once the new license key is received, navigate to the **Configuration -> License** page (Figure 18.24.1), enter the new license key (Figure 18.24.2) and select **Submit** (Figure 18.24.3).

Figure 18.23 – Server FingerPrint

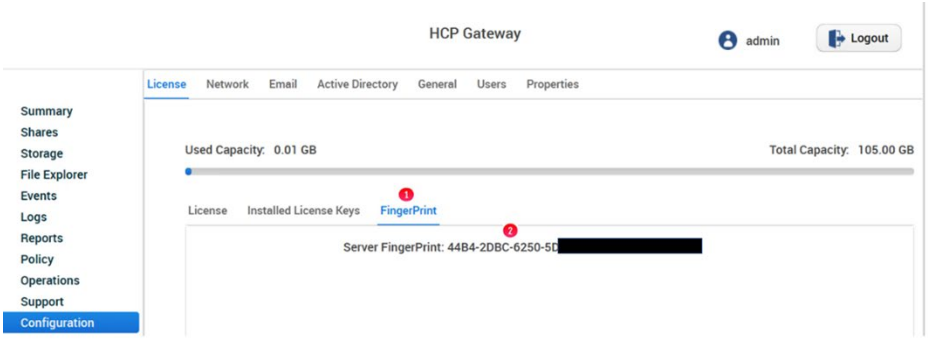
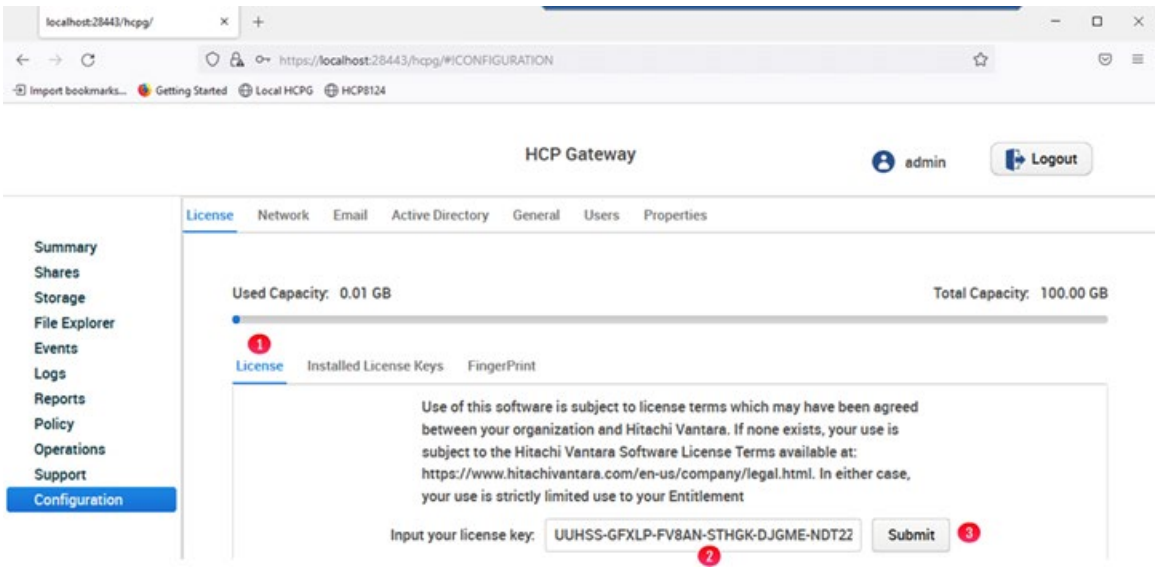
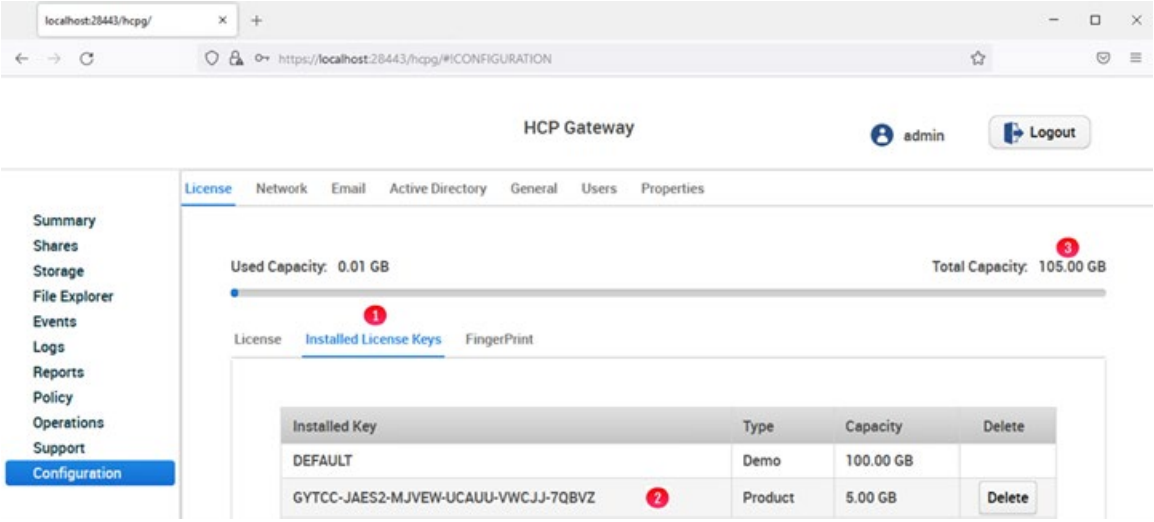


Figure 18.24 – Install New License Key



Step 26 –In the web browser such as Firefox, navigate to the **Configuration -> License -> Installed License Keys** page (Figure 18.25.1) to verify the new license key was installed (Figure 18.25.2) and the Total Capacity of the license increased by the capacity of the new license key (Figure 18.25.3).

Figure 18.25 – New License Key Installed



18.2 Windows Upgrade Backout Process

This section will cover the process to backout an upgrade of the HCP Gateway Windows software from version 4.2.0 to any 4.1.x version, for this example, version 4.1.5. The backout process is almost identical to the upgrade process. Refer to the steps in Section 18.1 above for assistance with any of the steps below.

You will need to be logged into the HCP Gateway server as a local administrator to perform these steps. Generally, an upgrade is composed of 2 pieces of software, the UI which is in the file named “hcpg-windows-ui-X.X.X.X.war” and the filter driver, also known as the “SAM VFS” service, which is in the file named “HCPG-X.X.X.X-signed.msi”. There will also be an updated copy of the “SAM” folder. Copy the upgrade software zip file of the old release to backout to the C:\Temp folder on the HCP Gateway server and unzip the file.

Below are the steps (time estimates are dependent on the hardware configuration and workload on the server):

1. (2 Mins) In the HCP Gateway UI (https://localhost:28443/hcpg), stop all the shares.
2. (2 Mins) In Windows Services, stop the SAM VFS, Wildfly and MySQL services.
3. (5 Mins) In Windows Control Panel -> Programs, uninstall SAM and reboot the server.
4. (5 Mins) Rename the C:\SAM folder to C:\SAM-4.2.0 (if an error occurs stating it cannot be done because another application is using the folder go to Windows Services and stop Wildfly).
5. (1 Mins) Copy the folders and files from the SAM folder in the previous version of the HCP Gateway install package in <unzipped location>\<HCPGWversion>\SAM to the C:\SAM.
6. (1 Mins) Copy the sam.properties file from the renamed directory in step 4 (C:\SAM-4.1.7\etc\sam folder) to C:\SAM\etc\sam.
7. (1 Mins) Install the HCPG-4.1.X.X-signed.msi from the old version 4.1.X.X HCP Gateway install package in <unzipped location>\<HCPGWversion>\, do not reboot, but leave the popup to reboot open.
8. (3 Mins) If the Windows Wildfly service is stopped, you must start it before this step.

   a. Open the Firefox or another web browser
   b. Go to the Wildfly Management Console (https://localhost:28443) -> Deployments
   c. Undeploy the existing 4.2.0 war file
   d. Deploy the old version hcpg-windows-ui-4.1.X.X.war from the old version 4.1.X.X HCP Gateway install package <unzipped location>\<HCPGWversion>\
   e. Change the Runtime name to hcpg.war
   f. Enable the war file
   g. Close the Firefox or other web browser
9. (5 Mins) Find the popup to reboot from Step 7 and click Yes to reboot the system.

HCP Gateway Database Replication

Replicating the MariaDB database is required when deploying Fail-over Clustering in Windows or when a production HCP Gateway needs to keep an HCP Gateway at a local and DR site synchronized with a DR HCP. Prior to configuring the database replication, verify that the HCP Gateway Version is version 4.1 or higher by navigating to the **Operations -> Support** tab in the HCP Gateway UI. This chapter is divided into two parts: Configuring Replication and Troubleshooting Database. You should only need to run the Configuring Replication section, unless you have issues, then you can run through the Troubleshooting Database Replication section.

WARNING: Do not cut and paste text from this document directly into a Windows or Linux HCP Gateway server. It is required to first copy the text to a Windows Notepad to remove any formatting, before copying from the Windows Notepad to the final destination.

IMPORTANT NOTE:

HeidiSQL and Dbeaver are GUI applications that can be used as a front-end for the MySQL CLI. HeidiSQL can be downloaded from https://www.heidisql.com/download.php and DBeaver can be downloaded from https://dbeaver.io

A. Configuring Replication

Please refer to the HCP Gateway Windows or Linux Database Replication Setup Guide for the details on configuring replication based on the customer requirements.

B. Troubleshooting Database Replication

Replication between HCP Gateway nodes is set to Master to Master. When replication from one HCP Gateway to another node fails there are three ways to recover:

1. Restart the Node that is out of sync
2. Manual Reset
3. Restore the database

About 90% of the time just restarting the Node will force the databases to resync.

The second option is a manual reset of the replication configuration.

Please refer Steps 3 through 6 of the Replication Use Case Chapter in the Windows or Linux DB Replication Guide for the details on resynching the replication.

For the third option, if Node 1 is out of service and not recoverable then the HCP Gateway software will have to be reinstalled and the database can be restored to the last backup. Contact Hitachi Vantara support for assistance. After the Node 1 is operational the databases will sync with Node 2 and the recovery process is done.

Antivirus Scanning

Antivirus (AV) scanning will impact performance of the HCP Gateway in normal usage. It can make the system inoperable if it is allowed to recall files from HCP. Therefore, we recommend using AV software that DOES NOT RECALL Offline files. Since Anti-Virus is mostly run on Windows servers, the main change for Linux is to exclude the OS, Database and Virtual File System filesystems from any scanning.

- **Sophos** has an option to prevent recalling offline files.
- **Windows Defender** does not have configurable setting for offline files, however in testing it ignored offline files and did not recall them for scanning.

If you have questions about a specific Antivirus software application, contact the Antivirus software vendor to see if they support not recalling offline files.

Which Directories can be scanned?

In Windows, the C:\ and D:\ drives should **never** be scanned since they only have the OS and database. The E:\ drive contains the virtual file system and the cache. The F: drive contains the local storage. Select folders on E:\ drive and all folders on the F: drive can be scanned.

In Linux, the "/" (root) filesystem and /var/lib/mysql filesystems should **never** be scanned since they only have the OS and database. The /storage filesystem contains the virtual file system, the cache, and the local storage. Select folders on the /storage filesystem can be scanned.

Antivirus software needs to **exclude** the following Windows directories from AV scanning to avoid issue with the HCP Gateway operation and to avoid recalling offline files:

C:\opt

C:\SAM

C:\Program Files\Eclipse Adoptium

C:\Program Files\SAM

C:\Program Files\MariaDB 10.4

D:\MariaDB

D:\Temp

E:\Backup (G:\Backup when using clustered Gateways)

E:\cache (G:\cache when using clustered Gateways)

E:\Reports (G:\Reports when using clustered Gateways)

E:\Restore (G:\Restore when using clustered Gateways)

E:\SAM (G:\SAM when using clustered Gateways)

E:\SAM_Link (G:\SAM_Link when using clustered Gateways)

Antivirus software needs to **exclude** the following Linux filesystems from AV scanning to avoid issue with the HCP Gateway operation and to avoid recalling offline files:

/ - the root filesystem

/var/lib/mysql

/tmp

/storage/Backup

/storage/sam

In Windows, only the following directories contain data files and could be scanned with AV software:

- **F:\Storage** – directory can be scanned when using any AV software. This directory is used only if you have an additional copy of the data on local HCP Gateway storage.

In Linux, only the following directories contain data files and could be scanned with AV software:

- **/storage/local** – directory can be scanned when using any AV software. This directory is used only if you have an additional copy of the data on local HCP Gateway storage.

Windows Sophos AV Software

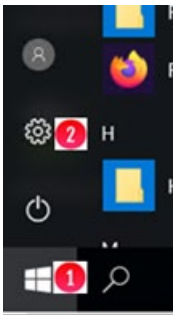
Here is an example for Sophos AV software setup:

1. Have the HCP Gateway VFS service, the executable is "C:\Program Files\SAM\SAM-Monitor.exe" excluded in Sophos in the Scanning Exclusions in the Threat Protection Policy for the HCP Gateway server.
2. Have the Wildfly service, the executable is "C:\opt\wildfly-XX.0.0.Final\bin\service\amd64\wildfly-service.exe" excluded in Sophos in the scanning. Exclusions in the Threat Protection Policy for the HCP Gateway server.
3. Enable option to exclude offline files.
4. Exclude the SAVOnAccess and Sophos Endpoint Defense filter drivers from the whole E:\ drive (data storage).
5. Only select folders noted above should be scanned on the E:\ drive.

Windows Defender Software

1. Does not have a setting for excluding offline files, but in our testing, it ignored offline files.
2. Only select folders noted above should be scanned on the E:\ drive.
3. Select the **Window Start button** (Figure 20.1.1) and select **Settings** (Figure 20.1.2).

Figure 20.1 - Windows Settings

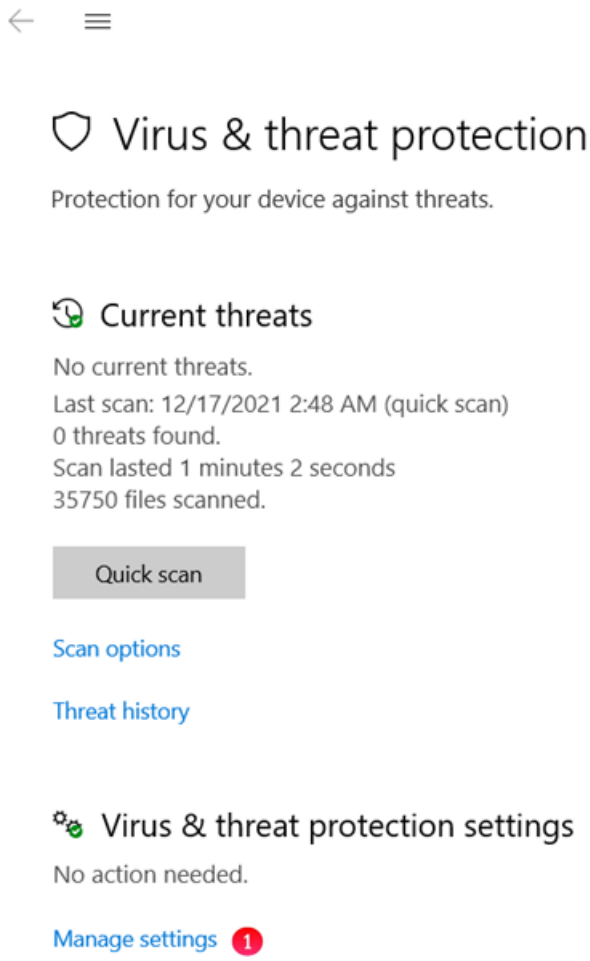


4. In Settings, enter **Virus** (Figure 20.2.1) then select **Virus & threat protection** (Figure 20.2.2).

Figure 20.2 - Virus Settings

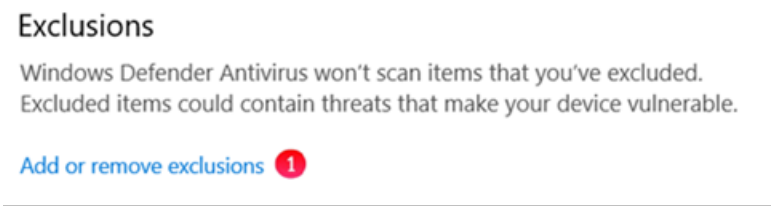
5. In **Virus & threat protection settings**, select **Manage settings** (Figure 20.3.1).

Figure 20.3 - Manage Settings



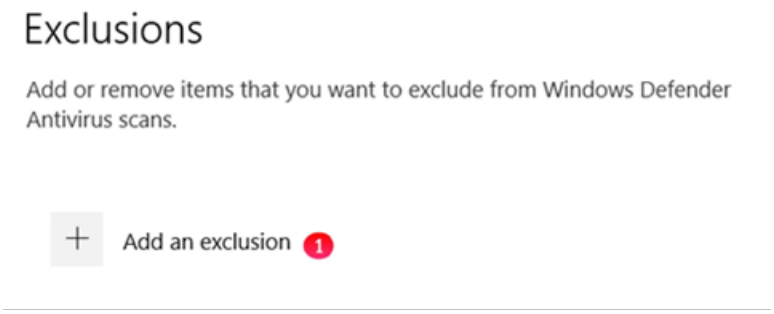
6. In Exclusions, select **Add or remove exclusions** (Figure 20.4.1).

Figure 20.4 - Add exclusions



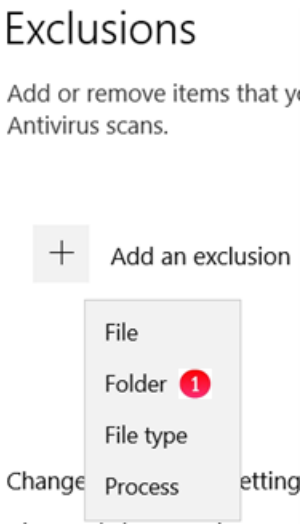
7. In Exclusions, select **Add an exclusion** (Figure 20.5.1).

Figure 20.5 - Add an exclusion



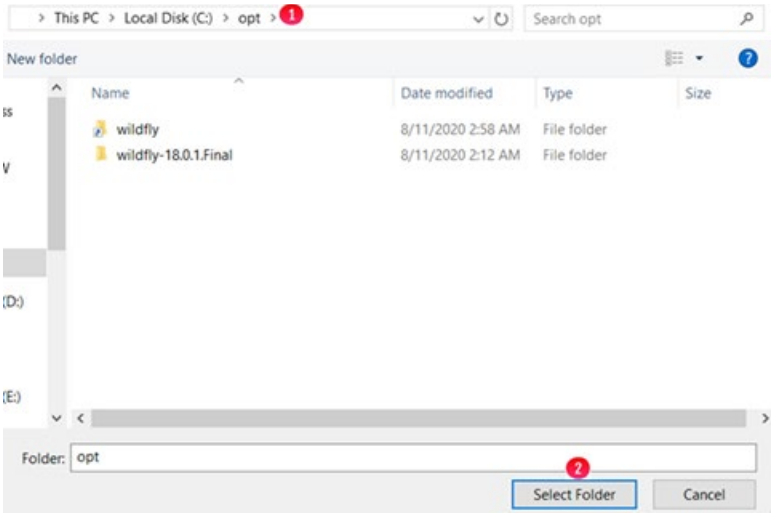
8. In Exclusions, select **Folder** (Figure 20.6.1).

Figure 20.6 - Add an exclusion



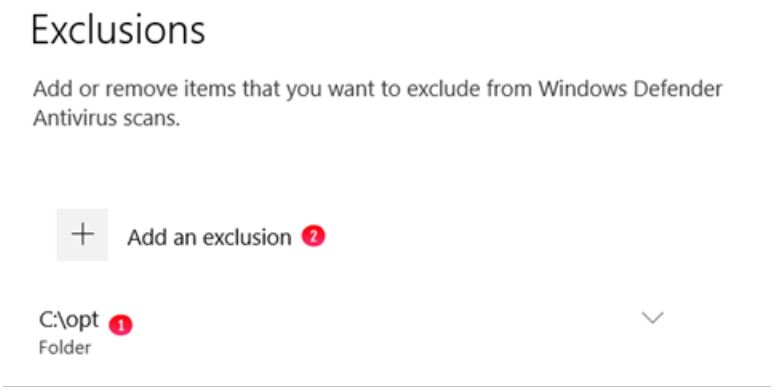
9. In the Windows File Explorer that opens, select a folder from the list above (Figure 20.7.1), for this example **C:\opt**. Select **Select Folder** (Figure 20.7.2).

Figure 20.7 - Select Folder



10. Notice that the **C:\opt** folder is now excluded (Figure 20.8.1). Select **Add an exclusion** (Figure 20.8.2) and repeat Steps 8 and 9 for all of the folders in the list above.

Figure 20.8 - Select Folder



Disaster Recovery

This covers the most common HCP Gateway deployment configurations and the disaster recovery process for each. It is not going to cover complex scenarios like daisy chaining Fail-over clusters across many sites. The three most common HGP Gateway configurations are:

- Standalone HCP Gateway
- Replicated HCP Gateway Pair
- Fail-over Cluster

Each option will be covered independently below.

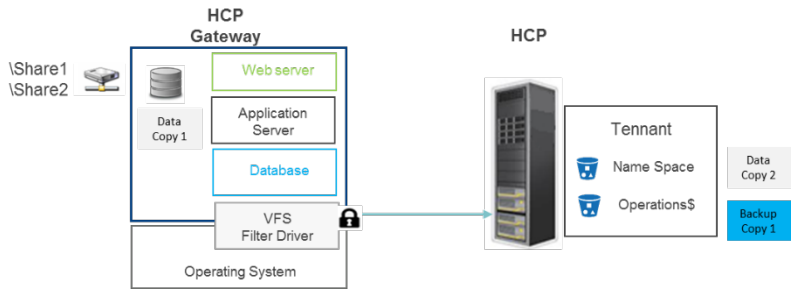
Note:

LACP is supported with HCP Gateway networking. Verify that the Gateway has the current versions of the Intel Chipset and NIC drivers installed. The latest version of the Chipset Driver is located at http://ctoportal.hitachivantara.com/hdsctoinfo/index.php?title=HCP

A. Standalone HCP Gateway

As the name suggests this is the most basic option with HCP Gateway using HCP for storage (Figure 21.1). It is assumed that the HCP is protecting the data, so we will focus on protecting the HCP Gateway configuration, Virtual File System, and the Policy settings. These items are contained in the database and configuration files, so both must be protected.

Figure 21.1 – Standalone HCP Gateway



These items can be protected using the internal backup utility or using a 3rd party backup application. The internal backup utility is found in the **Operations -> Backup** page of the HCP Gateway UI. This utility backs up the database and configuration files to a local drive, network drive or to a share configured to archive to the HCP. It is best practice to use the HCP option. The internal backup utility can be set to run multiple times per day to minimize the potential for data loss.

If the HCP Gateway software is operational then recovering the system is automated. In the HCP Gateway UI go to the **Operations -> Restore** page and follow the instructions in the **Recover from Backup** chapter. If the HCP Gateway installation was lost then a new HCP Gateway must be installed, configured for networking, software license applied and then the Restore operations can be followed from the **Restore HCP Gateway to a Different Server** chapter.

Suppose a network share was used for backup and it was lost in the natural disaster too. Then you should contact Support and after a new HCP Gateway instance is installed and IP assigned then we can reconstruct the Shares by recovering the meta data from the object headers in the HCP at the DR site.

B. Replicated HCP Gateways

In this configuration (Figure 21.2) one HCP Gateway is replicating its database, which contains the virtual file system, to another HCP Gateway. The two HCP Gateways are typically at different locations (Figure 21.2); however, they could be at the same location (Figure 21.3). One HCP Gateway is active and designated as the primary and all traffic gets routed to it. The second HCP Gateway is in a passive state or in standby mode. The database replication keeps the second HCP Gateway up to date and ready to take over when required.

Figure 21.2 – Replicated Standalone HCP Gateway Multi- site

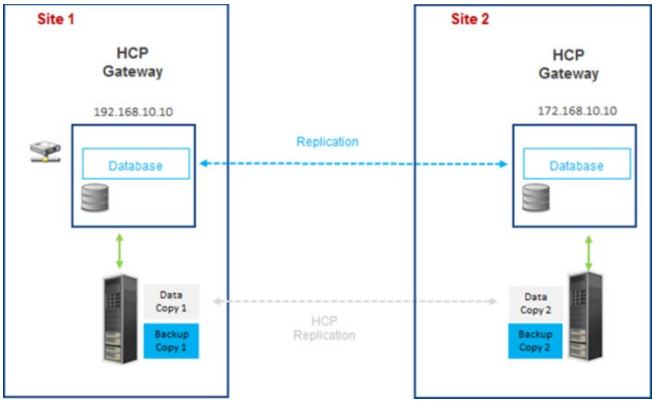
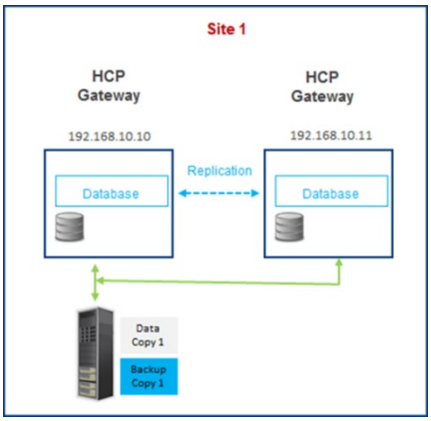


Figure 21.3 – Replicated Standalone HCP Gateway Single site

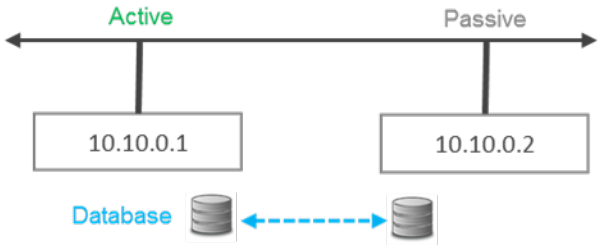


Prior to discussing fail-over and recovery processes we need to discuss networking. This section provides some basic networking options to consider. Your Network team will most likely have a strategy to provide HA for your HCP Gateway systems. The three basic networking and recovery options are:

- Independent IP Addresses with manual fail-over
- Automatic DNS Failover with Redundancy
- HA Proxy using shared IP addresses

1. **Independent IP Addresses with manual failover**
   This is the simplest networking option as each HCP Gateway (Figure 21.4) is configured with a different fixed IP address. Users and applications only have access to the primary IP address (10.10.0.1). If the active gateway were to crash and not be available the IT team would most likely be alerted by their clients. They could then manually change configurations over to the passive node (Ex. 10.0.0.2) making it the active node.

Figure 21.4 – Manual Failover

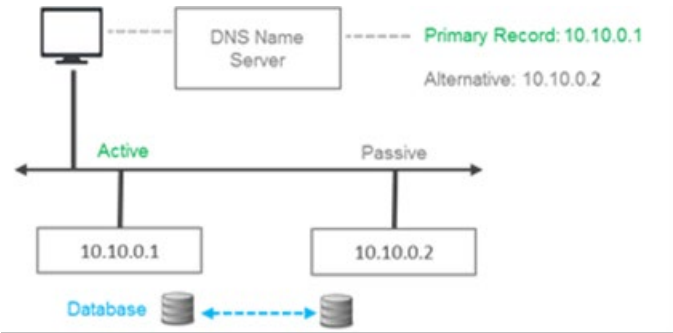


The advantage of this approach is it is simple to implement, requires minimal IT skills and no additional network equipment. The downside is that there will be outages and the transition period will be the longest of the three options.

2. **Automatic DNS Failover with Redundancy**
   This method introduces automation by leveraging DNS capabilities (Figure 21.5) for dynamically changing endpoints. With DNS Failover enabled if the gateway with the primary IP address is unavailable, then users would be pointed to a backup gateway's IP address. To implement failover on the server side, you'll need to monitor all the servers listed in the DNS records—the primary server and additional redundant servers. The DNS TTL setting determines how often a server is checked. If the primary server goes down, the DNS server should automatically switch the DNS A record to list the IP address for the working server first.

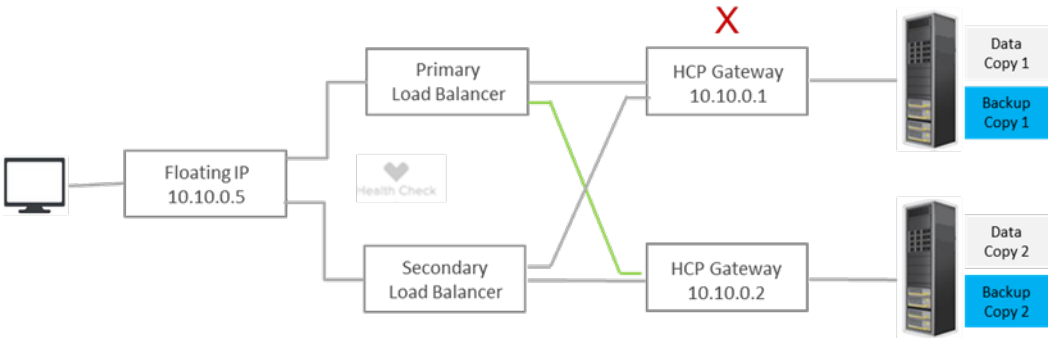
   The advantage of this option is DNS will automatically fail-over and fail back during the next TTL check of the primary IP address. The disadvantage of this approach is the TTL setting will need to be lowered to a tolerable loss of access (e.g., 30 or 90 seconds). This could be considered an expensive action to check on the server so frequently in large environments.

Figure 21.5 – DNS Alternative Address



3. **Floating IP Address**
   If you like automation, but need to minimize transition time during a Gateway failure then the Floating IP Address configuration will be the best choice. A virtual IP address is accessed, and a pair of load balancers will determine which HCP Gateway will serve up the file request. They will automatically transition between each other and to the secondary Gateway if the primary goes off line. The advantage of this configuration is it is automation at its best with a near zero down time during a transition. The disadvantage of this approach is additional network complexity and additional CAPEX and OPEX cost for buying and managing the load balancers (Figure 21.6).

Figure 21.6 – Floating IP addresses



Each of the three networking options use the active-active database replication between the HCP Gateways to keep them in synch. If the primary Gateway crashes the options presented are manual and automatic methods for enabling the secondary Gateway to continue to service requests. The question is now how the primary Gateway gets synchronized with the secondary Gateway so it can resume its role as the primary Gateway. There are three ways to recover the primary HCP Gateway application and configuration; these methods are independent to your network configuration.

The database recovery options are:

1. Restart the primary Gateway and since the databases are configured as “active/active” they will synchronize. This process will work, assuming the primary Gateway software did not need to be installed. Then if the manual fail-over process was selected the administrator will have to manually change the client/application IP addresses back to use the primary Gateway.
2. If the Gateway was down for a long period of time, then export the database, copying it to the other Gateway and then importing the database may be the fastest

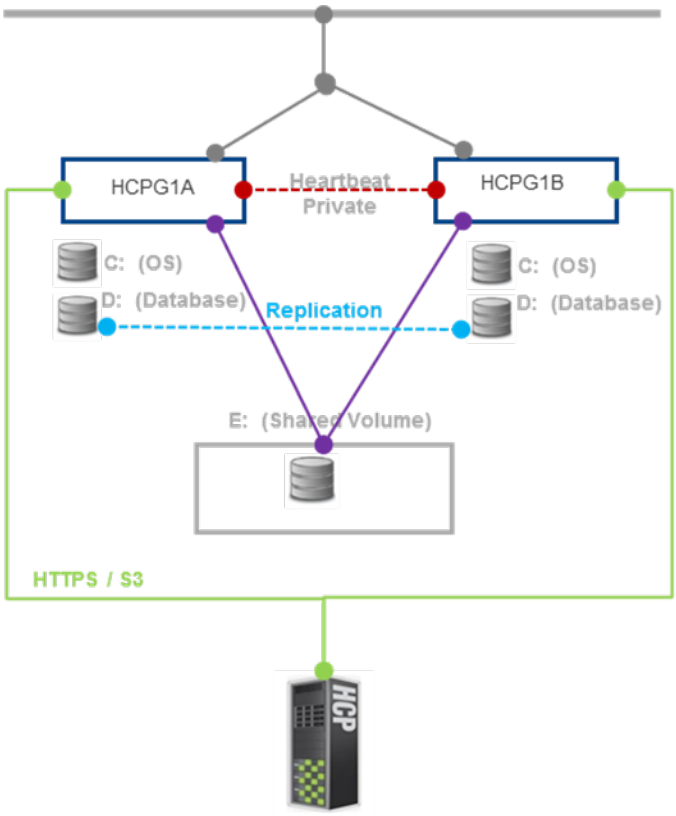
approach. Then if the manual fail-over process was selected the administrator will have to manually change the client/application IP addresses back to use the primary Gateway.

3. The hybrid approach may be the best approach if the network has limited bandwidth. Once a new HCP Gateway has been spun up the administrator can use the UI to start the Restore process in the Operations menu (see the **Recover from Backup** chapter). This will get the bulk of the database back to the last good backup. Then the native resynch process will fill in the gaps for the time after the backup to current time.

C. Clustered Gateways

In many ways the Failover cluster configuration is similar to Replicated Gateways using Floating IP Addresses since both approaches use a virtual IP address. The Windows cluster designates one Gateway node to be the primary and handle all of the traffic. Unlike the Floating IP approach, the cluster will fail over from the primary Gateway to the secondary Gateway when the heartbeat is lost. The failback process is manual administrative process performed by the Windows system administrator or Gateway administrator. The specific steps are covered in the Windows Clustering Guide. Prior to failing back, the original Gateway needs to be back in an operational state and the databases resynchronized. The processes of getting the HCP Gateway in an operational state have been previously covered as have the options to resynchronize the databases (Figure 21.7).

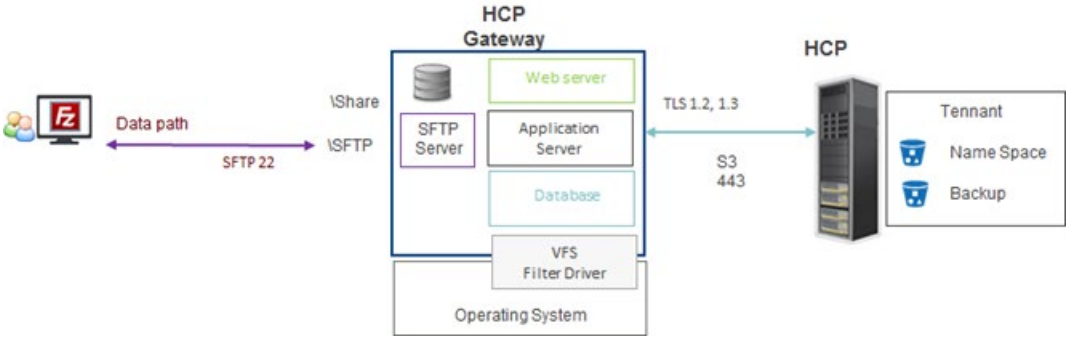
Figure 21.7 – Failover Cluster



SFTP on Gateway Server

Setting up an SFTP Server on HCP Gateway (Figure 22.1).

Figure 22.1 – SFTP



Today the SFTP is limited to a single Share on the HCP Gateway in Windows, there is no limit in Linux. Note that applications like FileZilla create hard links when moving or renaming a file on the SFTP server. This creates problems for the HCP Gateway, so the file move and file rename functions have been disabled.

The steps 1 – 15 in this chapter are for Windows, the Linux instructions are after those steps.

This example will be used for Windows access to a share using sftp: sftp Administrator@10.6.3.10

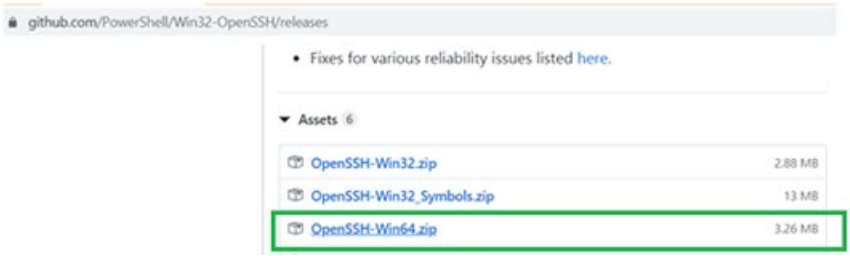
First setup a share (refer to the **HCP Gateway Shares** chapter for assistance), for this example, the name is SFTP.

Windows SFTP on HCP Gateway Server

Step 1: Remote Desktop to the HCP Gateway and log in as the administrator or using assigned Active Directory account. In Windows File Explorer, check for the existence of the folder **"C:\Program Files\OpenSSH"**. If it exists, skip to Step 8.

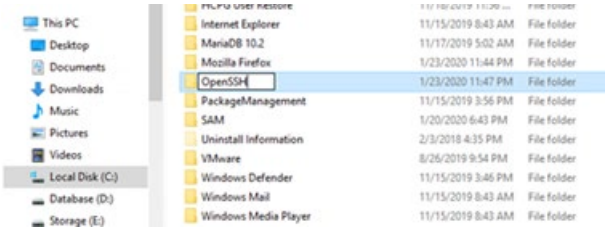
Step 2: Open Firefox browser and download the latest 64-bit OpenSSH Server from Github or download it from the HCPG_Software bundle on the SharePoint site. The example below (Figure 22.2) is for Windows (https://github.com/PowerShell/Win32-OpenSSH/releases)

Figure 22.2 – Download OpenSSH



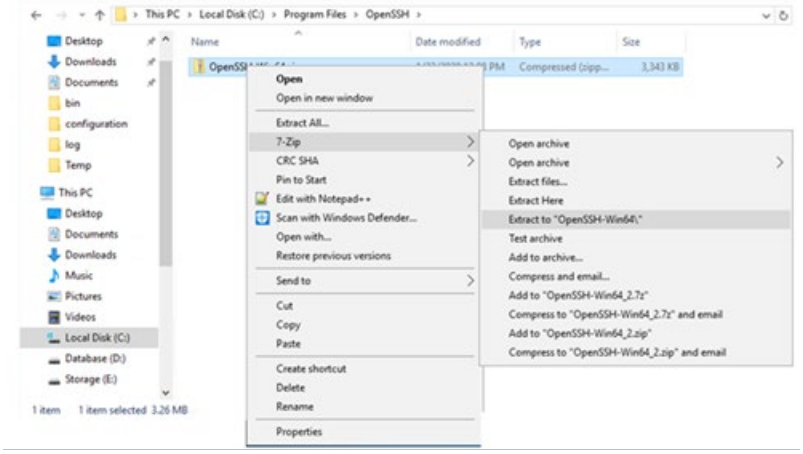
Step 3: Use Explorer (Figure 22.3) to create a new directory 'C:\Program Files\OpenSSH\'

Figure 22.3 – Create Directory



Step 4: Using 7z or similar program to extract the file contents (Figure 22.4) to 'C:\Program Files\OpenSSH\'

Figure 22.4 – Unzip

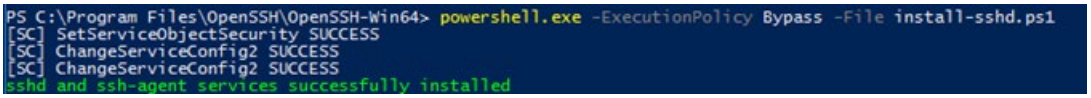


Step 5: Open Windows Powershell and use the “cd” command to change to the directory **"cd C:\Program Files\OpenSSH\OpenSSH-Win64"**

Step 6: Use PowerShell to install the sshd application (Figure 22.5). It is best to copy the text from this document into a Windows Notepad on the HCP Gateway and the copying it from the Notepad window to the PowerShell window to remove any formatting characters in this document.

PS C:\Program Files\OpenSSH\OpenSSH-Win64> **powershell.exe -ExecutionPolicy Bypass -File install-sshd.ps1**

Figure 22.5 – Install



Step 7: Enable SSH through the firewall (note this is one line) (Figure 22.6)

PS C:\Program Files\OpenSSH\OpenSSH-Win64> **New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd)' -Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22**

Figure 22.6 – Firewall Rules

```
PS C:\Program Files\OpenSSH\OpenSSH-Win64> New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd)' -Enabled
True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22


Name                  : sshd
DisplayName           : OpenSSH Server (sshd)
Description           :
DisplayGroup          :
Group                 :
Enabled               : True
Profile               : Any
Platform              : {}
Direction             : Inbound
Action                : Allow
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping      : False
Owner                 :
PrimaryStatus         : OK
Status                : The rule was parsed successfully from the store. (65536)
EnforcementStatus     : NotApplicable
PolicyStoreSource     : PersistentStore
PolicyStoreSourceType : Local
```

Step 8: Verify the SFTP Service is working. Open PowerShell as an Administrator and run the following 4 commands:

start-service ssh-agent

start-service sshd

net stop sshd

net start sshd

Step 9: Using File Explorer, browse to the OpenSSH configuration directory and Open the sshd_config file using NotePad++

C:\ProgramData\ssh\sshd_config

Step 10: Scroll towards the bottom of the file and modify the following lines after the **'#Banner none'** line to match the text below. Change the IP address HCPG-Single to the IP address or DNS name of your Gateway. Only 1 share is currently supported on HCP Gateway for SFTP. In Windows File Explorer, navigate to the E:\SAM folder and right-click on each Archive# folder, check the Properties -> Sharing tab to find the Archive# of the share you created for SFTP. Then use that Archive# on the **ChrootDirectory** line. Then save the file and close Notepad++.

Logging

SyslogFacility AUTH

LogLevel VERBOSE

#Restricts logon through SFTP to only these users

#AllowGroups mydomain\sftpgroup

#We specify that we only allow logons for connections originating from IP 10.6.3.10.

#AllowUsers *@HCPG-Single

ChrootDirectory E:\SAM\Archive1

PermitTunnel no

AllowAgentForwarding no

AllowTcpForwarding no

X11Forwarding no

Step 11: Open a DOS command prompt window as an Administrator and run the following commands, substituting the reference to “SFTP” in the argument “\\localhost\SFTP” with the name of the share you created for SFTP, for example “\\localhost\<your-share-name>”.

fsutil behavior set SymlinkEvaluation L2R:1

mklink /D C:\hcp \\localhost\SFTP

mklink /J C:\hcp_share C:\hcp

Step 12: In the PowerShell Window, stop and then start the ssh service

PS C:\Program Files\OpenSSH\OpenSSH-Win64> **net stop sshd**

PS C:\Program Files\OpenSSH\OpenSSH-Win64> **net start sshd**

Step 13: Setup the sshd to start automatically

PS C:\Program Files\OpenSSH\OpenSSH-Win64> **Set-Service sshd -StartupType Automatic**

Step 14: Stop the Service

PS C:\Program Files\OpenSSH\OpenSSH-Win64> **net stop sshd**

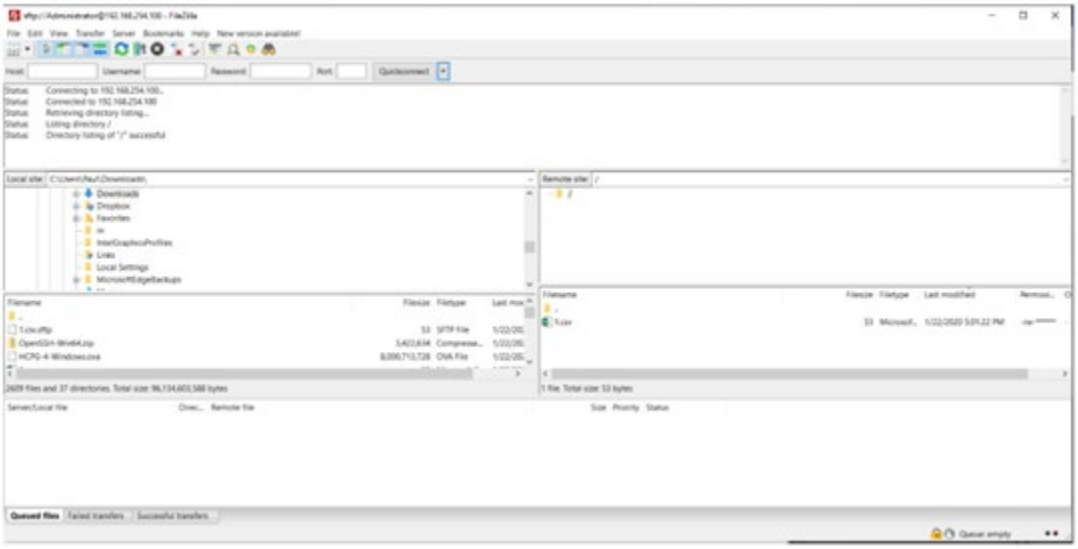
Step 15: Verify it restarts

PS C:\Program Files\OpenSSH\OpenSSH-Win64> **net start sshd**

Congratulations, the SFTP Service is now ready to be used.

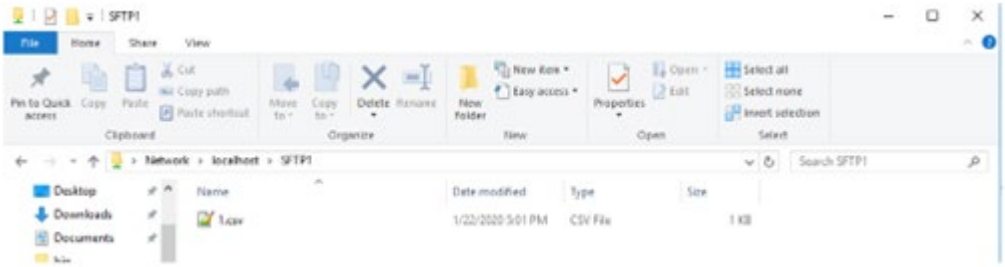
A utility like FileZilla or WinSCP can be used to connect to the SFTP share (Figure 22.7) (sftp Administrator@10.6.3.10) substituting your Gateway IP address for “10.6.3.10”.

Figure 22.7 – What the SFTP Target looks like to Client Using FileZilla



Below is a picture of the STFP share on HCP Gateway (Figure 22.8).

Figure 22.8 – View from Gateway



Linux SFTP on HCP Gateway Server

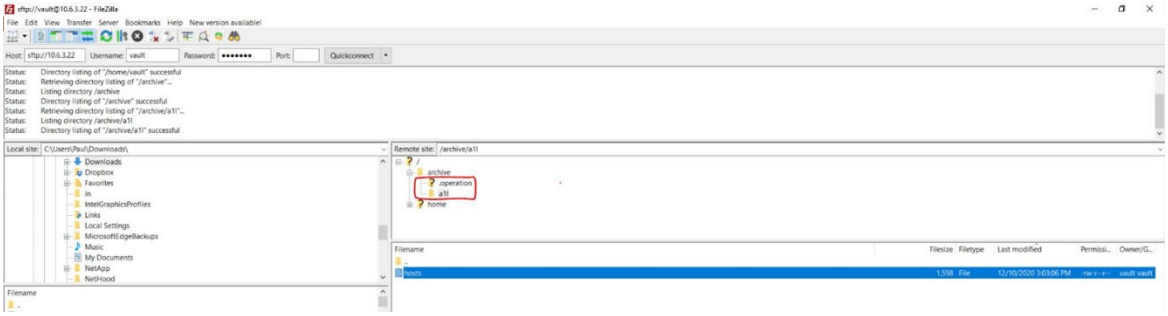
The SFTP software is already installed on the Linux HCP Gateway.

This example will be used for Linux access to a share using sftp: sftp vault@10.6.3.10

First setup a share (refer to the **HCP Gateway Shares** chapter for assistance).

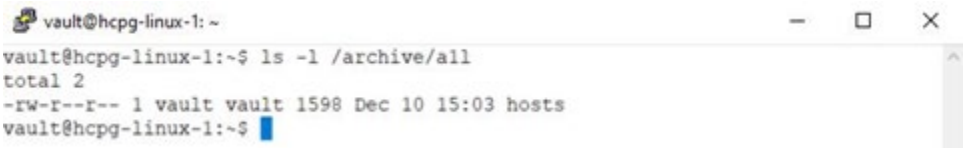
A utility like FileZilla or WinSCP can be used to connect to the SFTP share (Figure 22.9) (sftp vault@10.6.3.22) **substituting your Gateway IP address for "10.6.3.22"**. The shares are under the /archive folder.

Figure 22.9 – What the SFTP Target looks like to Client Using FileZilla



Below is a picture of the STFP share on HCP Gateway (Figure 22.10).

Figure 22.10 – View from Gateway



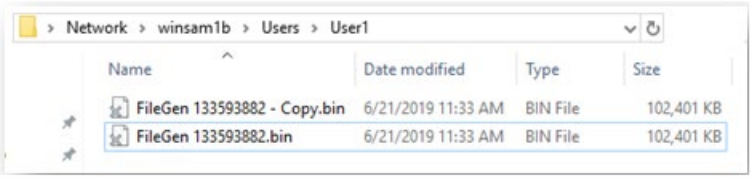
HCP Gateway Quotas

Quotas on HCP Gateway are **not** supported. Quotas cannot be enforced on HCP Gateway due to use of offline files (Size on disk = 0).

Quotas cannot be enforced

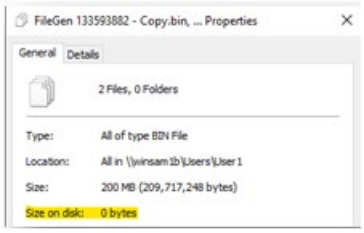
Files have been archived to HCP Gateway (Figure 23.1) and are offline:

Figure 23.1 – Explorer View



But “Size on disk” is zero bytes (Figure 23.2):

Figure 23.2 – File Properties



Administrator Privileged Delete

The Privileged Delete feature allows the user(s) assigned the **Privileged Delete** permission in the Share page of the HCP Gateway UI to delete files under retention. This feature is available in the HCP Gateway UI File Explorer page. If files are under a Legal Hold, the Legal Hold policy needs to be removed before the Administrator can use the Privileged Delete feature.

IMPORTANT NOTE:

Privileged Delete is **NOT** available when using an HCP Gateway Share with HCP for Cloud Scale storage, the **Delete** button in the UI File Explorer page will be greyed out.

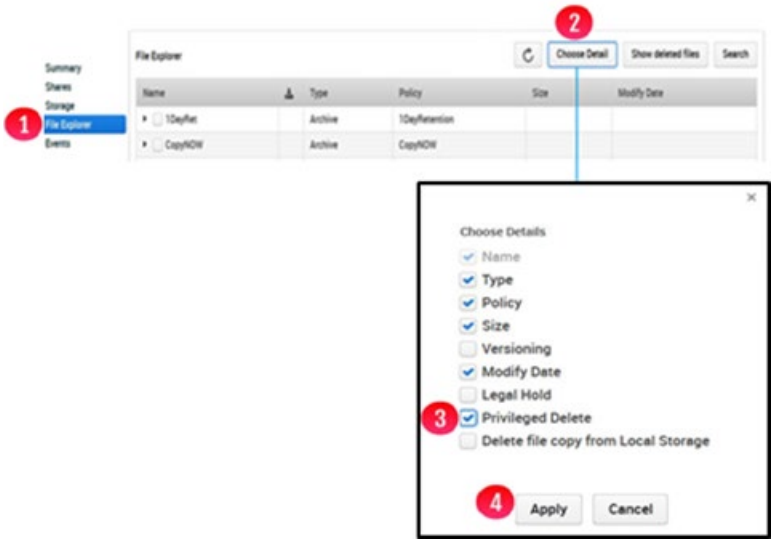
NOTE:

This feature will delete the file off the share and the local storage. However, it will not delete the file off the long term or Object Storage system like HCP. Also, if the file is only saved on local storage, you can use the feature to delete the file off the share, but you will not be able to delete the file off the local storage.

Step 1: In a web browser, open the HCP Gateway UI and log in as a user that is assigned the **Privileged Delete** permission for the share.

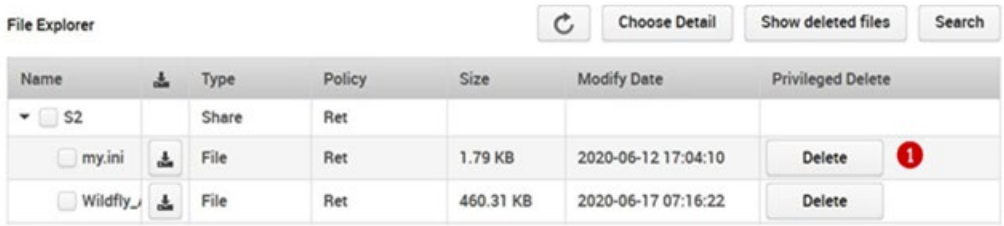
Step 2: Click the **File Explorer** tab (Figure 24.1.1), then click **Choose Detail** (Figure 24.1.2). Select the **Privileged Delete** (Figure 24.1.3) option, then click **Apply** (Figure 24.1.4) to apply the setting. Note that you may have to follow this step every time you enter the File Explorer tab.

Figure 24.1 – Apply Admin Privileged Delete



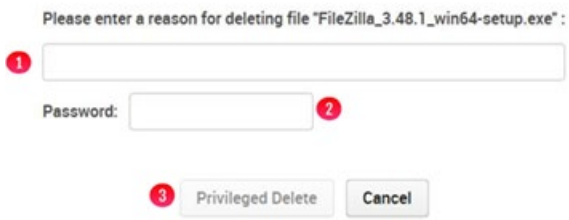
Step 3: Select the file to delete and click **Delete** (Figure 24.2.1). If the file is under a Legal Hold, you will not be able to Privileged Delete the file until the Legal Hold is removed.

Figure 24.2 – Select file to Privileged Delete



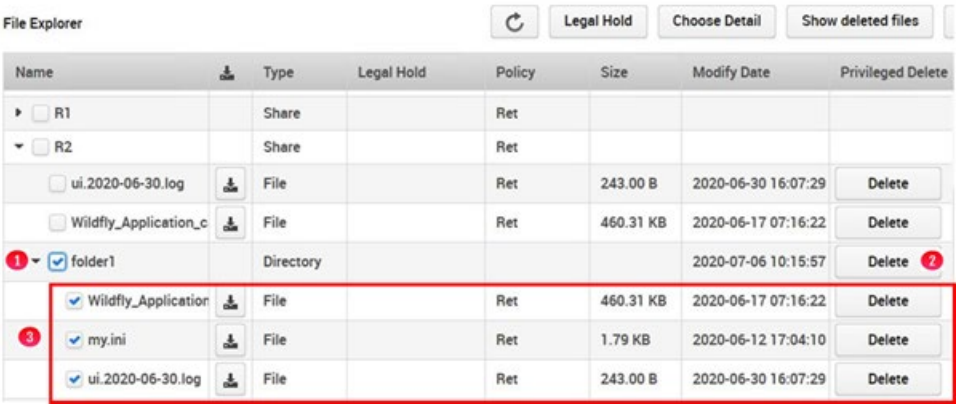
Step 4: Enter the reason to delete the file (Figure 24.3.1). Enter the password of the user you are logged into the HCP Gateway UI (Figure 24.3.2). Once you enter the reason to delete and the password, the **Privileged Delete** button (Figure 24.3.3) will become active. Click **Privileged Delete** (Figure 24.3.3) to delete the file from the share. After the file is **Privilege Deleted**, the file content will still be stored on the storage.

Figure 24.3 – Enter reason for Privileged Delete



Step 5: Alternatively, you can select a folder to Privileged Delete (Figure 24.4.1) and click **Delete** (Figure 24.4.2). Notice that all the files in the folder are now selected for **Privileged Delete** (Figure 24.4.3). You will not be able to Privileged Delete any files in the folder that are under a Legal Hold, until the Legal Hold is removed. Enter the reason to delete the folder(s) and file(s) (Figure 24.3.1). Enter the password of the user you are logged into the HCP Gateway UI (Figure 24.3.2). Once you enter the reason to delete and the password, the **Privileged Delete** button (Figure 24.3.3) will become active. Click **Privileged Delete** (Figure 24.3.3) to delete the file from the share. After the file is **Privilege Deleted**, the file content will still be stored on the storage.

Figure 24.4 – Select folder to Privileged Delete



Note:

This step only deletes the file(s) off the share.

If you deleted a file by mistake and want to undelete the file, refer to the steps in the **Recover Previous Versions and Deleted Files** chapter, Section 16.3 **Recovery of Deleted Files by Administrator**.

If you want to remove the file content from the storage(s), such as Local and/or Object Storage, refer to the steps in the **HCP Gateway Operations** chapter, Section 15.4 **Delete on Storage**.

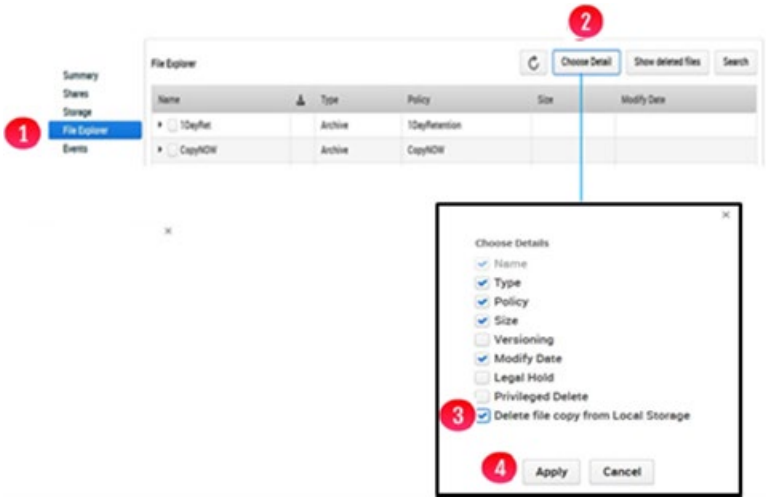
Delete File Copy off Local Storage

The **Delete File Copy Off the Local Storage** feature allows the user(s) assigned the **Privileged Delete** permission in the Share page of the HCP Gateway UI, to delete files off the Local Storage, when the Storage Group contains both Local Storage and another storage, such as a namespace on an Object Storage system like HCP. The file must be saved on the other Storage before you will be able to delete it off the Local Storage.

Step 1: In a web browser, open the HCP Gateway UI and log in as the user with the **Privileged Delete** permission for the share you want to delete the file copy off the local storage.

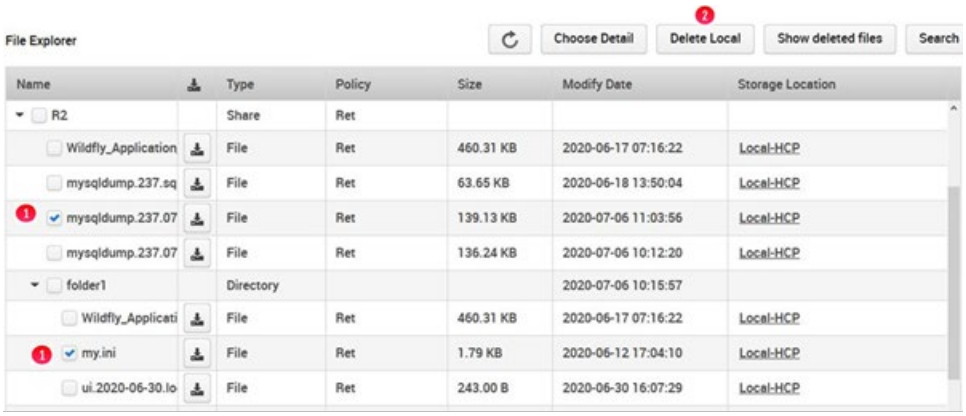
Step 2: Click the **File Explorer** tab (Figure 25.1.1), then click **Choose Detail** (Figure 25.1.2). Select the **Delete file copy from Local Storage** (Figure 25.1.3) option, then click **Apply** (Figure 25.1.4) to apply the setting. Note that you may have to follow this step every time you enter the File Explorer tab.

Figure 25.1 – Choose Delete file copy from Local Storage Detail



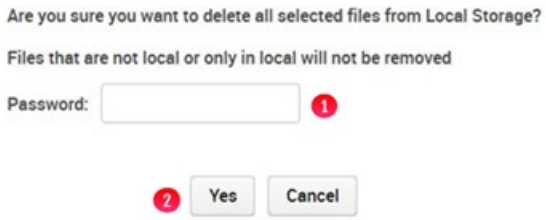
Step 3: Browse to the share, then the folder and select the file(s) to delete off the Local Storage by selecting the name(s) of the file in the **Name** column (Figure 25.2.1) then click **Delete Local** (Figure 25.2.2).

Figure 25.2 – Select files to Delete Copy Off Local Storage



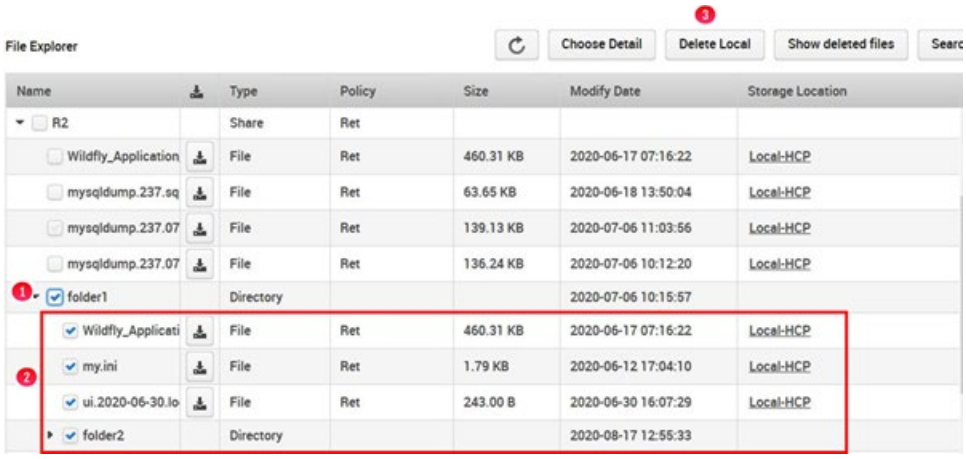
Step 4: Enter the password for the user that you logged in as to the HCP Gateway UI (Figure 25.3.1). Click **Yes** to delete the copy of the file(s) off the Local Storage (Figure 25.3.2). Note that files that were already deleted from local storage or are only on local storage will not be removed from local storage.

Figure 25.3 – Delete Copy Off Local Storage



Step 5: Alternatively, you can select a folder(s) of files to delete off local storage (Figure 25.4.1) Notice that all the files and folders in the folder are now selected for **Delete file copy from Local Storage** (Figure 25.4.2). Click **Delete Local** (Figure 25.4.3).

Figure 25.4 –Select Folder(s) to Delete Copy Off Local Storage



Step 6: Enter the password for the user that you logged in as to the HCP Gateway UI (Figure 25.3.1). Click **Yes** (Figure 25.3.2) to delete the copy of the file(s) off the Local

Storage. Note that files that were already deleted from local storage or are only on local storage will not be removed from local storage.

Enabling Windows Server Features

Enabling Windows Server 2016/2019 features:

- SNMP
- User Auditing

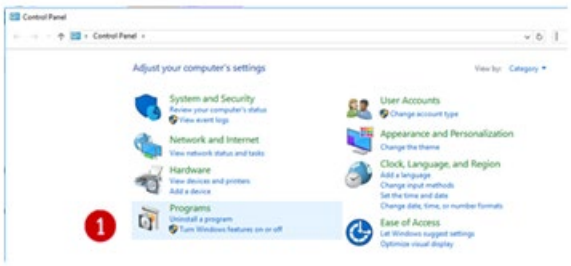
1. **Install SNMP Service**
   Simple Network Management Protocol (SNMP) is an application layer protocol used to monitor and manage network devices and their functions. Supported SNMP versions are defined by the operating system (Windows Server 2016/2019 and Debian 10), not by HCP Gateway. The SNMP Service must be installed and UDP ports 160 and 161 need to be enabled. The status of HCP Gateway VFS Service and Shares can be monitored via SNMP.

   Windows Server 2016/2019 does not come with SNMP Service installed. Windows Server 2016/2019 currently supports SNMP v2c. Microsoft does not plan to support v3. This section will cover the basic SNMP installation process, which can also be found in the Windows Server Administration Guide.

The following steps are required to be taken within the Control Panel.

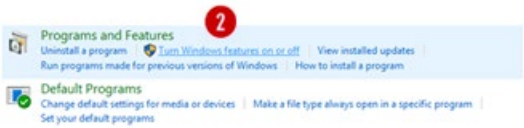
Step 1 - Select Programs (Figure 26.1.1)

Figure 26.1 - Select programs



Step 2 - Select Turn Windows features on or off (Figure 26.2.2)

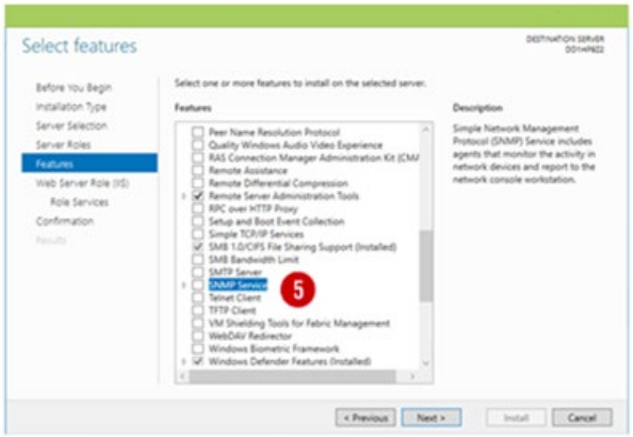
Figure 26.2 – Turn Off Features



Step 3– In the **Add Roles and Features** window, select **Role-based or feature-based installation** then click **Next**. Select the Gateway server from the list then click **Next**.

Step 4 - Select SNMP Service from list of features (Figure 26.3.5)

Figure 26.3 - Select SNMP

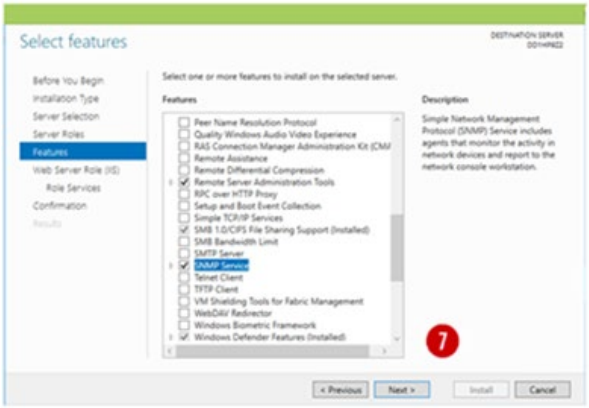


Step 5 – In the **Add features that are required for SNMP Service**, click on the Add Features button (Figure 26.4.6).

Figure 26.4 - Select Add Features

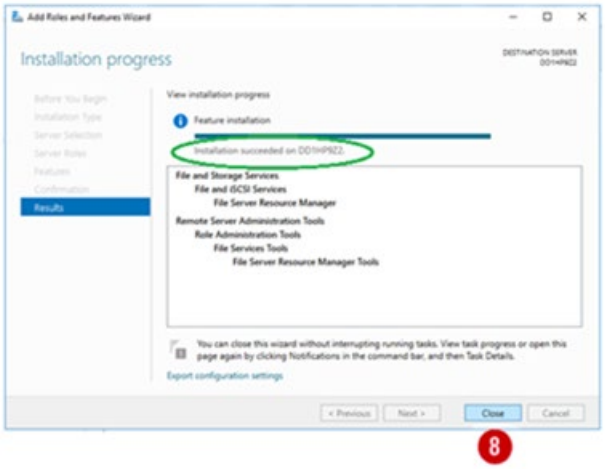
Step 6 – Note SNMP check box is now checked and then click on the **Next** button (Figure 26.5.7).

Figure 26.5 - Select SNMP



Step 7 – Click **Install** to install SNMP. Click on the **Close** button (Figure 26.6.8) to close the dialog box.

Figure 26.6 - Install

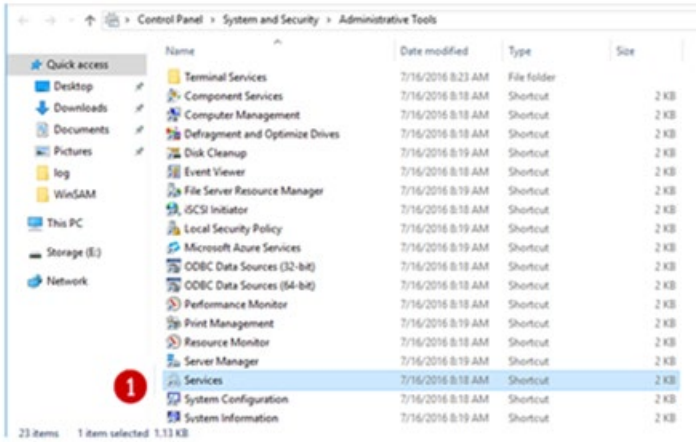


2. **Configure SNMP Service**

   Now that the SNMP Service has been installed it must be configured by taking the following steps:

   Step 1 – Open Windows **Services** (Figure 26.7.1) panel from the Administrative Tools menu

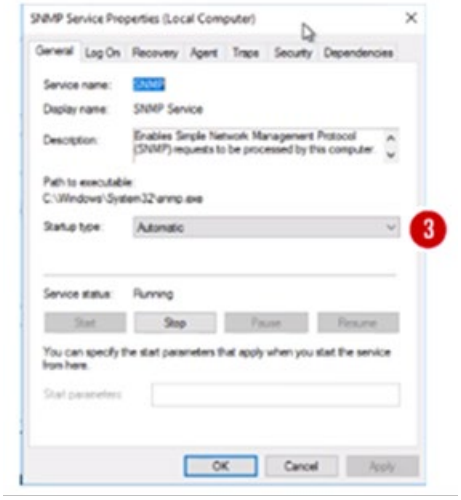
Figure 26.7 - Select Service



Step 2 – Select the **SNMP Service** and right click to bring up the **Properties** tab.

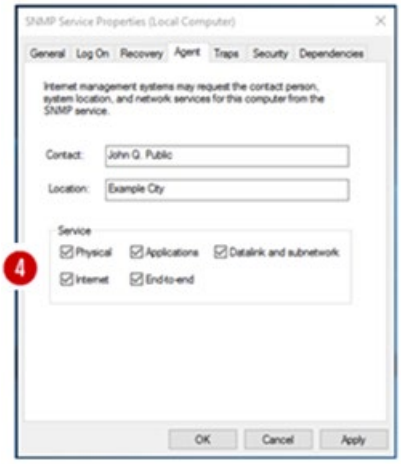
Step 3 - Select **Automatic** as the Startup type (Figure 26.8.3) to have the service always running, even after rebooting the server.

Figure 26.8 - Automatic start



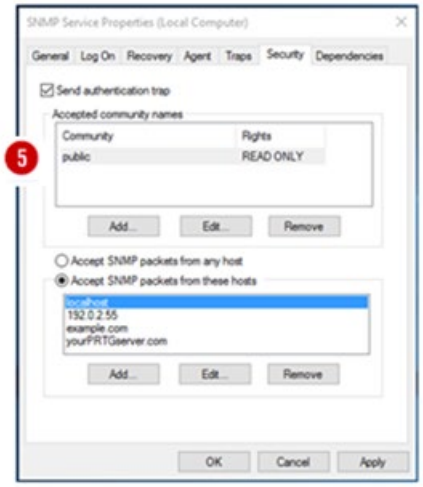
Step 4 –For monitoring purposes, you should also check all services on the **Agent** tab (Figure 26.9.4) to have all SNMP values available.

Figure 26.9 - Select Agent



Step 5 – Adjust security parameters in the **Security** tab. For example, add the community name **public** with **READ ONLY** rights and **accept SNMP packets** from at least the address of your monitoring server (Figure 26.10.5).

Figure 26.10 - Adjust Security

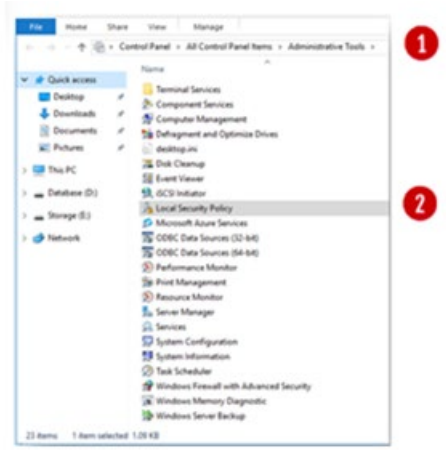


SNMP is now successfully configured on your Window Server.

3. **Windows File Access Auditing**
   This section will explain how to enable file access auditing in Windows Server 2016/2019. This will log failed and successful attempts to access objects in the file system by accounts defined at the folder level. These attempts are logged in the Windows Event Viewer.

   Step 1 – Open **Control Panel -> System and Security -> Administrative Tools** (Figure 26.11.1)
   Step 2 – Double-click on **Local Security Policy** (Figure 26.11.2)

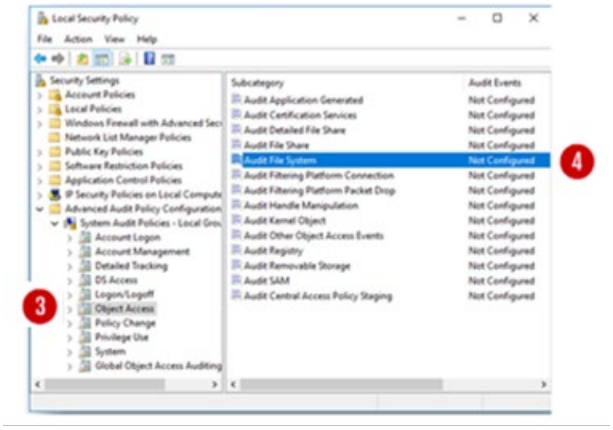
Figure 26.11 – Local Security



Step 3 – Open **Advanced Audit Policy Configuration**, then open **System Audit Policies,** then open **Object Access** (Figure 26.12.3).

Step 4 – Right-click on **Audit File System** (Figure 26.12.4) and click **Properties**.

Figure 26.12 – Audit File System

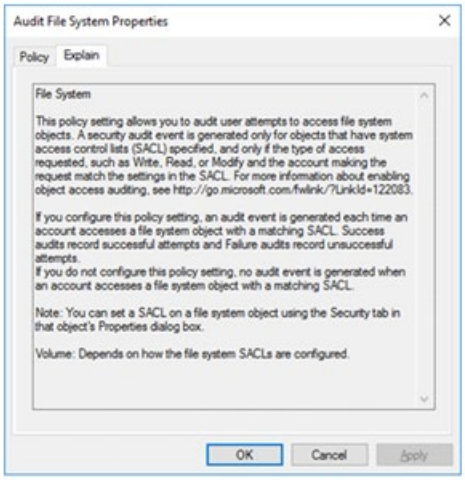


Step 5 – Select check box for **Configure the following audit events,** then select **Success and Failure** (Figure 26.13.5)

Figure 26.13 – Configure Audit Events

Click **Explain** (Figure 26.14) to view the explanation of the policy settings, then click **OK** to save the configuration (Figure 26.13.6).

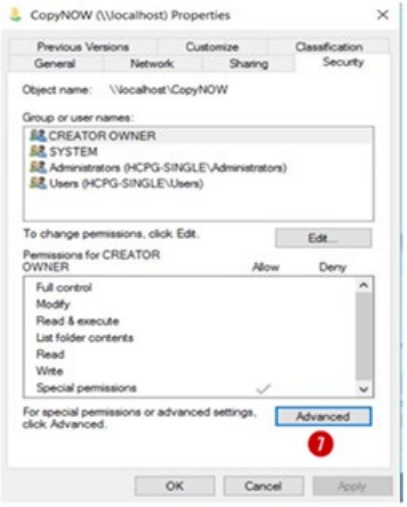
Figure 26.14 – Explanation



Step 6 – To apply Auditing Policy to Folders, in Windows File Explorer, browse to the desired folder and then right click the folder.

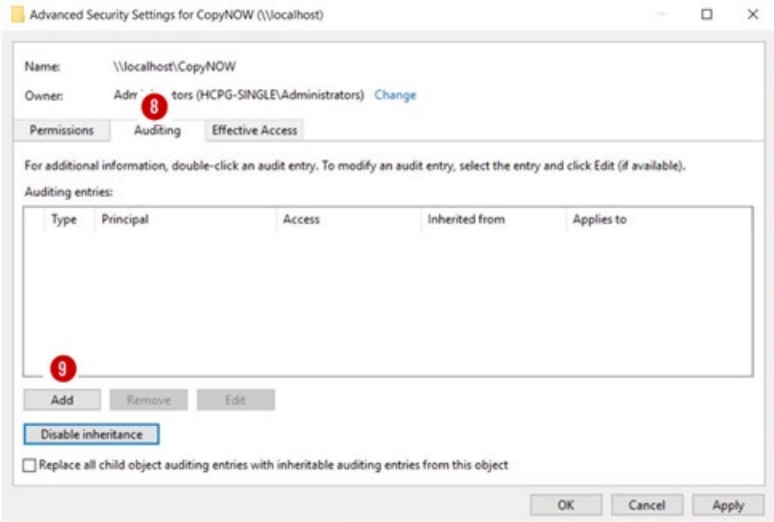
Step 7 – **Select Properties -> Security**. Then select the **Advanced** button (Figure 26.15.7).

Figure 26.15 – Advanced Settings



Step 8 – In the Advanced Security Setting of the folder, select the **Auditing** tab (Figure 26.16.8).

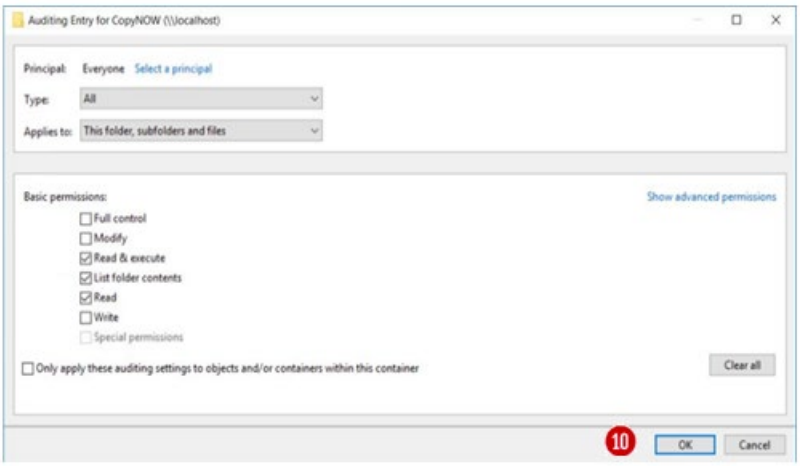
Figure 26.16 – Auditing



Step 9 – Then select the **Add** button (Figure 26.16.9) to choose which users are to be audited.

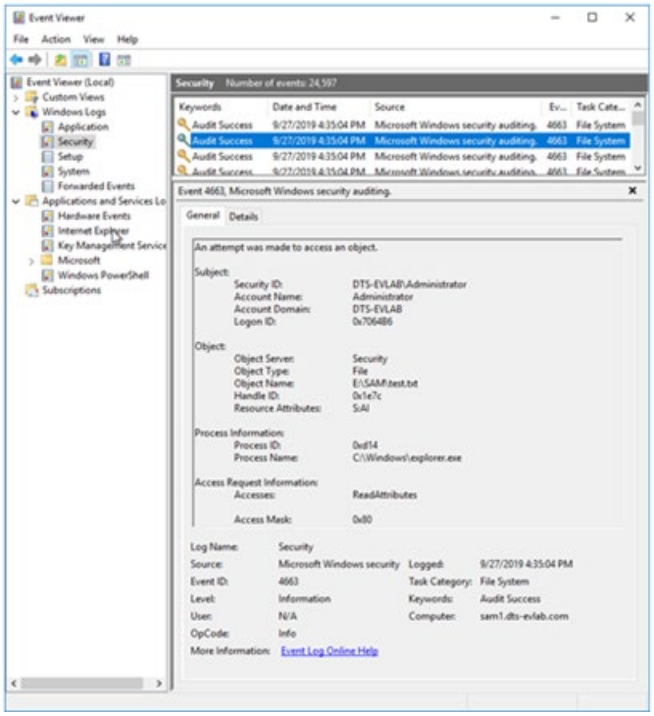
Step 10 – Complete the form and click **OK** button (Figure 26.17.10). The example shows **Everyone** selected and the Type option choice is **All** and **the Applies to** option choice is **This folder, subfolder, and files** (Figure 26.17).

Figure 26.17 – Auditing



Step 11 – To view the audit events, open the Windows Event Viewer and look for event ID 4663 (Figure 26.18)

Figure 26.18 – View Events


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Lo
Hardware Events
Internet Explorer
Key Management Service
Microsoft
Windows PowerShell
Subscriptions
Security Number of events: 24,597
Keywords Date and Time Source Ev... Task Cate...
Audit Success 9/27/2019 4:35:04 PM Microsoft Windows security auditing. 4663 File System
Audit Success 9/27/2019 4:35:04 PM Microsoft Windows security auditing. 4663 File System
Audit Success 9/27/2019 4:35:04 PM Microsoft Windows security auditing. 4663 File System
Event 4663, Microsoft Windows security auditing.
General Details
An attempt was made to access an object.
Subject:
Security ID: DTS-EVLAB\Administrator
Account Name: Administrator
Account Domain: DTS-EVLAB
Logon ID: 0x706d86
Object:
Object Server: Security
Object Type: File
Object Name: E:\SAM\test.txt
Handle ID: 0x1e7c
Resource Attributes: S:AI
Process Information:
Process ID: 0xd14
Process Name: C:\Windows\explorer.exe
Access Request Information:
Accesses: ReadAttributes
Access Mask: 0x80
Log Name: Security
Source: Microsoft Windows security Logged: 9/27/2019 4:35:04 PM
Event ID: 4663 Task Category: File System
Level: Information Keywords: Audit Success
User: N/A Computer: sam1.dts-evlab.com
OpCode: Info
More Information: Event Log Online Help

LDAP authentication to Active Directory via SSL certificate

Pre-Requisites

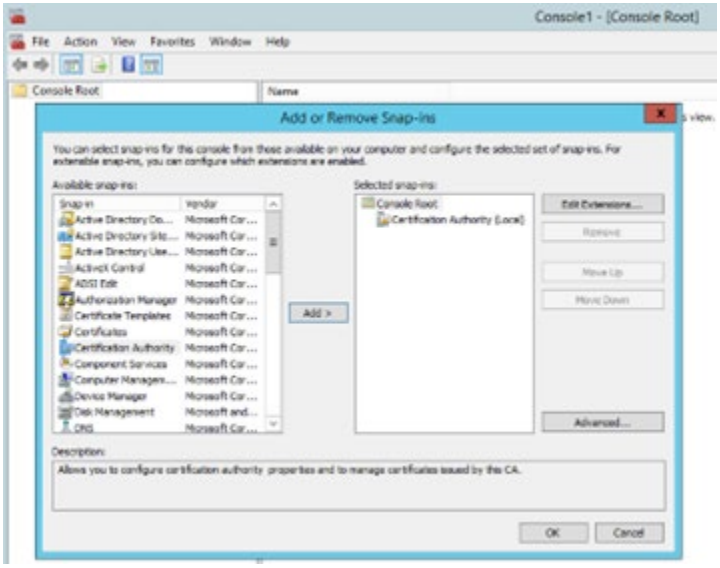
Active Directory Certificate Services installed on the Active Directory Domain controller. This will give you the Certification Authority Snap-in you need to complete these steps.

Enable LDPS on domain controller

On Domain Controller:

Step 1 - Right Click the Windows Start Button, select **Run**. Type **'mmc'** then **press the enter key**, select **File, Add/Remove Snap-in**. Next, select **Certification Authority** then click **Add.** Verify the radio button is checked next to Local computer, click **Finish**, then click **OK** (Figure 27.1).

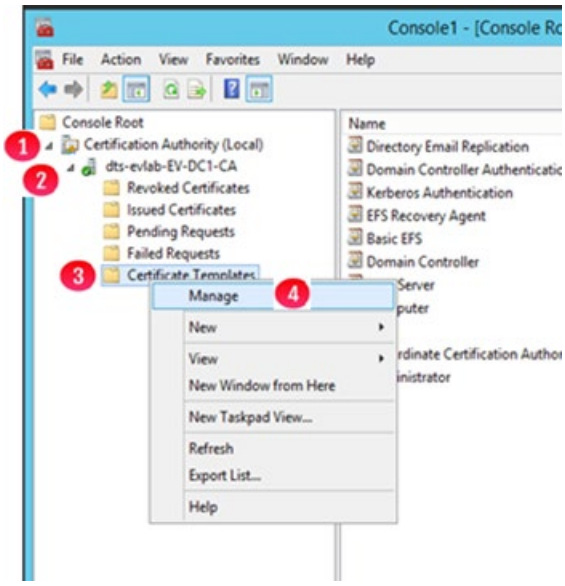
Figure 27.1 – Add Snap-ins



Step 2 - Certification Authority MMC:

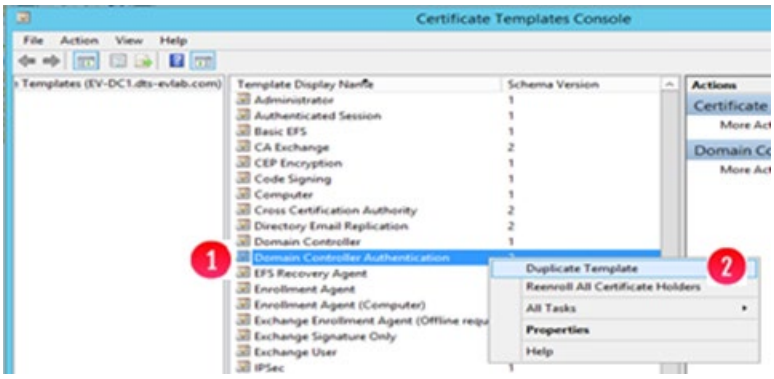
Expand **Certification Authority (Local)** (Figure 27.2.1) expand the domain-domain controller name (Figure 27.2.2), right click **Certificate Templates** (Figure 27.2.3), select **Manage** (Figure 27.2.4).

Figure 27.2 – Certification Authority



Step 3 - Right click on the template **Domain Controller Authentication** (Figure 27.3.1), select **Duplicate Template** (Figure 27.3.2).

Figure 27.3 – Select Duplicate Template



Step 4 - Verify the following settings:

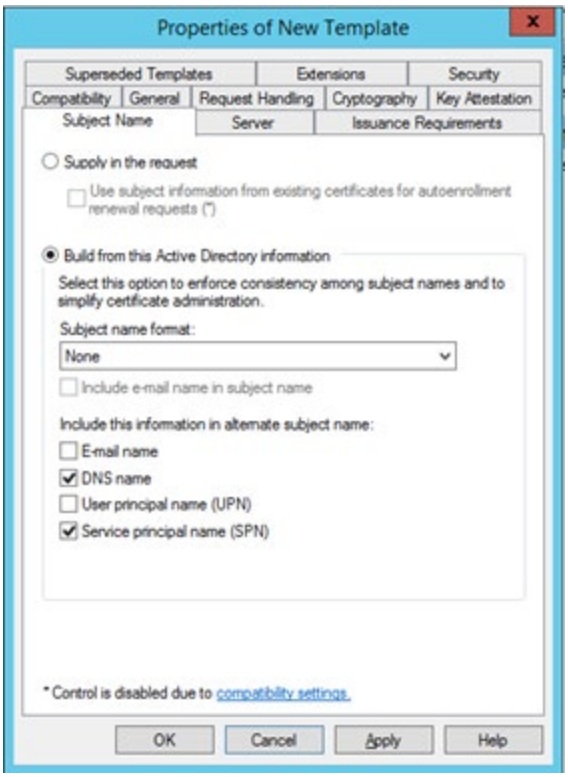
- **General tab:**
  - Set Template Display Name: **LDAP_Authentication** (Figure 27.4.1)
  - Select proper validity period (Figure 27.4.2)
  - Publish in AD: **No** (Figure 27.4.3)

Figure 27.4 – Verify General

Step 5 - Verify the following settings:

- **Subject Name** tab
  - **DNS** and **SPN** checked (Figure 27.5)

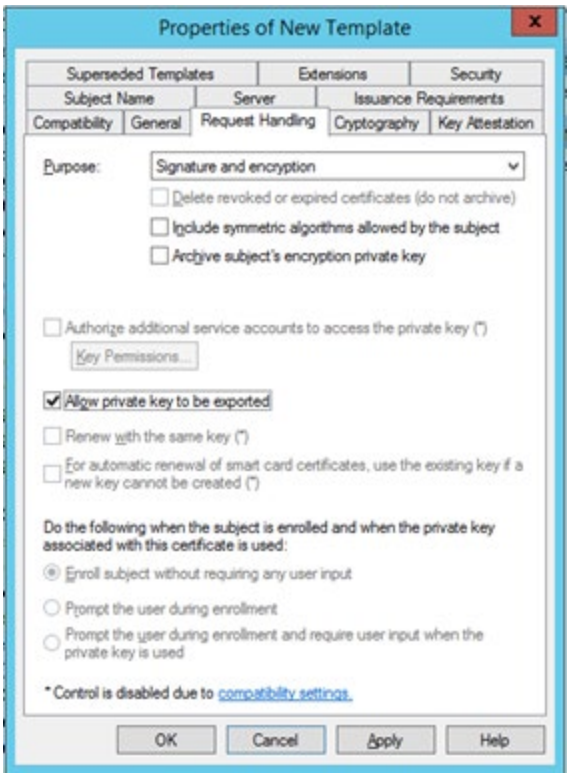
Figure 27.5 – Verify Subject Name



Step 6 - Verify the following settings:

- **Request Handling** tab
  - Select **Allow private key to be exported** (Figure 27.6)
  - Click **OK** to save the properties

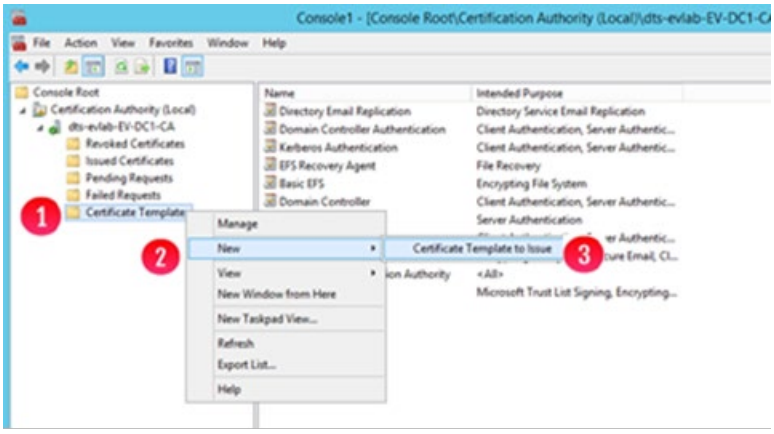
Figure 27.6 – Verify Subject Name



Step 7 - Certificate Authority MMC:

Right click **Certificate Templates** (Figure 27.7.1), the click New (Figure 27.7.2), then click **Certificate Template to Issue** (Figure 27.7.3).

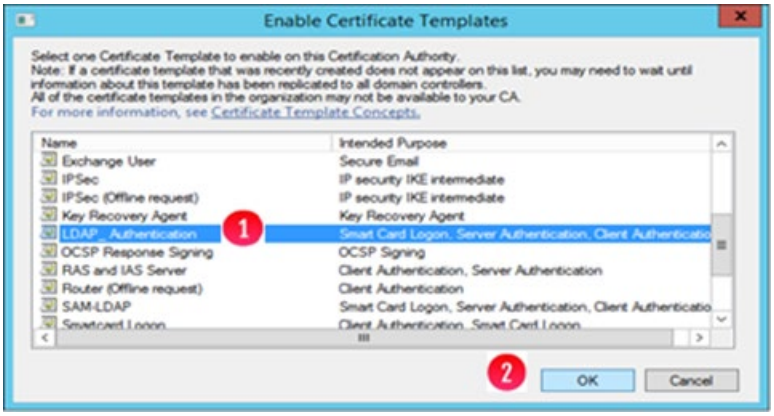
Figure 27.7 – Certificate Template to Issue



Step 8 – Enable Certificate Templates:

In the **Enable Certificate Templates** window, select **LDAP_Authentication** (Figure 27.8.1) then click OK (Figure 27.8.2).

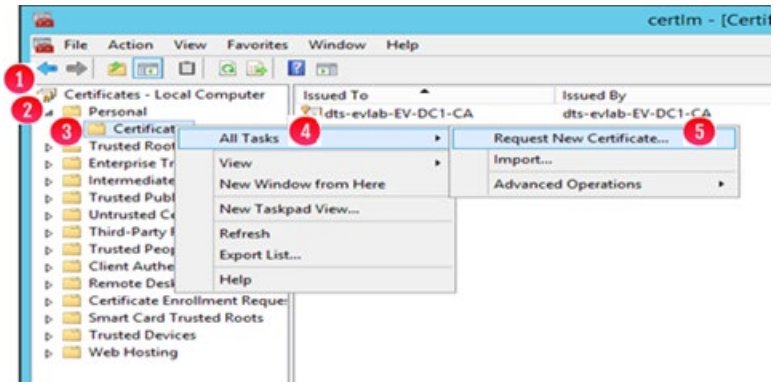
Figure 27.8 – Enable Certificate Templates



Step 9 – Requesting a Certificate for Server Authentication:

In the **Certificates MMC**, select **Certificates** – **Local Computer** (Figure 27.9.1), **Personal** (Figure 27.9.2), right click on **Certificates** (Figure 27.9.3), then select **All Tasks** (Figure 27.9.4), then select **Request New Certificate** (Figure 27.9.5).

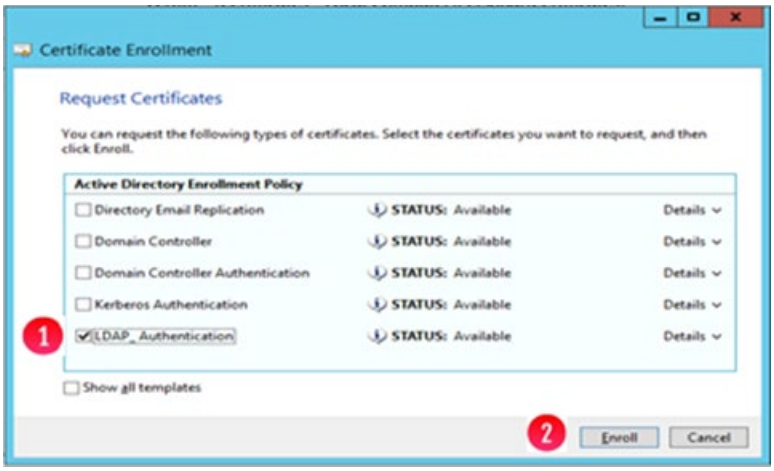
Figure 27.9 – Requesting a Certificate for Server Authentication



Step 10 – Certificate Enrollment:

On the **Certificate Enrollment** screen click **Next**, click **Next** on **Active Directory Enrollment Policy**, select **LDAP_Authentication** (Figure 27.10.1), click **Enroll** (Figure 27.10.2), then click **Finish**.

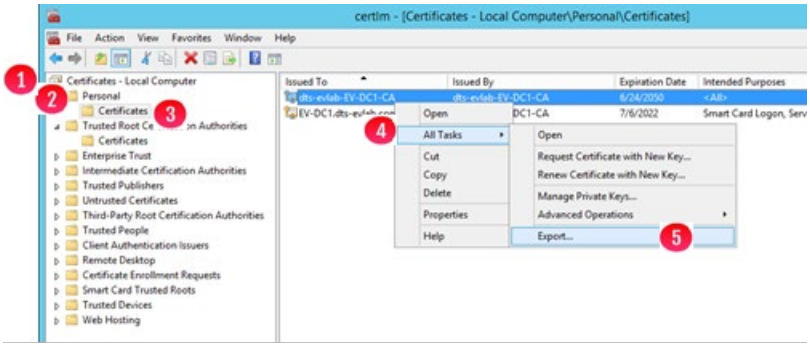
Figure 27.10 – Certificate Enrollment



Step 11 – Export the Certificate Authority and the LDAP Certificates:

In the **Certificates MMC**, select **Certificates – Local Computer** (Figure 27.11.1), then **Personal** (Figure 27.11.2), then **Certificates** (Figure 27.11.3), then right click the DC certificate, then select **All Tasks** (Figure 27.11.4), then select **Export** (Figure 27.11.5).

Figure 27.11 – Export the Certificate Authority and the LDAP Certificates



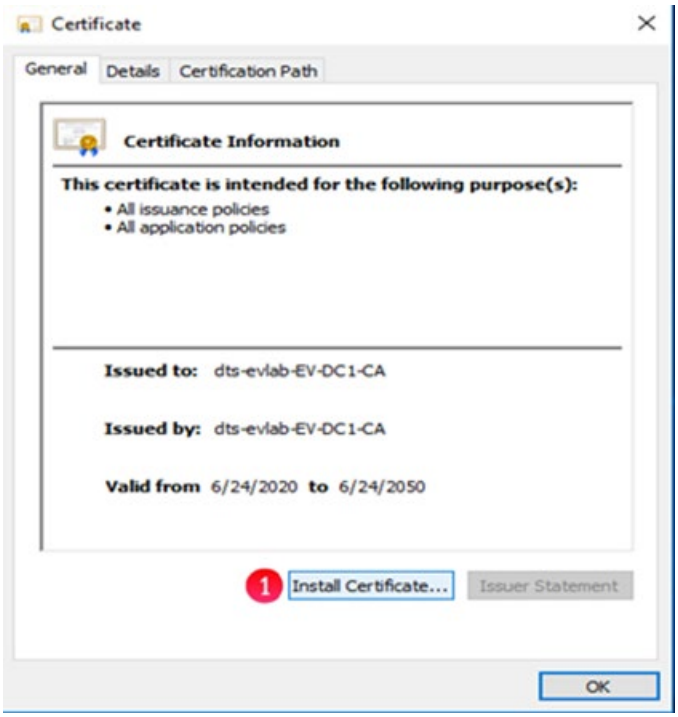
Step 12 - Certificate Export Wizard:

1. In the **Certificate Export** wizard click **Next**
2. then in the **Export Private Key** window select **'No, do not export the private key'**, then click **Next**
3. then in the **Export File Format** window select **'Base-64 encoded X.509'**, then click **Next**,
4. then in the **File to Export** window click the **Browse** button, then enter a name (for example)- **Domain_CA**, then click **Save**, then click **Next**
5. then in the **Completing the Certificate Export Wizard** window click **Finish**, the click on **OK** on the message **'The export was successful'**.

Step 13 – Install Certificate:

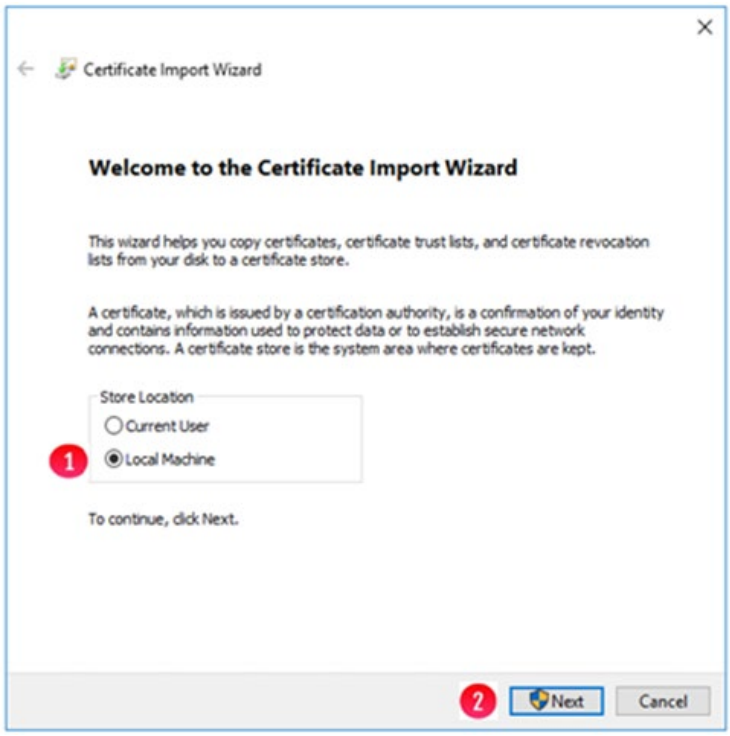
1. Copy this certificate to the HCP Gateway server and double click on it to open it.
2. Click on **Install Certificate** (Figure 27.12.1)

Figure 27.12 – Install the Certificate



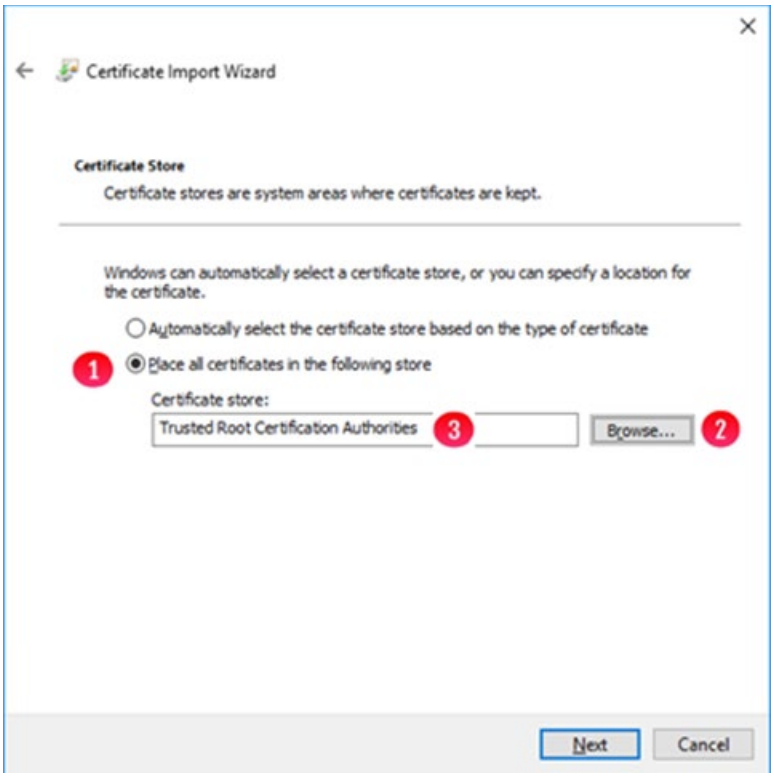
3. In the **Welcome to the Certificate Import Wizard** window, select **Local Machine** (Figure 27.13.1) then click **Next** (Figure 27.13.2).

Figure 27.13 – Local Machine



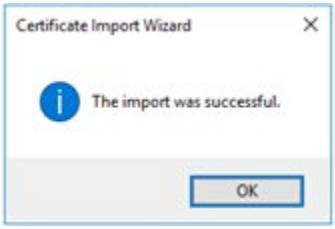
4. In the **Certificate Store** window, select **Place all certificates in the following store** (Figure 27.14.1), click the Browse button (Figure 27.14.2) and browse to the **Trusted Root Certification Authorities** (Figure 27.14.3), then click **OK**. In the **Certificate Store** window, click **Next**, then in the **Completing the Certificate Import Wizard** window, click **Finish**.

Figure 27.14 – Certificate Store



5. In the **Certificate Import Wizard** window, click **OK** (Figure 27.15).

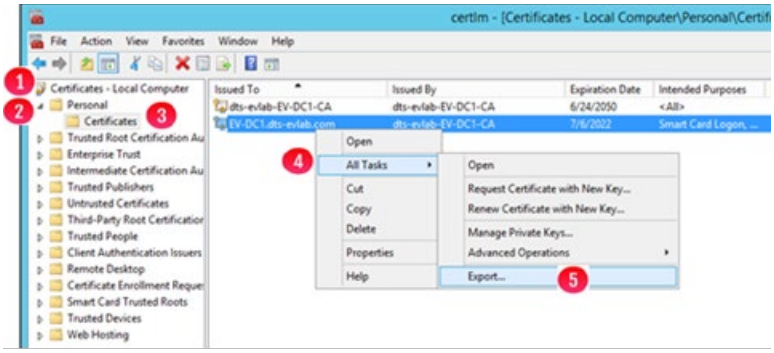
Figure 27.15 – Certificate Import Wizard Success



Step 14 - Export HCP gateway UI certificate:

The next export will be for the certificate used to import in the HCP Gateway UI. In the **Certificates MMC**, select **Certificates** – **Local Computer** (Figure 27.16.1), then **Personal** (Figure 27.16.2), then **Certificates** (Figure 27.16.3), then right click the DC certificate, then select **All Tasks** (Figure 27.16.4), then select **Export** (Figure 27.16.5).

Figure 27.16 – Export the Certificate Authority for HCP Gateway UI



Step 15 - Certificate Export Wizard:

1. In the **Certificate Export** wizard click **Next**
2. then in the **Export Private Key** window select **'No, do not export the private key'**, then click **Next**
3. then in the **Export File Format** window select **'Base-64 encoded X.509'**, then click **Next**,
4. then in the **File to Export** window click the **Browse** button, then enter a name (for example)- **Domain_ldap**, then click **Save**, then click **Next**
5. then in the **Completing the Certificate Export Wizard** window click **Finish**, the click on **OK** on the message **'The export was successful'**.

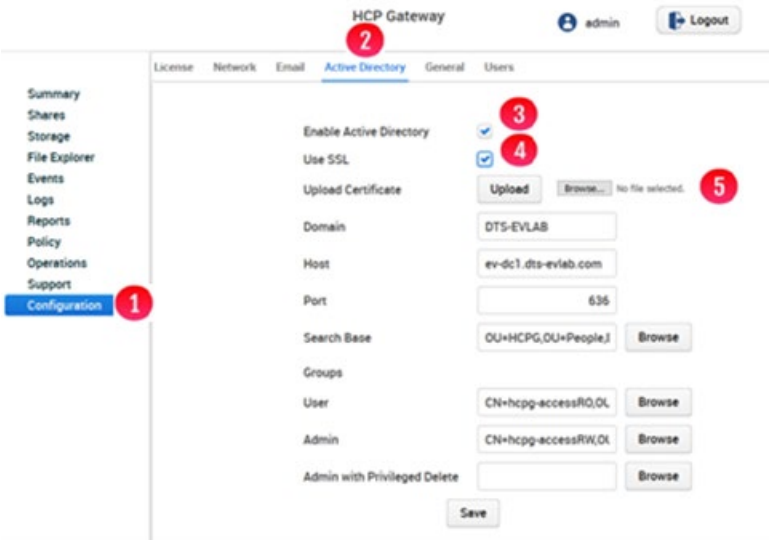
Step 16 - Configure HCP Gateway UI for certificate authentication

1. Copy the domain_ldap.cer certificate file you exported to the HCP Gateway server or your local computer.
2. In a web browser, enter the URL for the HCP Gateway UI, if you are on the Gateway the URL will be https://localhost:28443/hcpg. Then Log in with the **admin** credentials. (Figure 27.17).

Figure 27.17 HCP Gateway UI login

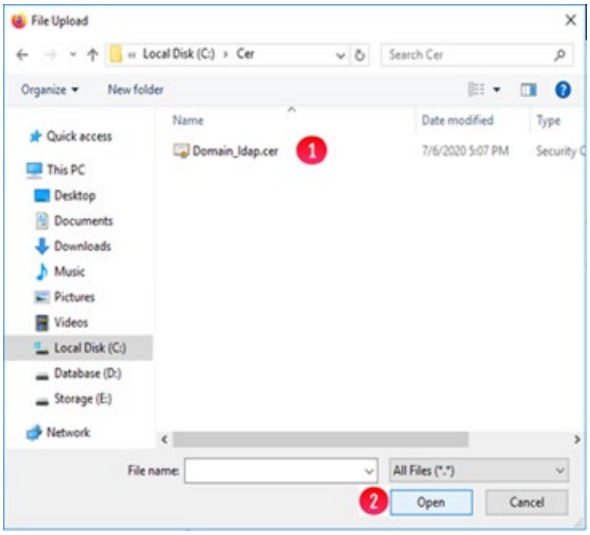
3. Click **Configuration** (Figure 27.18.1) on left navigation panel, select **Active Directory** from top menu (Figure 27.18.2), select **Enable AD** (Figure 27.18.3), then select **SSL** (Figure 27.18.4), then select **Browse** (Figure 27.18.5).

Figure 27.18 HCP Gateway UI Active Directory



4. Select the certificate that you copied to the HCP Gateway server or your local computer, for this example, **Domain_ldap.cer** (Figure 27.19.1), the click **Open** (Figure 27.19.2).

Figure 27.19 HCP Gateway UI File Upload

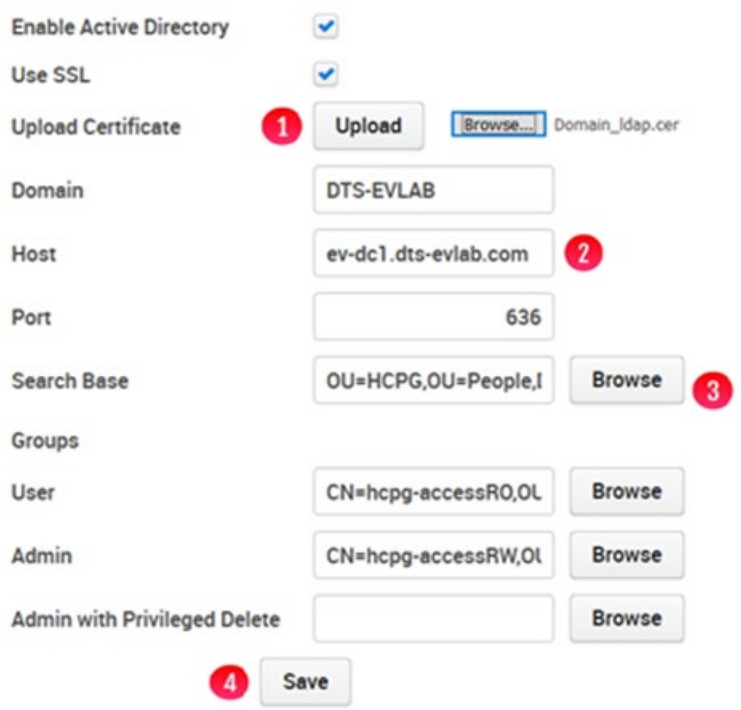


5. Click **Upload** (Figure 27.20.1).

6. Be sure to enter the fully qualified domain name of the AD domain controller in the **Host** field (Figure 27.20.2). Verify connection by clicking **Browse** next to **Search Base** (Figure 27.20.3), enter the proper AD credentials, then click **Connect**.

7. Click **Save** (Figure 27.20.4) to save the AD settings.

Figure 27.20 - HCP Gateway UI File Upload


Enable Active Directory
Use SSL
Upload Certificate
1
Upload
Browse...
Domain_ldap.cer
Domain
DTS-EVLAB
Host
ev-dc1.dts-evlab.com
2
Port
636
Search Base
OU=HCPG,OU=People,I
Browse
3
Groups
User
CN=hcpg-accessRO,OU
Browse
Admin
CN=hcpg-accessRW,OU
Browse
Admin with Privileged Delete
Browse
4
Save

Restore HCP Gateway to a Different Server

Step 1 – Ensure an HCP Gateway backup was run on the original server that you want to restore to a different server and you will be directed to copy it to an appropriate location on the new server.

On original server

Refer to the **HCP Gateway Operations** chapter, **Section 1, Backup**, for information on how to configure the HCP Gateway backup to write the backup to an HCP namespace. Ensure that the backup location is \\localhost\operation$ (Figure 28.1W.1) in Windows or **/archive/.operation** in Linux (Figure 28.1L). If no backup exists, i.e., there is no entry in the **System Backup History** pane (Figure 28.1W/L.2), then click **Backup Now** on the HCP Gateway UI **Operations -> Backup** page (Figure 28.1W/L.3) to run a backup of the HCP Gateway.

NOTE:

On a Windows Cluster node, set the backup location to \\<cluster-name-or-ip-address>\operation$.

Figure 28.1W – Windows - Operations -> Backup Now

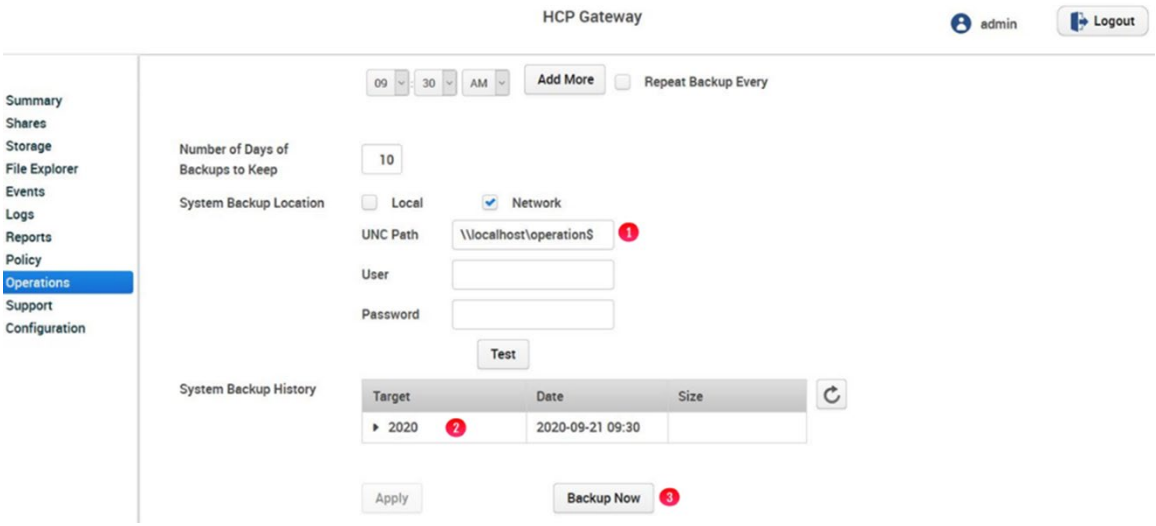
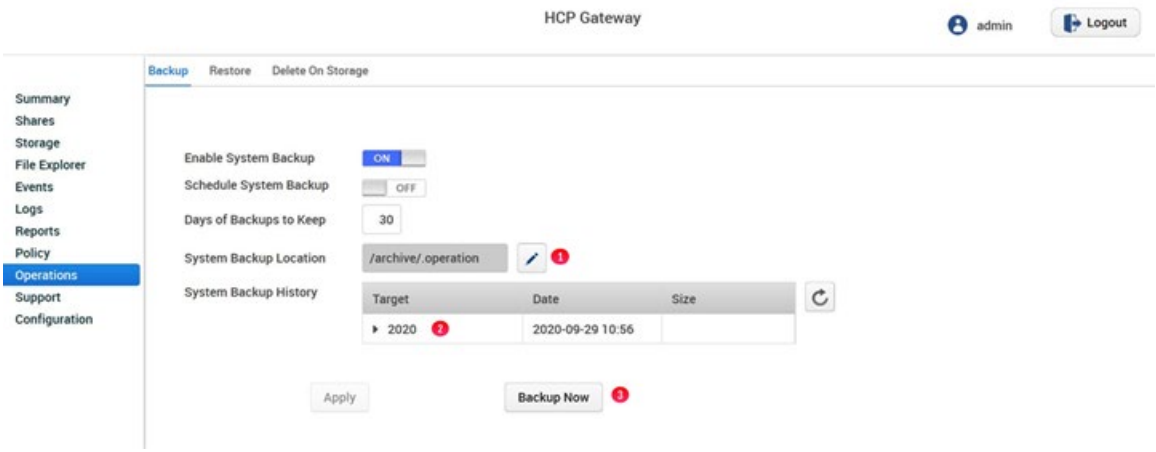


Figure 28.1L – Windows - Operations -> Backup Now



Step 2 – Deploy a new HCP Gateway with the same or newer version of HCP Gateway software.

On new server - New server deployed with latest version of HCP Gateway software, update configuration files to match original server

Check the new server system time and time zone, make sure the time and time zone are the same as the original server. If you don't have access to the original server, make sure the time on the new server is not set before the time of the backup on the original server.

In Windows, stop the Windows Services **SAM VFS** and **Wildfly**. Copy the **backup_<TIMESTAMP>.zip** file (Figure 28.2W.2) from the **operation$** share on the original server (Figure 28.2W.1) or the HCP Backup namespace <for example: **backup_2020-09-21_09-30.zip**> to **C:\Temp\Restore** on the new server.

In Linux, stop any Shares in the HCP Gateway UI. Then stop the **SAM License (saml)** and **Wildfly** services by using **putty** to open a ssh session to the HCP Gateway, login as the user **vault** with the password, then issue the command **sudo systemctl stop saml** and **sudo systemctl stop wildfly**. Copy the **backup_<TIMESTAMP>.zip** file (Figure 28.2L.2) from the **/archive/.operation** share on the original server (Figure 28.2L.1) or the HCP Backup namespace <for example: **backup_2020-09-29_10-56.zip>** to **/home/vault/restore** on the new server.

Figure 28.2W – Windows File Explorer – backup zip file

Figure 28.2L – Linux – Copy backup zip file

```
vault@hcpg-linux-1: ~
vault@hcpg-linux-1:~$ ls -lR /archive/.operation/Backup  1
/archive/.operation/Backup:
total 0
drwxrwxr-x 1 vault vault 0 Sep 29 10:56 2020

/archive/.operation/Backup/2020:
total 0
drwxrwxr-x 1 vault vault 0 Sep 29 10:56 09

/archive/.operation/Backup/2020/09:
total 0
drwxrwxr-x 1 vault vault 0 Sep 29 10:56 29

/archive/.operation/Backup/2020/09/29:
total 3503
-rw-r--r-- 1 root root 3586974 Sep 29 10:56 backup_2020-09-29_10-56.zip  2
vault@hcpg-linux-1:~$
```

In Windows, unzip the backup file from the old server that you copied into the **C:\Temp\Restore** folder on the new server. Open the file **C:\SAM\etc\sam\sam.properties** (Figure 28.4W.1) in **Notepad++**, set the **backup.***, **binlog.name, primary.server, server.id** (Figure 28.3W2 on original server and Figure 28.4W2 on new server) **and storage.dir** the same as in the file **C:\Temp\Restore\SAM\etc\sam\sam.properties** (Figure 28.3W.1) from the unzipped backup file. Add the line **point.protect=no** (Figure 28.4W.3) to the end of the **C:\SAM\etc\sam\sam.properties** file on the new server. Save the **C:\SAM\etc\sam\sam.properties** file on the new server.

In Linux, change directory to the **/home/vault/restore** folder on the new server and unzip the backup file from the old server that you copied into the **/home/vault/restore** folder on the new server by issuing the command **7z e backup_2020-09-29_10-56.zip**. Edit the file **/etc/sam/sam.properties** on the new server (Figure 28.4L.1) and set the **backup.***, **binlog.name, primary.server, server.id** (Figure 28.3L2 on original server and Figure 28.4L2 on new server) **and storage.dir** the same as in the file **/home/vault/restore/sam.properties** (Figure 28.3L.1) from the unzipped backup file from the original server. Save the **/etc/sam/sam.properties** file on the new server.

Figure 28.3W – Windows - Original server sam.properties

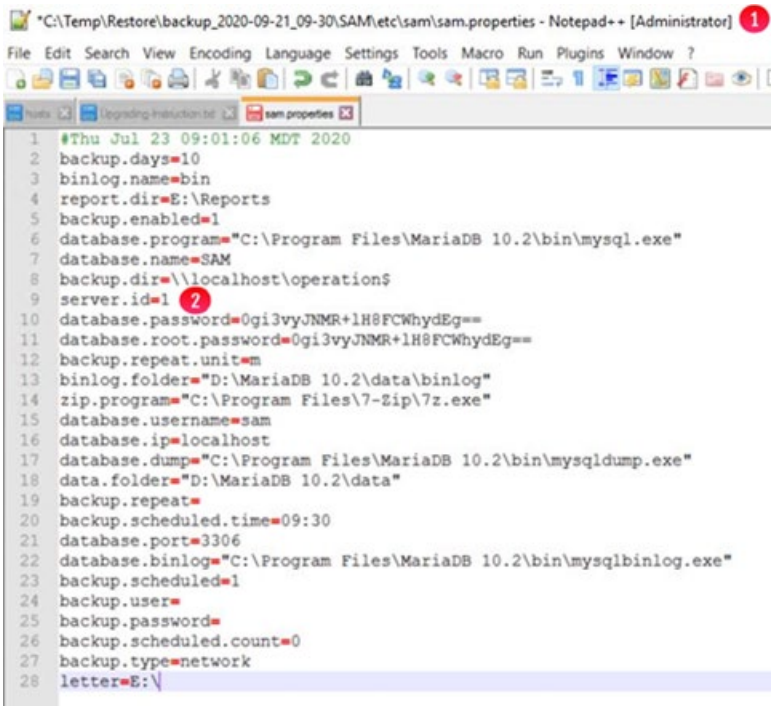


Figure 28.4W – Windows - New server sam.properties

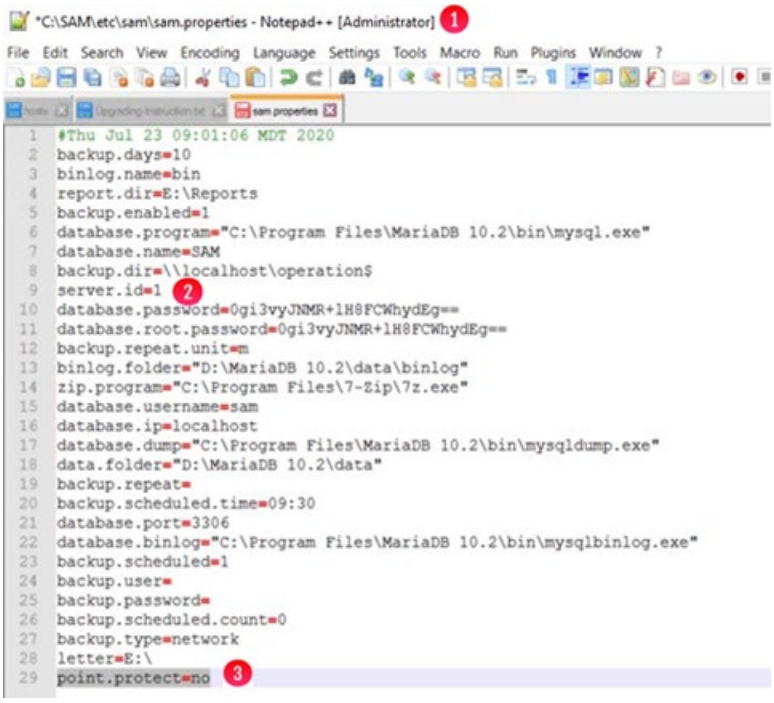


Figure 28.3L – Linux - Original server sam.properties

```
vault@hcpg-linux-1: ~
vault@hcpg-linux-1:~$ cat /etc/sam/sam.properties
#Mon Sep 14 06:25:02 MDT 2020
backup.days=30
backup.dir=/archive/.operation
backup.enabled=1
backup.list=/etc/sam/backup.list
backup.repeat=
backup.scheduled=0
binlog.folder=/var/log/mysql/binlog
binlog.name=hcpg-1-bin
cache.dir.priority=1
cache.dir=/storage/sam
database.binlog=/usr/bin/mysqlbinlog
database.dump=/usr/bin/mysqldump
database.ip=127.0.0.1
database.name=SAM
database.password=0gi3vyJNMR+lH8FCWhydEg==
database.port=3306
database.program=/usr/bin/mysql
database.root.password=0gi3vyJNMR+lH8FCWhydEg==
database.username=sam
primary.server=true
report.dir=/storage/reports
sam.version=1.1
server.id=1
storage.dir=/storage/local
tenant.mode=0
ui.test.login=true
vault@hcpg-linux-1:~$
```

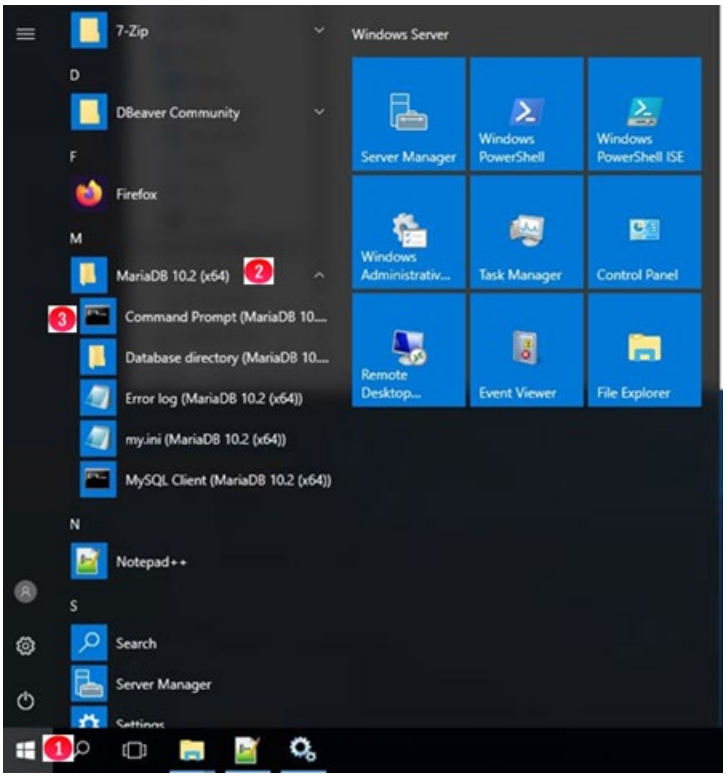
Figure 28.4L – Linux - New server sam.properties

```
vault@hcpg-linux-restore: ~/restore
#Mon Sep 14 06:25:02 MDT 2020
backup.days=30
backup.dir=/archive/.operation
backup.enabled=1
backup.list=/etc/sam/backup.list
backup.repeat=
backup.scheduled=0
binlog.folder=/var/log/mysql/binlog
binlog.name=hcpg-1-bin
cache.dir.priority=1
cache.dir=/storage/sam
database.binlog=/usr/bin/mysqlbinlog
database.dump=/usr/bin/mysqldump
database.ip=127.0.0.1
database.name=SAM
database.password=0gi3vyJNMR+lH8FCWhydEg==
database.port=3306
database.program=/usr/bin/mysql
database.root.password=0gi3vyJNMR+lH8FCWhydEg==
database.username=sam
primary.server=true
report.dir=/storage/reports
sam.version=1.1
server.id=1
storage.dir=/storage/local
tenant.mode=0
ui.test.login=true
~
"/etc/sam/sam.properties" 27 lines, 673 characters
```

Step 3 – Restore the database from the original server onto the new server.

In Windows, open the MariaDB Command Prompt by clicking the **Windows Start** button (Figure 28.5W.1), open the **MariaDB (x64)** menu (Figure 28.5W.2), and select **Command Prompt MariaDB** (Figure 28.5W.3).

Figure 28.5W – Open Command Prompt MariaDB



In Windows, issue the command **mysql -uroot -p4tomcat2** (Figure 28.6W.1). Note that if you changed the database root password when you deployed the HCP Gateway server, then use that password instead of the default.

In Linux, in the **putty** ssh session, issue the commands **sudo -i**, (Figure 28.6L.1), change directory to **/home/vault/restore** (Figure 28.6L.2) and then **mysql -uroot -p4tomcat2** (Figure 28.6L.3). Note that if you changed the database root password when you deployed the HCP Gateway server, then use that password instead of the default.

In the MySQL client, enter the commands:

drop database SAM; (Figure 28.6W.2 in Windows and Figure 28.6L.4 in Linux)

create database SAM; (Figure 28.6W.3 in Windows and Figure 28.6L.5 in Linux)

use SAM; (Figure 28.6W.4 in Windows and Figure 28.6L.6 in Linux)

In Windows, import the database backup from the **sam.<TIMESTAMP>.sql** file (for this example **sam.2020-09-21_09-30.sql**) from the unzipped backup folder in the **C:\Temp\Restore** folder into the new server database by issuing the following command:

source C:\Temp\Restore\backup_2020-09-21_09-30\sam.2020-09-21_09-30.sql (Figure 28.6W.5)

In Linux, import the database backup from the **SAM.<TIMESTAMP>.sql** file (for this example **SAM.2020-09-29_10-56.sql**) from the unzipped backup folder in the **/home/vault/restore** folder into the new server database by issuing the following command:

source /home/vault/restore/SAM.2020-09-29_10-56.sql; (Figure 28.6L.7)

Figure 28.6W – Windows - MySQL Commands to restore SAM database

```
Administrator: Command Prompt (MariaDB 10.2 (x64)) - mysql -uroot -p4tomcat2
Setting environment for MariaDB 10.2 (x64)

C:\Windows\system32>mysql -uroot -p4tomcat2 (1)
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 252
Server version: 10.2.32-MariaDB-log Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> drop database SAM; (2)
Query OK, 253 rows affected (0.14 sec)

MariaDB [(none)]> create database SAM; (3)
Query OK, 1 row affected (0.00 sec)

MariaDB [(none)]> use SAM; (4)
Database changed
MariaDB [SAM]> source C:\Temp\Restore\backup_2020-09-21_09-30\sam.2020-09-21_09-30.sql (5)
Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)
```

Figure 28.6L – Linux - MySQL Commands to restore SAM database

```
vault@hcpg-linux-restore: ~/restore
vault@hcpg-linux-restore:~/restore$ sudo -i (1)
root@hcpg-linux-restore:~# cd /home/vault/restore (2)
root@hcpg-linux-restore:/home/vault/restore# mysql -uroot -p4tomcat2 (3)
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 67
Server version: 10.4.14-MariaDB-1:10.4.14+maria~buster-log mariadb.org binary di
stribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> drop database SAM; (4)
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> create database SAM; (5)
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> use SAM; (6)
Database changed
MariaDB [SAM]> source /home/vault/restore/SAM.2020-09-29_10-56.sql; (7)
Query OK, 0 rows affected (0.000 sec)

Query OK, 0 rows affected (0.000 sec)

Query OK, 0 rows affected (0.000 sec)

Query OK, 0 rows affected (0.000 sec)
```

In both Windows and Linux, issue the command **use SAM;** (Figure 28.7W/L.1) to make sure the MySQL client is using the **SAM** database. **Drop** the **license** table by issuing the

command **drop table license**; (Figure 28.7W/L.2) in the **SAM** database because the license from the old server will not be valid on the new server. Contact Hitachi Support to generate a new license key for the new server. Issue the command **exit** (Figure 28.7W/L.3) to close the MySQL client.

Figure 28.7W – Windows - MySQL Commands to drop license table

```
MariaDB [sam]> use SAM;
Database changed
MariaDB [SAM]> drop table license;
Query OK, 0 rows affected (0.00 sec)

MariaDB [SAM]> exit
Bye

C:\Windows\system32>
```

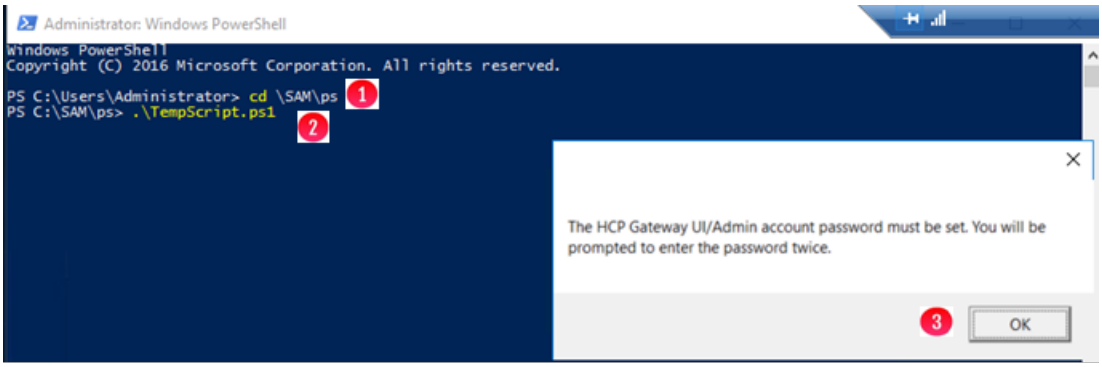
Figure 28.7L – Linux - MySQL Commands to drop license table

```
Query OK, 0 rows affected (0.000 sec)

Query OK, 0 rows affected (0.000 sec)

Query OK, 0 rows affected (0.000 sec)

MariaDB [SAM]> use SAM;
Database changed
MariaDB [SAM]> drop table license;
Query OK, 0 rows affected (0.001 sec)

MariaDB [SAM]> exit
Bye
root@hcpg-linux-restore:/home/vault/restore#
```

The new server now has all the information about the files in its HCP Gateway database. If you had local storage on the old server, you will now need to connect that storage from the old server to this new server in order to be able to access the file content.

Optionally in Windows, you can reset the server passwords to the passwords from original server, refer to the **VM Deployment Guide** chapter **Changing HCP Gateway Passwords** for details. To start the process to change the passwords, open a Windows PowerShell window, change directory to **\SAM\ps** (Figure 28.8.1) and enter the command **.\TempScript.ps1** (Figure 28.8.2). Then click **OK** in the popup window (Figure 28.8.3) to start the process to reset the UI admin password.

Figure 28.8 – Reset password



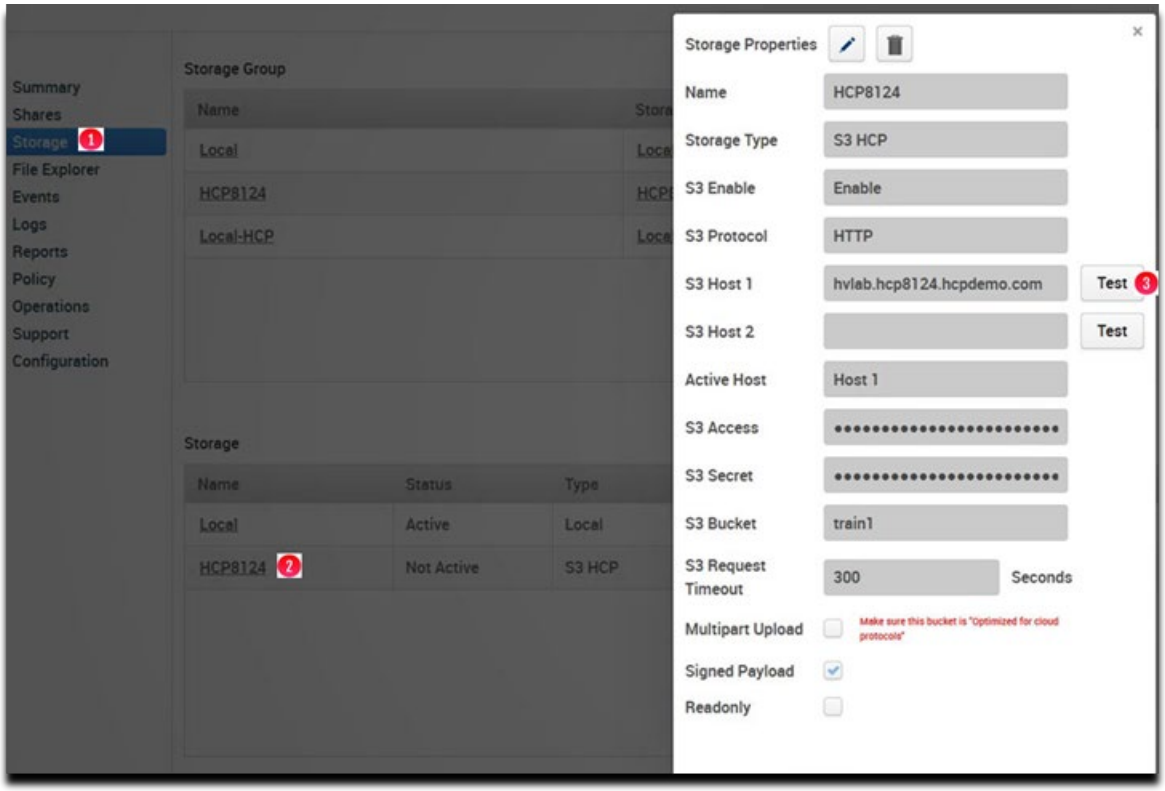
Step 4 – Test the HCP storage.

In Windows, reboot the new Gateway then open a web browser and login to HCP Gateway UI using the URL https://localhost:28443/hcpg, as the user **admin.**

In Linux, reboot the Gateway then open a web browser and login to HCP Gateway UI using the URL **Error! Hyperlink reference not valid.**, as the user **admin.**

Navigate to the **Storage** page (Figure 28.9.1), click on the **Name** of each HCP Storage (Figure 28.9.2) and then click the **Test** button (Figure 28.9.3) to make sure that all of the HCP storages are active.

Figure 28.9 – Test HCP Storage



Step 5 – Start the shares.

Login to the Gateway UI, select Shares and if the shares are Off Line, select the Start button for each share that needs to be started.

At this point, all of the file content is on the HCP Gateway storage, local and/or HCP, and none of the files are in the cache on the HCP Gateway. For the shares where the Enable Cache is set to Yes and for shares with a Server Mode Copy policy, the file content will be copied from the storage to the cache the first time you read a file.

Step 6 – Optionally configure the HCP Gateway Backup in the **Operations -> Backup** page in the UI. If the old server is no longer running, the on the new server in the HCP Gateway UI, navigate to the **Operations -> Backup** page and ensure that the backup configuration is using **Network** and \\localhost\operation$ for Windows and **/archive/.operation** for Linux. Refer to the HCP Gateway Operations chapter in this document for more information.

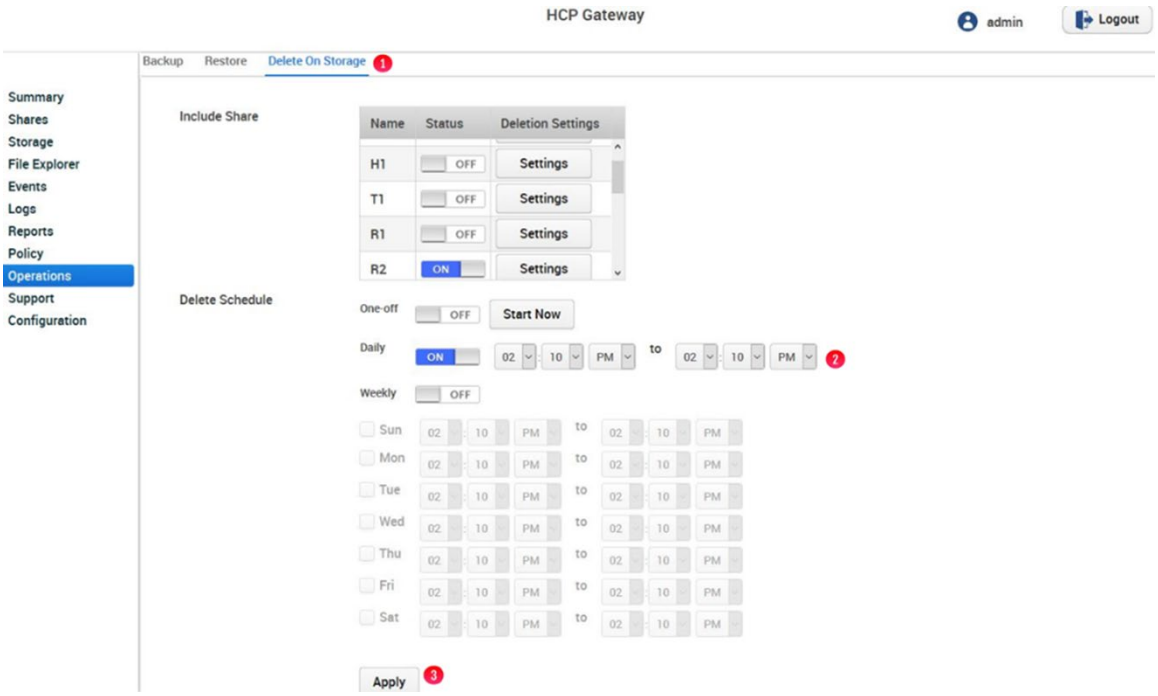
NOTE:

On a Windows Cluster node, set the backup location to \\<cluster-name-or-ip-address>\operation$.

Step 7 – Reset the Delete on Storage schedule.

In the HCP Gateway UI, navigate to the **Operations -> Delete On Storage** page (Figure 28.10.1). If there is an existing **Delete Schedule** (Figure 28.10.2), click the **Apply** button (Figure 28.10.3) at the bottom of the page to set the schedule in the new server.

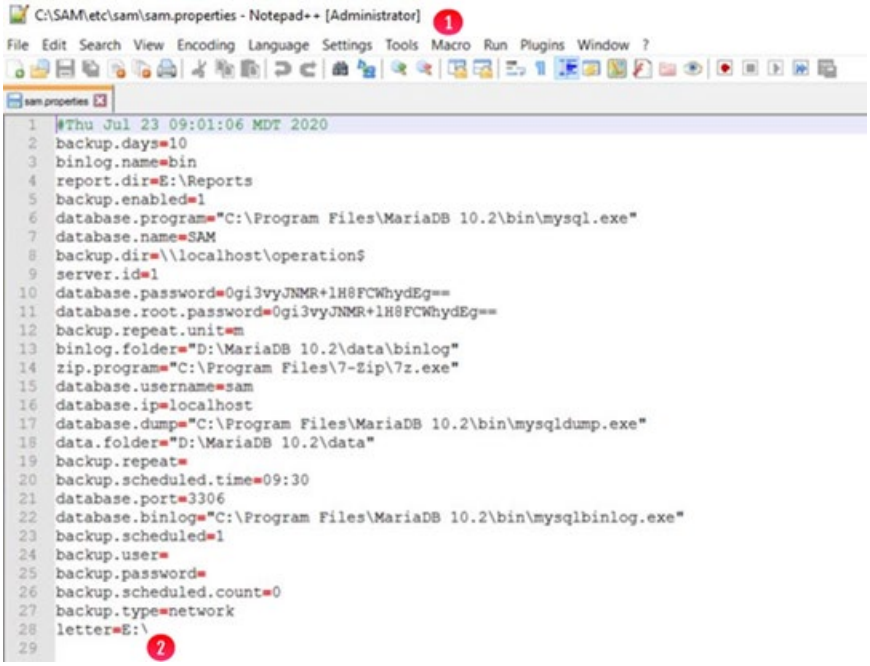
Figure 28.10 – Set Delete on Storage Schedule



Step 8 – (Windows only) Remove the **point.protect=no** line from the **C:\SAM\etc\sam\sam.properties** file.

Open the file **C:\SAM\etc\sam\sam.properties** file (Figure 28.11.1) with **Notepad++** and remove the line that contains **point.protect=no** (Figure 28.11.2). Save the file and exit **Notepad++**. Then in the **Windows Services** panel, restart the **SAM VFS** service, which will restart all of the shares.

Figure 28.11 – Remove point.protect=no


C:\SAM\etc\sam\sam.properties - Notepad++ [Administrator]
1
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
sam.properties
#Thu Jul 23 09:01:06 MDT 2020
backup.days=10
binlog.name=bin
report.dir=E:\Reports
backup.enabled=1
database.program="C:\Program Files\MariaDB 10.2\bin\mysql.exe"
database.name=SAM
backup.dir=\\localhost\operation$
server.id=1
database.password=0gi3vyJNMR+lH8FCWhydEg==
database.root.password=0gi3vyJNMR+lH8FCWhydEg==
backup.repeat.unit=m
binlog.folder="D:\MariaDB 10.2\data\binlog"
zip.program="C:\Program Files\7-Zip\7z.exe"
database.username=sam
database.ip=localhost
database.dump="C:\Program Files\MariaDB 10.2\bin\mysqldump.exe"
data.folder="D:\MariaDB 10.2\data"
backup.repeat=
backup.scheduled.time=09:30
database.port=3306
database.binlog="C:\Program Files\MariaDB 10.2\bin\mysqlbinlog.exe"
backup.scheduled=1
backup.user=
backup.password=
backup.scheduled.count=0
backup.type=network
letter=E:\
2

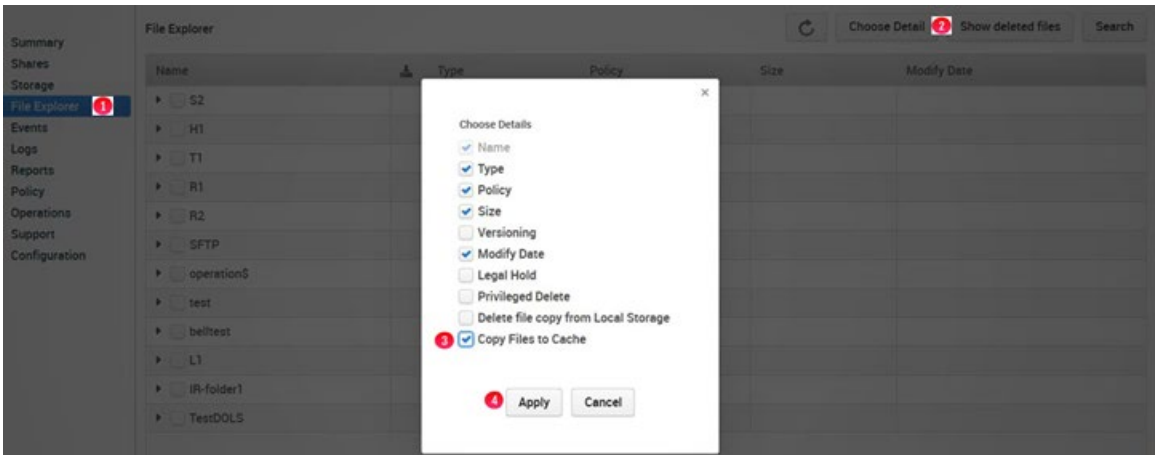
Copy Files to Cache

The Copy Files to Cache feature allows the user(s) assigned the Privileged Delete permission in the Share page of the HCP Gateway UI, to copy file content from HCP storage, for example an HCP namespace, to the HCP Gateway cache for fast access. The share must have the **Enable Cache** set to **Yes** for the files to remain in the cache after ingest, or after the next access of the file if the file was released from cache by the cache watermark. See the HCP Gateway Shares chapter for the details on this setting.

Step 1: In a web browser, open the HCP Gateway UI and log in as the user with the **Privileged Delete** permission for the share you want to copy file content from storage to cache.

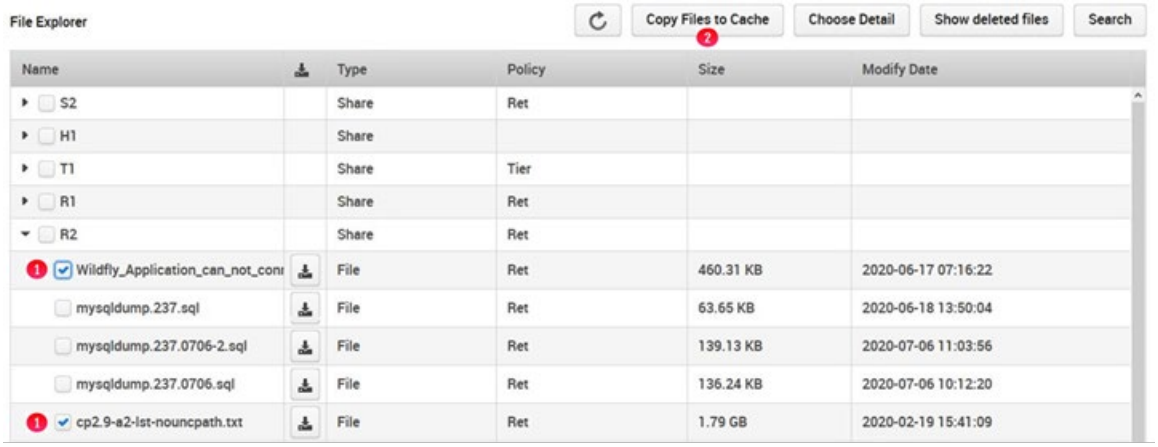
Step 2: Click the **File Explorer** tab (Figure 29.1.1), then click **Choose Detail** (Figure 29.1.2). Select the **Copy Files to Cache** (Figure 29.1.3) option, then click **Apply** (Figure 29.1.4) to apply the setting. Note that you may have to follow this step every time you enter the File Explorer tab.

Figure 29.1 – Choose Copy Files to Cache Detail



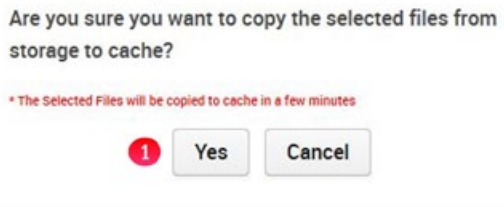
Step 3: Browse to the share, then the folder and select the file(s) to copy from Storage to cache by selecting the name of the file in the **Name** column (Figure 29.2.1) then click **Copy Files to Cache** (Figure 29.2.2).

Figure 29.2 – Select files to Copy to Cache



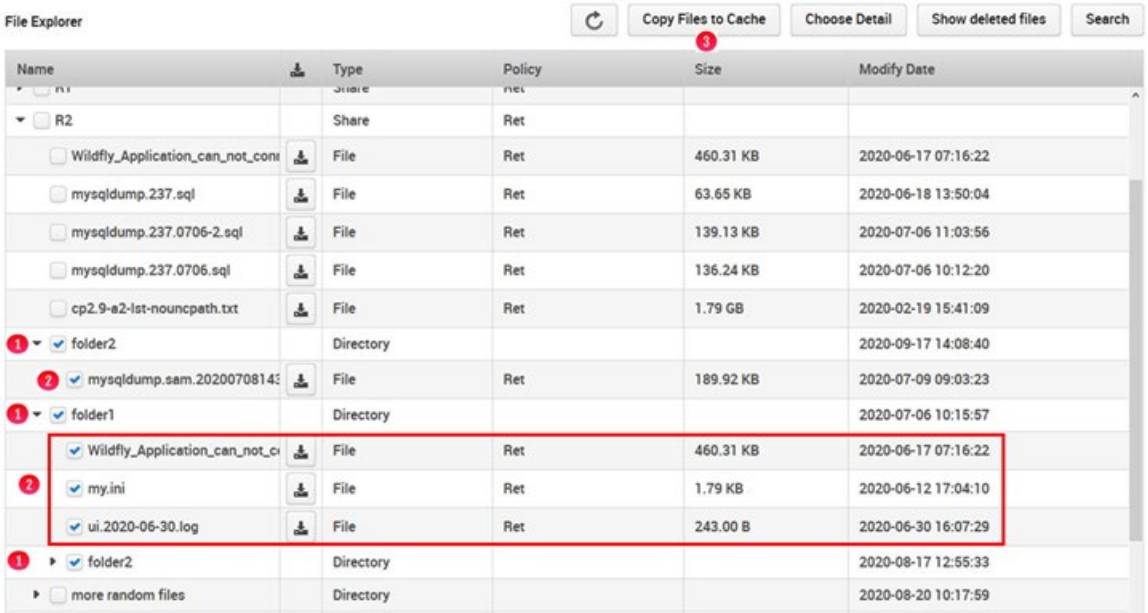
Step 4: Click **Yes** to copy of the file(s) from storage to Cache (Figure 29.3.1). Note that the amount of time to copy the files from storage to cache depends on how much data was selected.

Figure 29.3 – Confirm selection



Step 5: Alternatively, you can select a folder(s) of files to copy from storage to Cache (Figure 29.4.1) Notice that all the files and folders in the folder are now selected for copying from storage to Cache (Figure 29.4.2). Click **Copy Files to Cache** (Figure 29.4.3).

Figure 29.4 –Select Folder(s) to Copy Files to Cache



NOTE:

Refer to Chapter 12 HCP Gateway File Explorer for an example of how to automatically select files to copy to cache.

Step 6: Click **Yes** to copy of the file(s) from storage to Cache (Figure 29.5.1). Note that the amount of time to copy the files from storage to cache depends on how much data was selected.

Figure 29.5 – Confirm selection

Upgrade MariaDB 10.2 to 10.4

In the HCP Gateway version 4.1.3, the MariaDB database application was upgraded from version 10.2 to version 10.4. If the Gateway that is running is not using MariaDB version 10.4, then follow these directions to upgrade the MariaDB database application.

Windows MariaDB Upgrade Process

This chapter will cover the process to upgrade the HCP Gateway Windows MariaDB database application from version 10.2 to version 10.4.

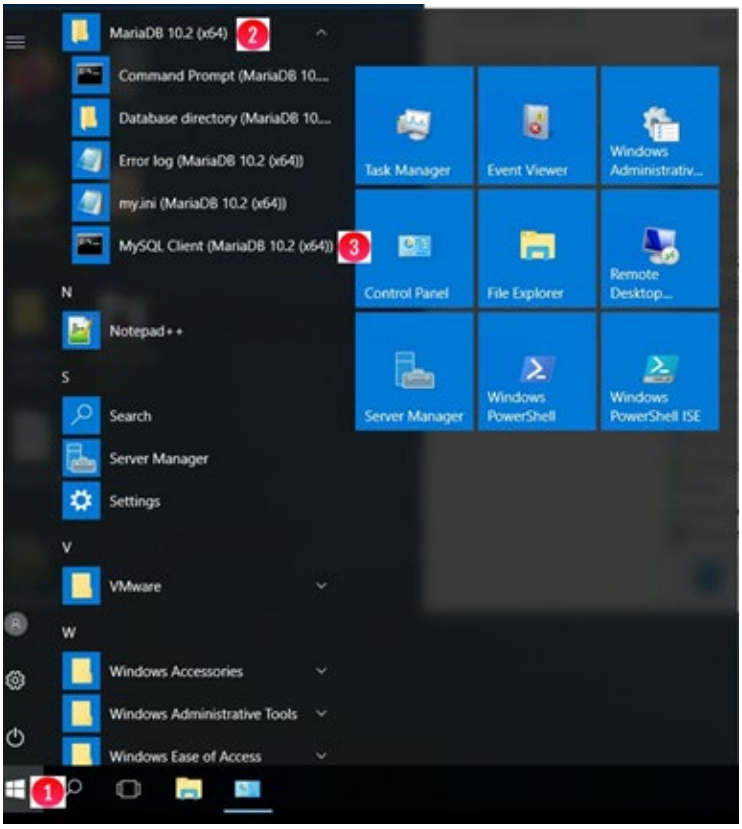
Note:

In MariaDB version 10.4 the database is installed in D:\MariaDB\data instead of in version 10.2 where the database was installed in D:\MariaDB 10.2\data.

Login to the HCP Gateway Windows OS as the local Administrator.

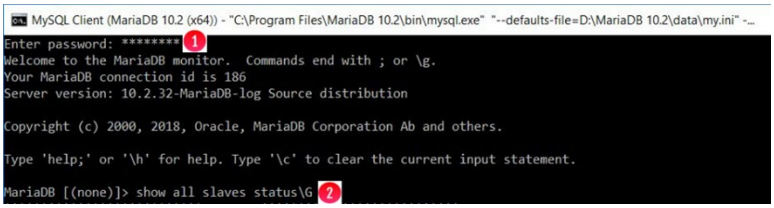
Step 1 – If database replication is configured, on all replication nodes, select the **Windows Start button** (Figure 30.1.1), then select the **MariaDB 10.2 (x64)** folder (Figure 30.1.2), then select **MySQL Client (MariaDB 10.2 (x64))** (Figure 30.1.3). If database replication is not configured, skip to Step 4.

Figure 30.1 – Open MySQL Client



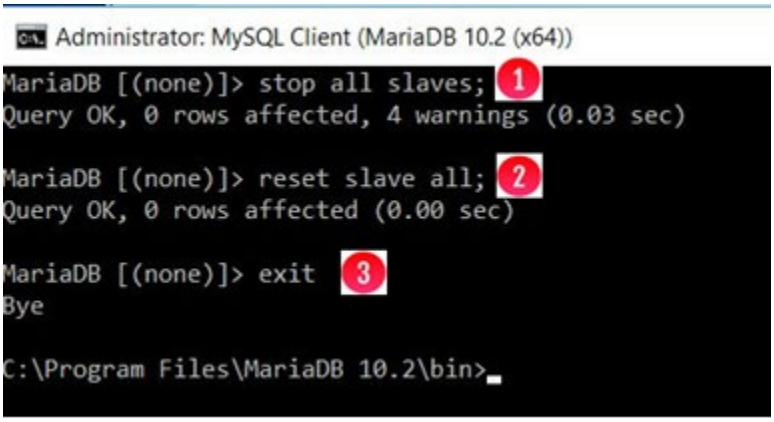
Step 2 – On all nodes, when prompted, enter the **database root password** (Figure 30.2.1). Check the replication status by issuing the **show all slaves status\G** command (Figure 30.2.2). It is required to resolve any errors before continuing.

Figure 30.2 –Check Replication Status



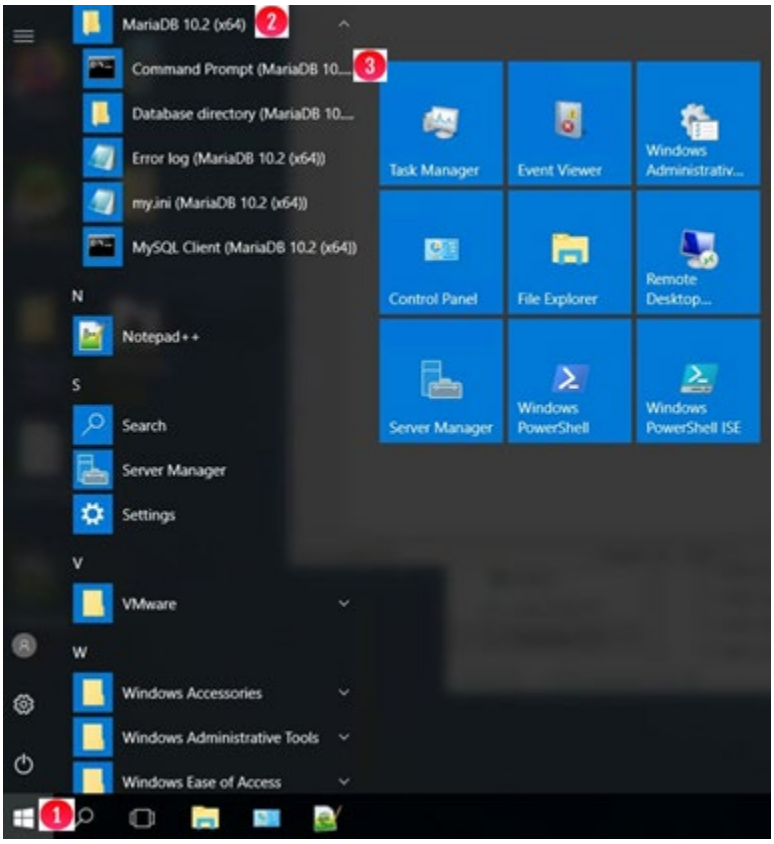
Step 3 – On all nodes, stop the replication by issuing the **stop all slaves**; command (Figure 30.3.1) and reset the replication by issuing the **reset slave all;** command (Figure 30.3.2). Issue the **exit** command to close the MySQL Client (Figure 30.3.3). Close the **MySQL Client** window.

Figure 30.3 – Stop and Reset Replication



Step 4 – On all nodes, select the **Windows Start button** (Figure 30.4.1), open the **MariaDB 10.2 (x64)** folder (Figure 30.4.2), then select **Command Prompt (MariaDB 10.2 (x64))** (Figure 30.4.3).

Figure 30.4 – Open MariaDB Command Prompt

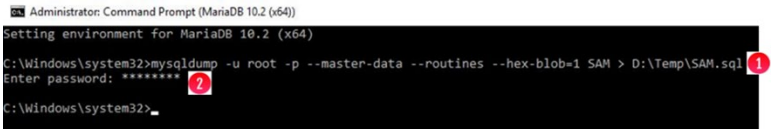


Step 5 – On all nodes, make a backup copy of the SAM database by issuing the command **mysqldump -u root -p --master-data --routines --hex-blob=1 --ssl=1 SAM > D:\Temp\SAM.sql** (Figure 30.5.1). If the D:\Temp folder does not exist (the error "The system cannot find the path specified." will be displayed), create the D:\Temp folder then run the command again. When prompted, enter the database root password (Figure 30.5.2).

NOTE:

This step will make a backup copy the SAM database.

Figure 30.5 – Backup SAM Database



Step 6 – On all nodes, make a copy of the **D:\MariaDB 10.2\data\my.ini** by issuing the **copy "D:\MariaDB 10.2\data\my.ini" D:\Temp** command (Figure 30.6.1). Create the **D:\Temp\cert** folder by issuing the **mkdir D:\Temp\cert** command (Figure 30.6.2). Make a copy of the **D:\MariaDB 10.2\cert** directory by issuing the copy **"D:\MariaDB 10.2\cert" D:\Temp\cert** command (Figure 30.6.3).

Figure 30.6 – Backup MariaDB Configuration Files

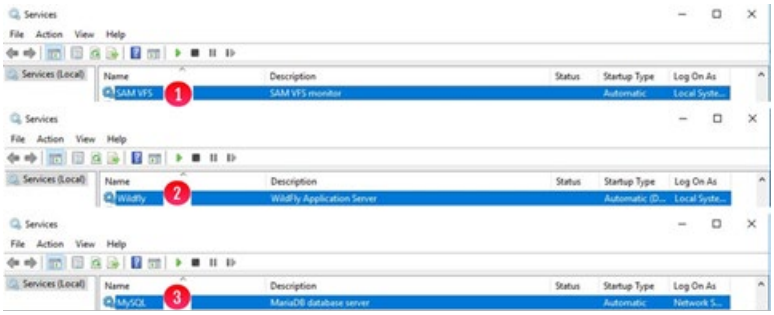
```
Administrator: Command Prompt (MariaDB 10.2 (x64))
Setting environment for MariaDB 10.2 (x64)

C:\Windows\system32>mysqldump -u root -p --routines --hex-blob=1 SAM > D:\Temp\SAM.sql
Enter password: ********

C:\Windows\system32>copy "D:\MariaDB 10.2\data\my.ini" D:\Temp        (1)
        1 file(s) copied.

C:\Windows\system32>mkdir D:\Temp\cert        (2)

C:\Windows\system32>copy "D:\MariaDB 10.2\cert"  D:\Temp\cert\        (3)
D:\MariaDB 10.2\cert\ca-cert.pem
D:\MariaDB 10.2\cert\ca-key.pem
D:\MariaDB 10.2\cert\client-cert.pem
D:\MariaDB 10.2\cert\client-key.pem
D:\MariaDB 10.2\cert\client-req.pem
D:\MariaDB 10.2\cert\client.p12
D:\MariaDB 10.2\cert\mariadb-ca-cert.crt
D:\MariaDB 10.2\cert\server-cert.pem
D:\MariaDB 10.2\cert\server-key.pem
D:\MariaDB 10.2\cert\server-req.pem
       10 file(s) copied.

C:\Windows\system32>_
```

Step 7 – On all nodes, open the Windows **Services** panel and if running, stop the **SAM VFS** (Figure 30.7.1), **Wildfly** (Figure 30.7.2) and **MySQL** (Figure 30.7.3) services.

NOTE:

If upgrading nodes in a Microsoft Failover Cluster, only 1 node, the active node should have the SAM VFS service running. Use the Failover Cluster Manager to take the SAM VFS service offline on the active node.

Figure 30.7 – Stop Windows Services

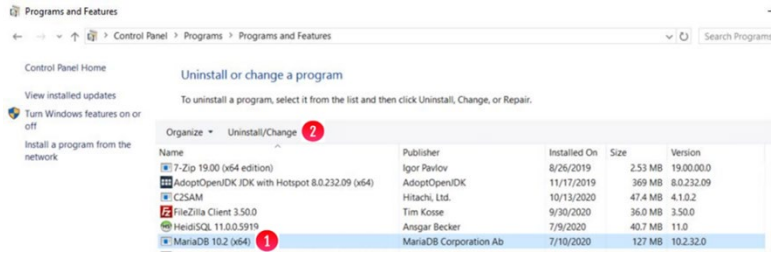


Step 8 – On all nodes, open Windows **Control Panel** and select **Uninstall a Program** (Figure 30.8.1).

Figure 30.8 – Windows Control Panel

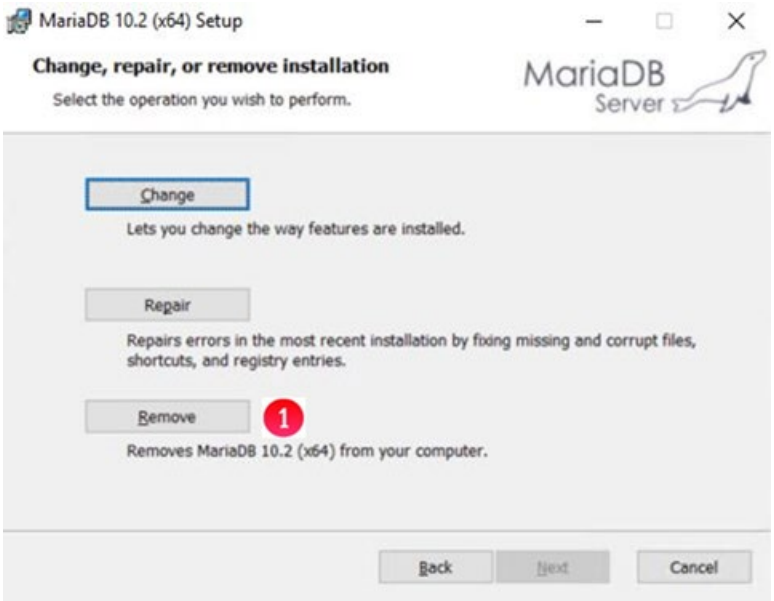
Step 9 – On all nodes, select **MariaDB 10.2 (x64)** (Figure 30.9.1) and select **Uninstall/Change** (Figure 30.9.2).

Figure 30.9 – Windows Control Panel



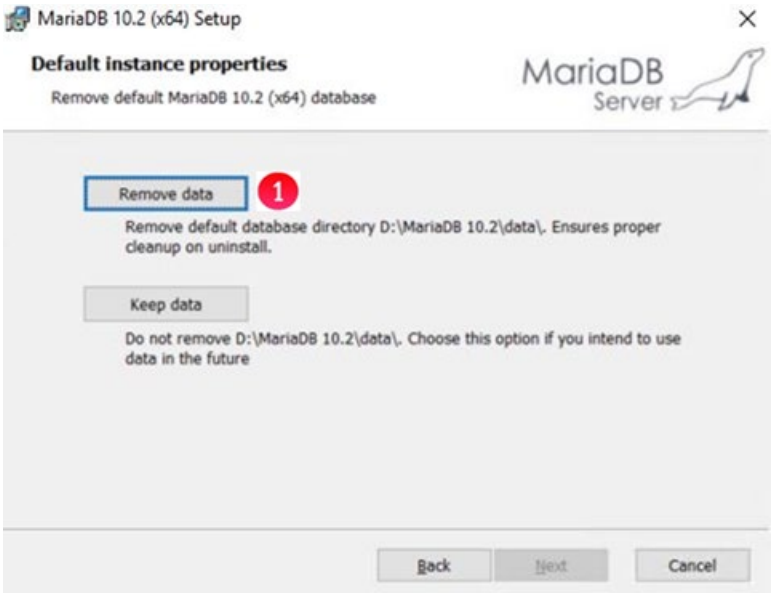
Step 10 – On all nodes, select **Next** in the **Welcome to the MariaDB 10.2 (x64) Setup Wizard**. In the **Change, repair or remove installation** screen, select **Remove** (Figure 30.10.1).

Figure 30.10 – MariaDB Setup Wizard



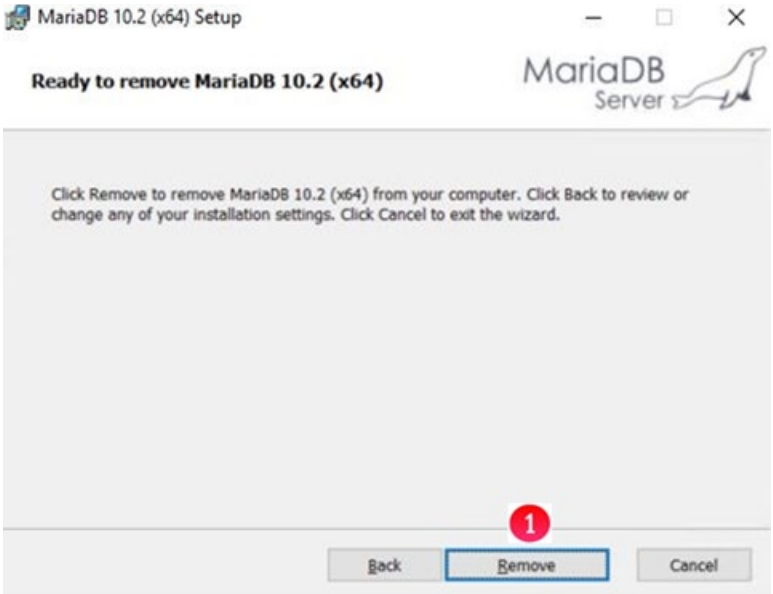
Step 11 – On all nodes, select **Remove data** (Figure 30.11.1).

Figure 30.11 – MariaDB Setup Wizard 2



Step 12 – On all nodes, select **Remove** (Figure 30.12.1).

Figure 30.12 – MariaDB Setup Wizard 3

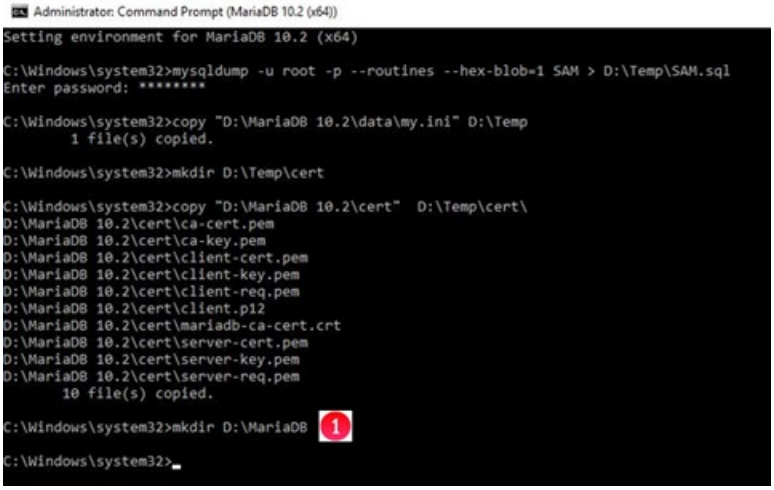


Step 13 – On all nodes, when the uninstall completes, select **Finish** (Figure 30.13.1).

Figure 30.13 – MariaDB Uninstall Complete

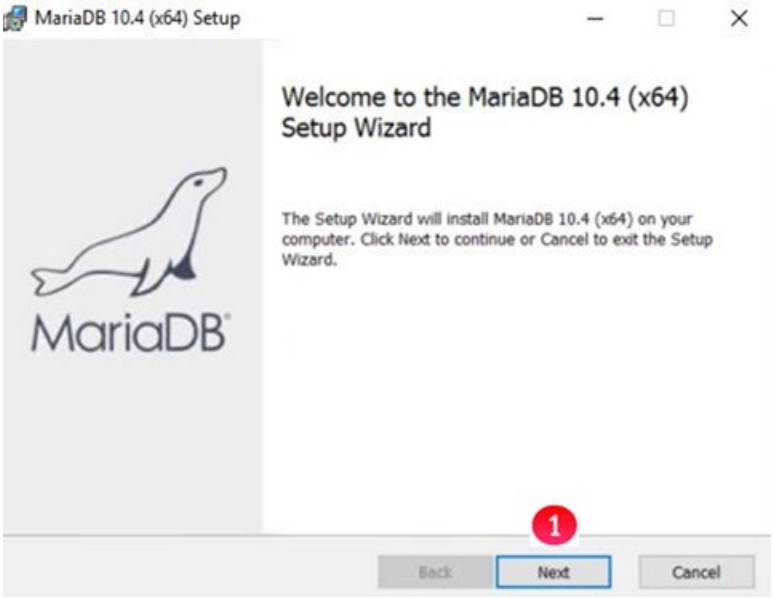
Step 14 – On all nodes, create the D:\MariaDB folder by issuing the command **mkdir D:\MariaDB** (Figure 30.14.1).

Figure 30.14 – Create D:\MariaDB folder



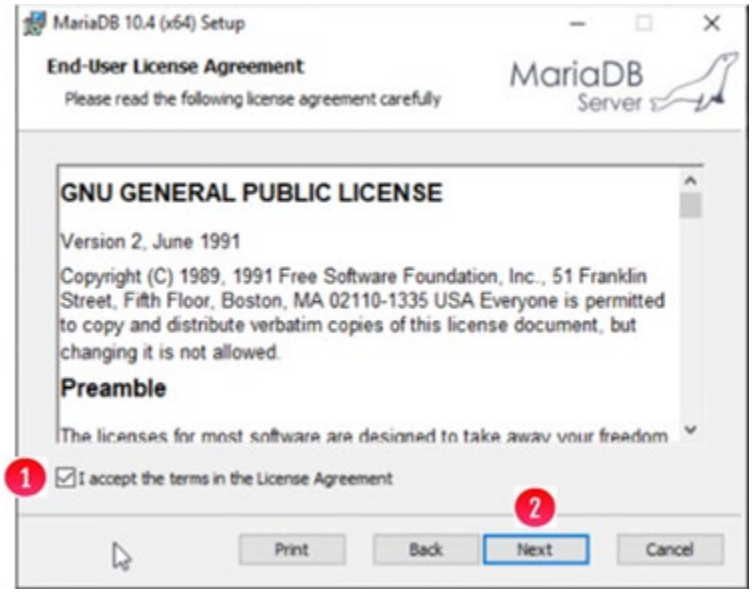
Step 15 – On all nodes, in Windows File Explorer, double-click on the **mariadb-10.4.22-winx64.msi** that is included in the HCP Gateway 4.2.0 software release upgrade package. In the **Welcome to the MariaDB 10.4 (x64) Setup Wizard,** select **Next** (Figure 30.15.1).

Figure 30.15 – MariaDB 10.4 Setup Wizard



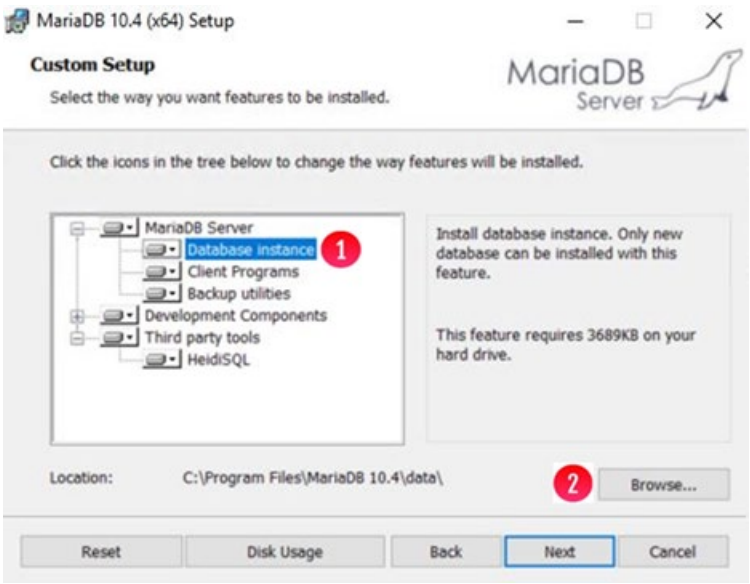
Step 16 – On all nodes, select the box to accept the License Agreement (Figure 30.16.1), then select **Next** (Figure 30.16.2).

Figure 30.16 – End-User License Agreement



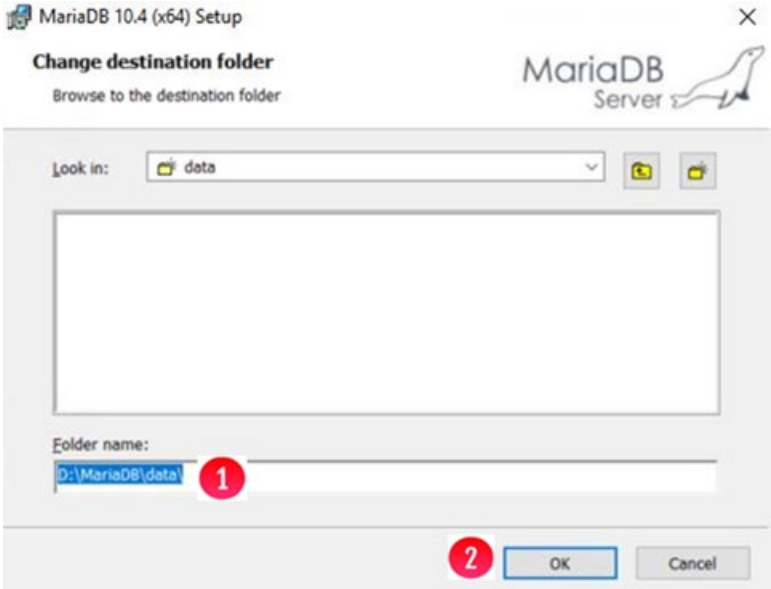
Step 17 – On all nodes, select **Database instance** (Figure 30.17.1), then select **Browse** (Figure 30.17.2).

Figure 30.17 – End-User License Agreement



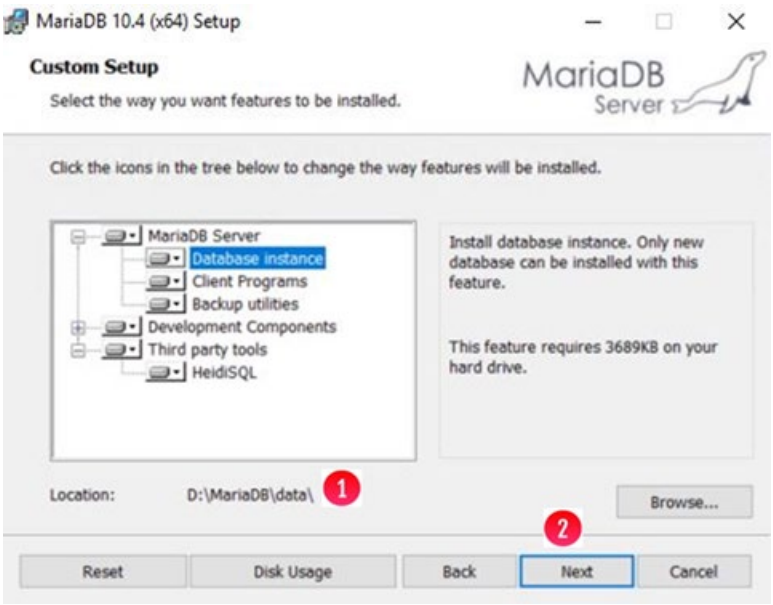
Step 18 – On all nodes, enter the folder name **D:\MariaDB\data** (Figure 30.18.1), then select **OK** (Figure 30.18.2).

Figure 30.18 – Change Destination Folder



Step 19 – On all nodes, verify the **Location is D:\MariaDB\data** (Figure 30.19.1), then select **Next** (Figure 30.19.2).

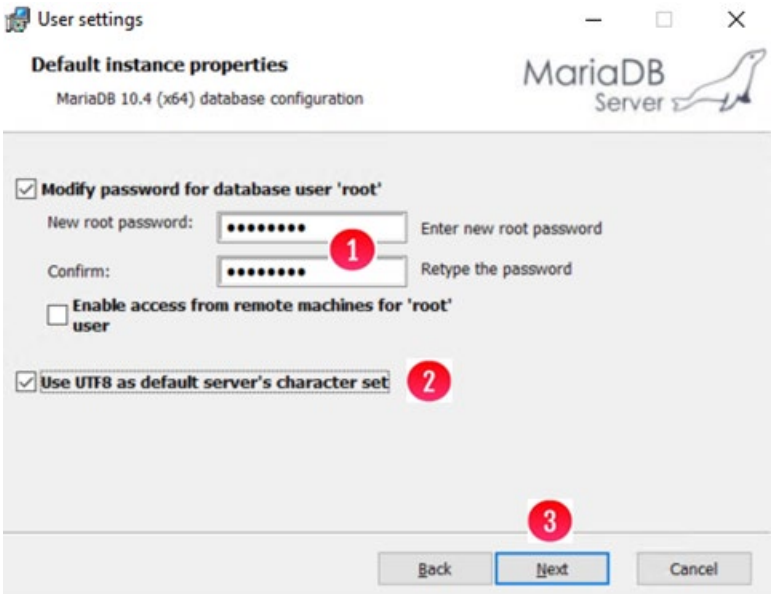
Figure 30.19 – Custom Setup



Step 20 – On all nodes, enter the default root password **4tomcat2** (Figure 30.20.1), select **Use UTF8 as default server's character set** (Figure 30.20.2), then select **Next** (Figure 30.20.3).

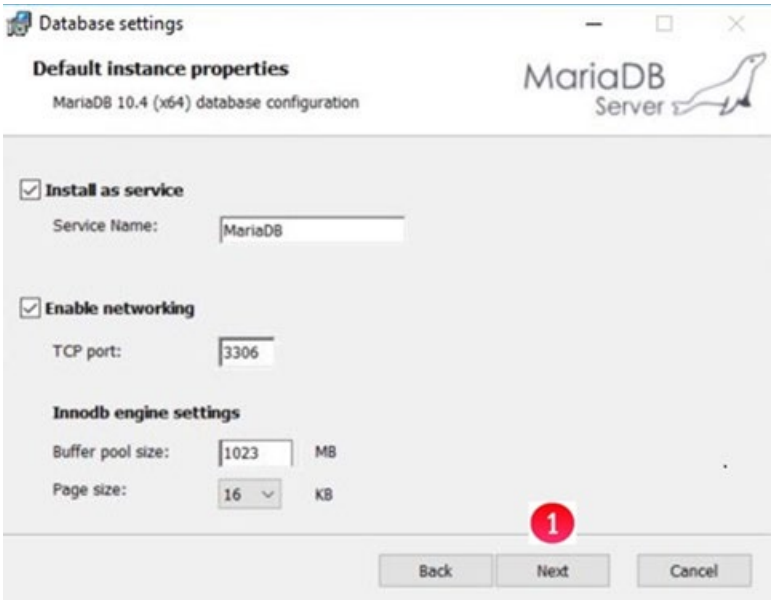
WARNING: When the Gateway was first deployed or if the password reset script was run before Gateway version 4.1.5, if the database **root** user account password was set to something other than the default **4tomcat2,** then enter the same password here that was entered when the Gateway was deployed or the password reset script was run.

Figure 30.20 – User Settings



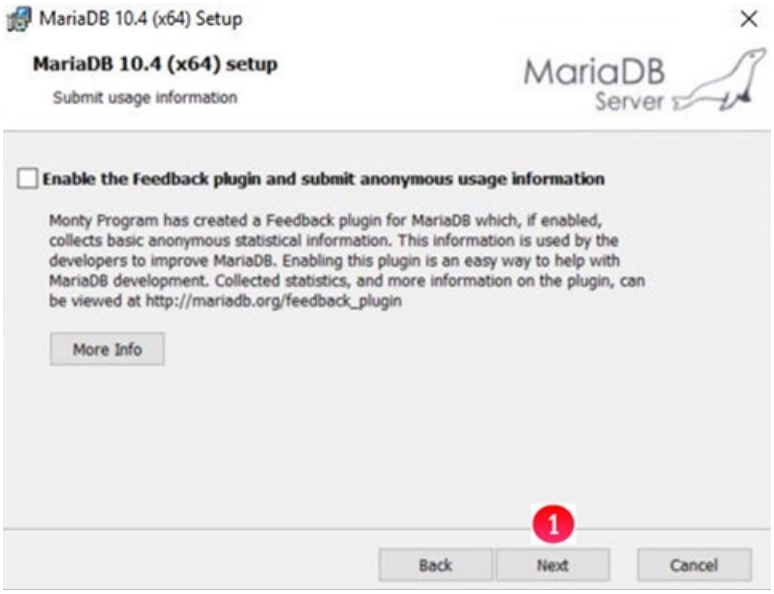
Step 21 – On all nodes, accept all the defaults, do not change anything, then select **Next** (Figure 30.21.1).

Figure 30.21 – Database Settings



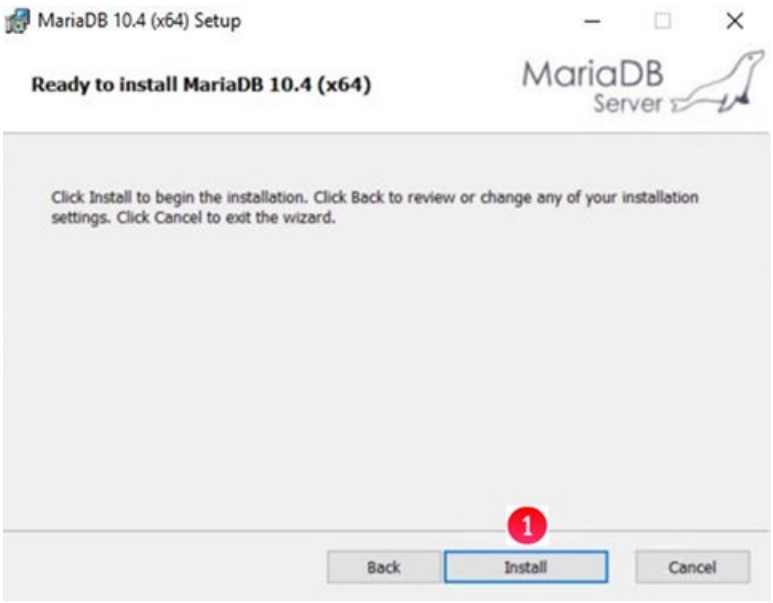
Step 22 – On all nodes, accept all the defaults, do not change anything, then select **Next** (Figure 30.22.1).

Figure 30.22 – Submit usage information



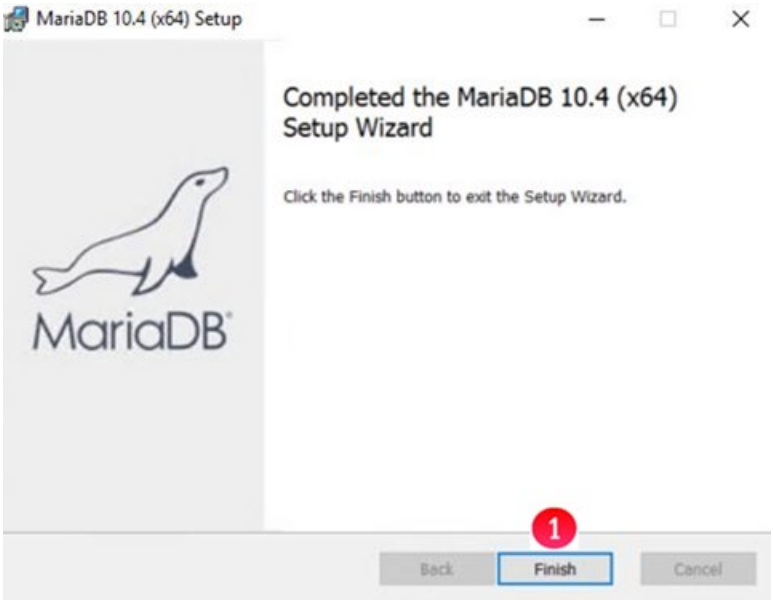
Step 23 – On all nodes, select **Install** (Figure 30.23.1).

Figure 30.23 – Ready to install



Step 24 – On all nodes, select **Finish** (Figure 30.24.1).

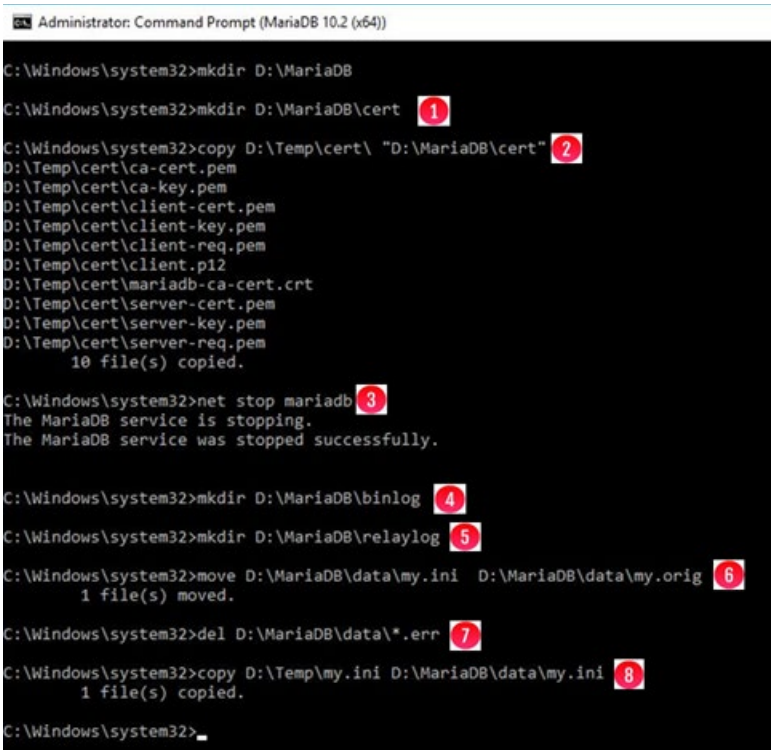
Figure 30.24 – Completed Setup



Step 25 – On all nodes, create the folder **D:\MariaDB\cert** by issuing the command **mkdir D:\MariaDB\cert** (Figure 30.25.1). Restore the database certificate files to the **D:\MariaDB\cert** folder by issuing the command **copy D:\Temp\cert\ "D:\MariaDB\cert"** (Figure 30.25.2). Stop the Windows Service MariaDB by issuing the command **net stop mariadb** (Figure 30.25.3). Create the **D:\MariaDB\binlog** folder by issuing the command **mkdir D:\MariaDB\binlog** (Figure 30.25.4). Create the **D:\MariaDB\relaylog** folder by issuing the command **mkdir D:\MariaDB\relaylog** (Figure 30.25.5). Backup the new MariaDB my.ini configuration file by issuing the command **move D:\MariaDB\data\my.ini D:\MariaDB\data\my.orig** (Figure 30.25.6). Delete the MariaDB error log file by issuing the command **del D:\MariaDB\data*.err** (Figure 30.25.7). Restore the original MariaDB **my.ini**

configuration file by issuing the command **copy D:\Temp\my.ini D:\MariaDB\data\my.ini** (Figure 30.25.8)

Figure 30.25 – MariaDB 10.4 configuration



Step 26 – On all nodes, open Notepad++ and edit the MariaDB 10.4 configuration file **D:\MariaDB\data\my.ini**. Change any path names referencing the **C:** drive from **MariaDB 10.2** to **MariaDB 10.4**. Change any path names referencing the **D:** drive from **MariaDB 10.2** to **MariaDB**. If needed, add the line **tmpdir=D:/Temp** (Figure 30.26). If not already done, add a **'#'** at the beginning of the line to comment out the line **ssl-cipher = TLSv1.2**. If not already done, change the lines **log_bin** and **relay-log** to include the node number,

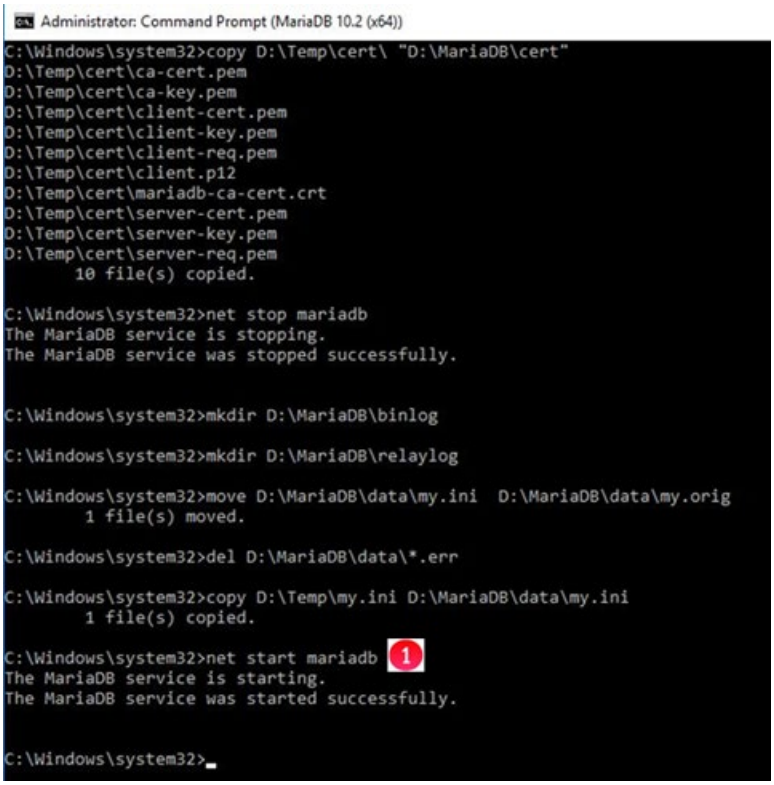
log_bin=D:/MariaDB/binlog/hcpg-1-bin and **relay-log=D:/MariaDB/relaylog/hcpg-1-relay** for node **1, log_bin=D:/MariaDB/binlog/hcpg-2-bin** and **relay-log=D:/MariaDB/relaylog/hcpg-2-relay** for node **2**, etc. If not already done, remove the line **innodb_buffer_pool_size=2047M**. Save the updated **my.ini** file and close Notepad++.

Figure 30.26 – Update MariaDB 10.4 configuration file

```
plugin-dir=C:/Program Files/MariaDB 10.4/lib/plugin

datadir=D:/MariaDB/data
tmpdir=D:/Temp

ssl-ca   = "D:/MariaDB/cert/ca-cert.pem"
ssl-cert = "D:/MariaDB/cert/server-cert.pem"
ssl-key  = "D:/MariaDB/cert/server-key.pem"
#ssl-cipher = TLSv1.2

log_bin          = D:/MariaDB/binlog/hcpg-1-bin

relay-log        = D:/MariaDB/relaylog/hcpg-1-relay
```

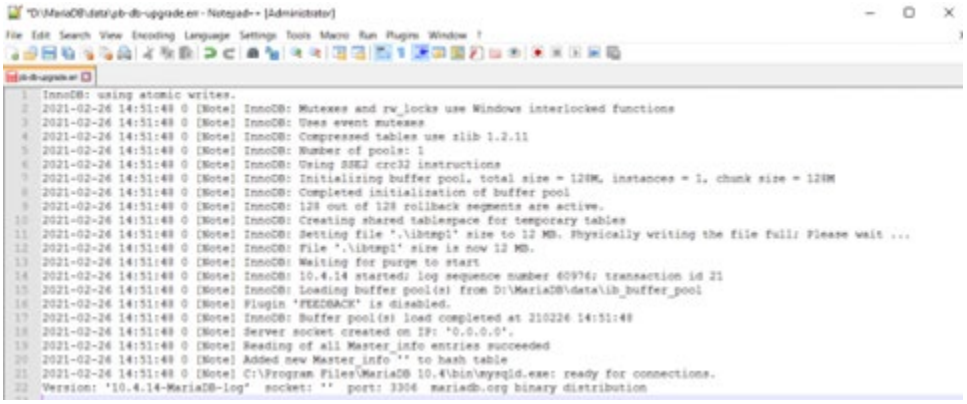
Step 27 – On all nodes, start the MariaDB service by issuing the command **net start mariadb** (Figure 30.27.1).

Figure 30.27 – Start MariaDB Service



Step 28 – On all nodes, check the MariaDB error log by opening the **D:\MariaDB\data*.err** file in Notepad++ (Figure 30.28), where * is the Windows name of the HCP Gateway. Resolve any errors before continuing to the next step.

Figure 30.28 – Check MariaDB Error Log



Step 29 – On all nodes, in a MariaDB Command Prompt, open the MariaDB CLI by issuing the command **"c:\Program Files\MariaDB 10.4\bin\mysql.exe" -uroot -p4tomcat2** (Figure 30.29.1), including the double quotes in the command name. Create the SAM database by issuing the command **create database SAM;** (Figure 30.29.2). Create the SAM user by issuing the following commands then issue the command **exit** to exit the MariaDB CLI:

WARNING: When the Gateway was first deployed or if the password reset script was run before Gateway version 4.1.5, if the database **sam** user account password was set to something other than the default **4tomcat2**, then enter the same password here that was entered when the Gateway was deployed or the password reset script was run.

"c:\Program Files\MariaDB 10.4\bin\mysql.exe" -uroot -p4tomcat2 (Figure 30.29.1)

create database SAM; (Figure 30.29.2)

GRANT ALL ON *.* TO sam@localhost IDENTIFIED BY '4tomcat2' REQUIRE SSL WITH GRANT OPTION; (Figure 30.29.3)

GRANT ALL ON *.* TO sam@127.0.0.1 IDENTIFIED BY '4tomcat2 REQUIRE SSL WITH GRANT OPTION '; (Figure 30.29.4)

GRANT FILE ON *.* TO sam@localhost IDENTIFIED BY '4tomcat2'; (Figure 30.29.5)

GRANT FILE ON *.* TO sam@127.0.0.1 IDENTIFIED BY '4tomcat2'; (Figure 30.29.6)

FLUSH PRIVILEGES; (Figure 30.29.7)

FLUSH TABLES; (Figure 30.29.8)

exit (Figure 30.29.9)

Figure 30.29 – Create SAM database and sam user

```
Administrator: Command Prompt (MariaDB 10.2 (x64))
C:\Windows\system32>"c:\Program Files\MariaDB 10.4\bin\mysql.exe" -uroot -p4tomcat2 (1)
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 9
Server version: 10.4.14-MariaDB-log mariadb.org binary distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database SAM; (2)
Query OK, 1 row affected (0.007 sec)

MariaDB [(none)]> GRANT ALL ON *.* TO sam@localhost IDENTIFIED BY '4tomcat2'; (3)
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> GRANT ALL ON *.* TO sam@127.0.0.1 IDENTIFIED BY '4tomcat2'; (4)
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]>
MariaDB [(none)]> GRANT FILE ON *.* TO sam@localhost IDENTIFIED BY '4tomcat2'; (5)
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> GRANT FILE ON *.* TO sam@127.0.0.1 IDENTIFIED BY '4tomcat2'; (6)
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]>
MariaDB [(none)]> FLUSH PRIVILEGES; (7)
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> FLUSH TABLES; (8)
Query OK, 0 rows affected (0.017 sec)

MariaDB [(none)]> exit (9)
Bye

C:\Windows\system32>_
```

Step 30 – On all nodes, restore the database from the backup you made earlier with mysqldump, by issuing the command **"c:\Program Files\MariaDB 10.4\bin\mysql.exe" –uroot –p4tomcat2 SAM < D:\Temp\SAM.sql** (Figure 30.30.1).

Figure 30.30 – Restore SAM database

```
Administrator: Command Prompt (MariaDB 10.2 (x64))
C:\Windows\system32>"c:\Program Files\MariaDB 10.4\bin\mysql.exe" -uroot -p4tomcat2 SAM < D:\Temp\SAM.sql (1)

C:\Windows\system32>_
```

IMPORTANT NOTE:

If the database restore fails with the error in Figure 30.31, then in a MariaDB Command Prompt, open the MariaDB CLI by issuing the command "c:\Program Files\MariaDB 10.4\bin\mysql.exe" -uroot -p4tomcat2 (Figure 30.32.1), including the double quotes in the command name. Reset the replication slave, even if this is an HCP Gateway Single node, by issuing the command reset slave; (Figure 30.32.2). Then issue the command exit (Figure 30.32.3) to exit the MariaDB CLI. Then re-run Step 30 above.

Figure 30.31 – Database restore error

```
C:\Windows\system32>mysql -uroot -p4tomcat2 SAM < C:\temp\SAM.sql
ERROR 1201 (HY000) at line 22: Could not initialize master info structure for ''; more error messages can be found in th
e MariaDB error log
```

Figure 30.32 – Database reset slave

```
Administrator: Command Prompt (MariaDB 10.4 (x64))
Setting environment for MariaDB 10.4 (x64)

C:\Windows\system32>"c:\Program Files\MariaDB 10.4\bin\mysql.exe" -uroot -p4tomcat2 (1)
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 21
Server version: 10.4.14-MariaDB-log mariadb.org binary distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> reset slave; (2)
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> exit (3)
Bye

C:\Windows\system32>_
```

Step 31 – WARNING: If replication is configured on the nodes, then refer to the HCP Gateway Database Replication Guide for your replication configuration and reset the replication on all the nodes before continuing to the next step.

Step 32 – On all nodes, open the **C:\SAM\etc\sam\backup.list** file in Notepad++ and change the MariaDB configuration path to **D:\MariaDB\data\my.ini** (Figure 30.33.1).

Figure 30.33 – Update Backup.list file

```
*C:\SAM\etc\sam\backup.list - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
backup.list
1  # Backup List
2
3  # SAM configuration directory
4  C:\SAM\etc\sam\
5
6  # SAM bin directory
7  C:\SAM\bin\
8
9  # Wildfly files
10 C:\opt\wildfly\standalone\configuration\standalone.xml
11 C:\opt\wildfly\modules\system\layers\base\com\mysql\
12 #C:\opt\wildfly\modules\system\layers\base\com\filepool\
13
14 # MariaDB configuration
15 D:\MariaDB\data\my.ini (1)
16
17 # Restore
18 C:\SAM\restore
19
```

Step 33 – On all nodes, open the **C:\SAM\etc\sam\sam.properties** file in Notepad++. Change the references on the **C:** drive from **MariaDB 10.2 to MariaDB 10.4** as shown in Figure 30.34. Change the references on the **D:** drive from **MariaDB 10.2** to **MariaDB** as shown in Figure 30.34.

Figure 30.34 – Update sam.properties file

```
database.program="C:\Program Files\MariaDB 10.4\bin\mysql.exe"
database.dump="C:\Program Files\MariaDB 10.4\bin\mysqldump.exe"
database.binlog="C:\Program Files\MariaDB 10.4\bin\mysqlbinlog.exe"

data.folder="D:\MariaDB\data"

binlog.folder="D:\MariaDB\binlog"
```

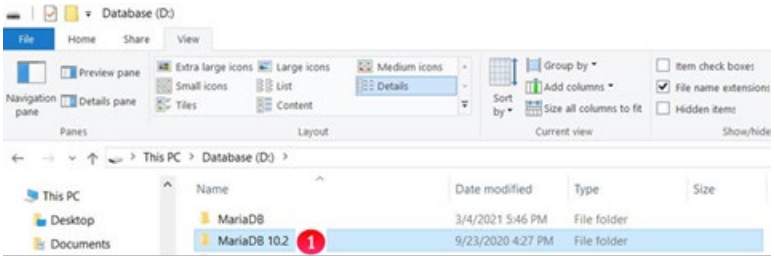
Step 34 – On all nodes, open the Windows **Services** panel and if not running, start the **SAM VFS** (Figure 30.35.1), and **Wildfly** (Figure 30.35.2) services.

> **NOTE:**
>
> If upgrading nodes in a Microsoft Failover Cluster, only 1 node, the active node should have the SAM VFS service running. Use the Failover Cluster Manager to bring the SAM VFS service online on the active node.

Figure 30.35 – Start Windows Services

Step 35 – On all nodes, delete the **D:\MariaDB 10.2** folder (Figure 30.36.1). If this MariaDB upgrade is part of upgrading the HCP Gateway software, go back to Step 5 in **Chapter 18 HCP Gateway Software Upgrade**.

Figure 30.36 – Delete D:\MariaDB 10.2 folder



Upgrade MariaDB 10.4.X to 10.4.22

Starting with HCP Gateway version 4.1.4 and prior to HCP Gateway version 4.1.8, the MariaDB database application version was 10.4.14. Starting with HCP Gateway version 4.1.8 and prior to HCP Gateway version 4.2.0, the MariaDB database application version was 10.4.21. Starting with HCP Gateway version 4.2.0, the 10.4.22 version of the MariaDB application is required. If the HCP Gateway is using MariaDB version 10.4.21 or a lower version of 10.4, then follow the directions in this chapter to upgrade the MariaDB database application to version 10.4.22. If the HCP Gateway is using a version of MariaDB 10.2, it is required to use the instructions in **Chapter 30 Upgrade MariaDB 10.2** to **10.4** to upgrade the MariaDB application.

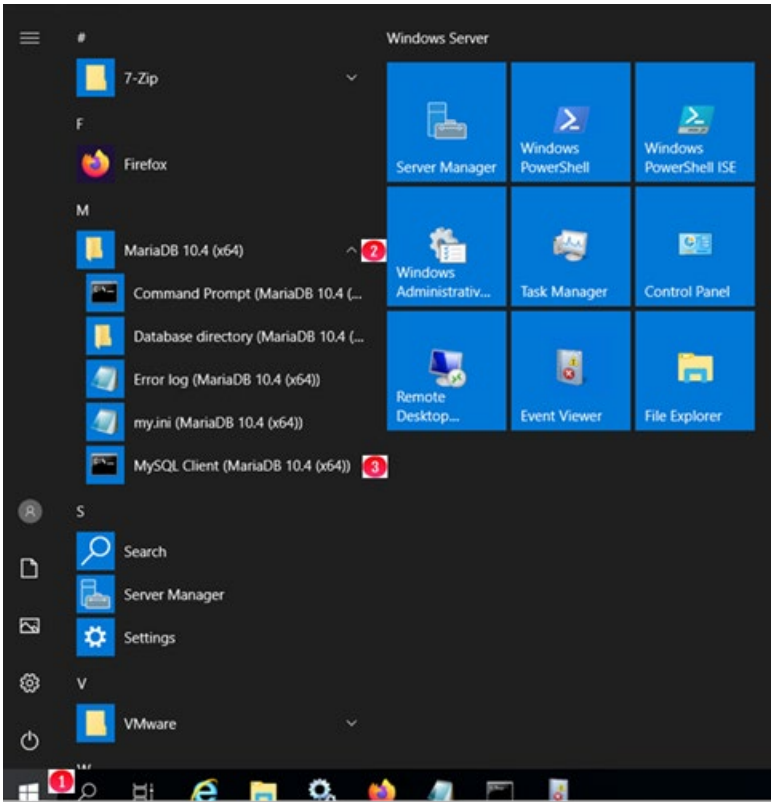
Windows MariaDB Upgrade Process

This chapter will cover the process to upgrade the HCP Gateway Windows MariaDB database application from version 10.4.21 or a lower version of 10.4 to version 10.4.22. Wait at least 5 minutes after the last file was written to the HCP Gateway so there will be no file processing during this upgrade.

Login to the HCP Gateway Windows OS as the local Administrator.

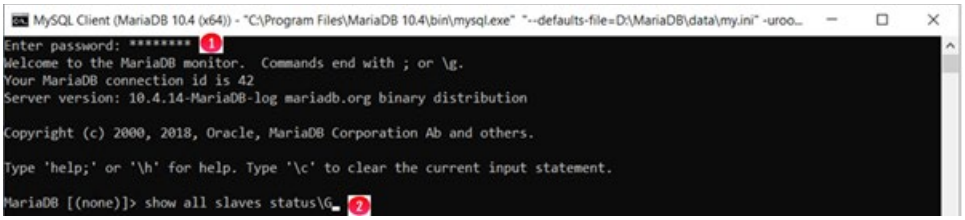
Step 1 – If this is just a single HCP Gateway and database replication is not configured, skip to Step 4. Select the **Windows Start button** (Figure 31.1.1), then select the **MariaDB 10.4 (x64)** folder (Figure 31.1.2), then select **MySQL Client (MariaDB 10.4 (x64))** (Figure 31.1.3).

Figure 31.1 – Open MySQL Client



Step 2 – On all nodes, when prompted, enter the **database root password** (Figure 31.2.1). Check the replication status by issuing the **show all slaves status\G** command (Figure 31.2.2). It is required to resolve any errors before continuing.

Figure 31.2 –Check Replication Status



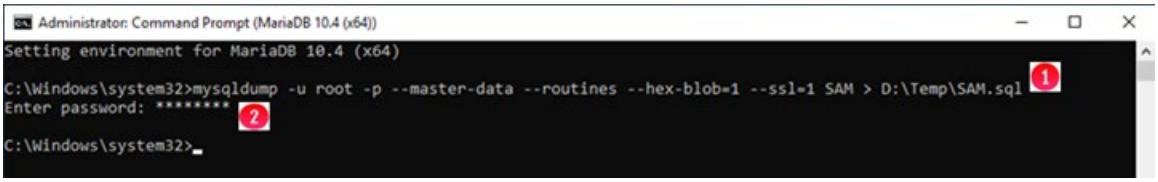
Step 3 – On all nodes, stop the replication by issuing the **stop all slaves**; command (Figure 31.3.1). Issue the **exit** command to close the **MySQL Client** (Figure 31.3.2). Close the MySQL Client window.

Figure 31.3 – Stop Replication

```
MariaDB [(none)]> stop all slaves; 1
Query OK, 0 rows affected, 4 warnings (0.03 sec)

MariaDB [(none)]> exit 2
Bye

C:\Program Files\MariaDB 10.4\bin>
```

Step 4 – On the single HCP Gateway, or on all nodes if database replication is configured, select the **Windows Start button** (Figure 31.1.1), then select the **MariaDB 10.4 (x64)** folder (Figure 31.1.2), open a **Command Prompt (MariaDB 10.4 (x64))**. Make a backup copy of the SAM database by issuing the command **mysqldump -u root -p --master-data --routines --hex-blob=1 --ssl=1 SAM > D:\Temp\SAM.sql** (Figure 31.4.1). If the **D:\Temp** folder does not exist (the error "The system cannot find the path specified." will be displayed), create the **D:\Temp** folder then run the command again. When prompted, enter the database root password (Figure 31.4.2).

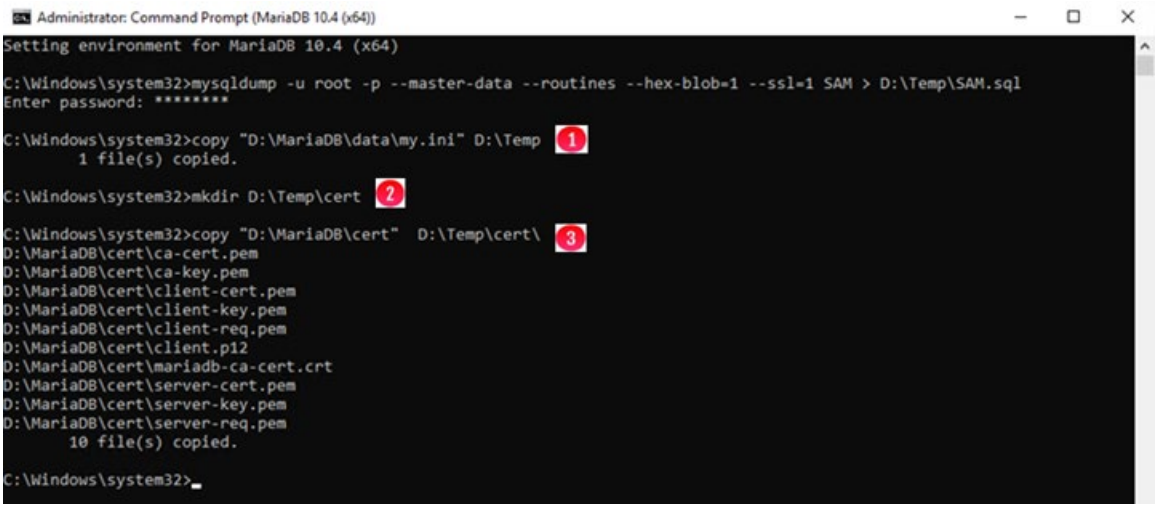
Figure 31.4 – Backup SAM Database



Step 5 – On the single HCP Gateway, or on all nodes if database replication is configured, make a copy of the **D:\MariaDB\data\my.ini** file by issuing the copy **"D:\MariaDB\data\my.ini" D:\Temp** command (Figure 31.5.1). Create the **D:\Temp\cert** folder by issuing the **mkdir D:\Temp\cert** command (Figure 31.5.2). Make a copy of the

D:\MariaDB\cert directory by issuing the **copy "D:\MariaDB\cert" D:\Temp\cert\ command** (Figure 31.5.3).

Figure 31.5 – Backup MariaDB Configuration Files

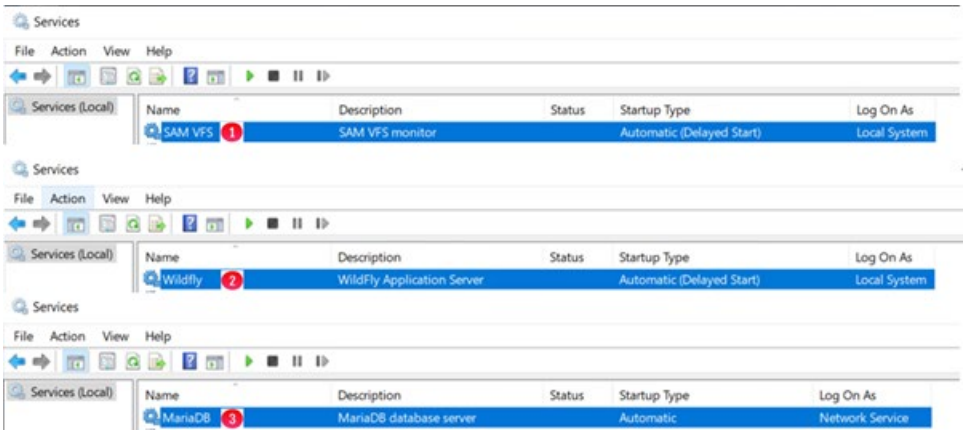


Step 6 – On the single HCP Gateway, or on all nodes if database replication is configured, open the Windows Services panel and if running, stop the **SAM VFS** (Figure 31.6.1), **Wildfly** (Figure 31.6.2) and **MariaDB** (Figure 31.6.3) services.

NOTE:

If upgrading nodes in a Microsoft Failover Cluster, only 1 node, the active node should have the **SAM VFS** service running. Use the Failover Cluster Manager to take the **SAM VFS** service offline on the active node.

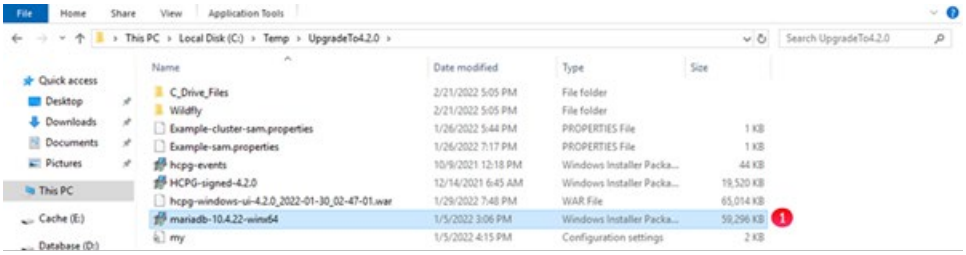
Figure 31.6 – Stop Windows Services



Step 7 – On the single HCP Gateway, or on all nodes if database replication is configured, close any open web browsers such as Firefox or Internet Explorer. Open Windows **File**

Explorer to the folder where the upgrade zip file was unzipped and double-click on the file **mariadb-10.4.22-winx64.msi** (Figure 31.7.1).

Figure 31.7 – MariaDB 10.4.22 installer

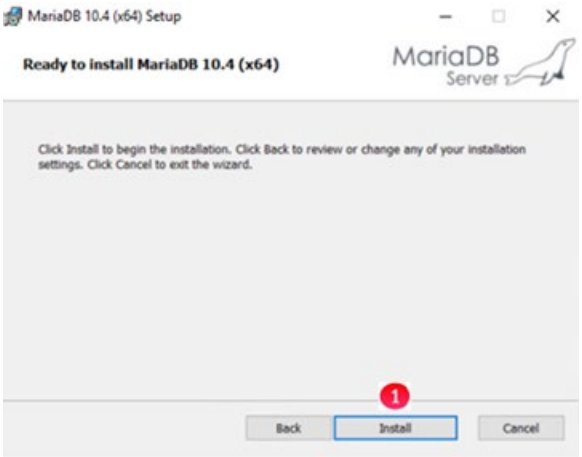


Step 8 – On the single HCP Gateway, or on all nodes if database replication is configured, select **Next** in the **Welcome to the MariaDB 10.4 (x64) Setup Wizard**. In the **Ready to install MariaDB 10.4 (x64)** screen, select **Install** (Figure 31.8.1).

NOTE:

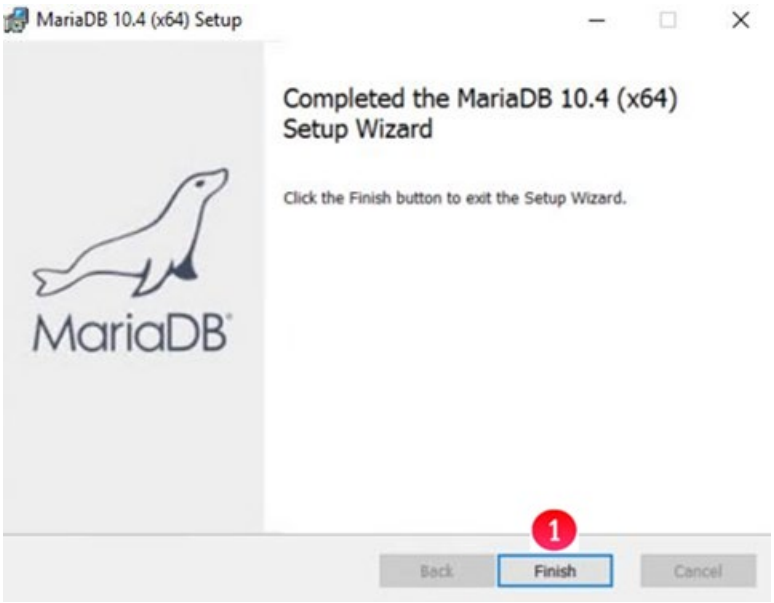
If any applications such as MariaDB, Firefox, Internet Explorer or VMWare services or tools are running, accept the default to attempt to close and restart the applications.

Figure 31.8 – MariaDB Setup Wizard



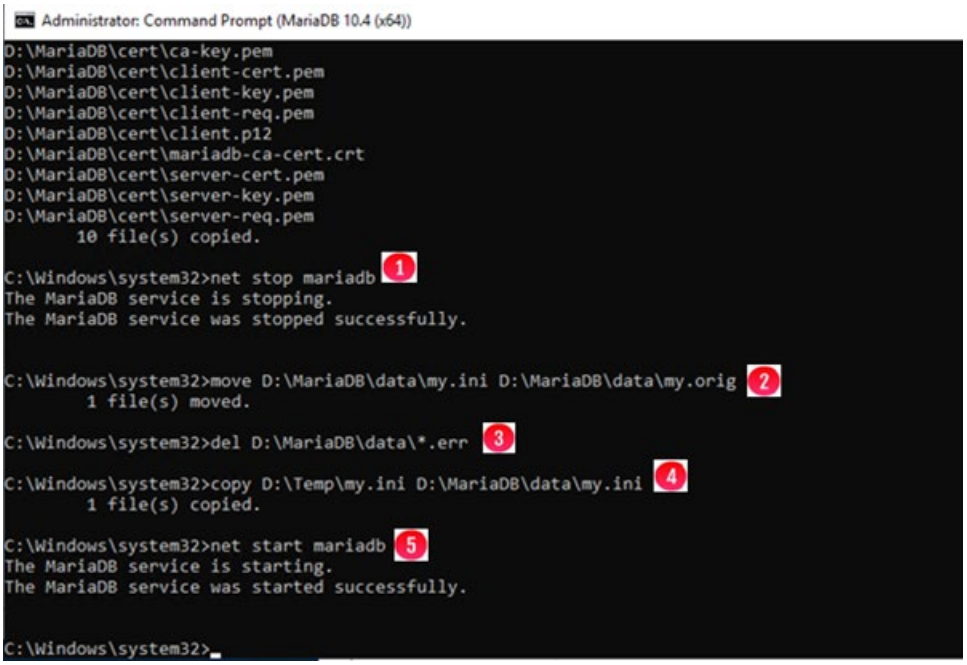
Step 9 – On the single HCP Gateway, or on all nodes if database replication is configured, select **Finish** (Figure 31.9.1) in the **Completed the MariaDB 10.4 (x64) Setup Wizard**.

Figure 31.9 – Finish MariaDB Setup Wizard



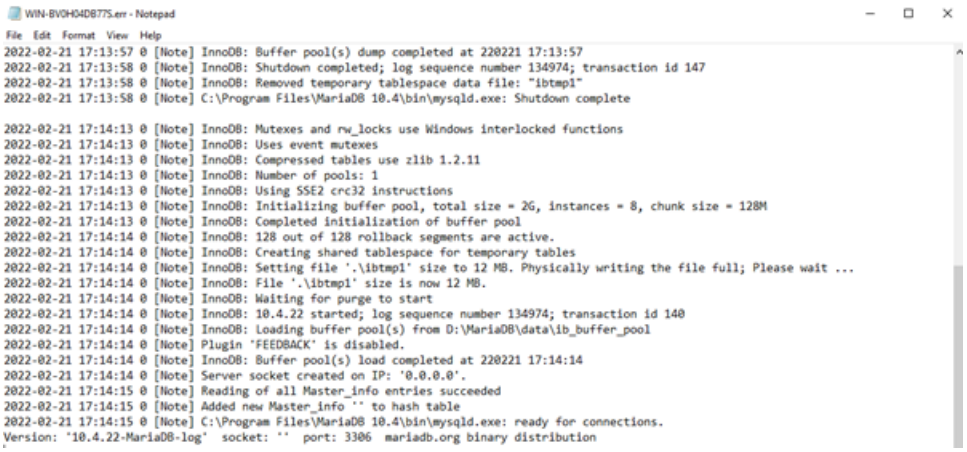
Step 10 – On the single HCP Gateway, or on all nodes if database replication is configured, in the MariaDB Command Prompt window, stop the MariaDB service by issuing the command **net stop mariadb** (Figure 31.10.1). Backup the new MariaDB my.ini configuration file by issuing the command **move D:\MariaDB\data\my.ini D:\MariaDB\data\my.orig** (Figure 31.10.2). Delete the MariaDB error log file by issuing the command **del D:\MariaDB\data*.err** (Figure 31.10.3). Restore the original MariaDB **my.ini** configuration file by issuing the command **copy D:\Temp\my.ini D:\MariaDB\data\my.ini** (Figure 31.10.4). Start the MariaDB service by issuing the command **net start mariadb** (Figure 31.10.5).

Figure 31.10 – Check MariaDB Error Log



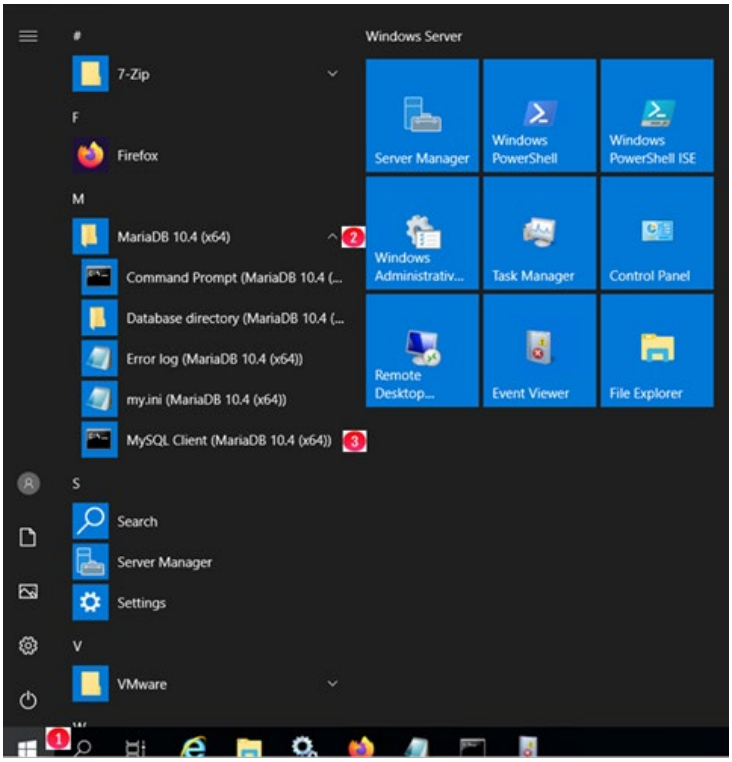
Step 11 – On the single HCP Gateway, or on all nodes if database replication is configured, check the MariaDB error log by opening the **D:\MariaDB\data*.err** file (Figure 31.11), where * is the Windows name of the HCP Gateway. Resolve any errors before continuing to the next step.

Figure 31.11 – Check MariaDB Error Log



Step 12 – If this is just a single HCP Gateway and database replication is not configured, skip to Step 14. On all nodes where replication is configured, select the **Windows Start button** (Figure 31.12.1), then select the **MariaDB 10.4 (x64)** folder (Figure 31.12.2), then select **MySQL Client (MariaDB 10.4 (x64))** (Figure 31.12.3).

Figure 31.12 – Open MySQL Client



Step 13 – On all nodes where replication is configured, when prompted, enter the **database root password** (Figure 31.13.1). Start all the replication slave by issuing the command **start all slaves**; (Figure 31.13.2). Check the replication status by issuing the **show all slaves status\G** command (Figure 31.13.3).

IMPORTANT NOTE:

It is required to resolve any errors before continuing.

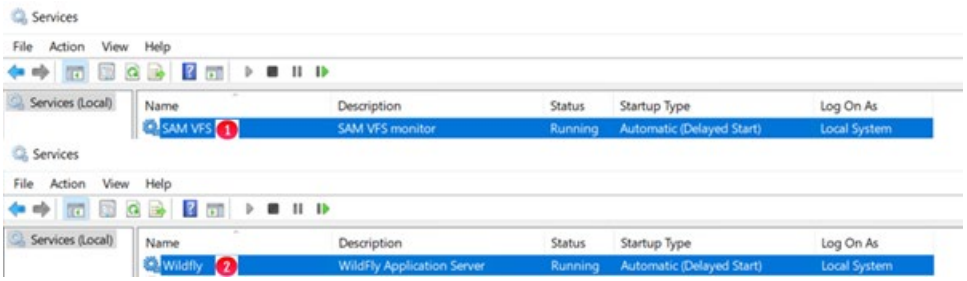
Figure 31.13 – Check Replication Status

Step 14 – On the single HCP Gateway, or on all nodes if database replication is configured, open the Windows **Services** panel and if not running, start the **SAM VFS** (Figure 31.14.1), and **Wildfly** (Figure 31.14.2) services. If this MariaDB upgrade is part of upgrading the HCP Gateway software, go back to Step 5 in **Chapter 18 HCP Gateway Software Upgrade**.

NOTE:

If upgrading nodes in a Microsoft Failover Cluster, only 1 node, the active node should have the **SAM VFS** service running. Use the Failover Cluster Manager to bring the **SAM VFS** service online on the active node.

Figure 31.14 – Start Windows Services



Upgrade Wildfly to Version 19

Starting with HCP Gateway version 4.2.0, an upgrade to version 19 of the Wildfly application is required.

This chapter will provide the instructions for upgrading the Wildfly application to version 19.

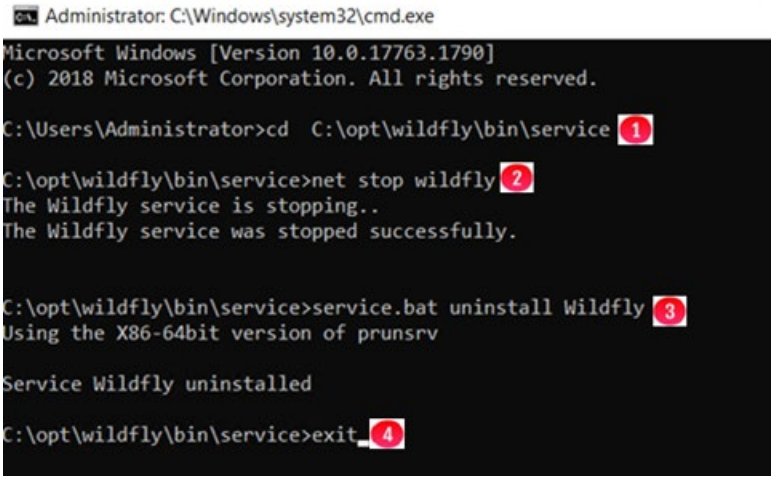
IMPORTANT NOTE:

Do not delete the old Wildfly folder as you will need some files and configuration information from it. Do not overwrite the new **C:\opt\wildfly-19.0.1.Final\standalone\configuration\standalone.xml** with the old **C:\opt\wildfly-18.0.1.Final\standalone\configuration\standalone.xml**!

WARNING: When copying text from this document to an HCP Gateway, it is required to copy the text into a Notepad, or Notepad++ window first to remove any special formatting characters from Microsoft Word or Adobe Acrobat.

Step 1 – Open a DOS Command Prompt window as Administrator and change directory to the **C:\opt\wildfly\bin\service** folder by issuing the command **cd C:\opt\wildfly\bin\service** (Figure 32.1.1). Stop the Wildfly service by issuing the command **net stop wildfly** (Figure 32.1.2). If the Wildfly service does not stop, open the Windows Services panel and check if Wildfly is stopped. Sometimes it takes Wildfly longer than the timeout window to stop. Remove the Wildfly service by issuing the command **service.bat uninstall Wildfly** (Figure 32.1.3). Close the DOS command prompt window by issuing the command **exit** (Figure 32.1.4).

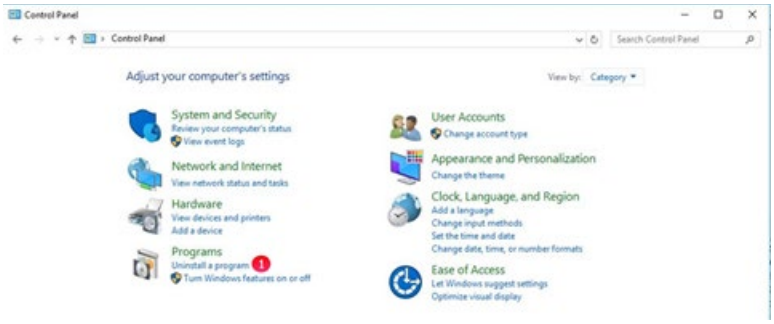
Figure 32.1 – Remove Wildfly Service



Step 2 – The **"AdoptOpenJDK JDK with Hotspot 8.0.XXX.XX (x64)"** program now needs to be removed and the **Eclipse Temurin OpenJDK11U-jdk_x64_windows_hotspot_11.0.13_8** program installed. Select the Windows Start Menu

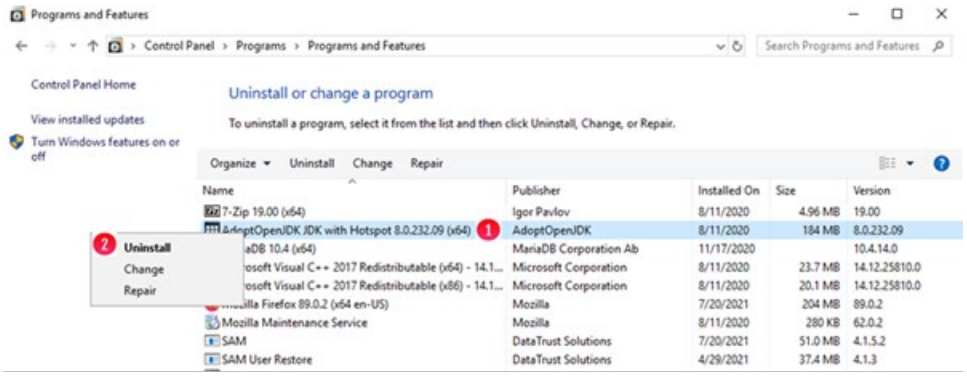
located at the bottom left of the screen. Select the “Control Panel” icon. In the “Control Panel” window, under the “Programs” section, select **“Uninstall a program”** (Figure 32.2.1).

Figure 32.2 – Control Panel



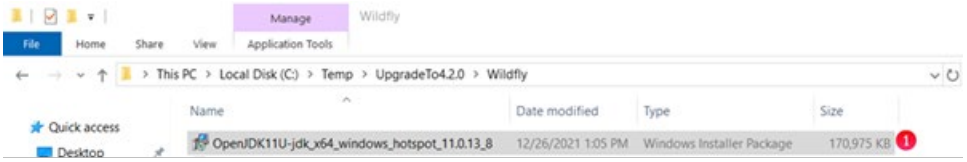
Step 3 – In the “Program and Features” window, right-click the **“AdoptOpenJDK JDK with Hotspot 8.0.XXX.XX (x64)”** program (Figure 32.3.1) and select “**Uninstall**” (Figure 32.3.2). Select **Yes** to confirm.

Figure 32.3 – Uninstall Program



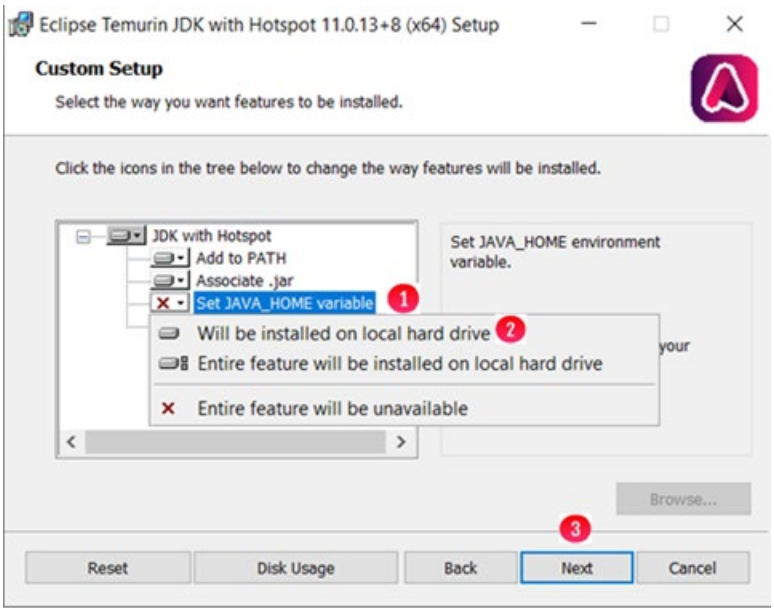
Step 4 – In Windows File Explorer navigate to the location that you downloaded the new version of the HCP Gateway software. In the Wildfly folder, double-click on the **OpenJDK11U-jdk_x64_windows_hotspot_11.0.13_8.msi** file (Figure 32.4.1).

Figure 32.4 – Windows File Explorer



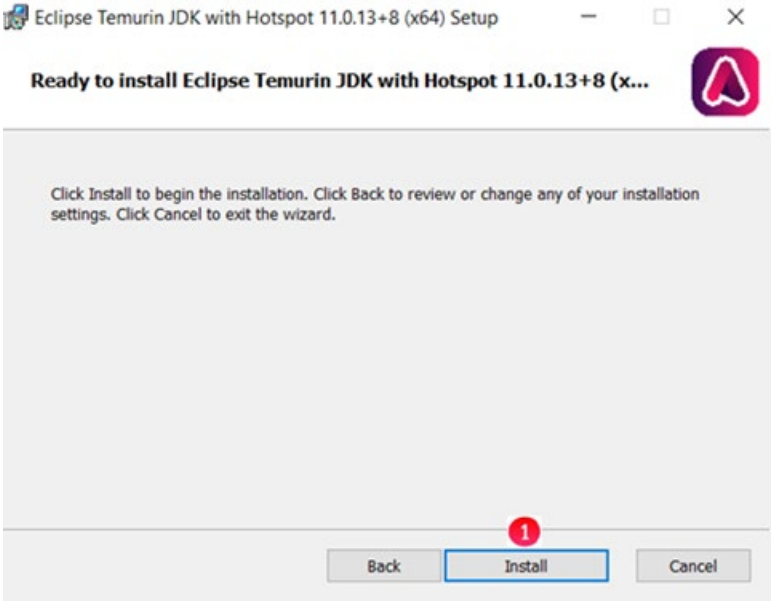
Step 5 – In the **Eclipse Temurin JDK with Hotspot 11.0.13+8 (x64) Setup** window, select **Next**. In the next window, if prompted to accept the License Agreement, select the box to accept the License Agreement and select **Next**. In the **Custom Setup** window, select **Set JAVA_HOME variable** (Figure 32.5.1), select **Will be installed on local hard drive** (Figure 32.5.2) then select **Next** (Figure 32.5.3).

Figure 32.5 – Custom Setup



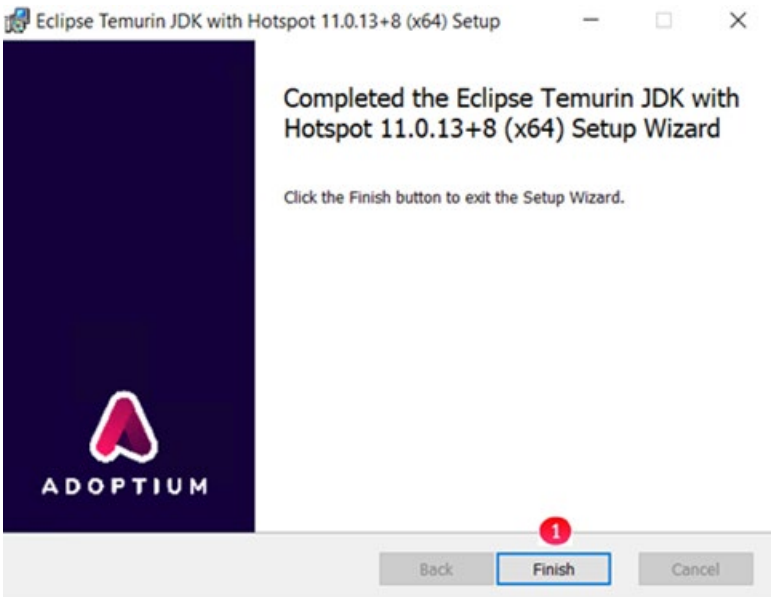
Step 6 – In the **Ready to install Eclipse Temurin JDK with Hotspot 11.0.13+8 (x64) Setup** window, select **Install** (Figure 32.6.1).

Figure 32.6 – Ready to Install



Step 7 – When the installation is complete, select **Finish** (Figure 32.7.1).

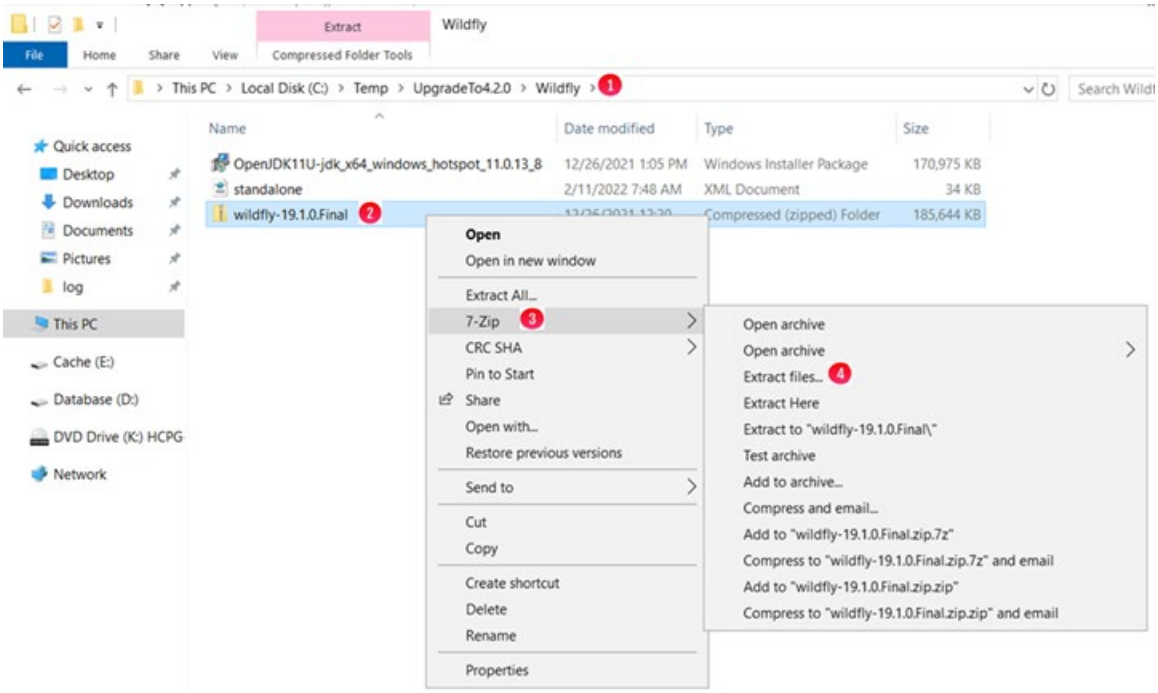
Figure 32.7 – Installation Complete



Step 8 – Close all open windows like Control Panel and Windows File Explorer and use the Power button in the Windows Start Menu to **restart** the HCP Gateway.

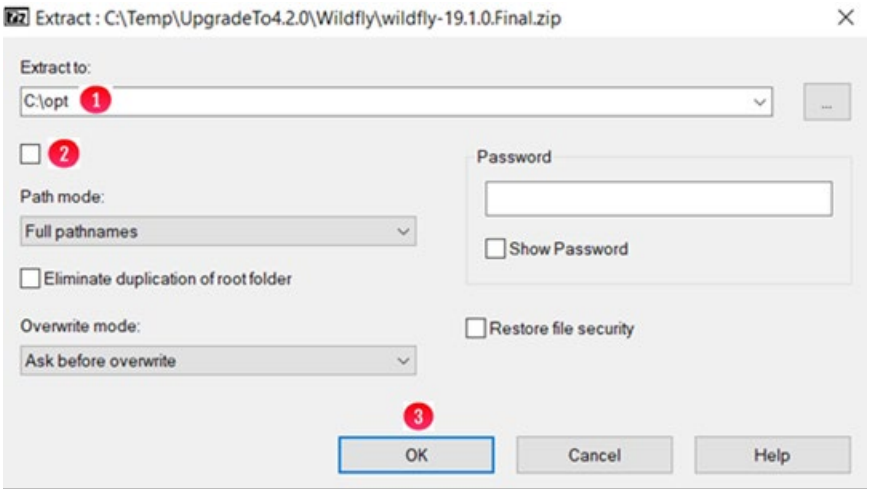
Step 9 – Logon to the HCP Gateway as the local Administrator. Open a Windows File Explorer and navigate to the Wildfly folder in the folder where the upgrade release package was unzipped (Figure 32.8.1). Right-click on the **wildfly-19.1.0.Final** compressed zip folder (Figure 32.8.2). Select **7-Zip** (Figure 32.8.3). Select **Extract files** (Figure 32.8.4).

Figure 32.8 – 7zip Extract files



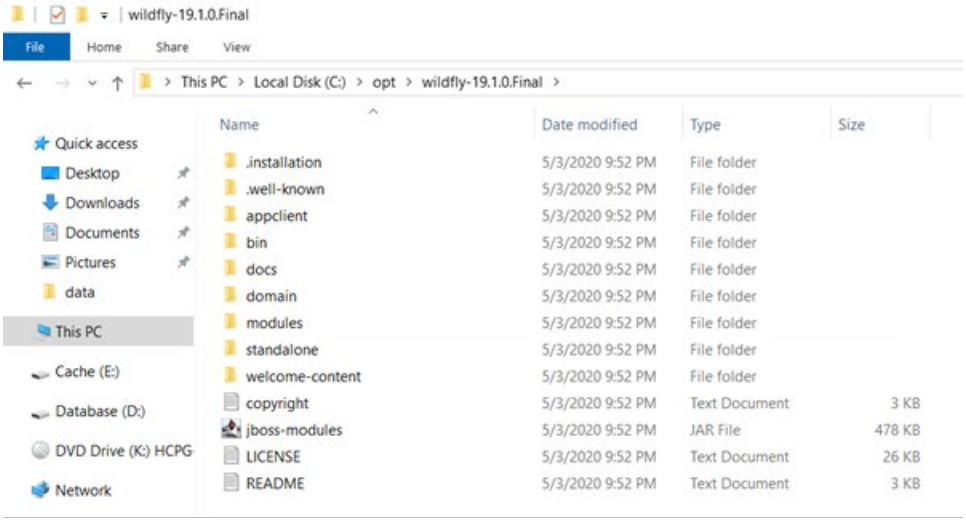
Step 10 – Change the **Extract to** folder to **C:\opt** (Figure 32.9.1). Unselect the box below the **Extract to** text box (Figure 32.9.2). Leave the other selections at the default and verify they match the screenshot in Figure 32.9. Select **OK** (Figure 32.9.3).

Figure 32.9 – 7zip Extract parameters



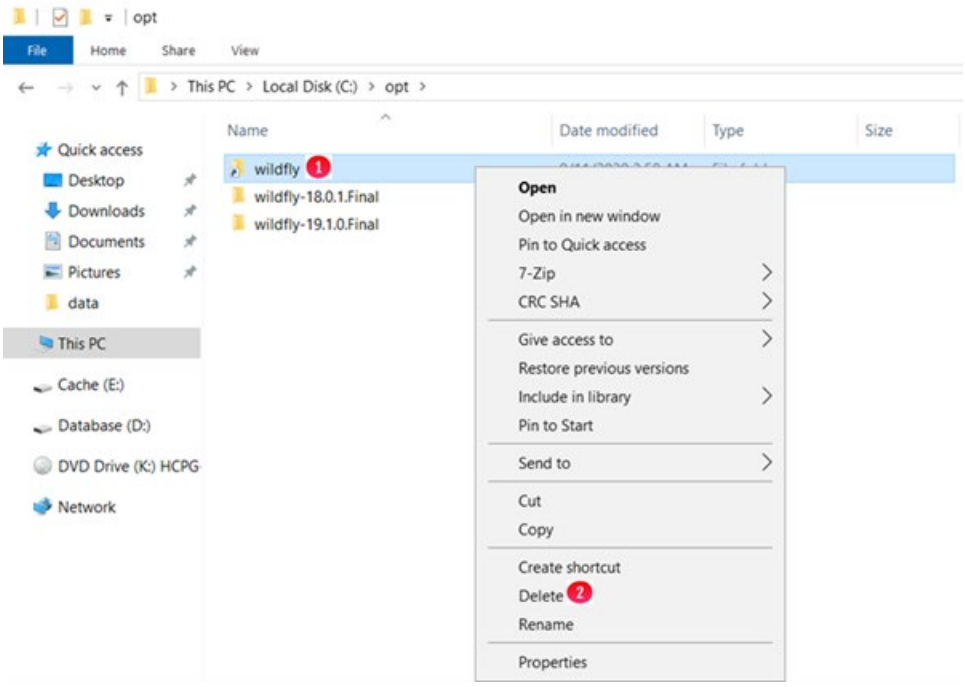
Step 11 – In Windows File Explorer, verify that the folder **C:\opt\wildfly-19.1.0.Final** was extracted properly and matches the screenshot in Figure 32.10.

Figure 32.10 – Wildfly 19 extracted



Step 12 – In Windows File Explorer, right-click the **C:\opt\wildfly** (Figure 32.11.1) link and select **Delete** (Figure 32.11.2).

Figure 32.11 – Delete Wildfly link

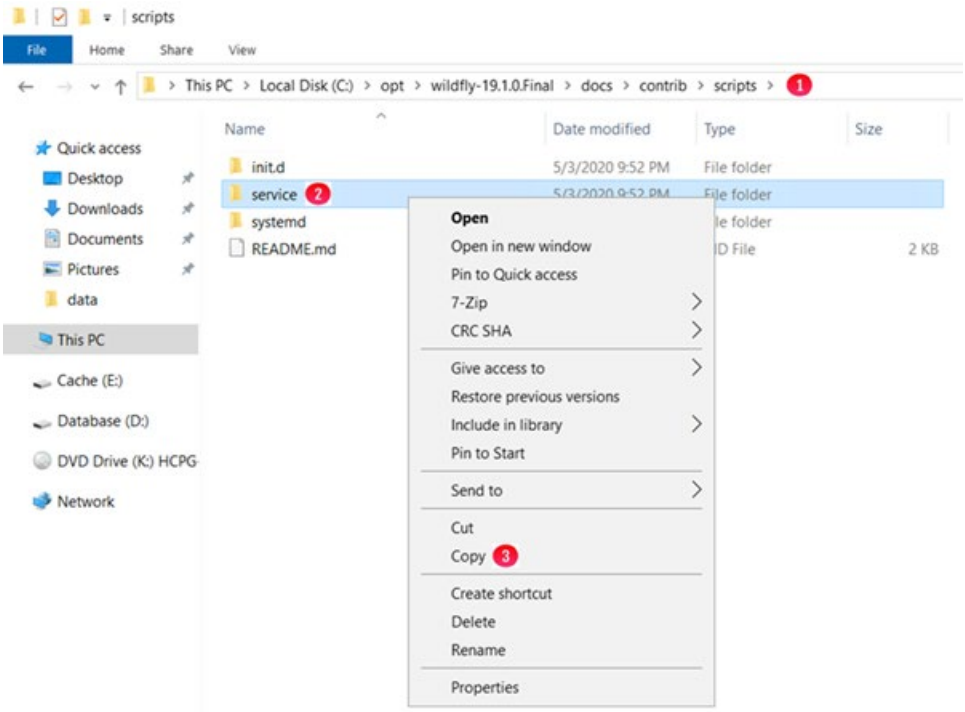


Step 13 – Open a DOS Command Prompt as Administrator and create a new Wildfly link by issuing the command **mklink /D C:\opt\wildfly C:\opt\wildfly-19.1.0.Final** (Figure 32.12.1).

Figure 32.12 – Create Wildfly link

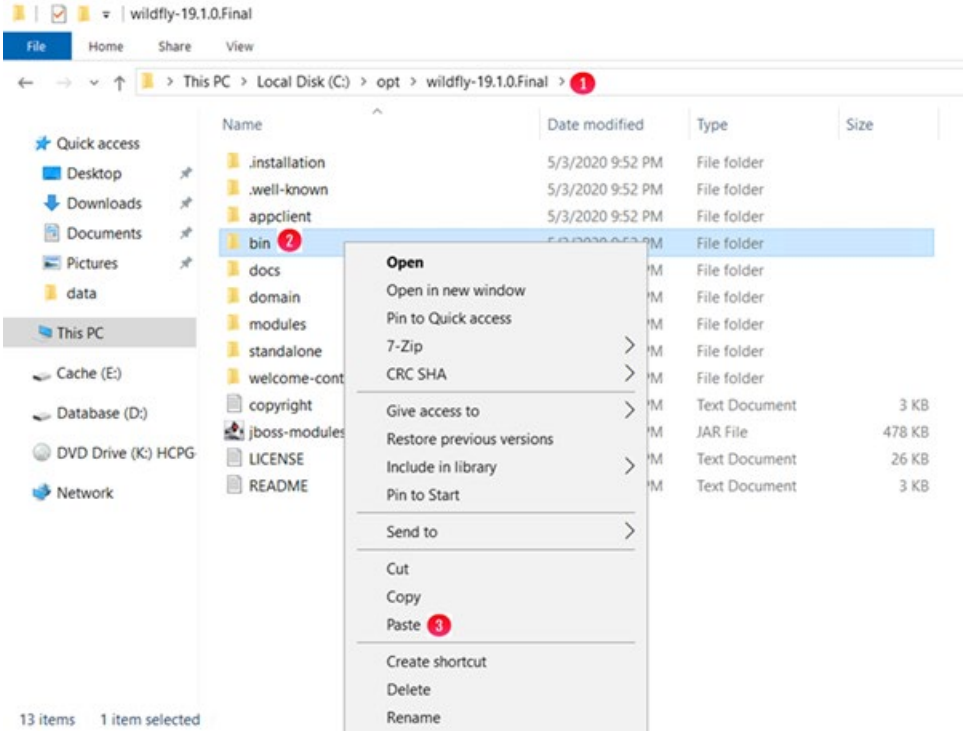
Step 14 – In Windows File Explorer, navigate to the **C:\opt\wildfly-19.1.0.Final\docs\contrib\scripts** folder (Figure 32.13.1), right-click the **service** folder (Figure 32.13.2) and select **Copy** (Figure 32.13.3).

Figure 32.13 – Copy Wildfly service folder



Step 15 – In Windows File Explorer, navigate to the **C:\opt\wildfly** folder (Figure 32.14.1), left-click on the **bin** folder, then right-click on the bin folder (Figure 32.14.2) and select **Paste** (Figure 32.14.3).

Figure 32.14 – Paste Wildfly service folder

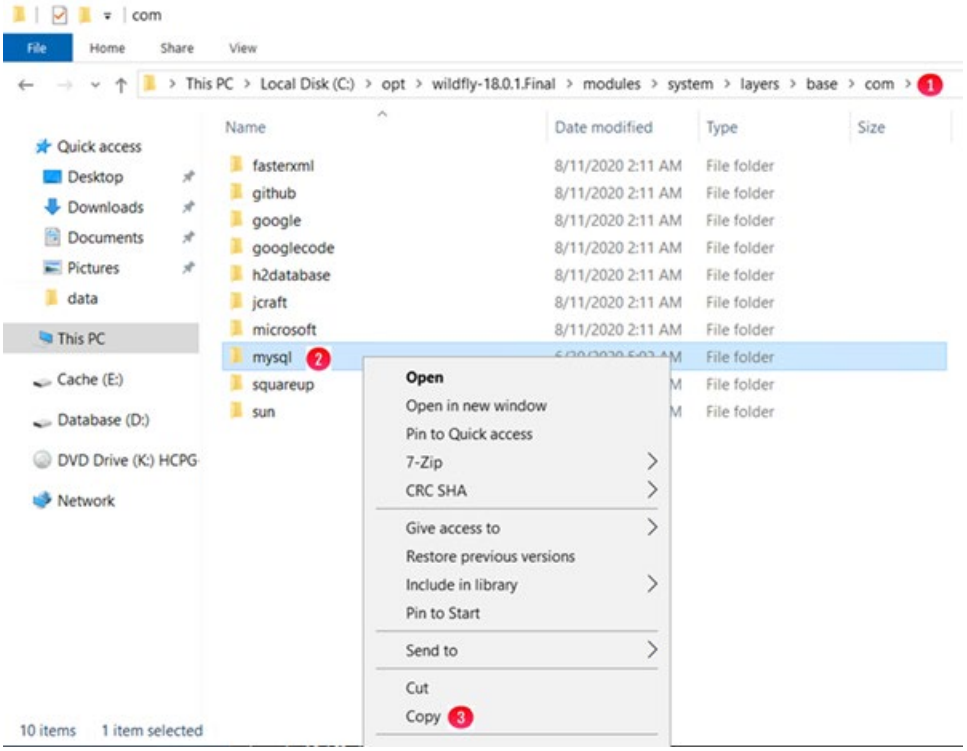


Step 16 – In the DOS Command Prompt, change directory to **C:\opt\wildfly\bin\service** by issuing the command **cd C:\opt\wildfly\bin\service** (Figure 32.15.1). Install the Wildfly service by issuing the command **service install** (Figure 32.15.2).

Figure 32.15 – Install Wildfly service

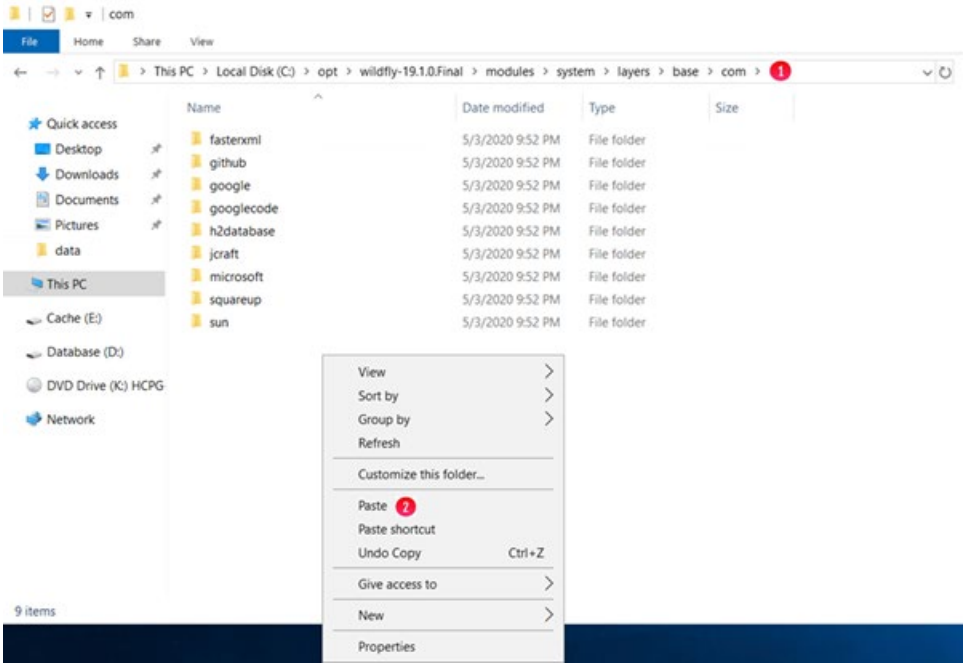
Step 17 – In Windows File Explorer, browse to the old path **C:\opt\wildfly-18.0.1.Final\modules\system\layers\base\com** (Figure 32.16.1). Right-click the folder **mysql** (Figure 32.16.2). Select **Copy** (Figure 32.16.3).

Figure 32.16 – Copy MySQL module



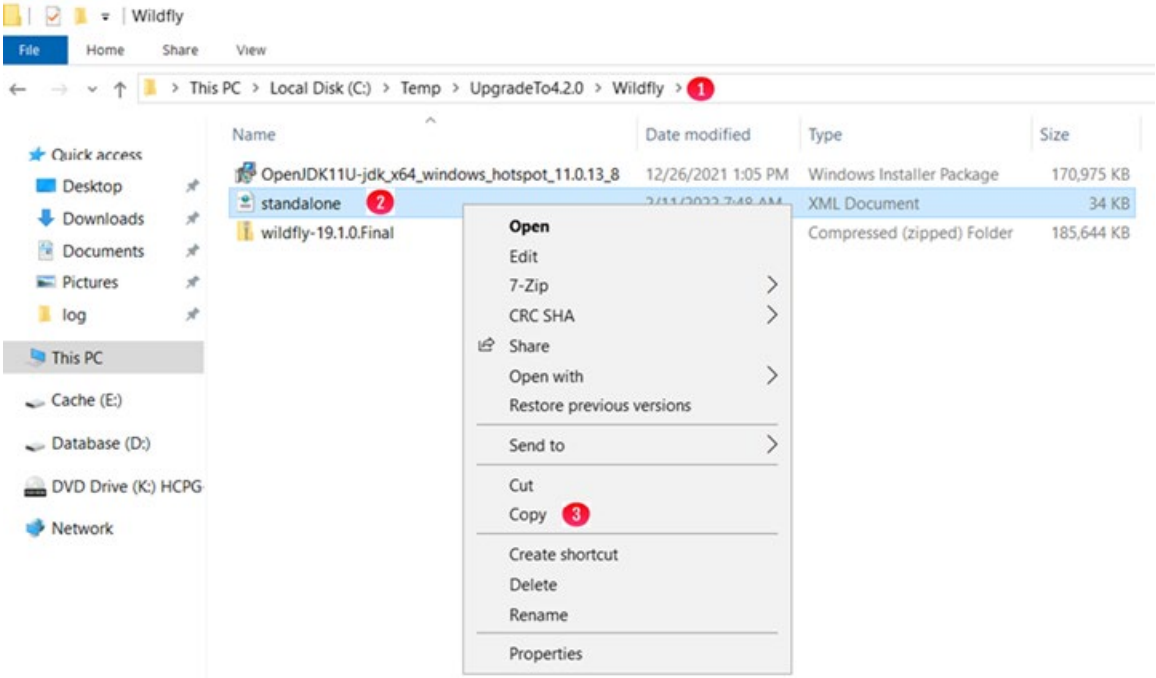
Step 18 – In the Windows File Explorer, browse to the new path **C:\opt\wildfly-19.1.0.Final\modules\system\layers\base\com** (Figure 32.17.1). Right-click in the white space below the sun folder and select **Paste** (Figure 32.17.2).

Figure 32.17 – Paste MySQL module



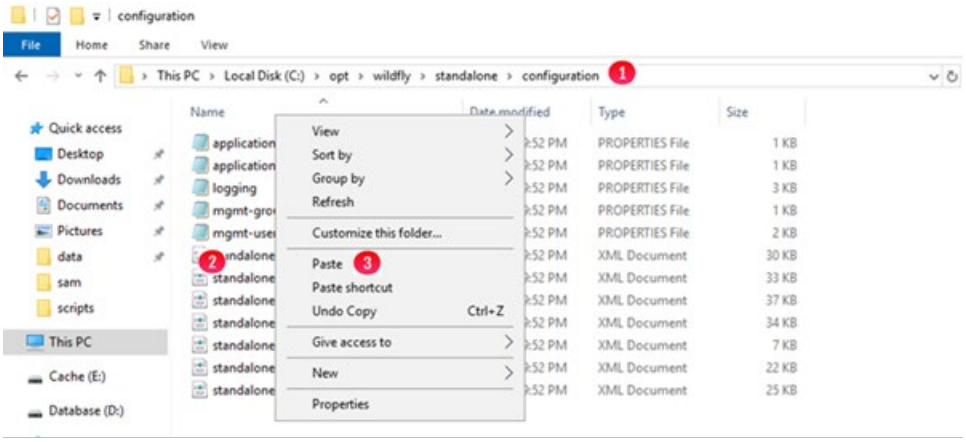
Step 19 – In the Windows File Explorer, navigate to the Wildfly folder in the folder where the upgrade release package was unzipped (Figure 32.18.1). Left-click then right-click on the **standalone.xml** file (Figure 32.18.2). Select **Copy** (Figure 32.18.3).

Figure 32.18 – Copy standalone.xml



Step 20 – In the Windows File Explorer, navigate to the **C:\opt\wildfly\standalone\configuration** folder (Figure 32.19.1). Right-click on the area with the file names (Figure 32.19.2), select **Paste** (Figure 32.19.3). When prompted, be sure to select **Replace the file in the destination**.

Figure 32.19 – Paste standalone.xml



Step 21 – In a Notepad++ or Notepad application, open both the old file **C:\opt\wildfly-18.1.0.Final\standalone\configuration\standalone.xml** and the new file **C:\opt\wildfly-19.1.0.Final\standalone\configuration\standalone.xml**. In the old file **C:\opt\wildfly-18.1.0.Final\standalone\configuration\standalone.xml** search for the string **<security-domain name="ds-encrypted"**. In the new file **C:\opt\wildfly-19.1.0.Final\standalone\configuration\standalone.xml** search for the string **<security-domain name="ds-encrypted"**. If the password (Figure 32.20.1) is different in the new file **C:\opt\wildfly-19.1.0.Final\standalone\configuration\standalone.xml**, copy the password from the old file **C:\opt\wildfly-18.1.0.Final\standalone\configuration\standalone.xml** to the new file **C:\opt\wildfly-19.1.0.Final\standalone\configuration\standalone.xml**. If the password was changed in the new file, save the new file **C:\opt\wildfly-19.1.0.Final\standalone\configuration\standalone.xml**. Close both the old file **C:\opt\wildfly-18.1.0.Final\standalone\configuration\standalone.xml** and the new file **C:\opt\wildfly-19.1.0.Final\standalone\configuration\standalone.xml**.

Figure 32.20 – new file Datasource ds-encrypted

Step 22 – In the DOS Command Prompt, build the SSL Keystore by issuing the command **keytool -genkeypair -alias localhost -keyalg RSA -keysize 2048 -validity 1825 -keystore C:\opt\wildfly\standalone\configuration\server.keystore -dname "CN=Wildfly,OU=Web Services,O=Datatrust Solutions,L=Louisville,ST=CO,C=US" -keypass hcpgXDB -storepass hcpgXDB** (Figure 32.21.1).

NOTE:

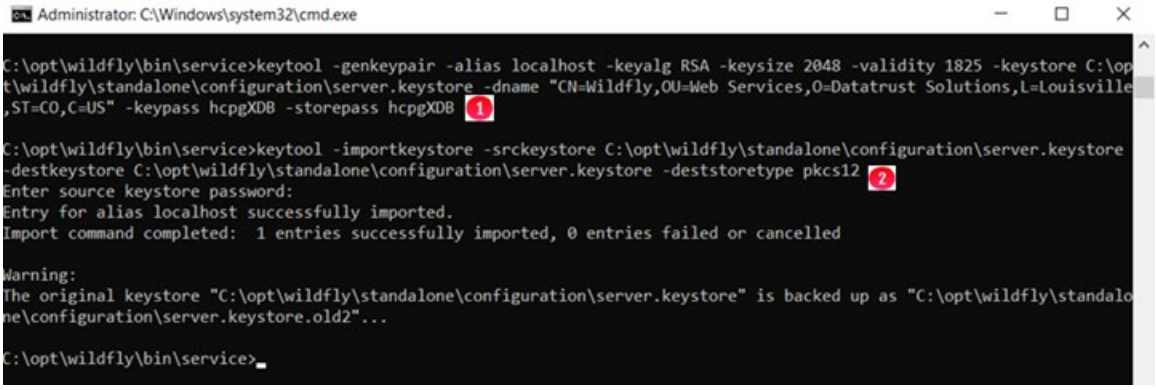
Some customer sites may need a san (not storage san) flag to work-ext san=dns:hcpg-single

Import the SSL Keystore by issuing the command **keytool -importkeystore -srckeystore C:\opt\wildfly\standalone\configuration\server.keystore -destkeystore C:\opt\wildfly\standalone\configuration\server.keystore -deststoretype pkcs12** (Figure 32.21.2).

NOTE:

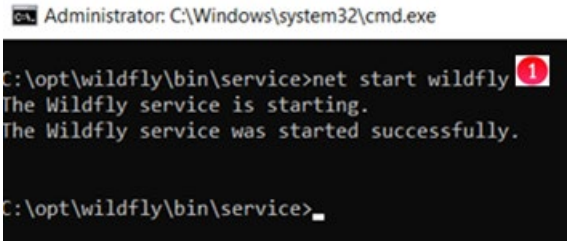
When prompted, the source keystore password is: hcpgXDB

Figure 32.21 – Build and Import SSL Keystore



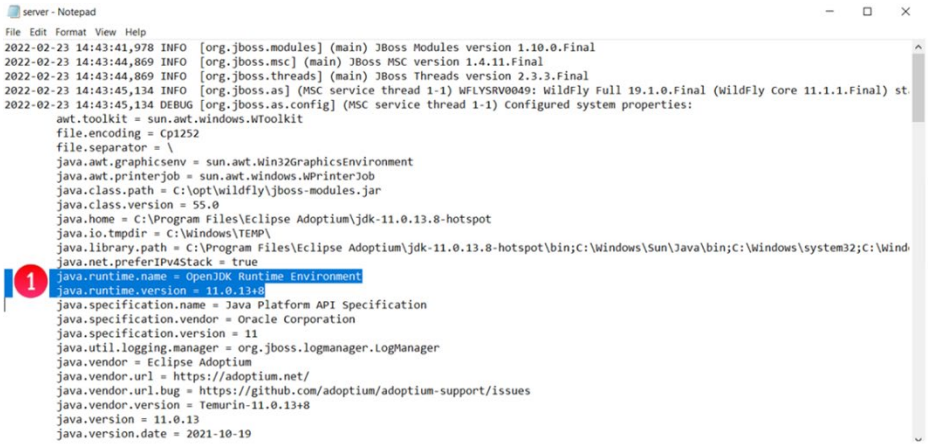
Step 23 – In the DOS Command Prompt, start the Wildfly service by issuing the command **net start wildfly** (Figure 32.22.1).

Figure 32.22 – Start Wildfly Service



Step 24 – In the Windows File Explorer, navigate to the folder **C:\opt\wildfly\standalone\log** and open the **server.log** file in either Notepad++, or Notepad. Look for the Java runtime properties (Figure 32.23.1). If this is the first time that Wildfly is started, it will be at the top/beginning of the file, otherwise search near the bottom of the file. There should be no errors in the server.log, you can ignore the WARN's about keystore(s).

Figure 32.23 – Start Wildfly Service



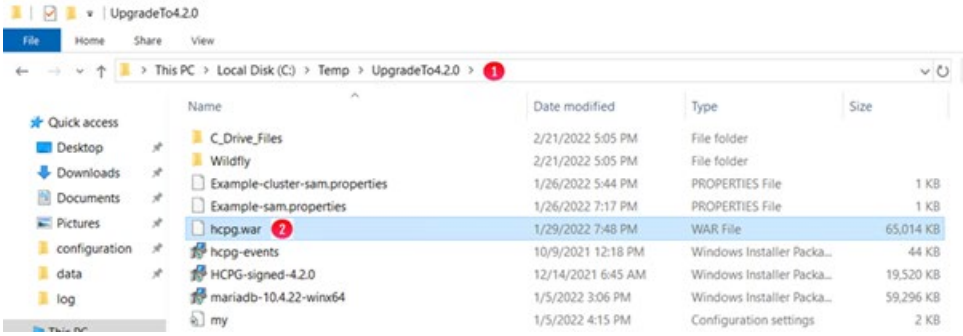
Step 25 – In the DOS Command Prompt, change directory to **C:\opt\wildfly\bin** by issuing the command **cd C:\opt\wildfly\bin** (Figure 32.24.1). Add the Wildfly **admin** user by issuing the command **add-user.bat** (Figure 32.24.2). When prompted for the type of user to add, select the default a (Figure 32.24.3) for a management user. When prompted for the Username, enter **admin** (Figure 32.24.4). When prompted that the user admin already exists, select the default **a** (Figure 32.24.5) to update the existing user password and roles. When prompted for the password, enter **0rgan1c@HV** (Figures 32.24.6) and 32.24.7). When prompted for the groups to belong to, leave blank and press the **Enter key** (Figure 32.24.8). When prompted is the new user is going to be used for the AS process, enter **no** (Figure 32.24.9). When prompted, press any key to continue (Figure 32.24.10).

Figure 32.24 – Update Wildfly admin user

```
Administrator: C:\Windows\system32\cmd.exe
C:\opt\wildfly\bin\service>cd C:\opt\wildfly\bin (1)

C:\opt\wildfly\bin>add-user.bat (2)

What type of user do you wish to add?
 a) Management User (mgmt-users.properties)
 b) Application User (application-users.properties)
(a): a (3)

Enter the details of the new user to add.
Using realm 'ManagementRealm' as discovered from the existing property files.
Username : admin (4)
User 'admin' already exists and is disabled, would you like to...
 a) Update the existing user password and roles
 b) Enable the existing user
 c) Type a new username
(a): a (5)
Password recommendations are listed below. To modify these restrictions edit the add-user.properties configuration file.

 - The password should be different from the username
 - The password should not be one of the following restricted values {root, admin, administrator}
 - The password should contain at least 8 characters, 1 alphabetic character(s), 1 digit(s), 1 non-alphanumeric symbol(s
)
Password : (6)
Re-enter Password : (7)
What groups do you want this user to belong to? (Please enter a comma separated list, or leave blank for none)[  ]: (8)
Updated user 'admin' to file 'C:\opt\wildfly\standalone\configuration\mgmt-users.properties'
Updated user 'admin' to file 'C:\opt\wildfly\domain\configuration\mgmt-users.properties'
Updated user 'admin' with groups  to file 'C:\opt\wildfly\standalone\configuration\mgmt-groups.properties'
Updated user 'admin' with groups  to file 'C:\opt\wildfly\domain\configuration\mgmt-groups.properties'
Is this new user going to be used for one AS process to connect to another AS process?
e.g. for a slave host controller connecting to the master or for a Remoting connection for server to server EJB calls.
yes/no? no (9)
Press any key to continue . . . (10)

C:\opt\wildfly\bin>_
```

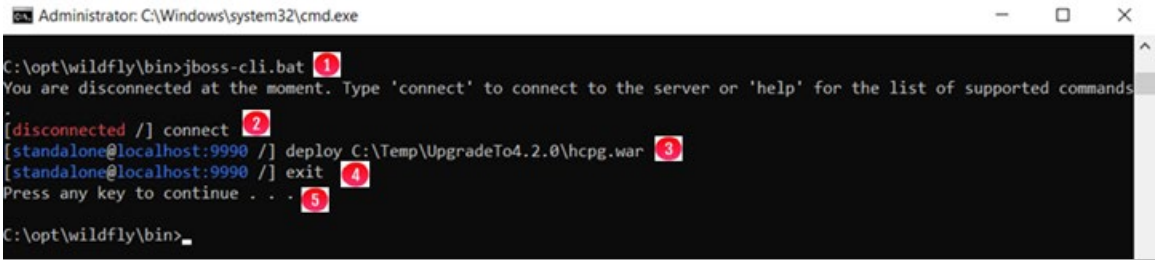
Step 26 – In the Windows File Explorer, navigate to the folder where the upgrade zip file was unzipped, for this example **C:\Temp\UpgradeTo4.2.0** (Figure 32.25.1). Rename the file **hcpg-windows-ui-4.2.0_2022-01-30_02-47-01.war to hcpg.war** (Figure 32.25.2).

Figure 32.25 – Rename war file



Step 27 – In the DOS Command Prompt, connect to the JBoss CLI by issuing the command **jboss-cli.bat** (Figure 32.26.1). Enter **connect** (Figure 32.26.2). Deploy the UI war file by issuing the command **deploy C:\Temp\UpgradeTo4.2.0\hcpg.war** (Figure 32.26.3). Enter **exit** (Figure 32.26.4). When prompted, press any key to continue (Figure 32.26.5).

Figure 32.26 – Deploy war file



Step 28 – Open the Windows Services panel, verify that the **Wildfly** service **Startup Type** is set to **Automatic (Delayed Start)** (Figure 32.27.1). If not, right-click on the **Wildfly** service, select **Properties** and set the **Startup Type to Automatic (Delayed Start)** (Figure 32.28.1) then select **OK** (Figure 32.28.2). Close the Windows Services panel.

Figure 32.27 - Wildfly Service

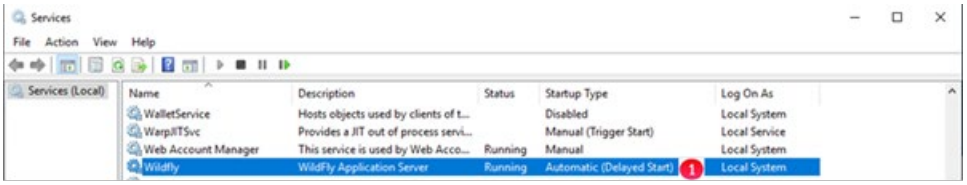
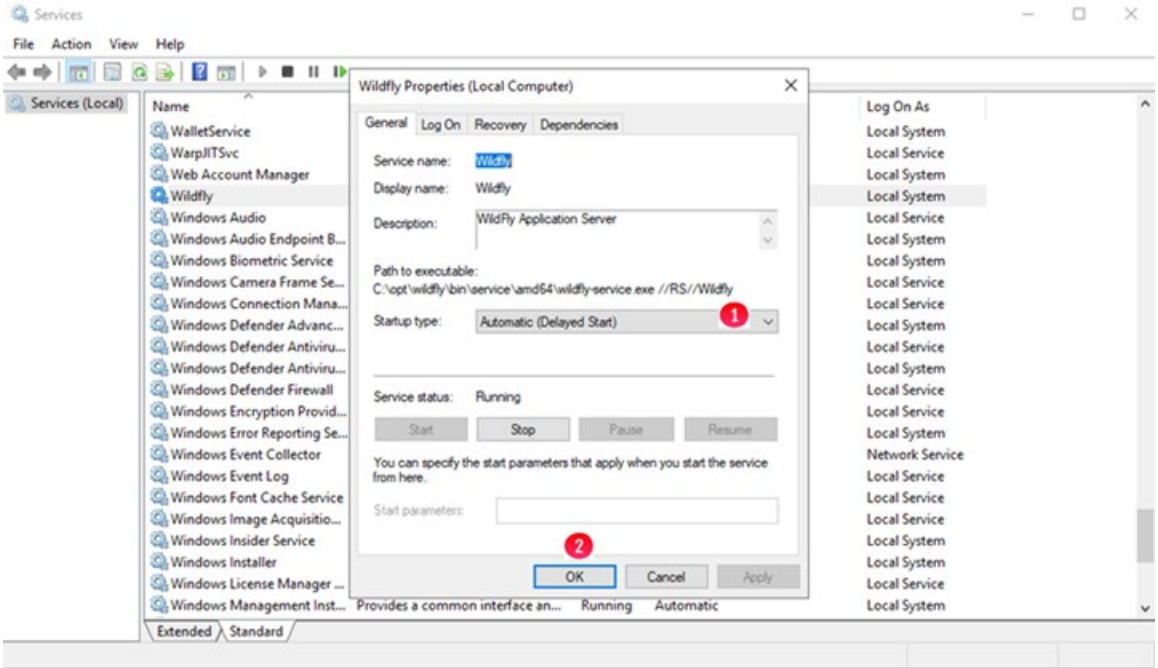


Figure 32.28 - Wildfly Service Properties



IMPORTANT NOTE:

The Wildfly version 19 application supports TLS versions 1.2 and 1.3. Microsoft Internet Explorer does not support TLS version 1.3, so it cannot be used to access the HCP Gateway UI. Starting with HCP Gateway version 4.2.0, use a web browser such as Firefox to access the HCP Gateway UI.

Step 29 – If upgrading Wildfly to version 19 was part of the upgrade of the HCP Gateway software to version 4.2.0, go back to **Chapter 18 HCP Gateway Software Upgrade** Step 21 to complete the upgrade.

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