Hitachi Content Platform Gateway Installation Supplement Guide

Confidential – Internal use only

Release Version 4.1

Windows & Linux

The purpose of this document is to cover any additional information that may be required for installing the Hitachi Content Platform (HCP) Gateway software.

FE-HCPG011-00

April 2020

Table of Contents

Chapter 1 Login Information

The purpose of this document is to provide additional information needed for installing and setting up Hitachi Content Platform (HCP) Gateway software.

> **WARNING**: For security reasons **ALL** the default passwords must be changed after first login. The new passwords should be securely stored by the customer. Reboot is required.

Administrator Logins (default):

Windows OS Administrator:

Username: administrator
password: hvlab124!

Linux OS Administrator:

Username: vault
password: 0rgan1c

HCP Gateway Management Console Administrator:

Username: admin
password: admin

Password Change:

When doing VM deployment, upon first login to the HCP Gateway Operating System, the default passwords 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 Forcing Password Change chapter.

Chapter 2 Known Issues and Restrictions

Known Issues and Restrictions:

1. **HCP Gateway Management Console port has changed:**
   Please note that port 28080 (HTTP) is no longer being used and requires port 28443 (HTTPS) for access.

2. **Editing files with Windows Notepad that are no longer in the local cache fails to overwrite existing files and the user must use "Save as"**
   a. Notepad does not work well for editing stubbed/virtual files that are no longer in the local cache.
   b. Please use either Notepad++ or MS Office applications.

3. **"Include Retention" Policy Restrictions**
   a. The first character in the Include filter can only be lowercase. Uppercase characters are **not** allowed.
   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.

4. **When using Server mode the files are R/W and not under retention**
   a. Files will remain R/W on both the Gateway and HCP systems.
   b. Do **not** combine "Copy" policy and "Include Retention" setting. This is **not** supported.

5. **Retention on a Subfolder**
   When retention is set on a subfolder (e.g. retention is set on Colorado subfolder in the following path "G:\abc\sales\usa\Colorado"), the path before the subfolder becomes fixed and cannot be deleted, renamed or in any way modified.

6. **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.

7. **How to work around the Password Reset hang issue during VM deployment:**

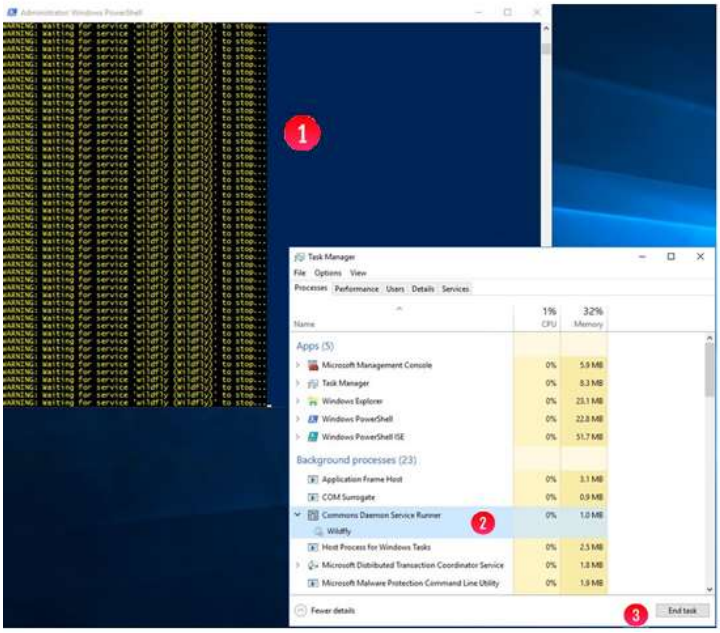
   Step 1 – Open the Windows PowerShell window using the icon in the system taskbar (Figure 2.1.1).

   Figure 2.1 – Open PowerShell Window

   Step 2 – If the Windows PowerShell window displays the message "**WARNING: waiting for service "wildfly (wildfly)**" to stop…" (Figure 2.2.1), then open Windows Task Manager, locate the "Background processes" named "Commons Daemon Service Runner" that is running the service "Wildfly" (Figure 2.2.2). Click the "***End Task***" button (Figure X.2.3) to stop the "Wildfly" service.

   The password reset prompt should appear now.

Figure 2.2 – End Wildfly Service



Chapter 3 HCP Settings

HCP Supported Versions

1. HCP 8.x – supported for both POC and Production deployments
2. HCP 7.3.x – only supported for POC deployments (**NOT** supported for production use)
    a. Only supports TLS 1.0 and does **not** support TLS 1.1 and 1.2.
    b. MPU is not supported – only supported on HCP 8.x or higher

S3 v4 Payload Signature

1. HCP 8.x supports both S3 v4 signed and unsigned payload
2. HCP 7.x only supports S3 v4 signed payload (does **not** support unsigned payload)

HCP Namespace Settings

3. **Assign Owner** to HCP Namespace
4. **Versioning** – Do **not** enable (file versioning is done by HCP Gateway)
5. **Retention** – Do **not** set retention (HCP Gateway will pass the retention settings for each file)
6. **MPU** (supported on HCP 8.x or higher) – Enable
7. **Settings –> ACLs** – Enable ACLs and Enforce ACLS
8. **Settings –> Optimization** – Enable Optimized for Cloud protocols only
9. **Protocols –> HTTP(S)** – Enable HTTPS
10. **Protocols –> HTTP(S)** – Enable HTTP
11. **Protocols –> HTTP(S)** – Enable REST API
    a. Select authenticated access only
    b. Enable Active Directory single sign-on (if needed)
12. **Protocols –> HTTP(S)** – Enable Hitachi API for Amazon S3
    a. Select Authenticated access only
    b. Enable Active Directory single sign-on (if needed)

HCP Tenant Settings

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

Chapter 4 Recommended HCP Gateway Settings

Recommended HCP Gateway settings:

1. **Server Mode** – please do **not** use **LOCAL** policy. We will likely disable this in the future. Always 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** – recommend **not** enabling the S3 v4 payload signature unless needed. If enabled it will have some performance impact.

3. **Encryption –** please use data encryption in either the HCP Gateway or HCP storage, but not in both. If encryption is needed, we recommend using encryption in HCP Storage.

4. **Compression** – please use data compression in either the HCP Gateway or HCP storage, but not in both.

Chapter 5 Linux vs. Windows Gateway Features

This comparison is based on Linux 4.0 and will be updated for Linux 4.1 release in April 2020.

Key feature differences between Linux and Windows Gateway:

Linux Gateway does NOT support the following features and data migration tools:

1. End user restore
2. Admin Auditing
3. Cache management using Watermarks
4. Virtual Snapshot and Share level restore
5. Linux Clustering is NOT supported in v4.0:
    a. NO UI for setting up Linux Clustering
    b. NO documentation for setting up Linux Clustering
6. HDI Migrator tool – intelligent in-place data takeover of NFS Shares
7. Copy to HCP Gateway (NAS Migration)
8. FSO (external Tiering to SAM) - Archive use case
9. Azure Storage

Linux Gateway is missing the following settings from the Management Console UI:

1. HCP Gateway as a Storage target – create copy of the data on another Gateway device
2. 'Replication' of VFS DB to another Gateway device

Linux Gateway does not auto negotiate the TLS version:

The Windows HCP Gateway will auto-negotiate TLS version with the storage system starting from 1.2 and walk in reverse to 1.1 and then 1.0. The Linux HCP Gateway will **not** auto-negotiate TLS version and will need to be configured correctly in the Linux OS.

In the Linux OS, the system SSL configuration (/etc/ssl/openssl.conf) needs to be changed to tell the libraries to use a lower TLS version. If HCP storage does not support TLS 1.2, then the MinProtocol and CipherString in the [system_default_sect] needs to be commented-out:

/etc/ssl/openssl.conf

```
...
[system_default_sect]
#MinProtocol = TLSv1.2
#CipherString = DEFAULT@SECLEVEL=2
```

Chapter 6 Active Directory Setup

Setting up AD for user authentication:

The customer's Active Directory administrator will need to provide the OU path information.

Here is an example (in a lab environment):

The active directory 'Domain' is: dts-evlab.com
The active directory 'Search Base' is: CN=Users,DC=dts-evlab,DC=com
The 'User' security group is: CN=hcpg,CN=Users,DC=dts-evlab,DC=com
The 'Admin' user is: CN=hcpgadmin,CN=Users,DC=dts-evlab,DC=com

Notice that the 'User' security group and 'Admin' user use the 'Search Base' to complete their respective OU fields.

In the HCP Gateway UI the above information is entered into the appropriate fields:

Domain:	dts-evlab.com
Search Base:	CN=Users,DC=dts-evlab,DC=com
User:	CN=hcpg,CN=Users,DC=dts-evlab,DC=com
Admin:	CN=hcpgadmin,CN=Users,DC=dts-evlab,DC=com

Chapter 7 Common Error / Warning Codes

Warning 769

Indicates that there is an issue writing files to HCP. The messages are warnings that are caused when the connection to the storage is lost and comes back. In the Management UI Summary page, please click the Refresh button for the Storage and make sure it has an “Active” status.

Warning 513

HCP Gateway doesn't see the folder that the file is located in. Please check the share to make sure the parent folder exists and that you have ACL permissions to modify the files in that folder.

OR

HCP Gateway doesn't completely save the file in the database the first time, so the code retries the save.

Chapter 8 HCP Gateway 4.1 Windows VMware Installation – High-level Steps

High level installation steps and sequence of events:

1. **Initial Deployment and Setup for Windows VMware**
    a. Deploy OVF Template
    b. Log into Windows OS as administrator
    c. Wait for the prompts to reset account credentials (New for 4.1 release)
        i. MariaDB\root
        ii. MariaDB\sam
        iii. UI\admin
        iv. UI\GlobalAdmin
    d. System will reboot with warning message (New for 4.1 release)
    e. Change the IP address – select YES for allowing the server to be Discoverable by other devices
    f. Set the Time Zone and Time Server
    g. Change the Computer Name
    h. Setup AD – add the Server to Active Directory Domain
    i. Turn on Windows Discovery
    j. Update VMware tools
    k. Add Capacity to Storage Volume
    l. Take a Snapshot

2. **Configure the HCP**
    a. Create an HCP Tenant and apply settings (see HCP Settings chapter)
    b. Create an HCP Namespace and apply settings (see HCP Settings chapter)

3. **Configure the Gateway**
    a. Login to Management Console UI (https://ipaddr:28443/hcpg)
    b. Create Storage Location
    c. Create Storage Group
    d. Create Policy
    e. Create Share
    f. Revision Management
    g. Set Cache Watermark policy

4. **Ask customer to activate MS Windows Server OS License (customers have 180 days)**
    Customers must supply the MS Windows Server OS license unless they purchased the HCP Gateway Server for SMB or HCP Anywhere Edge Server (which include the MS Windows Server OS license key).

Chapter 9 Force Password Change for HCP Gateway Application

When doing a VM deployment, the password change should happen after the initial login to the HCP Gateway Operating System.

Below are the steps to run the HCP Gateway change password process manually for physical server deployments or if the process fails or if the customer wants to change the passwords.

Running the PowerShell script will reset the registry entries to initiate the password change process after a reboot and login to the Windows OS:

1. Log into Windows OS as “administrator”.
2. Open a PowerShell console
3. Change directory to “C:\SAM\ps”
4. Run the script “setRunOnce.ps”
5. Reboot the HCP Gateway
6. Log in to Windows Operating System
7. Password Change will be initiated

Hitachi Vantara

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

Contact Information
USA: 1-800-446-0744
Global: 1-858-547-4526
HitachiVantara.com/contact