Hitachi Ops Center Protector

7.4

Quick Start Guide

MK-99PRT001-04
April 2022

Contents

Preface

This document describes how to install and use Hitachi Ops Center Protector.

Software version

This document revision applies to Ops Center Protector version 7.4. Please refer to the accompanying Release Notes for information on what's changed in this release.

Intended audience

This document is intended for system administrators, backup administrators and other users who are responsible for installing, configuring, and operating Hitachi Ops Center Protector.

This document in intended for users who want to install Hitachi Ops Center Protector.

For guidance on configuring Role Based Access Control, please refer to the accompanying User Guide.

Related documents

Main product guides:

- *Hitachi Ops Center Protector Software Release Notes*.
- *Hitachi Ops Center Protector Quick Start Guide*.
- *Hitachi Ops Center Protector User's Guide*.
- *Hitachi Ops Center Protector Oracle Application Guide*.
- *Hitachi Ops Center Protector VMware Application Guide*.
- *Hitachi Ops Center Protector Hyper-V Application Guide*.
- *Hitachi Ops Center Protector Microsoft SQL Application Guide*

Programming guides:

- *Hitachi Ops Center Protector REST API User Guide*.
- *Hitachi Ops Center Protector REST API Reference Guide*.
- *Hitachi Ops Center Protector REST API Change Log*.

Document conventions

This document uses the following typographic conventions:

Convention	Description
Bold	▪ Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click **OK**. ▪ Indicates emphasized words in list items.
Italic	▪ Indicates a document title or emphasized words in text. ▪ Indicates a variable, which is a placeholder for actual text provided by the user or for output by the system. Example: `pairdisplay -g group` (For exceptions to this convention for variables, see the entry for angle brackets.)
`Monospace`	Indicates text that is displayed on screen or entered by the user. Example: `pairdisplay -g oradb`
< > angle brackets	Indicates variables in the following scenarios: ▪ Variables are not clearly separated from the surrounding text or from other variables. Example: `Status-<report-name><file-version>.csv` ▪ Variables in headings.
[ ] square brackets	Indicates optional values. Example: [a | b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a | b } indicates that you must choose either a or b.
| vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [a | b] indicates that you can choose a, b, or nothing. { a | b } indicates that you must choose either a or b.

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

Icon	Label	Description
	Note	Calls attention to important or additional information.
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
	Caution	Warns the user of adverse conditions and/or consequences (for example, disruptive operations, data loss, or a system crash).
	WARNING	Warns the user of a hazardous situation which, if not avoided, could result in death or serious injury.

Conventions for storage capacity values

Physical storage capacity values (for example, disk drive capacity) are calculated based on the following values:

Physical capacity unit	Value
1 kilobyte (KB)	1,000 (10^3) bytes
1 megabyte (MB)	1,000 KB or $1{,}000^2$ bytes
1 gigabyte (GB)	1,000 MB or $1{,}000^3$ bytes
1 terabyte (TB)	1,000 GB or $1{,}000^4$ bytes
1 petabyte (PB)	1,000 TB or $1{,}000^5$ bytes
1 exabyte (EB)	1,000 PB or $1{,}000^6$ bytes

Logical capacity values (for example, logical device capacity, cache memory capacity) are calculated based on the following values:

Logical capacity unit	Value
1 block	512 bytes
1 cylinder	Mainframe: 870 KB Open-systems: ▪ OPEN-V: 960 KB ▪ Others: 720 KB

Logical capacity unit	Value
1 KB	1,024 (2^{10}) bytes
1 MB	1,024 KB or $1{,}024^2$ bytes
1 GB	1,024 MB or $1{,}024^3$ bytes
1 TB	1,024 GB or $1{,}024^4$ bytes
1 PB	1,024 TB or $1{,}024^5$ bytes
1 EB	1,024 PB or $1{,}024^6$ bytes

Accessing product documentation

Product user documentation is available on the Hitachi Vantara Support Website: https://knowledge.hitachivantara.com/Documents. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting help

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

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

Comments

Please send us your comments on this document to doc.comments@hitachivantara.com. Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara LLC.

Thank you!

Chapter 1: Introduction

This chapter describes the software installation and initial configuration tasks.

> **Note:**
>
> Before you install Ops Center Protector, confirm that your hardware and software meet the requirements that are outlined on the Ops Center Protector product website at https://www.hitachivantara.com/en-us/products/data-protection/data-instance-director.html#tech-specifications .

About Ops Center Protector

Ops Center Protector provides a modern, holistic approach to data protection, recovery and retention. It has a unique workflow based policy engine, presented in an easy-to-use whiteboard-style user interface that helps map copy-data management processes to business priorities. A wide range of fully integrated hardware storage-based and host-based incremental-forever data capture capabilities are included that can be combined into complex work flows to automate and simplify copy-data management. With these you can:

- Choose the right technology for each workload, based on service level requirements, but manage them from one place.
- Drag-and-drop a range of protection, retention and repurposing capabilities to easily create and manage complex work flows.
- Automate and orchestrate Hitachi storage-assisted snapshots, clones and replications to eliminate backup windows.
- Automate the mounting of Hitachi storage based snapshots, clones and replications for proxy backup and repurposing.

Protector supports a wide range of data storage targets, including repository, block, and file based storage.

Architecture

At the heart of Protector is the *Master*; a software component installed on a dedicated server that acts as a central hub, communicating with users via a REST interface and web based UI. The *Master* monitors and controls the activity of a set of *Clients*; software components installed on servers in the protected environment. Normally, the *Master* does not actively take part in data protection data flows; *Clients* do this themselves according to *rules* distributed from the *Master*.

A Protector installation thus consists of:

- A *Master* that controls the UI and the actions of all other nodes on the environment.

  Master nodes can coexist on the same network, allowing multiple Protector environments to coexist.

  Passive standby master nodes can be installed on a Windows failover cluster so that the standby can be brought online in the event that the active master fails.

  Note: It is recommended that the *Master* server not be assigned any other roles.

- Multiple *Clients* that participate directly in data protection data flows, acting as sources of data to be protected (e.g. database servers) and destinations capable of receiving backup data (e.g. repositories).

  Clients implement various different roles within a data flow and must be configured to perform these roles. This consists of ensuring the appropriate prerequisites are installed, and configuration via the UI.

  Client nodes can be installed on application clusters such as Oracle RAC.

  Each *Client* can only be authorized and controlled by one master.

The figure below shows a possible installation scenario where two completely independent Protector environments coexist on one network.

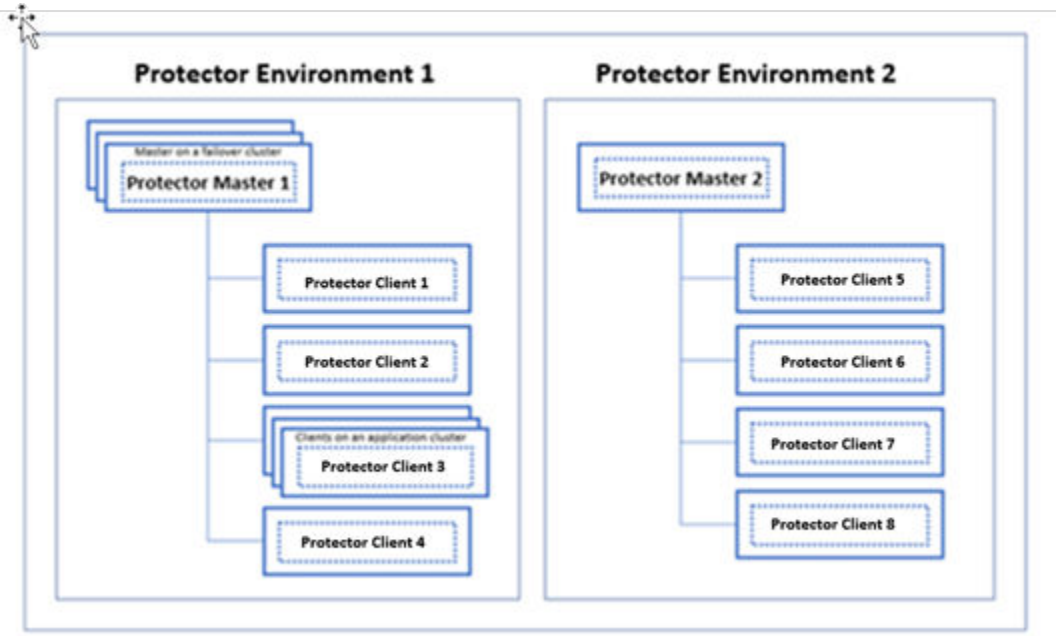


Figure 1 Possible installation scenario

Features and benefits

Ops Center Protector enables you to:

- Meet operational recovery, disaster recovery and long-term recovery challenges in a single, unified platform.
- Drive the backup window, recovery point objective (RPO) and recovery time objective (RTO) to near zero.
- Employ incremental-forever data capture at the block level helping to reduce secondary storage requirements by 90% or more.
- Use intuitive, drag-and-drop workflow creation, node and policy management wizards for administrative agility.
- Use Hitachi Thin Image snapshot orchestration for your critical data and applications.
- Easily create or adopt ShadowImage, Hitachi TrueCopy®, Universal Replicator, Global-Active Device and File Replication without scripting, on a scheduled or ad-hoc basis.
- Orchestrate application-consistent snapshot and clone management for Oracle.
- Orchestrate application-consistent snapshots and clones across other applications and file systems.
- Combine automated local snapshot and off-site replication for an end-to-end modern data protection and recovery solution.
- Automatically trigger snapshots and clones of remote replica data for secondary operations, such as test and development.
- Mount and unmount snapshots and clones automatically as part of an orchestrated policy workflow.
- Further reduce network and storage costs through source and target data deduplication.
- Protect VMware hypervisors and virtual machines.
- Support a broad range of storage types, including repositories and block storage.

Chapter 2: Installation and license activation

About licenses

Before using Ops Center Protector, you must enter one or more license keys using the user interface. You can obtain perpetual license keys by contacting your Hitachi Sales representative and providing the machine ID listed in the Protector License screen.

It is important to understand that the required license capacity is based on protected Front end capacity. This is the total size of the primary data set that can be protected. Primary data that is replicated to two sites only requires a license for the primary data, not the replicas. This applies to all node types.

Along with the required front end capacity license, other features require the following additional licenses:

- Mover Licenses

  Mover licenses (Backup Mover License and Storage Replication License in the following table) permit the use of IP-based backup to specified targets or storage-based operations to protect a certain capacity of source data. You must install one or both mover licenses depending on the backup copy architecture that implements data protection.

- Application Licenses

  Application licenses enable application or Hypervisor-aware protection. If you install an application license, you must also install a mover license that corresponds to the data protection operations that you want to use. The mover licenses supported for each application are listed in the following table.

The following table lists the licenses required for specific features:

Feature	License (version 7.3 and later)
Inclusive storage	**Licenses included with an array purchase**: ▪ Frame capacity Storage Replication Mover license ▪ 1 TB Backup Mover license ▪ Unlimited Filesystem license
Host-based backups (over IP)	**Backup Mover License**

Feature	License (version 7.3 and later)
Includes the following target nodes: ▪ Protector Repository ▪ Hitachi Content Platform ▪ AWS S3	Protects the following source node types and application nodes as listed in the Application license section: ▪ OS Host nodes ▪ VMWare nodes with the Protector agent installed ▪ VCenter nodes Also applies to Oracle RMAN backups using the Protector SBT channel connector.
Hardware storage replication Includes protection using array-based technologies for data provisioned from Hitachi Block storage.	**Storage Replication (Mover) License** Protects the following source node types and application nodes as listed in the Application license section: ▪ OS Host provisioned from Hitachi block ▪ VMware VM nodes with the Protector agent and physical RDMs ▪ Hitachi Block Host
Application-aware protection Includes the following target nodes: ▪ Protector Repository ▪ Hitachi Content Platform ▪ AWS S3 ▪ Hitachi Block	**Application Licenses** ▪ VMWare License (Backup or Storage Mover) ▪ Oracle Database License (Storage Mover only) ▪ SQL Server License - v7.3 and later (Storage Mover only) ▪ Hyper-V License (Storage Mover only) ▪ Filesystem (unlimited/no charge) (Backup or Storage Mover)
Host based over-the-wire encryption Refers to technologies that prevent data from being read during in transmission.	Available No-cost license available in selected regions based on export rules and restrictions imposed by the country of sale.

Feature	License (version 7.3 and later)
Host based data-at-rest encryption Refers to technologies that prevent data from being read when residing in a repository.	Available No-cost license available in selected regions based on export rules and restrictions imposed by the country of sale.

A free, five week *Gen3* trial license is included with Protector, providing 1PB for each front end capacity listed above without encryption and enabled for VSP G/F350, G/F370, G/F700, G/F900 storage arrays.

Note: Overrunning the licensed front end capacity does not stop Protector from protecting your data, however some features might be limited until you license the over-capacity data.

Hitachi Block prerequisites

The following prerequisites are mandatory if you plan to perform snapshotting and/or replication of Hitachi Block volumes. Please also refer to the Protector support matrices at https://www.hitachivantara.com/en-us/products/data-protection/ops-center-protector.html .

- A machine (known as an ISM) must be assigned that controls the Block storage device. This node must be a supported Windows or Linux machine with the Protector Client software installed.

  Caution: ISM nodes and their associated CMDs used to control storage devices must not be shared with applications other than those forming part of the Ops Center suite.

- All primary data (paths or application data) to be snapshotted or replicated within the same data protection policy must exist on the same storage device.
- The block storage hardware must:
  - Support the data protection technologies you intend to use
  - Have the correct firmware version installed
  - Have the correct SVOS version installed
- For all replication types the P-VOLs must be setup in the host group
- In order to resize logical devices represented by the Block Host node that are part of a replication or snapshot pair the array account must have the Support Personal permission.
- For UR, journals must be set up, although for HM800 and later arrays Protector can create journals
- For GAD, the quorum disks or quorum-less disks must be provided. In most cases, one quorum device between participating storage systems is satisfactory. Please refer to the *Global-Active Device User Guide* for best practices

- For GAD, the array should be configured to allow virtualized LDEVs if they are required (where supported by the array)
- Port security must be enabled.
- Primary volumes must be set up using other Hitachi tools prior to selection in Protector
- For application consistent snapshots, the application must be installed and configured to use P-VOLs on a storage array, see the relevant application guide for details on the application configuration
- The password for authorizing a Block Device node must contain only useable CCI command characters: `A-Za-z0-9'-./:@\_`
- The device must have adequate shared memory (see Provisioning and Technical Guides)
- Pools must be created using Storage Navigator prior to selecting the Target Storage in Ops Center Protector:
  - For standard mode (non-cascading) TI the TI Pools must be set up
  - For cascade mode TI the Dynamic Provisioning Pools must be set up to also be a hybrid pool, otherwise a TI pool will also be required
  - For SI, TC, UR and GAD the Dynamic Provisioning Pools must be set up
- The following licensed features may be required depending on the features being used:
  - Dynamic Provisioning
  - Storage Navigator
  - Thin Image (for TI snapshot and RTI replication scenarios)
  - ShadowImage (for SI replication scenarios)
  - TrueCopy (for TC replication scenarios)
  - Universal Replicator (for UR replication scenarios)
  - Global-Active Device (for GAD replication scenarios)
  - Remote Replication Extended (for 3DC scenarios)
- The Protector ISM node controlling the block storage device must have:
  - The correct version of Hitachi CCI installed.

    If CCI is not installed in the default location there are two options:
  - 1. Add a symbolic link from the default location to the install directory
    2. Configure Protector to use CCI in the custom location using the following instructions:
       a. Stop the Protector services on the ISM node
       b. Go to the directory <Protector home>\db\config
       c. Make the change to all files matching hitachivirtualstorageplatform*.cfg

d. Change the <BinDirectory> value from C:/HORCM/etc to the correct installation path

```
<!-- Install directory of CCI, override to change
installation directory. -->
```

```
<BinDirectory>C:/HORCM/etc</BinDirectory>
```

e. Ensure the change has been made to all files at per 3 including the default one.

f. Start the Protector services on the ISM node

- Access to a dedicated Command Device (CMD) on the storage device, set up as follows:

  WARNING: When running the Analyzer probe server, API Configuration Manager, and Protector ISM Client on the same VM, all components share the same command device, but API Configuration Manager and Protector ISM Client must access the storage systems using different credentials. This means that API Configuration Manager and Protector ISM client must use different login accounts when accessing the storage system.

  - Security disabled
  - User authentication enabled
  - Device group definition disabled
  - The CMD must be visible to the host OS where the Protector proxy resides
  - The CMD must be offline
  - The CMD must be added to the meta_resource only.
  - Multiple active command devices may be visible to a Protector proxy as long as each one represents a different block storage device. Behaviour is undefined if multiple active command devices represent the same block storage device, unless these are configured in the Protector proxy node fail-over priority list.
  - Fibre channel and IP command devices are supported.
  - Multipath for Command Devices is supported

- A dedicated user (specified when creating the Hitachi Block Device node) for Protector must be created on the storage device with at least the following roles:
  - Storage Administrator (Provisioning)
  - Storage Administrator (Local Copy)
  - Storage Administrator (Remote Copy)
  - Security Administrator (View & Modify).

  The user must also have access to Resource Group 0 on the storage device.

- Fibre connectivity (including zoning) and pre-configured RCU paths between arrays for remote replication technologies

Hitachi File prerequisites

The following prerequisites are mandatory if you plan to perform snapshotting and/or replication of Hitachi File volumes. Please also refer to the Protector support matrices at https://www.hitachivantara.com/en-us/products/data-protection/data-instance-director.html#tech-specifications:

- A machine must be assigned that controls the File storage device. This node must be a Windows or RedHat Linux machine with the Protector Client software installed.
- All primary data (paths or application data) to be snapshotted or replicated within the same data protection policy must exist on the same storage device.
- The following licensed features are required:
  - File Clone
  - NFS
  - Replication
- Protector requires an EVS (Enterprise Virtual Server) configured for file services and file systems mounted on it.
- Access configuration for NFS exports must include `norootsquash`

Note: Operating System Specific Requirements:

OS	Requirements
Linux	Access to Hitachi File requires: ▪ **`rescan-scsi-bus.sh`** CLI tool (see http://sg.danny.cz/sg/sg3_utils.html ▪ **`Multipath`** CLI command (install the multipath package)

Generation 1 Hitachi Content Platform prerequisites

If you plan to use the Generation 1 Hitachi Content Platform (HCP) with Ops Center Protector, then the following Search Facility Settings must be selected within the Settings tab of the HCP Management Console, for the Metadata Query Engine (MQE):

- Enable indexing
- Enable indexing of custom metadata

Click Update MQE Settings to reflect the changes.

- A Protector HCP node can only be created if the Protector Master node can directly connect to the HCP web interface.
- The tenant must have Enable management through APIs turned on in the **HCP Tenant Management Console**.
- The user should have at least the following enabled in the **HCP Tenant Management Console**:
  - Roles:
    - Administrator
    - Compliance
  - Permissions:
    - Read
    - Write
    - Delete
    - Privileged
    - Search

How to install/upgrade Protector on Windows and Linux or AIX

Before you begin

Caution: Thin Image snapshot operations default to *Provisioned using floating device*. In versions prior to 6.5, this setting would automatically fallback to *Fully provisioned* if the hardware storage device did not support floating devices. With the introduction of *Cascade mode* snapshots in version 6.5 (now the default mode), this automatic fallback has been removed. Consequently:

- Data flows created in versions prior to 6.5 that contain Thin Image snapshot operations, with cascade mode is enabled, will now fail if the underlying hardware does not support *floating device*. These data flows must be manually reconfigured to use the correct provisioning type. Please note that if these data flows also contain replication operations, then these will be re-evaluated when the modified data flows are re-activated.
- Data flows created in versions prior to 6.5 that contain Thin Image snapshot operations, with cascade mode enabled, will now fail if the P-VOLs have any pre-existing non-cascade mode snapshots. If cascade mode is to remain enabled then any non-cascade mode snapshots must be deleted.
- For data flows created in version 6.5 or later, if the hardware storage device on which Thin Image snapshot operations are performed does not support *Floating device* and *Cascade mode*, then Thin Image operations will fail, unless the appropriate settings are selected in the respective data flows.

Caution:

- Refer to the Protector support matrices at https://www.hitachivantara.com/en-us/products/data-protection/data-instance-director.html#tech-specifications before attempting installation, to ensure that you understand the infrastructure requirements, available functionality and upgrade paths for your particular environment.
- If you intend to use Protector with Hitachi storage hardware then refer to the following before proceeding:
  - Hitachi Block prerequisites (on page 14)
  - Refer section "Generation 1 Hitachi Content Platform prerequisites" in User Guide.

Note:

When upgrading, it is highly recommended (and often necessary) to upgrade all nodes to the same version. The recommended order in which to upgraded is:

1. Internet Connected Nodes. If ICNs are not upgraded first, they may not be able to be 'push upgraded' through the UI. ICNs may appear to go offline until the master is upgraded.
2. Master Node(s).
3. Clients acting as ISMs, controlling Hitachi Block and File storage devices.
4. Clients acting as Data Destinations, such as Repositories.
5. Clients acting as Data Sources, such as application servers.

Note:

- For a new installation, the Master node must be installed before any Client nodes.
- When installing a new Master, you must select the account to use for initial Protector log-on. This account must be a local OS account which is able to successfully log in to the machine. These credentials will be input to the Protector UI to enable the initial access control configuration to be performed.
- Read the release notes shipped with the installer to ensure that the currently installed version can be upgraded to the new version. It may be necessary to upgrade to an intermediate version first and perform additional actions prior to and after upgrading.
- You may need to create an exception in your anti-virus software when installing.
- DO NOT upgrade while replications are in the process of pairing. Any active replications must be in the paired state before upgrade is carried out.
- It is recommend that you perform an upgrade only after currently active backups have been completed.
- Before upgrading, unmount any mounted snapshots and replications.

- It is recommended to backup /protector folder to avoid any issue during OS upgrade.
- If you uninstall a Client node, you will need to delete it from the Nodes Inventory before subsequently reinstalling it. This ensures that the Master node regenerates new identifiers for that node. If you do not do this then the reinstalled Client will not be recognized.
- Operating System Specific Behaviour:

OS	Note
Linux	We recommend that Linux source nodes have a Logical Volume Manager (LVM) on each volume group.
Linux and AIX	Ensure you have execute permissions using the command **`chmod 755`**, before running the installer. A minimum of 10 GB of free space is required in the 'unused' portion of the volume that is to be backed up. This is in addition to the space required for the allocated storage area. For example, if 100 GB of usable storage is required, then the total disk size will be 110 GB (100 GB of usable storage and 10 GB of unused storage for snapshot administration).
AIX	It is only possible to install the Protector Client on an AIX node.

All nodes that will participate in a backup data flow need to have Ops Center Protector installed. A node used only to access the web based user interface does not need to have any components installed on it.

Procedure

1. Locate and run the installer appropriate for the target OS and hardware architecture.

   Tip: Protector can be installed directly from the command line if required. Refer section "Installing and upgrading Protector from the command line" from **User Guide** to the CLI reference in the User Guide for details of the installer's command line options.

   The installer filename has the following format:

   Protector-**R***m.n-m.n.n.nnnnn-ostype-proctype*

where:

- *m.n-m.n.n.nnnnn* - is the version and build number
- *ostype* - is the target operating system type:
  - **`Win`**
  - **`Linux`**
  - **`AIX`**
- *proctype* - is the target processor type:
  - **`x64`**

The **Setup** wizard will be launched if a GUI shell is available. If not then the same information will be presented using the text mode shell.

2. If a previous installation of Ops Center Protector is found, the installer will prompt you to upgrade or abort the installation.
   - Click **Yes** to upgrade the existing Protector installation on this node.

     Tip: When upgrading along a supported version upgrade path, any existing data flows, policies, schedules etc. will be preserved. If any further actions are required post upgrade, then these will be described in the Release Notes shipped with the new version.
   - Click **No** to exit the installer wizard, in which case no changes will be made to the current installation.
3. When the **Setup** wizard appears, a welcome message is displayed. Click **Next** to begin the installation.
4. When prompted, read the License Agreement.
   - Select **I accept the agreement** if happy to proceed and click **Next**.
   - Select **I do not accept the agreement** if not happy to proceed and click **Next**. The installation will be aborted and no changes will be made to the machine.

   License keys are entered once the installation is complete via the License Inventory in the UI (See "How to Add a License" in User Guide).
5. To install in a non-default location, enter the path in the **Installation Directory** field or use the folder browser. Click **Next**.

6. Select the type of installation then click **Next**.
   - **Master** Select this option to install the Master node in your network. If this is a new installation then the Master node must be installed before any Client nodes. The Master node is the central controller for all other nodes and serves as the connection point for the Web UI and REST API.

     Note: The Master node automatically has all the capabilities of a Client node. It is however recommended that the Master node functions only as a Master. Multiple Master nodes can coexist on the same network, however Client nodes can only be authorized and controlled by one Master node.
   - **Client** - Select this option to install all other node types. The specific roles assumed by Client nodes are defined via the Nodes Inventory once installation is completed (See section "How to add a node" in User Guide.). These roles include:
     - Data Sources (basic hosts, VMs, application servers, etc.)
     - ISMs (for controlling Hitachi Block and File storage hardware, etc.)

       Caution: ISM nodes and their associated CMDs used to control storage devices must not be shared with applications other than those forming part of the Ops Center suite.
     - Repositories (acting as host based backup storage destinations)
7. Specify a node name to be used within Ops Center Protector then click **Next**.

   Note: Node names are limited to a maximum of 64 characters. By default, the name is set to the machine's host name. This name is only used by Protector, and will not change the name set by the operating system.
8. If the **Master** is being installed:
   a. Select a local **User Account** for logging on to the Protector web user interface immediately after installation is complete. You must know the password associated with the selected account. The account used can be changed after installation of the Master. Click **Next**.
   b. Accept or edit the **Protector User Interface Port** used to connect to the web based UI. By default it is set to 443, but can be changed if you already have another web server running on that port.
9. If a **Client** is being installed:
   a. Enter the **Master Hostname or IP** address or a DNS resolvable name of the Master node. If it is known that this node will be operating over a non-secure network, then we recommend enabling the **Internet connected node** option. This will encrypt transmitted data as an extra security precaution. Over-the-wire encryption requires a license and may not be available in some territories.
10. When the wizard indicates that it is ready to begin the installation, click **Next**.
    Ops Center Protector files are copied to the designated directories and the necessary components installed.

11. When the wizard indicates that the installation is complete, you will have the option to **Start Hitachi Ops Center Protector User Interface Now** in a web browser. Click **Finish**.

    Note: You do not need to restart the machine. The installer starts all the necessary Ops Center Protector components on the system.

    If a third party firewall is installed on the network, Protector will generate firewall warnings when it starts running. See How to configure a third party firewall for Protector (on page 36).

12. If this is a new installation of a Master node, then use a web browser to log on to the user interface at: `https://<Master>/#/Login`, where *<Master>* is the IP address or DNS name of the Master node. Refer to How to configure a server-side SSL certificate using a UI (on page 37) to prevent security warnings being displayed by the web browser.

    Note: Initial logon must be done with the username specified for the **User Account** during the Master installation. The username must be qualified with the local domain name `master` as follows:

    `<username>@master`

    or

    `master/<username>`

    or

    `master\<username>`

13. Set the locale and time zone appropriate the location of the nodes you are working with.

    See "How to change the UI settings" in User Guide

14. If you are upgrading, the Dataflows should now be reactivated and all destination nodes should be manually resynchronized with their sources. The upgrade process is then complete.

15. Finally, refer to one of the following topics to setup accounts for those users that required access to the Protector user interface.

    - "How to configure basic role based access control" (Refer User Guide) to configure the minimum required access control functionality.
    - "How to configure advanced role based access control" (Refer User Guide) to configure full access control functionality.

How to install a Protector master or client on a Windows cluster

Before you begin

WARNING: This section only applies when clustering the master or protecting data without one of Protector's application integrations.

Do not use this method of installation in case you want to protect supported applications like Microsoft SQL Server or Microsoft Hyper-V. For these applications, install the client as you would for any regular standalone system (see How to install/upgrade Protector on Windows and Linux or AIX (on page 19)).

The Protector *Master* or *Client* capability can be installed on servers in a Windows cluster. Before starting the installation, review the following:

- Ensure that all servers meet the software prerequisites that are outlined in How to install/upgrade Protector on Windows and Linux or AIX (on page 19).
- Confirm that a cluster environment is set up and working correctly.
- For *Master* installations only, ensure that you have all the required license keys for Protector. A separate license key is required for each node in the cluster.

Protector installation for a cluster environment involves performing the following sub-tasks:

Procedure

1. Install Protector on each node in the cluster (see How to install Protector on a node in a cluster (on page 25)).
2. Add the *Cofio Hub* service (see How to add the hub service to a cluster (on page 26)).
3. For *Master* installations only:
   a. Add Protector licenses for each node (see How to add licenses to a clustered master (on page 27)).
   b. Add an authentication domain for the cluster (How to configure authentication for a cluster (on page 28)).

How to install Protector on a node in a cluster

To install Protector on a Windows Failover Cluster node:

Procedure

1. From the Windows **Failover Cluster Manager** console, identify the cluster server node that is currently in control (i.e. the node which has access to the shared disks).
2. Install Protector on the controlling node by running `Protector-m.n-m.n.n.nnnnn-WIN-ppp.exe`.
   The Protector **Setup** dialog is displayed. Click **Next**.
3. Read and accept the license agreement, then click **Next**.

4. Change the **Installation Directory** to the shared drive where you want install Protector. If Protector is already installed on another node in the cluster then select that install location. Click **Next**.

   For example, if your shared drive is `E:\` then the installation path might be on the shared drive: `E:\Hitachi\Protector`.

   Note: The Protector **Installation Directory** must be the same for all nodes in the cluster.

5. Select either the **Master** or **Client** installation type, then click **Next**.
6. Change the default **Node Name** to one that represents the entire cluster. If Protector is already installed on another node in the cluster then use that name. Click **Next** to start the installation.

   Note: The Protector **Node Name** must be the same for all nodes in the cluster.

7. If the **Master** is being installed:
   a. Select a local **User Account** for logging on to the Protector web user interface immediately after installation is complete. You must know the password associated with the selected account. The account used can be changed after installation of the Master. Click **Next**.
   b. Accept or edit the **Protector User Interface Port** used to connect to the web based UI.
8. If a **Client** is being installed:
   a. Enter the **Master Hostname or IP** address or a DNS resolvable name of the Master node.
9. When the wizard indicates that it is ready to begin the installation, click **Next**.
10. When the wizard indicates that the installation is complete, click **Finish**.
11. Open the Windows **Services** console, stop the *Cofio Hub* service and set its *Start Up Type* to *Manual*.

    The *Cofio Hub* service will be controlled by the Failover Cluster Manager in a clustered configuration.
12. From the **Failover Cluster Manager** console, invoke failover to the next node in the cluster, then repeat the above procedure.

How to add the hub service to a cluster

Complete the following steps on the active node in the cluster.

Procedure

1. In the **Failover Cluster Manager** console, configure a *Generic Service* for the cluster using the **High Availability Wizard**.
2. Select the *Cofio Hub* service from the list.
3. Name the service (e.g. *CofioHubSvc*) and assign an IP address, then click **Next**.
4. Select the shared disk that Protector is installed on.
5. Do not replicate any registry settings.

6. Confirm that all settings are correct and then proceed with configuring the service for high availability.
7. Review the report to ensure that the service was configured correctly, then click **Finish**.
8. If a **Master** is being installed, make a note of *Cofio Hub* service's IP address shown in the **Failover Cluster Manager** console. This will be used for accessing the Protector web UI.

   Note: If the web UI is not accessible at this address, check your firewall for the following:

   a. Ensure that Protector is not blocked by the firewall.
   b. Enable port 30304 (Protector) and port 443 (HTTPS).

9. If a **Client** is being installed, authorize the node in the Nodes Inventory.
10. Force a fail-over, to confirm that the Protector node remains online in the Nodes Inventory.

How to add licenses to a clustered master

Before you begin

Install the Protector Master on each of the nodes in the Windows cluster as described in How to install a Protector master or client on a Windows cluster (on page 25).

Because each machine in the cluster has a different machine ID, a separate license is required for each node:

Procedure

1. Navigate to the Protector web UI using the IP address for the *Cofio Hub* service.
2. Log in using the local machine credentials of `administrator@master`.
3. Add the license key for this machine following the procedure described in How to Add a License (on page 38).
4. To add the licenses for the remaining cluster nodes, browse to the installation directory, then navigate to the subdirectory `db\config`
5. Right click `License.xml` and open the file with **WordPad**.
   The following XML is displayed showing the license key for the active node:

```
<licenses>
    <entry>ADYFKAE9PMM9BM2KXDNWCEO8PSABE244U8GA</entry>
</licenses>
```

6. Copy line 2 (the license key for the currently active cluster node) and insert it as a new line below line 2.
7. Change the license key on line 3 to match the one provided for the second cluster node. The following XML should be displayed:

```
<licenses>
    <entry>ADYFKAE9PMM9BM2KXDNWCEO8PSABE244U8GA</entry>
```

```
    <entry>DFGA54AGFDFHDJK675HH86453GHTFGD553DR</entry>
</licenses>
```

8. Repeat for each additional node.
9. Save and close the file.

How to configure authentication for a cluster

Before you begin

Install Protector on each of the nodes in the Windows cluster as described in How to install a Protector master or client on a Windows cluster (on page 25).

During installation, a local administrator account is used. To complete a cluster installation, a domain administrator account must be set up within Protector that is available to all nodes in the cluster:

Procedure

1. Navigate to the Protector web UI using the IP address for the *Cofio Hub* service.
2. Log in using the local machine's `administrator@master` credentials.
3. Add an *Authentication Space* that will perform authentication for the cluster.
   a. Specify the Authentication Space **Name**.
   b. Select the required authentication type (e.g. **Active Directory**).
   c. Select the cluster node as the **Proxy**.
   d. Enter the **Active Directory Domain Name**.
4. Add an *ACP Association* that will provide administrator level access to Protector.
   a. Specify the ACP Association **Name**.
   b. Select the **User** *ACP Association* type.
   c. **Browse** for the required **User Name** from the **Authentication Space** specified in the previous step.
   d. Add the *Default Administrator* from the **Available Profiles** listed.
5. Log out of the web UI.
6. Log back into the web UI using the new `User@Domain` credentials specified in the above steps.
7. Force a fail-over, then log in again using the new credentials to confirm that Protector is still accessible.

How to remotely upgrade Protector client nodes

Before you begin

Caution: Thin Image snapshot operations default to *Provisioned using floating device*. In versions prior to 6.5, this setting would automatically fallback to *Fully provisioned* if the hardware storage device did not support floating devices. With the introduction of *Cascade mode* snapshots in version 6.5 (now the default mode), this automatic fallback has been removed. Consequently:

- Data flows created in versions prior to 6.5 that contain Thin Image snapshot operations, with cascade mode is enabled, will now fail if the underlying hardware does not support *floating device*. These data flows must be manually reconfigured to use the correct provisioning type. Please note that if these data flows also contain replication operations, then these will be re-evaluated when the modified data flows are re-activated.
- Data flows created in versions prior to 6.5 that contain Thin Image snapshot operations, with cascade mode enabled, will now fail if the P-VOLs have any pre-existing non-cascade mode snapshots. If cascade mode is to remain enabled then any non-cascade mode snapshots must be deleted.
- For data flows created in version 6.5 or later, if the hardware storage device on which Thin Image snapshot operations are performed does not support *Floating device* and *Cascade mode*, then Thin Image operations will fail, unless the appropriate settings are selected in the respective data flows.

Note:

- The *Manage Software Updates* RBAC activity must be assigned to users who perform upgrades. It is recommended that this activity is restricted to administrative users only.
- Upgrade of a Microsoft failover cluster node needs to be done locally, following a similar procedure to that described in How to install a Protector master or client on a Windows cluster (on page 25). It's not possible to upgrade remotely because the standby nodes in the cluster are not available. Attempting a remote upgrade will place the clustered Protector service in a failed state, taking it offline.
- Before upgrading unmount any mounted snapshots.
- DO NOT upgrade while replications are in the process of pairing. Any active replications must be in the paired state before upgrade is carried out.

An upgrade can be performed if the existing installation has become corrupted or a newer version of Ops Center Protector is available.

If upgrading, obtain the upgrade installer files from your Hitachi Vantara support representative.

When an upgrade starts, the Ops Center Protector services are shutdown, causing the upgrading *OS Host* node and any nodes for which it serves as a proxy, to go offline in the Nodes Inventory. Any active data flows using those nodes will be temporarily interrupted. These nodes will come back online again when the services are automatically restarted on the *OS Host* node, after the upgrade process is completed, and the affected data flows will resume operation.

Note: We recommend upgrading Ops Center Protector only after current backups have been completed.

Note:

When upgrading, it is highly recommended (and often necessary) to upgrade all nodes to the same version. The recommended order in which to upgraded is:

1. Internet Connected Nodes. If ICNs are not upgraded first, they may not be able to be 'push upgraded' through the UI. ICNs may appear to go offline until the master is upgraded.
2. Master Node(s).
3. Clients acting as ISMs, controlling Hitachi Block and File storage devices.
4. Clients acting as Data Destinations, such as Repositories.
5. Clients acting as Data Sources, such as application servers.

Procedure

1. Locate the installers and accompanying configuration files appropriate for the target OSs and hardware architectures in your Protector environment.

   The installer's executable and configuration filenames have the following format:

   Protector-**R***m.n-m.n.n.nnnnn-ostype-proctype*

   where:

   - *m.n-m.n.n.nnnnn* - is the version and build number
   - *ostype* - is the target operating system type:
     - **`Win`**
     - **`Linux`**
     - **`AIX`**
   - *proctype* - is the target processor type:
     - **`x32`**
     - **`x64`**
     - **`PPC`**

2. Copy both the installer and configuration files to the `C:\Programs Files\Hitachi\Protector\runtime\updater` folder on the Master node.

   This folder will need to be created manually if this is the first time an update has been applied.

3. Click **Nodes** on the Navigation Sidebar to open the Nodes Inventory

4. Select the nodes to be upgraded (Master first, then Clients), then click **Upgrade Clients** to start the upgrade process.

   Note:

   - Only *OS Host* Client and Master node types can be upgraded remotely
   - It is recommended to push out the upgrade to clients in batches of up to 20 nodes at a time.

   When upgrading the Master node, the UI will logout when the node's services are stopped by the installer. Wait a few minutes, then log back in again and complete the upgrade of the remaining nodes.

   When upgrading Client nodes, each one (and any nodes for which that Client acts as a *Proxy*) will go offline temporarily while the upgrade is applied.

   When the nodes come back online, the *Version* shown on the respective tile will be updated accordingly.

5. All active data flows should now be reactivated and all destination nodes should be resynchronized with their sources.

How to upgrade Protector from a version prior to 6.0

Before you begin

Caution:

Some features supported by your existing Protector 4.x or 5.x environment may not yet be supported by Protector 6.x. Ensure that you are fully aware of which features are not yet supported before upgrading.

ANY ATTEMPT TO UPGRADE WHEN USING AN UNSUPPORTED FEATURE WILL HAVE UNDEFINED CONSEQUENCES, INCLUDING POTENTIAL DATA LOSS.

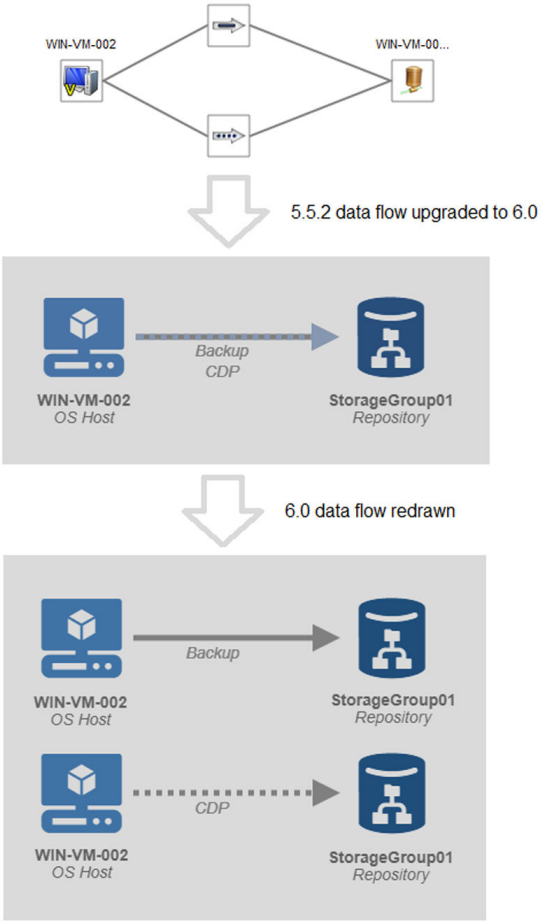
The installer will warn about features that are unsupported before upgrading but will not detect if unsupported features are being used in your existing environment.

Caution: Thin Image snapshot operations default to *Provisioned using floating device*. In versions prior to 6.5, this setting would automatically fallback to *Fully provisioned* if the hardware storage device did not support floating devices. With the introduction of *Cascade mode* snapshots in version 6.5 (now the default mode), this automatic fallback has been removed. Consequently:

- Data flows created in versions prior to 6.5 that contain Thin Image snapshot operations, with cascade mode is enabled, will now fail if the underlying hardware does not support *floating device*. These data flows must be manually reconfigured to use the correct provisioning type. Please note that if these data flows also contain replication operations, then these will be re-evaluated when the modified data flows are re-activated.
- Data flows created in versions prior to 6.5 that contain Thin Image snapshot operations, with cascade mode enabled, will now fail if the P-VOLs have any pre-existing non-cascade mode snapshots. If cascade mode is to remain enabled then any non-cascade mode snapshots must be deleted.
- For data flows created in version 6.5 or later, if the hardware storage device on which Thin Image snapshot operations are performed does not support *Floating device* and *Cascade mode*, then Thin Image operations will fail, unless the appropriate settings are selected in the respective data flows.

- Do not perform an upgrade while hardware replications are being paired. Wait for all pairings to complete.
- Ensure that no Hitachi Block or File snapshots are mounted before upgrading.
- Ensure that you have upgraded all nodes in your existing Protector environment to version 5.5.2 or later, following the supported upgrade path.
- You must upgrade all available nodes to version 6.x before starting to use the 6.x environment; existing *Client* nodes will not be recognised by the upgraded 6.x *Master*.
- Protector 6.x has improved, granular rules activation that allows rules to be activated for individual data flows without affecting existing rules for unrelated data flows. To take advantage of this, complex data flows should be refactored by splitting them into smaller individual flows. This is best done before upgrading because the Protector 6.x data flow editor has been designed to encourage the drawing of small, simple dataflows that can be managed independently.

- If you have data flows in your existing environment that connect a source node to a destination node using both a *Batch* and *Continuous* mover in parallel, then these will still compile correctly. However you will need to redraw them as two separate flows (on the same or separate data flow diagrams) if you want to modify them. This is best done before upgrading. See the example below:



- In previous versions it was possible to create a node group with mixed node types, although this would cause the rules compiler to generate an error. Protector 6.x enforces node groups containing nodes of the same type. Review your existing node groups to ensure that all member nodes are of the same type. This is best done before upgrading.

  When upgrading, the first node in a group is used to set the type of the group; any subsequent nodes that are of a different type are removed from the group. Warning logs are generated for any node which is removed from a group due to type mismatch.

- In previous versions a separate repository store was created for each source node being backed up, the mover type and the store template used. In Protector 6.x a separate repository store is also created for each policy. When upgrading a data flow where a source node backs up to a repository using two or more policies over a single mover (e.g. two batch backup policies with different RPOs), Protector 6.x will create a new store in the repository so that there is one store for each policy.

  When the rules are reactivated after upgrading, the store holding the legacy backups will complete a fast incremental resynchronization, since it is already populated. The new store will complete a full initial synchronization, since it needs to be populated with data from the second policy. This full resynchronization may involve a significant amount of data transfer.

  When restoring, remember that any backups created after the upgrade from data flows, where a source node backs up to a repository using two or more policies over a single mover, will be located in new stores.
- Legacy log messages cannot be viewed in Protector 6.x. If you need to refer to these messages after upgrading then export them prior to upgrade and view them in a text editor or spreadsheet. Ensure the log filters are set to their defaults so that all logs are exported. The export is limited to the last 25,000 log entries.
- Legacy notification events cannot be ported across to Protector 6.x. Make a note of each notification event so that they can be manually reconfigured after the upgrade is performed.
- Legacy versions of Protector made no distinction between *Repositories* and *Hardware Storage Device* proxies; in Protector 6.0 they are treated as separate entities. All legacy *Repositories* that were used solely for the purpose of acting as *Hardware Storage Device* proxies will be removed when upgrading.
- *Repositories* and *Hardware Storage Devices* will rebuild their backup indices into a new database. This may take some time to complete, so restore points will not be listed immediately.
- Protector 6.x no longer sets a retention on objects in HCP; it now deletes objects from HCP when they are no longer referenced by any snapshots in the repository from which they were tiered.

To upgrade Protector from a 5.5.2 or later environment to a 6.x environment:

Procedure

1. On the master node, run **`diagdata -f`** from a command prompt to preserve the current configuration and state files.

   These will be of use if for any reason the upgrade fails.
2. Follow the procedure described in How to install/upgrade Protector on Windows and Linux or AIX (on page 19) or How to install a Protector master or client on a Windows cluster (on page 25) as appropriate.

   Push upgrade from the UI cannot be used; you must upgrade to Protector 6.x using the install wizard or command line. The installer will take you through the upgrade process.
3. Once the upgrade process has been completed on all available nodes, log in to the Protector 6.x user interface.
4. Reactivate all data flows simultaneously.

Caution: You must initially reactivate ALL dataflows in one operation. If you do not, then any active block based replications that are not reactivated will be torn down.

Your Protector environment will now be upgraded to Protector 6.x and will be implementing your existing data protection policies.

Note:

- The rules compiler will generate warnings where data flows and policies need to be amended to take advantage of new Protector 6.x features.
- Some nodes may indicate that they are offline until after the rules have been reactivated for the first time following an upgrade.

5. Once you have set up RBAC, you must reconfigure the access permissions for legacy items. They will not yet be visible to any users other than the one performing the upgrade.

   Permissions for the following items will be affected:

   - Dataflows
   - Destination Templates
   - Notifications
   - Policies
   - Schedules

   When these items are created in Protector 6.x, the user creating them is given *Read/Write Access*, allowing that user to see and change them. Users with the RBAC *Override Ownership Permissions* privilege can also see and edit them. Nobody else will be able to read or modify these items unless granted access.

   When upgrading to 6.x, no *Permissions* are set for legacy items. This means that ONLY users with the RBAC *Override Ownership Permissions* privilege can see and edit them. For other users to see the upgraded items they will need to be granted access permissions.

   Users without the RBAC *Override Ownership Permissions* privilege are prevented from removing all permissions; although they can still remove their own access if required. Only users with the RBAC *Override Ownership Permissions* privilege can remove all permissions.

6. If you have not yet done so, refactor any large, complex or parallel data flows as described above.
7. If you have not yet done so, check that all nodes that were members of node groups are still present and that no warnings have been logged regarding node type mismatch as described above.
8. Re-configure the notification events that you made a note of prior to upgrading. These will have been deleted during the upgrade process.
9. VMware policies will work as before. However the policy wizard will not show any servers selected. The required selections must be remade.

How to configure a third party firewall for Protector

If a third party firewall is installed within your network, when processes are started as part of the Ops Center Protector software installation, firewall warnings might be generated.

Configure the firewall to allow communication between all Protector nodes on one open port: 30304 (TCP).

Additional ports that might need to be opened are:

- Protector User Interface, on port 443 (HTTPS), or the alternative specified during Master installation.
- Protector vCenter proxies, also on port 443 (HTTPS), use the VDDK and vSphere web API to talk to the vCenter.
- Protector VMware proxies, on port 902, are instructed by the vCenter to talk to the ESXi host for virtual disk transfer.

How to configure addresses for nodes on multiple networks

If your environment includes nodes connected to more than one network, e.g. a production network, backup network and the internet, then you will need to configure Ops Center Protector after installation in order to:

- Use one or more of those networks in preferential order depending on availability.
- Prevent (bar) the use of certain networks.
- Connect to remote nodes over the internet by defining an external IP addresses where those nodes may be contacted.

The following procedure must be performed on every node that is connected to the network in question:

Procedure

1. Open a command prompt as administrator.
2. Change directory to the `<Ops Center Protector install>\bin` folder.
3. Stop the Protector services by entering the command **`diagdata --stop hub`**.
4. Check the node's current configuration by entering the command **`setconfig -l`**

   Refer to "Changing a node's profile with **`setconfig`**" in User Guide.
5. To configure a preferred IP address for the node, enter the command **`setconfig -p`** *nnn.nnn.nnn.nnn* where *nnn.nnn.nnn.nnn* is the IP address for the node on the preferred network.

   Additional addresses may be added by listing them in order of preference separated by semicolons. Multiple addresses may need to be quoted depending on Operating System.

6. To configure a barred IP address for the node, enter the command **`setconfig -b`** *nnn.nnn.nnn.nnn* where *nnn.nnn.nnn.nnn* is the IP address for the node on the barred network.

   Additional addresses may be added by listing them in order of preference separated by semicolons. Multiple addresses may need to be quoted depending on Operating System.
7. To configure an external (internet) IP address for the node, enter the command **`setconfig -x`** *nnn.nnn.nnn.nnn* where *nnn.nnn.nnn.nnn* is the IP address for the node on the internet.

   Additional addresses may be added by listing them in order of preference separated by semicolons. Multiple addresses may need to be quoted depending on Operating System.
8. If you need to remove an address then enter the command **`setconfig -r`** *nnn.nnn.nnn.nnn* where *nnn.nnn.nnn.nnn* is the IP address.

   Additional addresses may be added by listing them in order of preference separated by semicolons. Multiple addresses may need to be quoted depending on Operating System.

   Note: The address(es) are removed from the preferred, barred and fixed list.
9. Review the node's new configuration by re-entering the command **`setconfig -l`**
10. Restart the Protector services by entering the command **`hub start`**.
11. Wait a few minutes, then reauthorise the node on the Master (See "How to authorize a node" in User Guide).

How to configure a server-side SSL certificate using a UI

There are two versions of the tool:

- `Certificatetool` This is a UI based tool and requires a windowing manager to be installed on the Master
- `Certificatetoolcli` This is CLI tool and can be run on a 'windows core installation' or a non-X11 linux installation

Before you begin

For Protector installations on Windows and Linux, there is a certificate tool which enables you to:

- Create a self-signed certificate
- Create a certificate signing request
- Install existing certificate

You will need the following Distinguished Names (DN) to create a CSR or self-signed certificate:

- Common Name (CN) - The fully qualified domain name (FQDN) to be secured.
- Organisation (O) - The legal incorporated name of your company.
- Organisational Unit (OU) - The department administering Protector.
- City/Locality (L)
- State/Country/Region (S)
- Country (C)
- Email Address - A point of contact in your Protector administrative team (optional)

How to Add a License

You must provide Ops Center Protector with a valid license key in order to use its features as follows:

Procedure

1. Click **Licenses** on the Navigation Sidebar to open the License Inventory.
2. Copy the **Machine ID** displayed at the top of the License Inventory and include this in your license request email to your Hitachi Vantara support representative.
3. When you have received your license key, click **Add** to open the Activate License Wizard.
4. Copy the license key provided by your vendor and paste it into the **Licence Key** field.
5. Click **Finish**.
   The License Details will be displayed. Review it to ensure that its expiry data is correct and that it provides the required features.

How to uninstall Protector

Before you begin

Caution:

- Uninstalling the Ops Center Protector Master does not deactivate active rules on Client nodes. To do this, you must deactivate all data flow(s) before uninstalling, or uninstall the Clients individually.
- Before uninstalling the Protector application the node (and any nodes proxied from it) must be removed from all dataflows, be unauthorized and deleted from the UI.

Operating System Specific Behaviour:

OS	Note

Linux and AIX	Completely removing Protector from a Linux or AIX machine is straight forward. Enter the following commands and follow the on-screen instructions:
	`/opt/hitachi/protector/uninstall`
	`rm -rf /opt/hitachi/protector`

Windows	Completely removing Protector from a Windows machine involves significantly more work, due partly to the additional functionality available on Windows nodes. Follow the steps listed below.

Procedure

1. Make a note of the path for the install directory and any repositories or ISMs. These will be required later if you wish to completely remove all traces of the installation and do not want to retain backup data stored in the repositories.
2. From the **Start** menu run **Uninstall Hitachi Ops Center Protector**. Alternatively, navigate to the installation directory and execute the command **`uninstall.exe`**.
   A dialog will be displayed asking you to confirm that you wish to proceed. Running the command **`uninstall.exe --mode unattended`** will cause the uninstall process to proceed without requiring user interaction; although popups may briefly appear before being automatically dismissed.
3. Click **Yes** to proceed with the uninstall process (or **No** to abort the process).
   A **Setup** dialog is displayed containing an **Uninstall Status** bar and information about what actions are currently being performed.
4. At some point during the uninstallation process you may be presented with a **Warning** dialog telling you that any repositories must be manually deleted. The uninstall process will pause until you click **OK**.
   Manual removal of repositories is covered later on.
5. Eventually an **Info** dialog will be displayed stating that the uninstall process is complete. Click **OK**.

6. Delete any repository directories noted down before uninstalling. Ensure that there are no files or windows open at these locations or attempts at deletion may fail.
   Protector and its repositories are now uninstalled and you can end the procedure at this point.

   Some artefacts will still remain on your machine. These items are left in place either to facilitate easier reinstallation or because they remained after upgrading from an earlier version or from a failed install. If you want to remove these artefacts, then continue with the following steps:
7. Delete the Protector installation directory tree noted down before uninstalling. Ensure that there are no files or windows open at this location or attempts at deletion may fail.
8. A hidden directory `Protector-RecycleBin` may remain in the root directory. This can be removed.
9. Delete the Bitrock installer log files `bitrock_installer.log` and `bitrock_installer_<nnnn>.log` normally located in `C:\Users\Administrator\AppData\Local\Temp`
10. Open the Windows **Registry Editor** from the **Start** > **Run...** dialog by entering `regedit.exe` in the **Open:** field.
    The **Registry Editor** window is displayed. Alternatively use the **`reg delete`** command from within a **Command Prompt**.
11. Carefully delete the following registry keys:

    Caution: Incorrectly editing the Registry can cause the operating system to become unstable or stop working. Exercise extreme caution when performing this step.

    - `HKEY_LOCAL_MACHINE\SOFTWARE\Cofio Software`
    - `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cofio Software`
    - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CofioHub`
    - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\dcefltr`
    - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sdrefltr`
    - `HKEY_LOCAL_MACHINE\SOFTWARE\Hitachi\Hitachi Ops Center Protector`
12. Confirm that the `dcefltr` and `sdrefltr` filter drivers are no longer installed on your system by entering the commands **`sc query dcefltr`** and **`sc query sdrefltr`**. You should see the following output in response to both commands:

    ```
    The specified service does not exists as an
    installed               service.
    ```

Next steps

Occasionally an uninstallation may fail to complete successfully. In this situation there are a number of things that can be done before retrying:

- Ensure any files or folders that can block the uninstallation are closed.
- Reboot the machine to return it to a known, stable state.
- Reinstall Protector over the existing partially uninstalled version. In most cases this will allow an uninstallation to be successfully re-performed.

Glossary

Archive
A copy that is created for long-term retention.

Asynchronous journalling
Transactions are written to disk and also placed in a journal log file, to protect against data loss in the event of a system failure. Transactions from the log file are sent to the destination machine.

Asynchronous replication
Transactions are held in memory before being sent over the network. If the network is unavailable then transactions are written to disk and sent to the destination machine when the connection is re-established. Asynchronous replication is optimal for connections with sporadic efficiency.

Backup
A copy that is created for operational and disaster recovery.

Bandwidth throttling
Used to control when and what proportion of available network bandwidth is used by Ops Center Protector for replication.

Batch backup
A process by which the repository is updated periodically using scheduled resynchronizations. This method involves a scan of the source machine's file system, but only the changed bytes are transferred and stored. This method is useful for data that does not change often, such as data contained on the operating system disk. Linux based source nodes are only able to perform batch backups.

Clone
An operation where a copy of the database is created in another storage location in a local or remote site.

COPY
A hardware orchestration related status code that indicates that a volume pair is being created. An initial copy or resynchronization is being performed.

Data flow
Identifies the data sources, movers and destinations participating in a backup, along with interconnection paths between them. Policies are assigned to each node to determine what type of data is backed up.

Data source
A machine hosting a file system or application where the Protector client software is installed.

Deduplication
A method of reducing the amount of storage space that your organization requires, to archive data, by replacing multiple instances of identical data with references to a single instance of that data.

Destination node
A machine that is capable of receiving data for the purposes of archiving. This machine might be the Ops Center Protector Repository or Block device.

Dynamic Provisioning Virtual Volume (DP-VOL)
Dynamic Provisioning Virtual Volume. A virtual volume that has no memory space. Used in Dynamic Provisioning.

Hitachi Open Remote Copy Manager (HORCM)

HORCM is a daemon process on the CCI server that communicates with the storage system and remote servers.

Intelligent Storage Manager (ISM)

A Protector Client node that acts as a proxy to Block storage devices.

ISM may also refer to the Intelligent Storage Manager process that runs within the Protector Client software.

License key

A unique, alphanumeric code that is associated with the unique machine ID that is generated during the Ops Center Protector installation. The license key must be activated in order to use the software.

Logical Device (LDEV)

An individual drive (or multiple drives in a RAID configuration) in the storage system. An LDEV might or might not contain any data and might or might not be assigned to any hosts. Each LDEV has a unique identifier, or address, within the storage system. The identifier is composed of the logical disk controller (LDKC) number, control unit (CU) number, and LDEV number.

The LDEV IDs within a storage system do not change. An LDEV formatted for use by open-system hosts is called a logical unit (LU).

Master node

The machine that controls the actions of other nodes within the Ops Center Protector network.

Metadata Store (MDS)

Records metadata that describes items that are held in repositories. The MDS supports indexing of stored data, thus enabling fast searches when locating data for restoration.

Mover

Defines the type of data movement operation to be performed between source and destination nodes, during the creation of a data flow. Batch movers perform block level data transfers on a scheduled basis, whereas continuous movers perform byte level data transfers on a near-continuous basis.

Node Group

Multiple machines of the same type can be assigned to one or more node groups. Within the Data Flow page, you can assign policies to nodes within node groups en-mass.

PAIR

A hardware orchestration related status code that indicates that a volume pair is now created. The initial copy has finished, and the paired volumes are synchronized.

PFUL

A hardware orchestration related status code that indicates that the amount of the data in the journal volume exceeds the threshold. The volume pair is not split and data continues to be copied.

PFUS

A hardware orchestration related status code that indicates that the amount of the data in the journal volume has reached 100% and the volume pair is split and data is no longer being copied.

Policy

A configurable data protection objective that is mapped to machines or groups, and to the data management agents that implement the policy. Multiple policies can be assigned to a single node.

Primary Volume (P-VOL)

The volume in a copy pair that contains the original data to be replicated. The data on the P-VOL is duplicated synchronously or asynchronously to the secondary volume (S-VOL).

PSUE

A hardware orchestration related status code that indicates that a volume pair is split due to an error.

PSUS

A hardware orchestration related status code that indicates that a volume pair is split by operation, or deleted from the storage system on the secondary site. This value is output for the P-VOL.

Raw Device Mapping (RDM)

Raw Device Mapping enables a LUN from a SAN to be directly connected to a VMware VM.

Recovery Point Objective (RPO)

The frequency at which a backup will occur. This governs the point in time to which data can be recovered should a restore be needed.

Refreshed Thin Image (RTI)

A local replication technique based on Thin Image snapshot. The S-VOL is refreshed based on a schedule or on demand. The S-VOL is a thin copy of the P-VOL and therefore needs the P-VOL to be available. Because the S-VOL is refreshed, its ID remains unchanged whenever its contents are updated.

Replication

An operation where a copy of the data is created in another local or remote location automatically.

Repository

A destination node that stores data from one or more source nodes. The Ops Center Protector Repository supports batch backup, archiving, and versioning policies.

Secondary Volume (S-VOL)

The volume in a copy pair that is the copy of the original data on the primary volume (P-VOL). See also primary volume.

SMPL

A hardware orchestration related status code that indicates that a volume is un-paired.

Snapshot (Thin Image)

A point in time copy of the data that is based on references to the original data.

Source node

Any node (server, workstation or virtual machine) that hosts data to be protected by Ops Center Protector. The source node has an Active Data Change Agent, which is responsible for monitoring the host file system and performing the relevant actions defined by the policies. Nodes need to be configured as a source node if they need to transfer locally stored data to a destination node, or implement data tracking, blocking and auditing functions. A node can be both a source and destination simultaneously.

SSUS

A hardware orchestration related status code that indicates that a volume pair is split by operation, or deleted from the storage system on the secondary site. This value is output for the S-VOL.

SSWS

A hardware orchestration related status code that indicates that the P-VOL and S-VOL are switched. The S-VOL is writable.

Synchronous replication

Transactions are transferred to the remote storage device immediately and the write operation is signaled as completed only once data is confirmed as written to both primary and secondary volumes. Synchronous replication is optimal for connections with high efficiency.

Virtual Storage Machine (VSM)

Virtual Storage Machine. A virtualised block storage device that exists within a physical storage array.

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