Hitachi Ops Center Administrator

11.0.4

Getting Started Guide

This guide lists the minimum system requirements and provides the necessary procedures to get Ops Center Administrator up and running.

MK-99ADM000-22
April 2025

Contents

Preface....6
Product version....6
Release notes....6
Accessing product documentation....6
Getting help....6
Comments....7
Chapter 1: Hitachi Ops Center Administrator environment....8
System requirements based on system scale....8
Minimum system requirements....9
Port requirements....12
Supported storage systems....24
Supported microcode/firmware....25
Supported fabric switches....25
Supported servers....26
Supported scalability limits....26
Chapter 2: Installing Ops Center Administrator....27
Installing Ops Center Administrator with the consolidated Ops Center preconfigured media....27
Installing Ops Center Administrator with the application installer....28
Modifying the Ops Center Administrator port in virtual appliance manager....38
Initial setup after installation....38
Changing the Podman network address....39
Configuring the Network Time Protocol server settings....39
Configuring DHCP server settings....40
Configuring SSO by integrating with Ops Center Common Services....41
Registering the Ops Center Administrator server with Ops Center....42
Enabling SSO with the Ops Center portal....44
Updating the Ops Center connection....45
Setting up SSL....45
Setting up SSL when Ops Center Administrator is running on the same server as Common Services....45
Generating and installing a signed SSL certificate....45

Installing a custom signed SSL certificate..... 47
Changing the si token authentication time-out in Ops Center Administrator using VAM..... 48
Enabling and downloading audit logs..... 49
Excluding directories from virus scanning..... 50
Creating Ops Center Users, User Groups, and Roles..... 50
Register Ops Center Protector in Ops Center Administrator 51
Suppressing a Podman upgrade to avoid unintentionally upgrading to an unsupported version..... 52
Changing the SELinux mode..... 52
Logging on to Ops Center Administrator..... 52
Launching the product from the Ops Center portal..... 52
Logging on through Ops Center SSO..... 53
Logging on from the Ops Center Administrator login screen..... 53
Resolving log on issues caused by reloading firewall services..... 54
Resolving log on issues caused by the firewall-cmd command..... 55
Logging on when Ops Center Administrator is not available..... 56

Chapter 3: Managing the Linux environment..... 59
Updating your Linux OS environment using Yellowdog Updater, Modified (YUM)..... 59
Updating your container using Yellowdog Updater, Modified (YUM)..... 59
Modifying the Ops Center Administrator server IP address..... 62
Modifying the Ops Center Administrator log settings..... 62

Chapter 4: Upgrading Ops Center Administrator..... 64
Upgrading Ops Center Administrator by using the application installer..... 64
Upgrading Ops Center Administrator by using backup and restore..... 72

Chapter 5: Adding a storage system..... 75
Onboarding and configuring block storage..... 75
Overview..... 75
Adding the first storage system..... 76
Adding a fabric switch..... 78
Adding servers 79
Onboarding and configuring software-defined storage..... 83
Overview of onboarding a VSP One SDS Block storage system..... 83
Adding the first VSP One SDS Block storage system..... 83

Chapter 6: Removing Ops Center Administrator..... 85
Removing Ops Center Administrator when using Docker..... 85
Removing Ops Center Administrator when using Podman..... 86

Appendix A: Migrating to Ops Center Administrator..... 88
Migrating host information to Ops Center Administrator..... 88
Copying server objects from Hitachi Storage Advisor Embedded to Ops Center Administrator..... 89
Appendix B: Modifying the internal port allocated by Ops Center Administrator for host mode..... 90
Modifying the internal port 90
Syntax rules for the port.properties file..... 90

Preface

Hitachi Ops Center Administrator is an infrastructure management solution that unifies storage management solutions such as storage provisioning, data protection, and storage management; simplifies the management of large-scale data centers by providing smarter software services; and is extensible to provide better programmability and control.

Product version

This document revision applies to Hitachi Ops Center Administrator version 11.0.4 or later.

Release notes

Read the release notes before installing and using this product. They may contain requirements or restrictions that are not fully described in this document or updates or corrections to this document.

Release notes are located on Support Connect at https://knowledge.hitachivantara.com/Documents.

Accessing product documentation

Product user documentation is available on: https://docs.hitachivantara.com. 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 comments to doc.feedback@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: Hitachi Ops Center Administrator environment

The Ops Center Administrator environment must meet minimum requirements to support management of various storage systems, servers, and fabric switches.

VSP One Block terminology

In some cases, the VSP One Block storage system terminology differs from other VSP models. However, for the following terms, the Administrator UI, API, and documentation still use the existing terms. So, when you see the following terms for VSP One Block, note the correct term as follows:

Term for VSP storage systems	Term for VSP One Block storage systems
External Parity Groups	External Volume Groups
Storage Advisor Embedded	VSP One Block Administrator
Gateway for Unified Management (GUM)	Embedded Storage Manager (ESM) or Storage Management Controller (SMC)

Note: The design of certain screens and components has been partially updated. As a result, some screenshots might differ from the current appearance of the screens.

System requirements based on system scale

Based on the sizing and scalability recommendations, you can identify the system requirements and scale your Ops Center Administrator environment to meet workload demands.

The following table provides guidelines for determining the size of your environment based on the number of management targets.

Note: The number shows the total number of resources in all the storage systems onboarded in Ops Center Administrator.

System Scale	Maximum number of resources				
	Storage				
	Volume	Storage	Volume Pair	LUN	Host Group
Small scale	5000	3	300	20,000	500
Medium scale	20,000	19	600	80,000	2,500
Large scale	50,000	30	1,200	200,000	5,000

Minimum system requirements

Verify that the Ops Center Administrator server meets or exceeds the minimum requirements to take advantage of all the Ops Center Administrator features.

Minimum system requirements (Podman)

Server	Minimum requirements
Hypervisor operating system	VMware® ESXi 7.0 or higher, Microsoft Hyper-V, Linux KVM **Note:** ▪ Use the product installers when running Hyper-V or KVM. ▪ Only VMware supports OVA installations.
Container runtime version for installation from tar file	Podman version 3.3.*x*, 3.4.*x*, 4.0.*x*, 4.1.*x*, 4.2.*x*, 4.4.*x*, 4.6.*x*, and 4.9.*x*.
Operating system for installation from tar file Linux	Podman Red Hat Enterprise Linux 8.8, 8.10, 9.2, and 9.4 Oracle Linux 8.8, 8.10, 9.2, and 9.4 For details on specific supported versions of Linux, see the Compatibility matrix.

Server	Minimum requirements

	The supported versions of Podman-dependent libraries are as follows:
	▪ containers-common
	  • For Podman 3.3.*x*, 3.4.*x*, 4.0.*x*, and 4.1.*x*: 1-3 to 1-39
	  • For Podman 4.2.x, 4.4.x, 4.6.x, and 4.9.x: 1-27 to 1-81 (RHEL/OL 8.x), 1-27 to 1-91 (RHEL/OL 9.x)
	▪ conmon
	  • 2.0.29 or later
	▪ runc (only required for RHEL/OL 8.x)
	  • 1.0.0-74 or later

Access for installation from tar file	Root user
Recommended drive type	SSD or a higher performance drive type
Available disk space	80 GiB under the Podman root directory (default directory: `/var/lib/containers`) In addition, a total of 10 GiB temporary, available space is required for installation using the application installer. This consists of 10 GiB under `/var/tmp`.
Memory	The required RAM and swap memories are determined according to the system requirements based on system scale. ▪ Small scale: 8 GiB (RAM) and 3 GiB (Swap) ▪ Medium scale: 10 GiB (RAM) and 3 GiB (Swap) ▪ Large scale: 10 GiB (RAM) and 3 GiB (Swap)

Server	Minimum requirements
	Because more swap memory is used instead of physical memory compared to earlier versions, the response of some APIs and graphical user interfaces can be slower immediately after installation or when you perform an operation that you have not used for a long time. To improve performance, we recommend applying the following memory settings: ▪ Small scale: 11 GiB (RAM) ▪ Medium scale: 12 GiB (RAM) ▪ Large scale: 13 GiB (RAM) **Note:** Ops Center Administrator v10.9.1 and later can manage a large number of resources, such as storage systems or volumes, with a fixed memory size. If you upgrade from a previous version to v10.9.1 or later, any changes that you made to the memory settings are automatically updated so there is no need to change the memory settings again.
CPU	4 vCPUs
A client computer that can run a supported browser	One of the following: ▪ Google Chrome (latest version of the stable channel) ▪ Firefox ESR 128.0 or later ▪ Microsoft Edge (latest version of the stable channel). Internet Explorer mode and Microsoft Edge for Linux are not supported. **Note:** These browsers are supported by Ops Center Administrator. If you want to launch another management tool from Ops Center Administrator, verify that the browsers are supported by the other management tool.

Requirements for using program products

To use Dynamic Tiering for pools and Thin Image for snapshots, make sure that the licenses are available and shared memory is installed.

Port requirements

The following lists the port requirements for Ops Center Administrator.

Ops Center Administrator ports and firewall settings

Ensure that the port numbers specified for use by the Ops Center Administrator server are different from the port numbers used by other programs installed on the same computer.

Table 1 Ports used by the Ops Center Administrator server

Port number	Description
443/tcp	Used for accessing the Ops Center Administrator UI from Ops Center Administrator clients. **Note:** If you are using Ops Center Administrator with Ops Center Common Services or Ops Center Protector, you must use a port other than the default (443), which causes a conflict. We suggest 20961/tcp.
161/tcp	Reserved.
161/udp	Reserved.
162/tcp	Reserved.
162/udp	Used for receiving SNMP traps from supported storage systems. You cannot change the settings by using Ops Center Administrator. If products using these ports are installed on the same computer, change the settings of those products.
21611/tcp[1]	Used to manage internal services included in the container runtime.
21601-21610/tcp[1], 21612-21619/tcp[1]	Used to manage internal services included in the container runtime. Required only when Ops Center Administrator is working in host mode[2].
21609/udp[1]	
21700-21799/tcp[1]	
31000-31999/udp[1]	Used to manage storage systems. Required only when Ops Center Administrator is working in host mode[2].

Port number	Description
33000-33999/udp[1]	

1. When Ops Center Administrator is working in host mode, you can change the port used for internal services by editing the port configuration file. For details on how to change the port numbers, see Modifying the internal port allocated by Ops Center Administrator for host mode (on page 90).

   The port number can only be changed after installation. If you select host mode during the initial installation or change the host mode during the upgrade installation, ensure that the Ops Center Administrator default port numbers are not in use. If other programs need to use these ports, stop them when the installation is in progress or the installation will fail.

   Changes to the internal service port numbers used in host mode are retained after an upgrade installation. However, they are not retained when performing an upgrade using backup and restore, as the internal port information is not migrated. In this case, ensure that the Ops Center Administrator default port numbers are not in use, and change the port number manually again after the installation. For more information, see Upgrading Ops Center Administrator by using backup and restore (on page 72).

2. For details about host mode, see Installing Ops Center Administrator with the application installer (on page 28).

In an environment with firewalls set up in the network that connects the Ops Center Administrator server, Ops Center Administrator clients, and storage systems, you must register ports used by Ops Center products as firewall exceptions.

Table 2 Port numbers to register as firewall exceptions between the Ops Center Administrator server and the Ops Center Administrator client

Originator		Destination	
Port number	**Machine**	**Port number**	**Machine**
any/tcp	Ops Center Administrator client	443/tcp or 20961/tcp (If using Ops Center Administrator with Ops Center Common Services or Ops Center Protector, you must use a port other than the default (443) and 20961 is recommended.)	Ops Center Administrator server

Table 3 Port numbers to register as firewall exceptions between the Ops Center Administrator server and storage systems

Originator		Destination		Remarks
Port number	**Machine**	**Port number**	**Machine**	
any/udp	▪ VSP One Block 20 ▪ VSP 5000 series ▪ VSP E series ▪ VSP G1x00, VSP F1500 ▪ VSP G200, G/F400, G/F600, G/F800 (controller) ▪ VSP G/F350, G/F370, G/F700, G/F900 (controller) ▪ VSP N series (controller)	162/udp	Ops Center Administrator server	-
any/tcp	Ops Center Administrator server	443/tcp	▪ VSP One Block 20 ▪ VSP 5000 series ▪ VSP E series (SVP/controller) ▪ VSP G1x00, VSP F1500 ▪ VSP G200, G/F400, G/F600, G/F800 (SVP/controller)	You can change the port number for the following models: ▪ VSP E series ▪ VSP G200, G/F400, G/F600, G/F800 (SVP) ▪ VSP G/F350, G/F370, G/F700, G/F900 (SVP) ▪ VSP N series (SVP)

Originator		Destination		Remarks
Port number	**Machine**	**Port number**	**Machine**	
			▪ VSP G/F350, G/F370, G/F700, G/F900 (SVP/ controller) ▪ VSP N series (SVP/ controller) ▪ VSP One SDS Block	
any/tcp	Ops Center Administrator server	1099/tcp	▪ VSP E series (SVP) ▪ VSP G1x00, VSP F1500 ▪ VSP G200, G/F400, G/F600, G/F800 (SVP) ▪ VSP G/F350, G/F370, G/F700, G/F900 (SVP) ▪ VSP N series (SVP)	-
any/tcp	Ops Center Administrator server	11099/tcp	VSP 5000 series	-
any/tcp	Ops Center Administrator server	51099/tcp	▪ VSP 5000 series ▪ VSP E series (SVP) ▪ VSP G1x00, VSP F1500 ▪ VSP G200, G/F400, G/F600, G/F800 (SVP)	-

Originator		Destination		Remarks
Port number	**Machine**	**Port number**	**Machine**	
			▪ VSP G/F350, G/F370, G/F700, G/F900 (SVP) ▪ VSP N series (SVP)	
any/tcp	Ops Center Administrator server	51100/tcp	▪ VSP 5000 series ▪ VSP G1x00, VSP F1500	Unused port numbers are allocated automatically from the described range during storage system registration and a firewall is also set. The allocated port numbers are used when starting the storage system. For details on how to confirm the port numbers that the SVP uses, see the storage system documentation.
any/tcp	Ops Center Administrator server	51100-51355/tcp	▪ VSP E series (SVP) ▪ VSP G200, G/F400, G/F600, G/F800 (SVP) ▪ VSP G/F350, G/F370, G/F700, G/F900 (SVP) ▪ VSP N series (SVP)	Unused port numbers are allocated automatically from the described range during storage system registration and a firewall is also set. The allocated port numbers are used when starting the storage system.

Originator		Destination		Remarks
Port number	**Machine**	**Port number**	**Machine**	
				For details on how to confirm the port numbers that the SVP uses, see the storage system documentation.
any/udp	Ops Center Administrator server	31001/udp	▪ VSP 5000 series ▪ VSP G1x00, VSP F1500	The allocated port numbers are used when selecting bridge mode during installation.
33000-33999/udp	Ops Center Administrator server	31001/udp	▪ VSP 5000 series ▪ VSP G1x00, VSP F1500	The allocated port numbers are used when selecting host mode during installation. You can change the port numbers after installing. For details, see Modifying the internal port allocated by Ops Center Administrator for host mode (on page 90).
any/udp	Ops Center Administrator server	31001-31002/udp	▪ VSP One Block 20 ▪ VSP E series (controller) ▪ VSP G200, G/F400, G/F600, G/F800 (controller) ▪ VSP G/F350, G/F370, G/F700, G/F900 (controller) ▪ VSP N series (controller)	The allocated port numbers are used when selecting bridge mode during installation.

Originator		Destination		Remarks
Port number	**Machine**	**Port number**	**Machine**	
33000-33999/udp	Ops Center Administrator server	31001-31002/udp	▪ VSP One Block 20 ▪ VSP E series (controller) ▪ VSP G200, G/F400, G/F600, G/F800 (controller) ▪ VSP G/F350, G/F370, G/F700, G/F900 (controller) ▪ VSP N series (controller)	The allocated port numbers are used when selecting host mode during installation. You can change the port numbers after installing. For details, see Modifying the internal port allocated by Ops Center Administrator for host mode (on page 90).
31001/udp	▪ VSP 5000 series ▪ VSP G1x00, VSP F1500	any/udp	Ops Center Administrator server	The allocated port numbers are used when selecting bridge mode during installation.
31001/udp	▪ VSP 5000 series ▪ VSP G1x00, VSP F1500	33000-33999/udp	Ops Center Administrator server	The allocated port numbers are used when selecting host mode during installation. You can change the port numbers after installing. For details, see Modifying the internal port allocated by Ops Center Administrator for host mode (on page 90).
31001-31002/udp	▪ VSP One Block 20 ▪ VSP E series (controller)	any/udp	Ops Center Administrator server	The allocated port numbers are used when selecting bridge mode during installation.

Originator		Destination		Remarks
Port number	**Machine**	**Port number**	**Machine**	
	▪ VSP G200, G/F400, G/F600, G/F800 (controller) ▪ VSP G/F350, G/F370, G/F700, G/F900 (controller) ▪ VSP N series (controller)			
31001-31002/udp	▪ VSP One Block 20 ▪ VSP E series (controller) ▪ VSP G200, G/F400, G/F600, G/F800 (controller) ▪ VSP G/F350, G/F370, G/F700, G/F900 (controller) ▪ VSP N series (controller)	33000-33999/udp	Ops Center Administrator server	The allocated port numbers are used when selecting host mode during installation. You can change the port numbers after installing. For details, see Modifying the internal port allocated by Ops Center Administrator for host mode (on page 90).

Table 4 Port numbers to register as firewall exceptions between the Ops Center Administrator client and storage systems

Originator		Destination		Remarks
Port number	**Machine**	**Port number**	**Machine**	
any/tcp	Ops Center Administrator client	443/tcp	▪ VSP One Block 20 ▪ VSP 5000 series ▪ VSP E series ▪ VSP G1x00, F1500 ▪ VSP G200, G/F400, G/F600, G/F800 (SVP) ▪ VSP G/F350, G/F370, G/F700, G/F900 (SVP) ▪ VSP N series models (SVP) ▪ VSP One SDS Block	This setting is required when using SSL for Storage Navigator. For ▪ VSP E series (SVP) ▪ VSP G200, G/F400, G/F600, G/F800 (SVP) ▪ VSP G/F350, G/F370, G/F700, G/F900 (SVP) ▪ VSP N series models (SVP). You can also change the port number.
any/tcp	Ops Center Administrator client	1099/tcp	▪ VSP E series (SVP) ▪ VSP G1x00, F1500 ▪ VSP G200, G/F400, G/F600, G/F800 (SVP) ▪ VSP G/F350, G/F370, G/F700, G/F900 (SVP) ▪ VSP N series models (SVP)	-
any/tcp	Ops Center Administrator client	11099/tcp	VSP 5000 series	-
any/tcp	Ops Center Administrator client	51099/tcp	▪ VSP 5000 series ▪ VSP E series (SVP)	-

Originator		Destination		Remarks
Port number	**Machine**	**Port number**	**Machine**	
			▪ VSP G1x00, F1500 ▪ VSP G200, G/F400, G/F600, G/F800 (SVP) ▪ VSP G/F350, G/F370, G/F700, G/F900 (SVP) ▪ VSP N series models (SVP)	
any/tcp	Ops Center Administrator client	51100/tcp	▪ VSP 5000 series ▪ VSP G1x00, F1500	Unused port numbers are allocated automatically from the described range during storage system registration and a firewall is also set. The allocated port numbers are used when starting the storage system. For details on how to confirm the port numbers used, see the storage system documentation.
any/tcp	Ops Center Administrator client	51100-51355/tcp	▪ VSP E series (SVP) ▪ VSP G200, G/F400, G/F600, G/F800 (SVP) ▪ VSP G/F350, G/F370, G/F700, G/F900 (SVP) ▪ VSP N series (SVP)	Unused port numbers are allocated automatically from the described range during storage system registration and a firewall is also set. The allocated port numbers are used when starting the storage system. For details on how to confirm the port numbers used, see the storage system documentation.

Originator		Destination		Remarks
Port number	**Machine**	**Port number**	**Machine**	
any/tcp	Ops Center Administrator client	any/tcp	▪ VSP 5000 series ▪ VSP E series (SVP) ▪ VSP G200, G/F400, G/F600, G/F800 (SVP) ▪ VSP G/F350, G/F370, G/F700, G/F900 (SVP) ▪ VSP N series (SVP)	This setting is required for secure communication between the storage system and Ops Center Administrator when launching Storage Navigator.

Table 5 Port numbers to register as firewall exceptions between the Ops Center Administrator server and the Ops Center Protector server

Originator		Destination		Remarks
Port number	**Machine**	**Port number**	**Machine**	
any/tcp	Ops Center Administrator server	443/tcp	Ops Center Protector server	This setting is required when adding or deleting High Availability or Asynchronous Remote Clone pairs.

Table 6 Port numbers to register as firewall exceptions between the Ops Center Administrator server and AD authentication servers

Originator		Destination		Remarks
Port number	**Machine**	**Port number**	**Machine**	
any/tcp	Ops Center Administrator server	389/tcp	AD server	Currently, only Microsoft Active Directory is supported for LDAP authentication. This port number is generally used. However, a different port number might be used for an authentication server.
any/tcp	Ops Center Administrator server	53/tcp	DNS server	The DNS server is required when using AD authentication.
any/udp	Ops Center Administrator server	53/udp	DNS server	The DNS server is required when using AD authentication.

Table 7 Port numbers to register as firewall exceptions between the Ops Center Administrator server and fabric switches

Originator		Destination		Remarks
Port number	**Machine**	**Port number**	**Machine**	
any/tcp	Ops Center Administrator server	22/tcp	▪ Cisco Switch ▪ Brocade Switch with Fabric OS 8.2.2a	This setting is required when changing zone settings according to attaching or detaching volumes. This port number is generally used. However, a different port number might be used for fabric switches.
any/tcp	Ops Center Administrator server	443/tcp	Brocade Switch with Fabric OS 9.x	This setting is required when changing zone settings according to attaching or detaching volumes.

Table 8 Port numbers to register as firewall exceptions between the Ops Center Administrator server and SNMP managers

Originator		Destination		Remarks
Port number	**Machine**	**Port number**	**Machine**	
any/udp	Ops Center Administrator server	162/udp	SNMP manager	This setting is required when an SNMP manager receives SNMP traps from Ops Center Administrator.

Supported storage systems

Hitachi Ops Center Administrator supports the Virtual Storage Platform (VSP) family storage systems.

Initial startup and initial setup of any supported storage system must be completed by a Hitachi Vantara representative or an authorized service provider.

Hitachi Ops Center Administrator supports the following storage systems:

- Block storage
  - VSP One Block 20
  - VSP 5000 series
  - VSP E series
  - VSP G1x00, F1500
  - VSP G/F350, G/F370, G/F700, G/F900
  - VSP G200, G/F400, G/F600, G/F800
  - VSP G400, G600, G800 with optional NAS modules
  - VSP N series
- Software-defined storage
  - VSP One SDS Block

TLS

The supported version of TLS are 1.2 and 1.3.

Supported microcode/firmware

Ops Center Administrator supports the following:

- VSP One Block 20 with microcode version A3-02-21 or later.
- VSP 5200, 5600, 5200H, 5600H with microcode version 90-08-0x or later.
- VSP 5100, 5500, 5100H, 5500H with microcode version 90-01-4x or later.
- VSP E1090, VSP E1090H with microcode version 93-06-01 or later.
- VSP E990 with microcode version 93-01-0x or later.
- VSP E590, E790, E590H, E790H with microcode version 93-03-21 or later.
- VSP G/F350, G/F370, G/F700, G/F900 with firmware version 88-01-0x or later.
- VSP G200, G/F400, G/F600, G/F800 with microcode version 83-06-01 or later.
- VSP G1x00, F1500 with microcode version 80-06-62 or later.
- VSP N series with microcode version 83-06-01 or later.
- VSP One SDS Block virtual machine models or bare metal models with software version 1.13 or later.

Note: After a storage system firmware/microcode upgrade, new features are not supported until you upgrade Ops Center Administrator.

Supported fabric switches

Ops Center Administrator supports the following Brocade® and Cisco® fabric switches.

- Brocade: Fabric OS 8.2.2a, 9.0.x, 9.1.x
- Cisco: MDS NX-OS Release 8.1(1) or later

Note: Before upgrading the Fabric OS of a Brocade switch from 8.x to 9.0.x or 9.1.x, you must remove the fabric switch from Ops Center Administrator. After the upgrade, onboard the fabric switch again. You cannot use the Update Fabric Switch option in Ops Center Administrator to upgrade the Fabric OS.

Supported servers

You can use Hitachi Ops Center Administrator to provision storage to servers running the following operating systems:

- VMware®
- Windows®
- HP-UX™
- Oracle Solaris™
- NetBSD®
- TRU64 UNIX®
- Novell NetWare®
- IBM® AIX®
- Linux®
- IRIX®

Note: Refer to the storage system documentation for the OS Type and Host Mode of the host groups associated with the storage system.

Supported scalability limits

The following table lists the maximum number of resources supported in Ops Center Administrator.

Resource	Scale
Storage systems	50
Servers	10,000
Volumes	1,500,000 over 50 storage systems

Chapter 2: Installing Ops Center Administrator

Ops Center Administrator is deployed on a virtual machine and accessed by a client computer. Review the minimum requirements before installing. You can also deploy the Ops Center Administrator OVA file as a VMware vSphere High Availability cluster or configure vSphere Fault Tolerance.

You install Ops Center Administrator by using one of the following options:

- Installing Ops Center Administrator with the consolidated Ops Center preconfigured media (on page 27)
- Installing Ops Center Administrator with the application installer (on page 28)

To install more than one Ops Center product at the same time, use the Express installers. For more information, see the *Hitachi Ops Center Installation and Configuration Guide*.

Note: If you change SELinux mode after installing Ops Center Administrator when using Podman, the Ops Center Administrator-related service may not work correctly. To prevent this, set up SELinux mode before installing.

Installing Ops Center Administrator with the consolidated Ops Center preconfigured media

If you are installing Ops Center Administrator as part of the Ops Center consolidated OVA, see the *Hitachi Ops Center Installation and Configuration Guide* for detailed information on installation and configuration. When you use the Ops Center consolidated OVA, Ops Center Administrator is automatically registered in Common Services on the same host. This means that Single Sign-On (SSO) is also automatically enabled. After you finish installing and configuring the consolidated OVA, return to this document and complete the Ops Center Administrator-specific configuration as described in Initial setup after installation (on page 38).

Note: The preconfigured media is for initial installation only or backup and restore upgrades. For in-place upgrades, you must use the application installer as described in Upgrading Ops Center Administrator by using the application installer (on page 64) or the Server Express installer as described in the *Hitachi Ops Center Installation and Configuration Guide*.

Installing Ops Center Administrator with the application installer

You can install Ops Center Administrator in a Linux environment that is running a supported version of a container runtime.

To enable maximum control of the environment, the application installer does not include a container runtime, an operating system, or a VM.

Before you begin

- Do not install container runtimes except Podman on the host OS.
- If you want to register Ops Center Administrator with Ops Center Common Services, do the following:
  - Install Python3 before running the installer.
  - Make sure that the host name of Ops Center Common Services is resolvable from the Ops Center Administrator server. If you want to use a host name that is not an FQDN, set the IP address and the host name in the `/etc/hosts` file for name resolution.
  - After modifying the `/etc/hosts` file, run the following command to restart the Ops Center Administrator-related service.

    ```
    # systemctl restart rainier
    ```

  - Make sure that you have a user account with Ops Center Common Services that has the "Application Administrator" role to run the script.
- During installation, you must select one of the following network modes for containers created by Ops Center Administrator:
  - Bridge mode (Recommended):

    This is the default network mode for the container runtime.

    In this mode, a dedicated network for the container is created on the host network. When selecting this mode, ensure that the kernel parameter `net.ipv4.ip_forward` is set to enabled in order to allow traffic forwarding from the host network to the container network.
  - Host mode:

    In this mode, the containers share the host network, and each container is allocated a host port number for internal services. This requires more port numbers than bridge mode. Select this mode only if you want to disable traffic forwarding from the host network to the container network. For details, see Port requirements (on page 12).

    Note: Before Ops Center Administrator v11.0.4, bridge mode was implicitly selected during installation. If you choose host mode during installation, the allocated port numbers for each container might conflict with those of other programs installed on the same computer, potentially causing installation failures. Additionally, each port used by the container to communicate with the external network must be explicitly registered as a firewall exception. This process is simplified in bridge mode because the virtual bridge used for communication is automatically added to the `firewalld` trusted zone by default. Therefore, we strongly recommend selecting bridge mode.

Verify the following:

- You have root access or normal access to the OS where you plan to install Ops Center Administrator. If you log in as a normal user, use the **`sudo`** command to complete the procedure as the root user.
- The available space on the server is 100 GiB including temporary space. For details, see Minimum system requirements (on page 9).

- The server has 8 to 10 GiB of available RAM. For details, see Minimum system requirements (on page 9).

  Note: Before starting the installation, as a best practice, do not install Ops Center Administrator in a location running other applications.

- If you select bridge mode during installation, IP forwarding and `br_netfilter` for the IP V4 network is installed on the operating system.

  Verify by using the **`sysctl`** command (1 means enabled):

```
# sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 1
# sysctl net.bridge.bridge-nf-call-iptables
net.bridge.bridge-nf-call-iptables = 1
```

- If you select bridge mode during installation, the OS running `firewalld` (for example, RHEL 8 or later) is configured to allow communication between containers as follows:
  - Enable communication by adding the container runtime network interface (for example, `cni-podman0`) to the trusted zone:

    ```
    # firewall-cmd --zone=trusted --change-interface=cni-podman0 --permanent
    ```

    ```
    # firewall-cmd --reload
    ```

  - Enable IP masquerading for the default zone:

    ```
    # firewall-cmd --add-masquerade --permanent
    ```

    ```
    # firewall-cmd --reload
    ```

- A supported version of container runtime is installed in a Linux environment.
  - If the supported version of Podman is not installed in the environment, you must configure Yellowdog Updater, Modified (YUM) settings to install packages over a network. The application installer connects to the configured YUM repository and installs the required version of Podman. The packages related to Podman are located in the latest BaseOS and AppStream repositories.
  - If you want to install or upgrade Podman yourself, you can run the following command:

    ```
    yum install podman required-version
    ```

    For example, to install Podman v3.3.x:

    ```
    yum install podman-3.3.*
    ```

    The asterisk indicates to obtain and install the latest patch version available in the repository.

    Note: Downgrading the Podman version is not supported.
  - If you install or upgrade Ops Center Administrator while suppressing the upgrade of Podman, the installation fails with the error - `[Error] Failed to install Podman x.x.x from package repository. Confirm the network or repository server setting, and retry.` Unlock the suppression and install or upgrade Ops Center Administrator again. After completing the installation, suppress the upgrade of Podman again.

    Note: You can upgrade Podman (major or minor version) during the installation or upgrade process, or after installing Ops Center Administrator. However, if you are upgrading Podman from version 3.x to 4.x, we recommend that you do so during the Ops Center Administrator installation. This is because upgrading Podman from version 3.x to 4.x after installation requires creating a backup of the existing Ops Center Administrator instance, removing it along with the Podman upgrade, reinstalling Ops Center Administrator, and then restoring the backup.
  - If you install Podman 3.3.x, or upgrade Podman from 3.3.x to any version, or run any Podman command on the server using Podman 3.3.x, a warning message `Failed to decode the keys [<key1>, <key2>, ..., <keyN>] from "/usr/share/containers/containers.conf"` may appear. Ignore this message because it does not affect Ops Center Administrator.
  - If you cannot use YUM to install Podman because your management server is not connected to the network, you must get the Podman software from the OS media (ISO image or CD-ROM).

    For example, the minimum supported version of Podman 3.3.x is available with Red Hat Enterprise Linux and Oracle Linux version 8.5, and Podman 4.2.x is available with version 9.1. Therefore, regardless of the OS version that you are using, you must download the OS that includes the Podman version you want to use.

    1. Download the Linux ISO image (for example, redhat 8.5 iso).

2. Mount the ISO image using the following command:

   `mount /dev/cdrom /media`

   For example: **`mount -o loop rhel-8.5-x86_64-dvd.iso /media`**

3. If the `/etc/yum.repos.d` directory contains an existing repo file, rename the file extension or delete it.
4. Create the yum repository file by running the following command:

   `vim /etc/yum.repos.d/local.repo`

5. Add the required definition lines as shown in the following examples, and then save and close the file:

   For Oracle Linux

```
[LocalRepo_BaseOS]name= LocalRepo_BaseOS
gpgcheck=0
enabled=1
baseurl=file:///media/BaseOS/
LocalRepo_AppStream]
name=LocalRepo_AppStream
gpgcheck=0
enabled=1
baseurl=file:///media/AppStream/
```

   For Red Hat Enterprise Linux

```
[LocalRepo_BaseOS]
name=LocalRepo_BaseOS
metadata_expire=-1
enabled=1
gpgcheck=0
baseurl=file:///media/BaseOS/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release

[LocalRepo_AppStream]
name=LocalRepo_AppStream
metadata_expire=-1
enabled=1
gpgcheck=0
baseurl=file:///media/AppStream/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
```

6. Verify the required library by running the following command:

```
yum repolist
```

7. Install podman by using the following command :

```
yum install podman-required-version
```

For example, to install Podman v3.3.x:

```
yum install podman-3.3.*
```

Procedure

1. In the Linux environment, configure the network interface that will access Ops Center Administrator.

   Ops Center Administrator supports user interface and API access by using an IPv4 address.
2. Copy the tar file `ops-center-administrator-xx.tar.gz` from the installation media to any folder in the Linux environment and unzip it.
3. Navigate to the unzipped folder and run `install.sh`.

   At the prompts, enter the following:

   a. `Enter the username for the installer:`

      Enter sysadmin

   b. `Enter the user password:`

      Enter sysadmin

   c. Enter the number corresponding to the network mode you want to select:

```
Select the network mode for containers.

1. bridge : (Recommended) Containers are isolated from the host's
            network namespace and communicate through the host's virtual
            bridge. This mode is suitable for most cases.

2. host   : Containers share the host's network namespace.
            Therefore, no IP forwarding is required. This mode is used when
            it is absolutely necessary to disable IP forwarding
            (net.ipv4.ip_forward=0).
Enter the number [default=1]:
```

   d. `Enter host's IP:`

      Enter the IP address for Ops Center Administrator. This IP address is also used for SNMP communications with the storage system.

   e. `Enter the Service port number (HTTPS, default 443):`

      Enter the service port for accessing Ops Center Administrator. The default service port is HTTPS, 443. You can proceed with the default service port or enter your own.

      Note: If you are using Ops Center Administrator with Ops Center Common Services or Ops Center Protector, you must enter a port other than the default (443), which causes a conflict. We suggest 20961.

f. If you want to register Ops Center Administrator with Ops Center Common Services during installation, enter `y` at the prompt:

```
Do you wish to configure Ops Center [y/n]
```

You are then prompted to enter a user name and password for Ops Center Common Services and the name and description of the Ops Center Administrator instance to register.

Note:

- If both Ops Center Administrator and Ops Center Common Services are v10.9.0 or later, then the token authentication time-out configured in Ops Center Common Services is reflected in Ops Center Administrator automatically. This time-out configuration applies not only to users managed in Ops Center Common Services, but also to local users in Ops Center Administrator.

  For details, see the Ops Center Portal Help.
- In Ops Center Administrator, the Auto-refresh setting configured in the Ops Center Portal is ignored.

Note: During installation, `vm.max_map_count` is set to 262144 in `/etc/sysctl.conf`.

The installation may take a few minutes. At completion, messages indicate the following:

- The application was successfully added.
- The API is ready.
- Any pre-existing app manager containers have been removed.

4. Set the SNMP IP address in the virtual appliance manager tool:

a. Open a browser and enter the following URL in the address bar:

```
https://ip-address:port/vam
```

where:

- *ip-address* is the IP address of the Ops Center Administrator server.
- *port* is the port number of the Ops Center Administrator. The default port number is `443` or `20961`.

The default login credentials are *`sysadmin/sysadmin`*

b. Click **Network Settings**, then enter the SNMP IP address for the storage system.

5. Suppress the upgrade of Podman to avoid unintentionally upgrading to the unsupported version.

For example, you can use `yum-plugin-versionlock` or you can add the `exclude` parameter to the `yum.conf` file.

Troubleshooting the installation

If the installation fails, try the following:

- If the installation fails with the (401) error code, the user name and password specified by the installer was incorrect. Retry the installation and ensure that you use the credentials sysadmin/sysadmin.
- Make sure your container runtime is working properly. If not, check the following network configuration:
  - If you select bridge mode during installation, confirm that the network interface (for example, `cni-podman0`) of the container runtime is in a trusted zone in your operating system.
  - If you select host mode during installation, confirm than the port numbers used by the container runtime are not allocated to other programs installed on the same computer. For details about port numbers used by the container runtime, see Port requirements (on page 12).

    If the required port numbers are allocated to other programs installed on the same computer, stop them and install Ops Center Administrator again.
- Check your YUM settings and the host network to make sure that your system can connect to the YUM repository.
- If you use a local YUM mirror repository server, confirm the HTTP server setting and whether the repository data that is gathered by the **`reposync`** command exists correctly.
- Delete all Ops Center Administrator containers, images, and files and then start the installation again.
- Check the Podman logs.

  Consult the container runtime documentation for more information on how to check logs.
- Journal entries may have additional information about the error. To view the journal log, connect to the host with the root user or a normal user account and run the following commands:

  Note: If you log in as a normal user, use the **`sudo`** command to complete the following procedure as the root user.

  ```
  journalctl --no-pager -u rainier
  ```

  If the issue persists, collect the installation log that was created under `/var/logs/rainier-install` and contact customer support.
- If the installation produces any warnings, they may point to the cause of the problem. Correct any issues the installer identifies, delete any Ops Center Administrator containers and images, and start the installation again. You can log in as the root user or a normal user. If you log in as a normal user, use the **`sudo`** command to complete the following procedure as the root user.

  To remove files, run the following commands:

  ```
  rm -f /opt/rainier/bin/rainier-getlogs
  ```

```
rm -f /opt/rainier/bin/rainier-replace-jdk
```

To remove container images and containers that you do not manage, run these commands with the root account:

1. `podman stop $(podman ps --format "{{.ID}} {{.Image}}" -a | grep "rdocker:6000/" | awk '{ print $1 }')`
2. `podman rm -fv $(podman ps --format "{{.ID}} {{.Image}}" -a | grep "rdocker:6000/" | awk '{ print $1 }')`
3. `podman rmi $(podman images --format "{{.ID}} {{.Repository}}" | grep "rdocker:6000/" | awk '{ print $1 }')`
4. `podman volume rm nginx-certificates`
5. `podman volume rm nginx-certificates-override`
6. `podman volume rm nginx-confd`
7. `podman volume rm nginx-log`

If, after powering on or running `ip-change`, you attempt to execute to the container:

```
[root@hid ~]# podman exec -it d00be2ea7a01 /bin/bash
```

and the result is:

```
OCI runtime exec failed: exec failed: container_linux.go:296: starting container process caused "process_linux.go:78: starting setns process caused \"fork/exec /proc/self/exe: no such file or directory\"": unknown
```

Run the following to restart the service:

```
[root@hid ~]# systemctl restart rainier
```

- If the Ops Center Administrator installation succeeded, but you cannot access Ops Center Administrator, confirm that the firewall exceptions are configured properly. For details, see Port requirements (on page 12).
- If the Ops Center Administrator installation succeeded, but registering with Ops Center Common Services failed, run the **`setupcommonservice`** command after the installed Ops Center Administrator goes online.

Next steps

Required

- Log on to Ops Center Administrator to verify the installation.
- Generate and install a signed SSL certificate. By default, the Ops Center Administrator installation package comes with a self-signed certificate that you can use to initially log in to Ops Center Administrator.

Optional

For more information on changing the Ops Center Administrator port number, see Modifying the Ops Center Administrator port in virtual appliance manager (on page 38).

Modifying the Ops Center Administrator port in virtual appliance manager

You can change the port for accessing Ops Center Administrator to avoid conflicts.

Before you begin

You can change the Ops Center Administrator port for instances that were installed using the application installer.

Procedure

1. Log in to virtual appliance manager (VAM) using the IP address for your Ops Center Administrator deployment: `https://ip-address:port/vam`

   The default credentials for an application installer installation are:

   - User name: sysadmin
   - Password: sysadmin

   You must change your password after you log in.
2. Click **Network Settings**, and then enter the HTTPS port you want to use.
3. Click **Submit.**

Result

Ops Center Administrator automatically restarts. You can log in using the new URL: `https://ip-address:port/vam`.

Note: When Ops Center Administrator is working in host mode, you can also change the port used for internal services by editing the port configuration file. For details, see Modifying the internal port allocated by Ops Center Administrator for host mode (on page 90).

Initial setup after installation

After installing Ops Center Administrator, continue by setting up the following as needed:

- NTP server
- DHCP server
- SSO
- Ops Center portal connection
- SSL
- Si token authentication time-out
- Audit logging
- Virus scanning
- Users, groups, and roles

- Ops Center Protector connection
- Podman
- SELinux mode

When you finish the setup, you can log in to the Ops Center Administrator UI.

Changing the Podman network address

When Ops Center Administrator is working in bridge mode, you can change the Podman network address.

Note: The Podman version must be 4.0 or later.

Procedure

1. Stop the services using the following command:

   ```
   # systemctl stop rainier
   ```

2. If the `/etc/containers/containers.conf.d` directory does not exist, create it.
3. Create a `subnet.conf` file in the `/etc/containers/containers.conf.d` directory and include the following:

   ```
   [network]
   default_subnet = "subnet"
   ```

   For example, you can change the subnet to `10.90.0.0/15`.

   ```
   [network]
   default_subnet = "10.90.0.0/15"
   ```

4. Check the Podman network backend using the following command:

   ```
   # podman info | grep networkBackend
   ```

   If the output result of this step is `networkBackend: cni`, then delete the bridge device.

5. Delete the bridge device using the following command:

   ```
   # ip link del cni-podman0
   ```

6. Restart the OS.

Configuring the Network Time Protocol server settings

NTP servers ensure time synchronization between network resources. To configure the Network Time Protocol (NTP) server settings, see your OS manual.

If you originally installed using the stand-alone preconfigured media, configure these settings from the Virtual Appliance Manager using the following procedure:

Procedure

1. Open a browser and enter the following URL in the address bar:

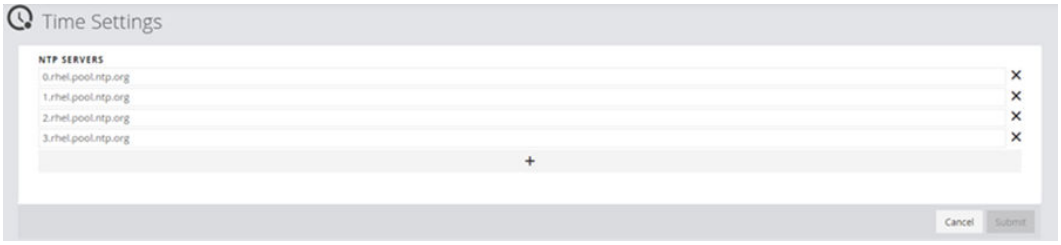
   ```
   https://ip-address:port/vam
   ```

   where:

   - *ip-address* is the IP address of the Ops Center Administrator server.
   - *port* is the port number of the Ops Center Administrator. The default port number is `443` or `20961`.

   The default login credentials are *`sysadmin/sysadmin`*

2. To add NTP servers to the virtual machine, click **Time Settings**. Adding NTP servers ensures that the Ops Center Administrator server is synchronized with the storage system environment.

3. To add an NTP server, click +.
4. Enter the NTP server host name.
5. Click **Submit**.

Configuring DHCP server settings

If your environment includes DHCP servers, you can configure the DHCP setting. For more information, see your OS manual.

If you originally installed using the stand-alone preconfigured media, configure network settings including DHCP from the virtual appliance manager using the following procedure:

Procedure

1. Open a browser and enter the following URL in the address bar:

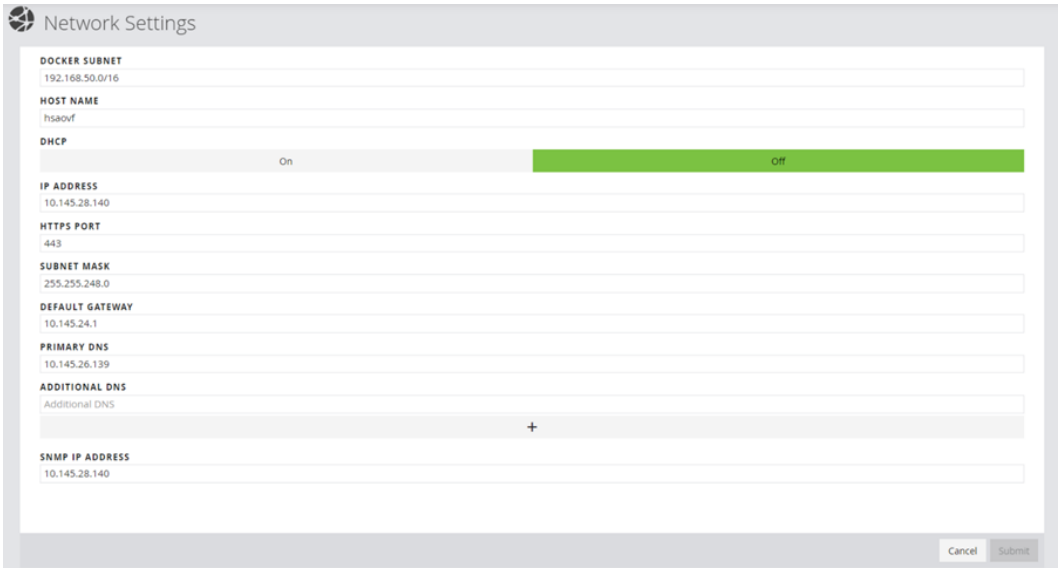
   ```
   https://ip-address:port/vam
   ```

   where:

   - *ip-address* is the IP address of the Ops Center Administrator server.
   - *port* is the port number of the Ops Center Administrator. The default port number is `443` or `20961`.

The default login credentials are `sysadmin/sysadmin`

2. Click **Network Settings**.



3. If your data center is using the IP address scheme 192.168.*.*, make sure that you provide another IP range that is not currently used in your environment. This is the specified range used by Ops Center Administrator.
4. Set the host name for the virtual machine.
5. If your environment includes DHCP servers, set **DHCP** to On. If you do not have a DHCP server, set **DHCP** to Off.
6. If you set **DHCP** to Off, enter the IP address of the Ops Center Administrator server.
7. Click **Submit**.

Configuring SSO by integrating with Ops Center Common Services

Registering Ops Center Administrator with Ops Center Common Services enables you to use Single sign-on (SSO), which controls the access of multiple related, yet independent, software systems. Using SSO, you can log in with a single ID and password to view and manage all registered Ops Center products as well as assign user access to them.

Note: If you installed using the consolidated Ops Center OVA, Ops Center Administrator is already registered with Common Services and you can skip this section.

You can either set up SSO when installing or upgrading Ops Center Administrator, or you can do it after.

- To set up SSO during installation or upgrade, enter the required information during the procedure. The installation or upgrade script prompts you to input the information, if necessary.
- To set up SSO after installation or upgrade, run the **`setupcommonservice`** command. To learn how to use this command, see Registering the Ops Center Administrator server with Ops Center (on page 42). If the host name, IP address, or port number of the server where Common Services is installed changes, you must register Ops Center Administrator again.

Registering the Ops Center Administrator server with Ops Center

You can register the Ops Center Administrator server with the Ops Center portal by running a script that comes with the software. After running this script, you can access Ops Center Administrator from the portal using the Ops Center credentials and call Ops Center Administrator APIs using the Ops Center access token.

Note:

- If you installed using the Ops Center OVA, Ops Center Administrator is already registered in Common Services.
- You cannot unregister Ops Center Administrator using the **`setupcommonservice`** command. To delete products, use the Ops Center portal.

Before you begin

- If Ops Center Administrator was installed with the application installer (not preconfigured media), install Python3 to run the script.
- Verify the following:
  - Host name of Ops Center Common Services is resolvable from the Ops Center Administrator server. If you want to use a host name that is not an FQDN, set the IP address and the host name in the `/etc/hosts` file for name resolution.

    Note: After modifying the `/etc/hosts` file, run the following command to restart the Ops Center Administrator-related service:

    ```
    # systemctl restart rainier
    ```

  - Ops Center Administrator server and the Common Services server are running.
  - Ops Center Common Services server is running v10.0.0-01 or later.
  - A user account exists with Common Services that has the "Application Administrator" role to run the script.

To register Ops Center Administrator with the Ops Center portal:

Procedure

1. Either open an SSH connection to the VM or open the VMware console and press **Alt+F2** to reach the console.
2. Log in as a root user or a normal user. If you log in as a normal user, use the **`sudo`** command to complete the following procedure as the root user.
3. Run the `/opt/rainier/bin/setupcommonservice` script with the following parameters:

   `csUsername`
   The Common Services username (optional). If you do not specify the `csUsername` option, you can input the Common Services username using interactive mode.

   `csUri`
   The URL of the Common Services server (required).

   `applicationHostAddress`
   The Ops Center Administrator server host name or an IP address (required).

   `applicationPort`
   The Ops Center Administrator port number (required).

   `applicationName`
   The Ops Center Administrator name to display in the Ops Center portal (required).

   `applicationDescription`
   A description of the Ops Center Administrator server to display in the Ops Center portal (optional).

   `tlsVerify`
   Indicates that Ops Center Administrator must perform SSL certificate verification when communicating with Ops Center. If set, you must select the `csUriCACert` option (optional).

   `csUriCACert`
   The CA certificate file to use for certificate verification when communicating with Ops Center. This option is mandatory if you set the `tlsVerify` option.

4. After the command runs successfully, Ops Center Administrator is shown in the portal.

Note:

- If both Ops Center Administrator and Ops Center Common Services are v10.9.0 or later, the token authentication time-out configured in Ops Center Common Services is reflected in Ops Center Administrator automatically. This time-out configuration applies not only to users managed in Ops Center Common Services, but also to local users in Ops Center Administrator. For details, see the Ops Center portal Help.
- In Ops Center Administrator, the Auto-refresh setting configured in the Ops Center Portal is ignored.

Example

The following is an example of running the command:

```
# /opt/rainier/bin/setupcommonservice --csUsername sysadmin --applicationPort 443 --
csUri https://common-services.example.com/portal --applicationHostAddress
administrator1.example.com --applicationName MyAdministrator1 --
applicationDescription foobar
Registering with following values:
Hostname: administrator1.example.com
Application Port: 443
Display Name: MyAdministrator1
Application Description: foobar
Registration Successful
```

Next steps

You can change the registered Ops Center Administrator server name and description in the portal. If you want to change other properties such as host name, port number, and so on, first remove Ops Center Administrator from the portal, and then run the script again with the required parameters.

Note: You must synchronize the time between the Ops Center Administrator server and the Ops Center Common Services server. Use NTP to synchronize the time between the servers.

Enabling SSO with the Ops Center portal

To enable SSO between Ops Center Administrator and the Ops Center portal, the portal host name must be resolvable by DNS or in the `/etc/hosts` file. Otherwise, SSO for Ops Center Administrator may not work correctly.

Note: After modifying the `/etc/hosts` file, run the following command to restart the Ops Center Administrator-related service:

```
# systemctl restart rainier
```

If you want to use an IP address instead of the host name of the Ops Center portal, do the following on the Ops Center portal server:

Procedure

1. Log in to the server running the Ops Center portal.
2. Run the **`cschgconnect.sh`** command on the server.

   For details on the **`cschgconnect.sh`** command, see the *Hitachi Ops Center Installation and Configuration Guide*.

Result

You can now sign on to Ops Center Administrator from the Ops Center portal.

Updating the Ops Center connection

If you already registered Ops Center Administrator with Ops Center, but need to update the Common Services user name, password, address (FQDN or IP), SSL certificate, or other parameters, you can run the **`setupcommonservice`** command as described in Registering the Ops Center Administrator server with Ops Center (on page 42).

Setting up SSL

You can configure secure communications between each of the Ops Center servers and clients. SSL certificates verify user identity and enhance security on the server. By default, the server uses a self-signed certificate. You can get a digitally signed SSL certificate from a trusted certificate authority (CA) by sending a certificate signing request (CSR). After you obtain the signed certificate, you import it to the server.

Setting up SSL when Ops Center Administrator is running on the same server as Common Services

Ops Center Administrator and the Ops Center Common Services must communicate over an SSL connection. To use the Common Services, you must configure a secure connection in the same way you configure secure connections with other servers. However, if Common Services is on the same server as Ops Center Administrator, you can simplify the SSL configuration by using the **`cssslsetup`** command. By using the **`cssslsetup`** command, you can configure SSL communication for all Hitachi Ops Center products installed on the same management server using a common secret key and server certificate.

For more information on the **`cssslsetup`** command and how to use it, see "Configuring SSL communications by using the cssslsetup command" in the *Hitachi Ops Center Installation and Configuration Guide*.

Generating and installing a signed SSL certificate

By default, the server uses a self-signed certificate. SSL certificates verify user identities and enhance security on the server. You can get a digitally signed SSL certificate from a trusted certificate authority (CA) by sending a certificate signing request (CSR). After you obtain the signed certificate, you import it to the server.

The following is a sample procedure for generating and installing a signed SSL certificate. The process of obtaining a certificate may be different within each organization.

Procedure

1. Open the virtual machine console and log in using root user or normal user credentials. If you log in as a normal user, use the **`sudo`** command to complete the following procedure as the root user.
2. Note the hostname of the VM (#hostname).

3. Run the **`openssl`** command and provide the Authentication sha256, depending upon the required security. Give the Fully Qualified Domain Name for host name.
   - The following example is for a certificate using RSA as the signature algorithm:

     ```
     # openssl req -nodes -newkey rsa:2048 -sha256 -keyout server.key -out
     server.csr
     ```

     The system returns the message: `Generating a RSA private key`
   - The following example is for a certificate using ECDSA as the signature algorithm:

     ```
     # openssl req -nodes -newkey ec:<(openssl ecparam -name secp384r1) -sha256 -
     keyout server.key -out server.csr
     ```

     The system returns the message: `Generating a EC private key`
4. Provide the information as prompted. For some fields there is a default value. Enter period ".", to leave a field blank.
   - **Country Name** (two-letter code)
   - **State or Province Name** (two-letter code)
   - **Locality name** (City)
   - **Organization Name** (Company)
   - **Organizational Unit Name** (Section or department)
   - **Common Name** (Your name or the server host name)
   - **Email Address**
5. When you receive the CSR file, send it to a certificate authority to obtain an SSL certificate.

   If you need help with this step, consult with customer support or an authorized service provider.
6. Open a browser and enter the following URL in the address bar:

   ```
   https://ip-address:port/vam
   ```

   where:
   - *ip-address* is the IP address of the Ops Center Administrator server.
   - *port* is the port number of the Ops Center Administrator. The default port number is `443` or `20961`.

   The default login credentials are *`sysadmin/sysadmin`*
7. Click **Certificate Settings**.
8. Import the certificate into the server.
   a. Open the signed certificate (received from the certificate authority) in a text editor.
   b. Open the private key file (generated in step 2) in a text editor.
   c. Copy the certificate file contents into the **CERTIFICATE** text box.

Note: Do not include the delimiters.

d. Open the private key.

```
# cat server.key
```

e. Copy the private key file contents into the **PRIVATE KEY** text box in the virtual appliance manager.

f. Click **Submit**.

Installing a custom signed SSL certificate

You can log in using SSH to the Ops Center Administrator server to install a custom signed SSL certificate.

Before you begin

Because the current installation always searches for disk space under the “root” partition, you must ensure that you have a partition with free space available. You cannot install Ops Center Administrator in a customized location.

Procedure

1. Log in using SSH to the Ops Center Administrator server.
2. Get the `server.key` file from the container:

```
podman cp $(podman ps --format "{{.ID}} {{.Image}}" -a | grep "rdocker:6000/
rainier-infra-proxy" | awk '{ print $1 }'):/etc/nginx/certificates/
server.key /tmp
```

3. Navigate to the `/tmp` folder and run the following command to create the `server.csr` file:
   - The following example is for a certificate using RSA as the signature algorithm:

```
# openssl req -new -newkey rsa:2048 -keyout server.key -out server.csr -nodes
```

   - The following example is for a certificate using ECDSA as the signature algorithm:

```
# openssl req -new -newkey ec:<(openssl ecparam -name secp384r1) -keyout
server.key -out server.csr -nodes
```

4. Send the `server.csr` file to the certification authority to get the `server.crt` file.
5. Open a browser and enter the following URL in the address bar:

```
https://ip-address:port/vam
```

where:

- *ip-address* is the IP address of the Ops Center Administrator server.
- *port* is the port number of the Ops Center Administrator. The default port number is `443` or `20961`.

The default login credentials are *`sysadmin/sysadmin`*

6. Click **Certificate Settings.**
   a. Copy the `server.crt` (from Step 4) content into the **CERTIFICATE** area.
   b. Copy the `server.key` content into the **PRIVATE KEY** area.
7. Click **Submit** and wait for five minutes.
8. Launch the Ops Center Administrator UI and verify the SSL certificate from your browser.

Changing the si token authentication time-out in Ops Center Administrator using VAM

You can change the Si token authentication time-out in Ops Center Administrator.

Procedure

1. Open a browser and enter the following URL in the address bar:

```
https://ip-address:port/vam
```

where:

- *ip-address* is the IP address of the Ops Center Administrator server.
- *port* is the port number of the Ops Center Administrator. The default port number is `443` or `20961`.

The default login credentials are *`sysadmin/sysadmin`*

2. Click **Service Settings**.
3. Change **si.token.expirationDuration** to any value suitable for your system, for example 6000. The duration setting is in seconds.
4. Click **Submit**.

Note:

- If Ops Center Administrator is registered in Ops Center Common Services and both are running v10.9.0 or later, the token expiration configured in Ops Center Common Services is reflected in **si.token.expirationDuration** automatically. In this case, you cannot change **si.token.expirationDuration** from Ops Center Administrator.
- In Ops Center Administrator, if you do not operate the UI for the time set for **si.token.expirationDuration**, you are logged out automatically. In the **Jobs** window, because it is periodically and automatically refreshed for the first 20 minutes, you are logged out after the time set for **si.token.expirationDuration** + 20 minutes.

Enabling and downloading audit logs

Log in to the Ops Center Administrator virtual appliance manager to download an audit log to the Ops Center Administrator server.

Before you begin

You must enable Audit Log Collection to collect log files. By default, the audit log is disabled. The file downloaded from Download Logs is empty if the audit log is not collected.

The actions logged are as follows:

- All Ops Center Administrator jobs
- Ops Center Administrator server starts
- Synchronous operations such as GET
- Virtual appliance manager operations
- Authentication (success / failure)
- Storage system refresh

The following information is included in the audit log:

- User
- Time/Date
- Operation Name
- Access source
- Status
- Details (if applicable)

Procedure

1. Open a browser and enter the following URL in the address bar:

```
https://ip-address:port/vam
```

where:

- *ip-address* is the IP address of the Ops Center Administrator server.
- *port* is the port number of the Ops Center Administrator. The default port number is `443` or `20961`.

The default login credentials are *`sysadmin/sysadmin`*

2. Click **Audit Log Settings**.
3. To enable audit log collection, click **Enabled**. You can change the **Retention Period**.
4. To download the log, click **Download Audit Logs** on the virtual appliance manager dashboard.

Excluding directories from virus scanning

Configure your antivirus application to exclude the following directories from scanning:

- /opt/rainier
- /var/logs
- /var/lib/containers/storage

Creating Ops Center Users, User Groups, and Roles

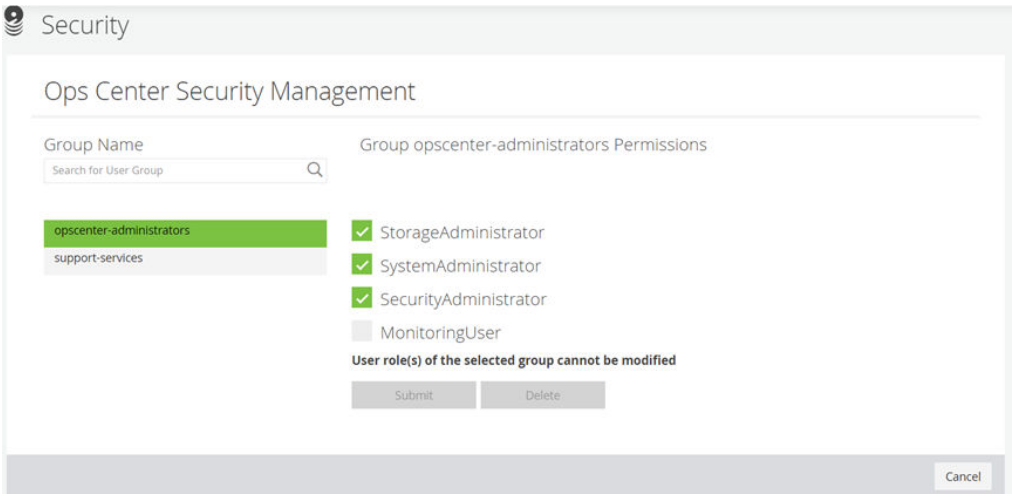
This section describes how to create a user and user group, then assign the role of Ops Center Administrator to the user group.

You can create users and user groups in Ops Center Common Services and assign roles to user groups in Ops Center Administrator. Role-Based Access Control (RBAC) either allows or denies users (and associated user groups) access to Ops Center Administrator based on the existing mapping between Common Services groups and Administrator-specific user roles.

Note: You can use users and user groups in an AD server by directly registering the AD domain with Ops Center Administrator and assigning the role of Ops Center Administrator to those user groups. For details, see “Administering security” in the *Hitachi Ops Center Administrator User Guide*. You must assign Ops Center Administrator roles to the user account even if the user account already has any Ops Center Common Services roles.

Procedure

1. Create an Ops Center user, and user group and assign the Ops Center role and user to the user group. Refer to the Ops Center Portal Help for details.
2. Launch Ops Center Administrator from the Ops Center portal or directly log in by using Ops Center SSO. Click the **Settings** tab > **Security Settings** to open the **Security** window.



Refer to “Assigning product-level roles from the Ops Center portal” in the Ops Center Portal Help for details.

3. In the **Group Name** field, enter the user group name you created.
4. Select the required Ops Center Administrator user roles for the user group and click **Update**.

Register Ops Center Protector in Ops Center Administrator

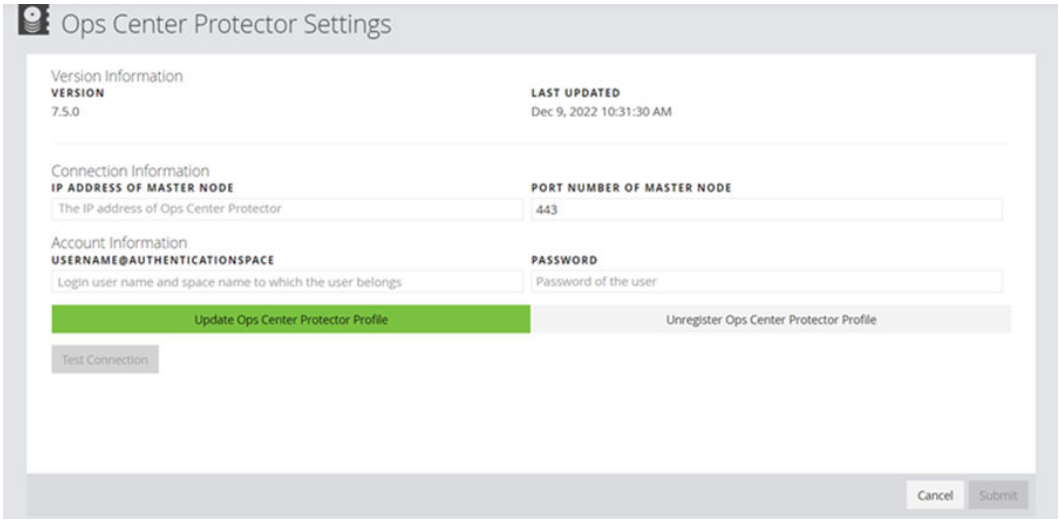
You can use Ops Center Administrator to register Ops Center Protector settings.

Before you begin

- Ops Center Protector must be installed.
- A user with permissions to perform pair management functions is identified.

Procedure

1. From the **Settings** tab, click **Ops Center Protector Settings**.



2. Under **Connection Information**, enter the IP address and the port number of the Master node. The default port number is 443.
3. Under **Account Information**, enter the user name and password of the Ops Center Protector user who can perform pair management functions for high availability or asynchronous remote clone.
4. Click **Test Connection** to verify that you connected to the Master node successfully.
5. Click **Submit**.

Suppressing a Podman upgrade to avoid unintentionally upgrading to an unsupported version

You can suppress the upgrade of Podman to avoid unintentionally upgrading to an unsupported version.

For example, you can use yum-plugin-versionlock or you can add the exclude parameter to the `yum.conf` file.

Changing the SELinux mode

You can change the SELinux mode by creating a backup file of your existing Ops Center Administrator instance, removing Ops Center Administrator, changing the SELinux mode, reinstalling Ops Center Administrator, and then restoring the backup.

Logging on to Ops Center Administrator

You can log on to Ops Center Administrator in the following ways:

- Launching the product from the Ops Center portal (on page 52)
- Logging on through Ops Center SSO (on page 53)
- Logging on from the Ops Center Administrator login screen (on page 53)

Launching the product from the Ops Center portal

Before you begin

Verify the following:

- Ops Center Administrator is registered with the Ops Center portal.
- An Ops Center user account exists with an Ops Center Administrator user role.

Procedure

1. Log on to the Ops Center portal
2. From the **Product** tab, select and click the target Ops Center Administrator.

Logging on through Ops Center SSO

Before you begin

Verify the following:

- Ops Center Administrator is registered with the Ops Center portal.
- An Ops Center user account exists with an Ops Center Administrator user role.

Procedure

1. Open a web browser.
2. Enter the URL for Ops Center Administrator in the address bar.

   ```
   https://ip-address:port-number
   ```

   where:

   - *ip-address* is the IP address of the Ops Center Administrator server.
   - *port-number* is the port number of the Ops Center Administrator server. The default port number is 443.
3. From the login screen of Ops Center Administrator, click **Log in with Ops Center credentials**.
4. Enter your username and password in the Ops Center portal and click **Log in**.

Logging on from the Ops Center Administrator login screen

Before you begin

Verify that you have an account with an Ops Center Administrator user role.

Procedure

1. Open a web browser.
2. Enter the URL for Ops Center Administrator in the address bar.

   ```
   https://ip-address:port-number
   ```

   where:

   - *ip-address* is the IP address of the Ops Center Administrator server.
   - *port-number* is the port number of the Ops Center Administrator server. The default port number is 443.
3. On the login screen of Ops Center Administrator, enter your username and password and click **Log in**.

Resolving log on issues caused by reloading firewall services

If you reload or restart a firewall service on the Ops Center Administrator server, connections to Ops Center Administrator from a web browser may fail. Some firewall services are reloaded or restarted internally during Ops Center Analyzer setup and during Ops Center Protector installation or removal.

If you reload or restart the `firewalld`, `iptables`, or `nftables` service, run the following command on the Ops Center Administrator server:

```
# systemctl restart rainier
```

The following table shows the commands that reload and restart firewall services.

Firewall services	Reloading commands	Restarting commands
firewalld	**`firewalld-cmd reload`**	**`systemctl restart firewalld`**
iptables	**`systemctl reload iptables`**	**`systemctl restart iptables`**
nftables	**`systemctl reload nftables`**	**`systemctl restart nftables`**

The following table shows the firewall services that are reloaded and restarted when Ops Center Analyzer is set up:

Events	Restarted firewall services
Installing Ops Center Analyzer viewpoint	firewalld
Changing the port number for the Ops Center Analyzer viewpoint server by using the **`changeportnumber`** command	firewalld
Installing the Ops Center Analyzer server	firewalld, iptables
Installing the Ops Center Analyzer detail view server	firewalld, iptables
Installing the Analyzer probe server	firewalld, iptables

The following table shows the firewall services that are reloaded and restarted when installing or removing Ops Center Protector:

Events	Firewall services to be restarted
Installing Ops Center Protector	iptables

Events	Firewall services to be restarted
Removing Ops Center Protector	iptables

Resolving log on issues caused by the firewall-cmd command

If you run the `firewall-cmd` command with the `--direct` option, connections to Ops Center Administrator from a web browser might fail.

The problem occurs when all the following conditions are met:

- The operating system is Red Hat Enterprise Linux 9.2 or later or Oracle Linux 9.2 or later.
- The firewalld is v1.2.5-2 or later.
- A chain or rule that can be added by using the `--direct` option of the `firewall-cmd` command does not exist.
- When any of the following actions are performed:
  - The `firewall-cmd` command is run with the `--direct` option.
  - Ops Center API Configuration Manager 11.0.1 or earlier is used.

Recovery

Recover from this issue by completing one of the following actions:

- Restart the Ops Center Administrator service by running the following command:

```
# systemctl restart rainier
```

- Reload the network for podman by running the following command:

```
# podman network reload --all
```

Workaround

- If Ops Center Administrator is not yet installed:
  1. Create a dummy chain to the firewall before installation by running the following

command:

```
# firewall-cmd --direct --permanent --add-chain ipv6 filter dummyChain
```

2. Reload `firewalld` service by running the following command:

```
# firewall-cmd --reload
```

- If Ops Center Administrator is already installed:
  1. Create a dummy chain to the firewall by running the following command:

```
# firewall-cmd --direct --permanent --add-chain ipv6 filter dummyChain
```

  2. Reload `firewalld` service by running the following command:

```
# firewall-cmd --reload
```

  3. Restart the Ops Center Administrator service by running the following command:

```
# systemctl restart rainier
```

After applying the workaround, if you complete any of the following actions, run the `# systemctl restart rainier` command and restart the Ops Center Administrator service:

- Run `firewalld-cmd reload`.
- Run `systemctl restart firewalld`.
- Install Ops Center Analyzer viewpoint.
- Change the Ops Center Analyzer viewpoint server port number by using the `changeportnumber` command.
- Install the Ops Center Analyzer server.
- Install the Ops Center Analyzer detail view server.
- Install the Ops Center Analyzer probe server.
- Install Ops Center Protector.
- Remove Ops Center Protector.

Logging on when Ops Center Administrator is not available

If Ops Center Administrator is not available and you have an administrator login account with the required permissions, you can log in directly to Device Manager - Storage Navigator.

Before you begin

Verify the following:

- You are managing one of the following storage systems:
  - VSP 5000 series
  - VSP E series
  - VSP G1x00, F1500
  - VSP G200, G/F400, G/F600, G/F800
  - VSP G/F350, G/F370, G/F700, G/F900,
- You have an Ops Center Administrator login account with the required permissions. For information on creating user accounts in Storage Navigator, see the storage system documentation.

Procedure

1. Start a web browser.
2. Enter the URL:
   - For VSP E590, E790, E590H, or E790H storage systems, enter `https://`*`IP-address-or-host-name-of-the-SVP`*`/dev/storage/9340006`*`XXXXX`*`/emergency.do` (where the model number is '934000' and '6*XXXXX*' indicates the system serial number)
   - For VSP E990 storage systems, enter `https://`*`IP-address-of-the-SVP`*`/dev/storage/9360004`*`XXXXX`*`/emergency.do` (where the model number is '936000' and '4*XXXXX*' indicates the system serial number)
   - For VSP E1090 or E1090H storage systems, enter https://*IP-address-of-the-SVP*/dev/storage/9380007*XXXXX*/emergency.do (where the model number is '938000' and '7*XXXXX*' indicates the system serial number)
   - For VSP 5000 series or VSP G1x00, F1500 storage systems, enter: `https://`*`IP-address-or-host-name-of-the-SVP`*`/sanproject/emergency.do`
   - For VSP G200 storage systems, enter: `https://`*`IP-address-or-host-name-of-the-SVP`*`/dev/storage/8320004`*`XXXXX`*`/emergency.do` (where the model number is '8320004' and '4*XXXXX*' indicates the system serial number)
   - For VSP G/F400, G/F600 or VSP N400, N600 storage systems, enter: `https://`*`IP-address-or-host-name-of-the-SVP`*`/dev/storage/8340004`*`XXXXX`*`/emergency.do` (where the model number is '8340004' and '4*XXXXX*' indicates the system serial number)
   - For VSP G/F800, VSP N800 storage systems, enter: `https://`*`IP-address-or-host-name-of-the-SVP`*`/dev/storage/8360004`*`XXXXX`*`/emergency.do` (where the model number is '8360004' and '4*XXXXX*' indicates the system serial number)

- For VSP G/F350 storage systems, enter `https://`*`IP-address-or-host-name-of-the-SVP`*`/dev/storage/8820004`*`XXXXX`*`/emergency.do` (where the model number is '882000' and '4*XXXXX*' indicates the system serial number).
- For VSP G/F370, G/F700, G/F900 storage systems, enter `https://`*`IP-address-or-host-name-of-the-SVP`*`/dev/storage/8860004`*`XXXXX`*`/emergency.do` (where the model number is '886000' and '4*XXXXX*' indicates the system serial number).

3. The following actions might be required to open the login dialog box, depending on your environment:
   - If a message indicates that the enhanced security configuration is enabled on the computer, select **In the future, do not show this message** and click **OK**.
   - If the SVP is set to support SSL-encrypted communication and security messages appear, make sure the certificate is correct and follow the instructions in the dialog box.
   - If a message indicates that certain web sites are blocked, make sure you have added the SVP to the trusted sites zone.
4. Enter the user ID and password for the account.
5. Click **Log In**.
6. If the Security Information dialog box opens, click **Yes**.
7. If an Adobe Flash Player local storage area pop-up dialog box opens, click **Allow** to open the Device Manager - Storage Navigator main window. The cache function of Flash Player optimizes the process of Device Manager - Storage Navigator. Denying the request might reduce processing speed.

Result

You are successfully logged in to Device Manager - Storage Navigator.

Note: If the login process fails three times by using the same user ID, Device Manager - Storage Navigator stops responding for one minute. This is for security purposes and is not a system failure. Wait, and then try again.

Chapter 3: Managing the Linux environment

You can update your Linux OS and container using the Yellowdog Updater, Modified (YUM).

Updating your Linux OS environment using Yellowdog Updater, Modified (YUM)

Install and manage new software for your Linux OS environment using Yellowdog Updater, Modified (YUM). YUM is a tool that automatically updates the Linux OS over a network.

Complete the following steps to use YUM to update your OS environment:

Procedure

1. Edit the YUM configuration file:

   If you need a proxy server only, without a user, add the following line to the [main] section of the `/etc/yum.conf` file:

   ```
   PROXY=http://your.proxy.server:port
   ```

   If the proxy requires a user name and password, add the following lines to the `yum.conf`.

   ```
   proxy_username=yum-user
   proxy_password=yum-user-password
   ```

2. Complete the software updates.

   `yum update openssl`

3. Validate the software version.

   `openssl version`

Result

Your OS environment is updated.

Updating your container using Yellowdog Updater, Modified (YUM)

Complete the following steps to use Yellowdog Updater, Modified (YUM) to update your container:

Before you begin

Verify the following:

- There are no backup or restore jobs running.
- There are no Administrator jobs running.

Procedure

1. Connect to the container that requires updating:

   ```
   podman exec -it container_id bash
   ```

2. Edit the YUM configuration file:

   If you need a proxy server only, without a user, add the following line to the [main] section of the `/etc/yum.conf`.

   ```
   PROXY=http://your.proxy.server:port
   ```

   If the proxy requires a user name and password, add the following lines to the `yum.conf` file.

   ```
   proxy_username=yum-user
   proxy_password=yum-user-password
   ```

3. Update the oraclelinux-release-el8 package.

   ```
   yum update oraclelinux-release-el8
   ```

4. Perform software updates.

   ```
   yum install bind-utils
   ```

   Note: If the host name of the yum repository is resolved in IPv6, the container cannot connect to the repository and the yum command may fail. In that case, add the following line to the [main] section of the `/etc/yum.conf` file:

   `ip_resolve=4`

5. Validate the domain.

   ```
   nslookup
   ```

   ```
   [root@hid yum.repos.d]# nslookup example.com
   Server: 172.17.24.20
   Address: 172.17.24.20#53

   Non-authoritative answer:
   Name: example.com
   Address: 10.7.42.0
   ```

```
Name: example.com
Address: 10.7.7.33
```

Note: Each step from 2 to 4 can also be run for all containers at the same time. If you want to configure all containers at the same time, skip step 1 and run commands from the host by referring to the following command examples:

For step 2

--For setting the proxy:

```
for containerid in $(podman container list -q) ; do
podman exec -it ${containerid} bash -c "sed -i -e \"/^\
[main\]$/a proxy=https://your.proxy.server:port\" /etc/
yum.conf" ; done
```

--For setting the proxy user:

```
for containerid in $(podman container list -q) ; do
podman exec -it ${containerid} bash -c "sed -i -e \"/^\
[main\]$/a proxy_username=yum-user\" /etc/yum.conf" ;
done
```

--For setting the proxy password:

```
for containerid in $(podman container list -q) ; do
podman exec -it ${containerid} bash -c "sed -i -e \"/^\
[main\]$/a proxy_password=yum-user-password\" /etc/
yum.conf" ; done
```

For step 3

```
for containerid in $(podman container list -q) ; do
podman exec -it ${containerid} bash -c "yum update
oraclelinux-release-el8"; done
```

For step 4

```
for containerid in $(podman container list -q) ; do
podman exec -it ${containerid} bash -c "yum install
bind-utils" ; done
```

If the host name of the yum repository is resolved in IPv6, the container cannot connect the repository and the yum command may fail. In that case, run the following commands.

```
for containerid in $(podman container list -q) ; do
podman exec -it ${containerid} bash -c "sed -i -e \"/^\
[main\]$/a ip_resolve=4\" /etc/yum.conf" ; done
```

Result

Your container is updated.

Modifying the Ops Center Administrator server IP address

You can change the IP address of the Ops Center Administrator server.

Procedure

1. Open a browser and enter the following URL in the address bar:

   ```
   https://ip-address:port/vam
   ```

   where:

   - *ip-address* is the IP address of the Ops Center Administrator server.
   - *port* is the port number of the Ops Center Administrator. The default port number is `443` or `20961`.

   The default login credentials are *`sysadmin/sysadmin`*
2. Click **Network Settings**, and then enter the new IP address you want to use under **IP ADDRESS** and **SNMP IP ADDRESS**.
3. Click **Submit**.
4. Change the Ops Center Administrator server IP address as described in your OS manual.
5. From the command prompt, log in to the OS using a root user or a normal user account. If you log in as a normal user, use the **`sudo`** command to complete the next step as a root user.
6. Restart all containers and services using the following command:

   ```
   # systemctl restart rainier
   ```

Result

You can log in using the new URL.

Modifying the Ops Center Administrator log settings

You can change the log settings of the Ops Center Administrator.

Procedure

1. Open a browser and enter the following URL in the address bar:

   ```
   https://ip-address:port/vam
   ```

   where:

   - *ip-address* is the IP address of the Ops Center Administrator server.
   - *port* is the port number of the Ops Center Administrator. The default port number is 443 or 20961.

The default login credentials are `sysadmin/sysadmin`.

2. Click **Application Log Settings**.
3. If you want to change the log size, enter the new size under **FILE SIZE**.
4. If you want to change the number of log files, enter the new number under **NUMBER OF FILES**.
5. Click **Submit**.

Note: Increasing the log size or number of files increases disk usage.

Chapter 4: Upgrading Ops Center Administrator

You can upgrade Ops Center Administrator by using the application installer or by restoring a backup of the previous version. The upgrade method depends on which version of the software you are currently running.

Note:

- Ops Center Administrator v10.9.x no longer supports the stand-alone preconfigured media. Instead, you must use the consolidated Ops Center preconfigured media, the Ops Center Server Express installer, or the application installer.
- Ops Center Administrator v10.9.1 and later can manage a large number of resources, such as storage systems or volumes, with a fixed memory size. If you upgrade from a previous version to v10.9.1 or later, any changes that you made to the memory settings are automatically updated so there is no need to change the memory settings again.

- If you are upgrading from v10.x or later with an in-place upgrade, you can use the application installer as described in Upgrading Ops Center Administrator by using the application installer (on page 64).
- If you are moving your Ops Center Administrator instance or upgrading from v10.x or later with backup and restore, you must upgrade by creating a backup of your existing Ops Center Administrator instance as described in Upgrading Ops Center Administrator by using backup and restore (on page 72).
- If you are migrating to a different container runtime (for example; migrating from Docker to Podman), you must upgrade by creating a backup of your existing Ops Center Administrator instance before removing the older container runtime and installing a new one. For more information, see Upgrading Ops Center Administrator by using backup and restore (on page 72).

Upgrading Ops Center Administrator by using the application installer

If you are running Ops Center Administrator v10.0.x or later, you can use the application installer to upgrade.

Before you begin

Verify the following:

- There is a total of 60 GiB of temporary available space. This includes the following:
  - 40 GiB under the Podman root directory (default directory: `/var/lib/containers`)
  - 10 GiB under `/var/tmp`
  - 10 GiB under `/tmp`
- There are no backup or restore jobs running.

- The Virtual Appliance Manager log level is set to INFO. Upgrading fails when the log level is set to DEBUG or TRACE.
- When you change to a different network mode during upgrading, do the following:
  - When you change the network mode to bridge mode, verify the following:

    IP forwarding and br_netfilter for the IP V4 network are installed on the operating system. For details, see Installing Ops Center Administrator with the application installer (on page 28).

    The OS running firewalld (for example, RHEL 8 or later) is configured to allow communication between containers. For details, see Installing Ops Center Administrator with the application installer (on page 28).
  - When you change the network mode to host mode, verify the following:

    Required port numbers for host mode are not allocated to other programs installed on the same computer. For details, see Port requirements (on page 12).

- If you also want to upgrade the container runtime version, verify the following additional prerequisites:

  Note: You can upgrade Podman (major or minor version) during the installation or upgrade process, or after installing Ops Center Administrator. However, if you are upgrading Podman from version 3.x to 4.x, we recommend that you do so during the Ops Center Administrator installation. This is because upgrading Podman from version 3.x to 4.x after installation requires creating a backup of the existing Ops Center Administrator instance, removing it along with the Podman upgrade, reinstalling Ops Center Administrator, and then restoring the backup.

  - If the supported version of Podman is not installed in the environment, you must configure Yellowdog Updater, Modified (YUM) settings to install packages over a network. The application installer connects to the configured YUM repository and installs the required version of Podman. The packages related to Podman are located in the latest BaseOS and AppStream repositories.

    If you want to install or upgrade Podman yourself, you can run the following command:

    ```
    yum install podman-required-version
    ```

    For example, to install Podman v3.3.x:

    ```
    yum install podman-3.3.*
    ```

    The asterisk indicates to obtain and install the latest patch version available in the repository.

    Note: Downgrading the Podman version is not supported.

  - If you install or upgrade Ops Center Administrator while suppressing the upgrade of Podman, the installation fails with the error - `[Error] Failed to install Podman x.x.x from package repository. Confirm the network or repository server setting, and retry.` Unlock the suppression and install or upgrade Ops Center Administrator again. After completing the installation, suppress the upgrade of Podman again.
  - If you install Podman 3.3.x, or upgrade Podman from 3.3.x to any version, or run any Podman command on the server using Podman 3.3.x, a warning message `Failed to decode the keys [<key1>, <key2>, ..., <keyN>] from "/usr/share/containers/containers.conf"` may appear. Ignore this message because it does not affect Ops Center Administrator.
  - If you cannot use YUM to install Podman because your management server is not connected to the network, you must get the Podman software from the OS media (ISO image or CD-ROM).

    For example, the minimum supported version of Podman 3.3.x is available with Red Hat Enterprise Linux and Oracle Linux version 8.5, and Podman 4.2.x is available with version 9.1. Therefore, regardless of the OS version that you are using, you must download the OS that includes the version of Podman that you want to use.

1. Download the Linux ISO image (for example, redhat 8.5 iso).
2. Mount the ISO image using the following command:

   `mount /dev/cdrom /media`

   For example: **`mount -o loop rhel-8.5-x86_64-dvd.iso /media`**
3. If the `/etc/yum.repos.d` directory contains an existing repo file, rename the file extension or delete it.
4. Create the yum repository file by running the following command:

   `vim /etc/yum.repos.d/local.repo`
5. Add the required definition lines as shown in the following examples, and then save and close the file:

   For Oracle Linux

```
[LocalRepo_BaseOS]name= LocalRepo_BaseOS
gpgcheck=0
enabled=1
baseurl=file:///media/BaseOS/
LocalRepo_AppStream]
name=LocalRepo_AppStream
gpgcheck=0
enabled=1
baseurl=file:///media/AppStream/
```

   For Red Hat Enterprise Linux

```
[LocalRepo_BaseOS]
name=LocalRepo_BaseOS
metadata_expire=-1
enabled=1
gpgcheck=0
baseurl=file:///media/BaseOS/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release

[LocalRepo_AppStream]
name=LocalRepo_AppStream
metadata_expire=-1
enabled=1
gpgcheck=0
baseurl=file:///media/AppStream/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
```
6. Verify the required library by running the following command:

   `yum repolist`
7. Install podman by using the following command :

```
yum install podman-required-version
```

For example, to install Podman v3.3.*x*:

```
yum install podman-3.3.*
```

During installation, the following files are created under `/tmp`. Delete them if they are no longer required:

- Application log
- Audit log
- Backup file

The installation log is created under `/var/logs/rainier-install`.

Note: When upgrading Ops Center Administrator, do not configure the **`noexec mount`** option for the file system including the `/tmp` and `/var/tmp` directories. To check whether the option is configured, run the **`mount`** command.

Procedure

1. Either open an SSH connection to the VM or open the VMware console and press `Alt +F2` to reach the console.
2. Log in using a root user or a normal user account. If you log in as a normal user, use the **`sudo`** command to complete the following procedure as the root user.
3. Copy the tar file `ops-center-administrator-xx.tar.gz` from the installation media to any folder in the Linux environment and extract it. Navigate to the extracted folder.
4. Navigate to the extracted folder and run the following command:

   `sudo ./install.sh`.
5. Log in when prompted.
   - When upgrading from Ops Center Administrator installed using the Ops Center preconfigured media or application installer:
     - User name: `sysadmin`
     - Password: Specify the current password. (default password: `sysadmin`)
   - When upgrading from Ops Center Administrator installed using the stand-alone preconfigured media:
     - User name: `service`
     - Password: Specify the current password. (default password: `Chang3Me!`)
6. At the following prompts, enter `y`:

   ```
   Older version exists. Do you want to upgrade? [y/n]:
   ```
7. At the following prompts, enter the corresponding number to change the network mode. Press Enter to keep the current mode.

   ```
   Current network mode is "bridge". Do you want to change it?
   ```

```
1. bridge : (Current) Containers are isolated from the host's
            network namespace and communicate through the host's virtual
            bridge. This mode is suitable for most cases.

2. host   : Containers share the host's network namespace.
            Therefore, no IP forwarding is required. This mode is used
            when it is absolutely necessary to disable IP forwarding
           (net.ipv4.ip_forward=0).

Enter the number [current=1]:
```

8. If you want to register Ops Center Administrator with Ops Center Common Services during installation, enter `y` at the prompt:

   ```
   Do you wish to configure Ops Center Common Services [y/n]:
   ```

   Ops Center Administrator begins upgrading.

9. If you change the network mode to host mode, restart the OS after the upgrade completes.
10. Suppress the upgrade of Podman to avoid unintentionally upgrading to an unsupported version.

    For example, you can use `yum-plugin-versionlock` or you can add the `exclude` parameter to the `yum.conf` file.

Troubleshooting the upgrade

If the installation fails, try the following:

- Check and resolve any error messages and then retry the installation.
- Verify that the Virtual Appliance Manager log level is set to INFO. Upgrading fails when the log level is set to DEBUG or TRACE.
- Check your YUM settings and the host network to make sure that your system can connect to the YUM repository.
- If you use a local YUM mirror repository server, confirm the HTTP server setting and whether the repository data gathered by the **`reposync`** command exists correctly.
- Restart the Podman service, verify that the older version is running, and then retry the installation.
- Check the Podman logs.

  For more information on how to perform these actions, consult your container runtime documentation.

- View the journal log entries to see whether there is additional error information by connecting to the host with a root user or a normal user account and running the following commands:

  Note: If you log in as a normal user, use the **`sudo`** command to complete the following procedure as the root user.

  - **`journalctl --no-pager`**
  - **`journalctl --no-pager -u rainier`**

- If an error message indicates a failure to create the data-app-manager container before the upgrade, perform the following procedure:

  1. Remove and reinstall Ops Center Administrator.
  2. Restore the settings using the `rainier-backup-yyyymmdd-hhmmss.tar.gz` file in `/tmp`. For details, see "Backing up and restoring system settings" in the *Hitachi Ops Center Administrator User Guide*.

- If an error message indicates a failure to take over the JDK used in the container before the upgrade, perform the following procedure to install the newer version of Ops Center Administrator with the bundled JDK applied, and then replace it with the required JDK.

  1. Create a backup copy of the latest log files in the `/var/logs/rainier-tool` directory. If the problem persists after completing the rest of this procedure, contact customer support and provide these log files.
  2. Remove and reinstall Ops Center Administrator.
  3. Restore the settings using the `rainier-backup-yyyymmdd-hhmmss.tar.gz` file in `/tmp`. For details, see "Backing up and restoring system settings" in the *Hitachi Ops Center Administrator User Guide*.
  4. Replace the JDK by manually running the `rainier-replace-jdk` command with the `--keep-java` option.

  Note: If the problem persists, contact customer support. Provide them the latest log files in the `/var/logs/rainier-tool` directory, along with the backup copy of the log files created in Step 1.

- If the installation produces any warnings or errors, they may point to the cause of the problem. Correct any issues the installer identifies, delete any Ops Center Administrator containers and images, and start the installation again.
- If the problem persists after the issues are corrected, try a fresh installation.

  1. Check that the backup file of the current version exists under the folder where `install.sh` is located and download the backup file.

     If the backup file does not exist, access the virtual appliance manager from the following URL, and download the backup file:

     ```
     https://ip-address:port/vam
     ```

where:

- *ip-address* is the IP address of the Ops Center Administrator server.
- *port* is the port number of the Ops Center Administrator. The default port number is `443` or `20961`.

The default login credentials are *`sysadmin/sysadmin`*

- For an environment where the application installer version was originally installed, remove the older version and start a fresh installation.
- For an environment where the preconfigured media installer version was originally installed, discard the current environment and perform a preconfigured media installation.

2. After the installation completes, apply the backup file.

Upgrading Ops Center Administrator by using backup and restore

You must use the backup and restore method for upgrading in the following cases:

- You are moving your Ops Center Administrator instance. In this case, you must upgrade by backing up your existing Ops Center Administrator instance, installing a newer version, and then restoring the previous instance. When upgrading, you can upgrade from 10.0.x or later to the current version.
- You are migrating to a different container runtime (for example; migrating from Docker to Podman). In this case, you must upgrade by creating a backup of your existing Ops Center Administrator instance before removing the older container runtime and installing a new one.

  When Ops Center Administrator is working in host mode, the user-defined port numbers for accessing the Ops Center Administrator are migrated but the internal service port numbers are not migrated to a new instance when you restore. In this case, ensure that the Ops Center Administrator default port numbers are not in use, and change the port number manually again after the installation. For details about required port numbers, see Port requirements (on page 12). To configure a port number in a new instance, see Modifying the internal port allocated by Ops Center Administrator for host mode (on page 90).

Procedure

1. Choose one of the following installation methods:
   - Use the preconfigured media ISO to deploy an OVA. The OVA installation deploys a VM with an operating system, Podman, and Ops Center Administrator. If the current version was deployed by using the stand-alone preconfigured media, you can use the consolidated Ops Center preconfigured media to deploy a new version.
   - Use the application installer to enable maximum control of the environment. The installer must be deployed in a Podman-compatible environment that contains only the Ops Center Administrator application.

     Note: If you use the json-file logging driver, set the maximum log size to 50 MiB and the maximum number of files to 5.
2. From the currently installed version, open a browser, and enter the following URL in the address bar:

   ```
   https://ip-address:port/vam
   ```

   where:
   - *ip-address* is the IP address of the Ops Center Administrator server.
   - *port* is the port number of the Ops Center Administrator. The default port number is `443` or `20961`.
   - When upgrading from Ops Center Administrator installed using the Ops Center preconfigured media or application installer:
     - User name: *sysadmin*
     - Password: Specify the current password. The default password is *sysadmin*.
   - When upgrading from Ops Center Administrator installed using the stand-alone preconfigured media:
     - User name: *service*
     - Password: Specify the current password. The default password is *Chang3Me!*.
3. When the virtual appliance manager opens in the browser, click the **Backup** icon () to download a backup file of the currently installed version. The file may take a few minutes to start downloading.

   Note: Ensure the virtual appliance manager log level is set to **INFO** before you upgrade. If it is set it to **DEBUG** or **TRACE**, the upgrade may fail with errors.

4. After downloading the backup file, shut down the currently installed version.
   - If you used the Ops Center Administrator installer method, delete the Ops Center Administrator containers and images on the system before running the new installer. For more information, see Removing Ops Center Administrator (on page 85).
   - If you used the Appliance model, the VM containing Ops Center Administrator is shut down at this time. You may want to determine a maintenance window to do this because Ops Center Administrator is unavailable until the upgrade is complete.
   - If the current version was deployed by using the application installer and if you want to migrate to a different container runtime (for example, migrating Docker to Podman), remove the old container runtime and then install the new container runtime on the host OS.
5. Deploy the next version using the method of your choice (preconfigured media or installer).
6. In the new instance of Ops Center Administrator, open a browser, and enter the following URL in the address bar:

   ```
   https://ip-address:port/vam
   ```

   where:
   - *ip-address* is the IP address of the Ops Center Administrator server.
   - *port* is the port number of the Ops Center Administrator. The default port number is `443` or `20961`.

   The default login credentials are *`sysadmin/sysadmin`*
7. When the virtual appliance manager opens in the browser, click the **Restore** icon (). You are prompted to upload the backup file that was downloaded earlier. Choose the file and upload it to the new Ops Center Administrator instance.

   The Ops Center Administrator appliance restarts. It may take up to an hour to restore the configuration. After the appliance is running, the upgrade is complete. (Optional) If the upgrade completed successfully, you can delete the VM containing the previous version of Ops Center Administrator.

Chapter 5: Adding a storage system

Onboarding a storage system is the process of associating it with Ops Center Administrator. After you onboard the storage system, you can manage it from the Ops Center Administrator dashboard.

Note: Do not onboard the same storage system to multiple Ops Center Administrator instances. This may exhaust SVP resources, which causes the SVP to slow or become unresponsive to the Administrator server.

For details on block storage, see Onboarding and configuring block storage (on page 75).

For details on software-defined storage, see Onboarding and configuring software-defined storage (on page 83).

Onboarding and configuring block storage

Onboarding a storage system is the process of associating it with Ops Center Administrator. After you onboard the storage system, you can manage it from the Ops Center Administrator dashboard.

Ops Center Administrator requires access to all resource groups on the storage system so that the workflows function correctly. Verify that the service processor (SVP) user name used to onboard a storage system in Ops Center Administrator has access to all custom resource groups and meta resource groups.

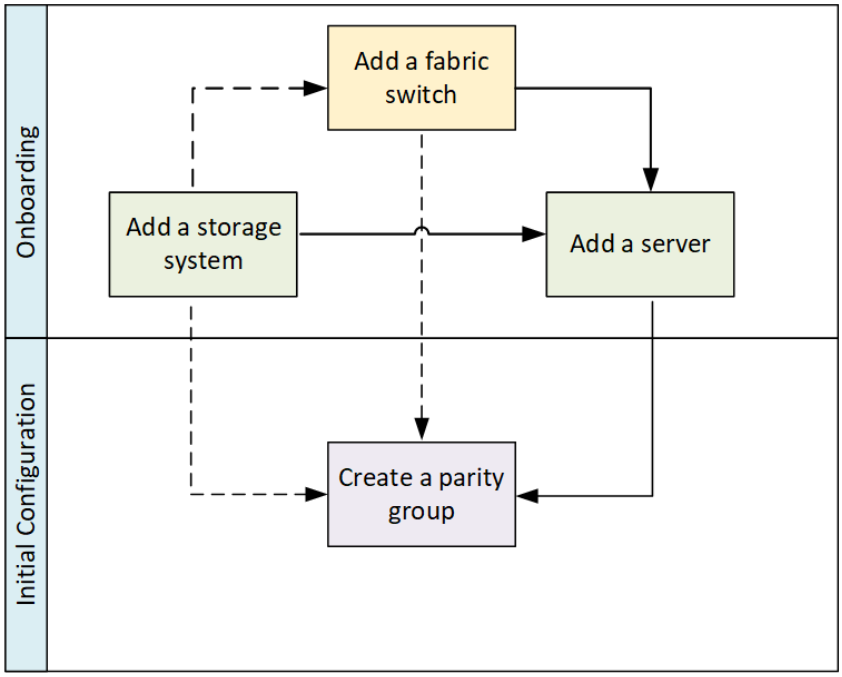
For information on onboarding software-defined storage, see Onboarding and configuring software-defined storage (on page 83).

Overview

Onboarding a storage system in Ops Center Administrator is more than adding a storage system to a list. You must add at least one server before you can provision volumes to the server on the storage system.

You must synchronize the time between the Ops Center Administrator server and the time on the storage systems. Use NTP to synchronize the time.

In the following workflow, the recommended path is marked with solid arrows and the dashed arrows indicate the optional paths. Before a storage system is available for use in the network, you must complete all of the tasks in the workflow.



Adding the first storage system

You must onboard a storage system before you can start using Ops Center Administrator.

Before you begin

- Ops Center Administrator needs access to all resource groups on the storage system so that the workflows function correctly. Verify that the user name used to onboard a storage system in Ops Center Administrator has access to all custom resource groups and meta resource groups.
- To receive storage systems alerts in Ops Center Administrator, the storage system must be set to SNMPv3. If storage systems have SNMPv1 or SNMPv2c settings configured, you can still manage them, but alert information is not shown in Ops Center Administrator. To receive alerts from these storage systems, you must change the SNMP setting to SNMPv3, and restart the Ops Center Administrator service so that the Ops Center Administrator server is added as an SNMP trap destination.
- To get alerts from two or more VSP G1x00, VSP F1500 storage systems, enable **Use a unique SNMP engine ID** for all VSP G1x00 and VSP F1500 as described in "Edit Advanced System Settings wizard" in the *Hitachi Virtual Storage Platform G1x00 and F1500 System Administrator Guide*.

Procedure

1. On the Ops Center Administrator dashboard, click **Add Storage System**.
2. Enter values for the following parameters in the **Onboard Storage System** window:

IP Address:

- VSP One Block: Enter the service IP address (IPv4) for the target storage system.
- All other VSP storage systems:
  - Storage system with an SVP: Enter the IP address (IPv4) of the external SVP for the target storage system.
  - Storage system without an SVP: Enter the GUM IP address (IPv4) of the controller for the target storage system.

User name and password:

Log in as a user who has administrator privileges on this storage system. For example, you can log in with the username `maintenance`.

Note: If the storage system has a virtual SVP, you can specify the SVP access port number following the IP address in the IP address field. The syntax is **`IP-address:Port-number`**.

3. Click **Submit**.
4. (Optional) Onboard other storage systems.

Result

The Jobs window is updated with a job called Create Storage System. If you are adding multiple storage systems, there is a job for each one.

Wait a while for Ops Center Administrator to add the storage system, then refresh the Jobs window to verify that the storage system has been onboarded.

Next steps

- Verify the storage system initial settings.
- Create parity groups.

Note:

- Parity groups for the following storage systems are created outside of Ops Center Administrator by a service representative:
  - VSP 5000 series
  - VSP G1x00 or VSP F1500
- You cannot create or modify parity groups for VSP One Block using Ops Center Administrator, but you can view them.

  To create or modify parity groups for configuring a pool, you must use VSP One Block Administrator. The pool configuration workflow in VSP One Block Administrator automatically handles the parity groups setup. For a detailed procedure, see "Creating a pool" in the *Hitachi Ops Center Administrator User Guide*.

Adding a fabric switch

You can add, update, or delete a fabric switch after onboarding a storage system in Ops Center Administrator.

After you add a fabric switch, you can choose to auto-create zones during volume provisioning. A fabric switch is required for any process that uses auto-select, such as host group creation and auto-selection of ports while attaching volumes to servers.

Before you begin

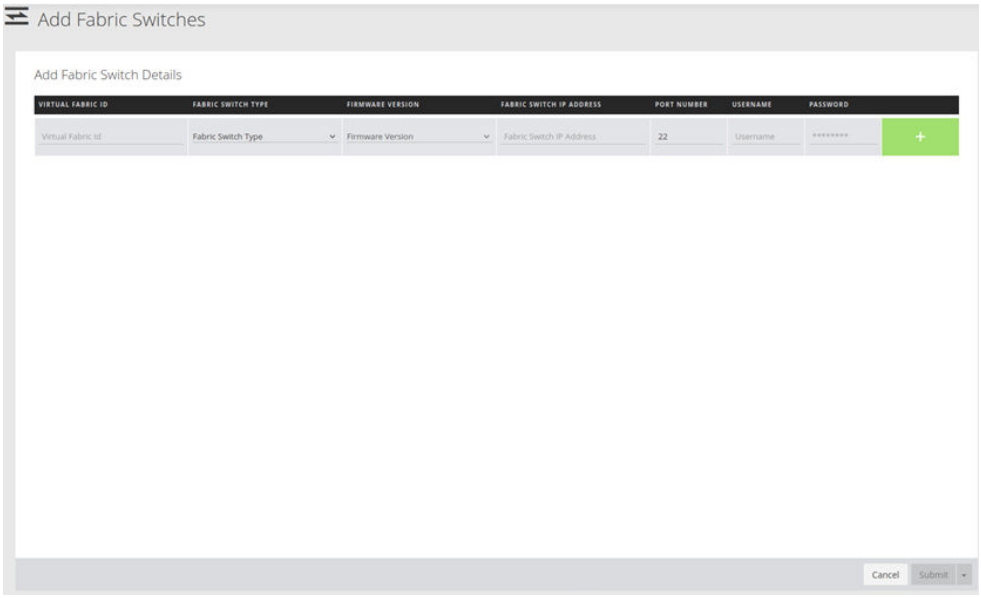
Verify the following:

- The switch is supported. Ops Center Administrator supports the following fabric switches:
  - Brocade®: Fabric OS 8.2.2a, 9.0.x, 9.1.x
  - Cisco®: MDS NX-OS Release 8.1(1) or later

  Note: Before upgrading the Fabric OS of a Brocade switch from 8.x to 9.0.x or 9.1.x, you must remove the fabric switch from Ops Center Administrator. After the upgrade, onboard the fabric switch again. You cannot use the Update Fabric Switch option in Ops Center Administrator to upgrade the Fabric OS.
- Servers and ports are connected according to the manufacturer instructions.
- There is an active zone set with at least one dummy zone available.
- The Ops Center Administrator server is connected to the same IP network and has access to the SNMP broadcast of Fibre Channel switches.
- You have the required information about the fabric switch:
  - Virtual Fabric ID (required only for Cisco switches)
  - Fabric Switch Type
  - Fabric Switch IP Address
  - Firmware Version (required only for Brocade switches)
  - Port Number
  - Username
  - Password
- You have the Admin role for the fabric switch.

Procedure

1. On the Ops Center Administrator dashboard, select the **Fabric Switches** ( ) icon to open the **Fabric Switches** window.
2. Click the plus sign (**+**) to open the **Add Fabric Switches** window.



3. Enter the following configuration information for the switch you are adding:
   - **Virtual Fabric ID**: For Cisco switches, the VSAN ID. Not applicable for Brocade switches.
   - **Fabric Switch Type**: Select **Brocade** or **Cisco**.
   - **Firmware Version**: Select the firmware version if you are adding a Brocade switch.
   - **Fabric Switch IP Address**

     To add or update a core switch, use the management IP address or the Active CP IP address.
   - **Port Number**

     If you are adding a Brocade switch with a firmware version of 9.0.0 or later, specify port number 443. For Brocade switches with firmware versions earlier than 9.0.0 or for Cisco switches, specify the ssh port number of the target fabric switch.
   - **Username**
   - **Password**
4. Click **Submit**.

Result

A job is started to add the fabric switch.

Adding servers

Add servers so you can attach volumes. You can add multiple server parameters from a file, or add one server at a time.

You can add servers using one of the following methods:

- Manually add information for one server at a time.
- Import a CSV (comma-separated values) file with information for multiple servers (one in each row).

  The CSV file must have the following headings:

  - For Fibre:
    - Name, OSType, WWNs (comma-separated list of WWNs)
    - (Optional) Description, IPAddress and WWNsUserDefinedNames (comma-separated list of user-defined names for WWNs).
  - For FC-NVMe:
    - Name, OSType, Host NQN
    - (Optional) Description, IPAddress, WWNs (comma-separated list of WWNs), and WWNsUserDefinedNames (comma-separated list of user-defined names for WWNs).
  - For iSCSI:
    - Name, OSType, IscsiName (comma-separated list of names)
    - (Optional) Description, IPAddress, ChapUser, ChapSecret and IscsiNamesUserDefinedNames (comma-separated list of user-defined names for iSCSI Names).

Valid OSType values are as follows:

- AIX
- HP_UX
- LINUX
- NETWARE
- OVMS
- SOLARIS
- TRU64
- VMWARE
- VMWARE_EX
- WIN
- WIN_EX

Note: See the storage system documentation for the OS Type and Host Mode of the host groups associated with the storage system.

Procedure

1. On the Ops Center Administrator dashboard, click the **Servers** () icon. Then click the plus sign (**+**) to open the **Add Server** window.


Add Servers
CSV Import
Fibre Servers
SERVER NAME
DESCRIPTION
IP ADDRESS
OS TYPE
app-server-01
Description
IP Address
HP UX
WWN LIST
WWN
10:00:00:05:33:26:f7:21
WWN USER-DEFINED NAMES
Server1_HBA1, Server1_HBA2
FC-NVMe Servers
SERVER NAME
DESCRIPTION
IP ADDRESS
OS TYPE
app-server-02
Description
IP Address
AIX
WWN
HOST NQN
50:00:00:00:00:00:00:00, 50:00:00:00:00:00:00:01
nqn.test_02
WWN USER-DEFINED NAMES
Server1_HBA1, Server1_HBA2
iSCSI Servers
SERVER NAME
DESCRIPTION
IP ADDRESS
OS TYPE
app-server-03
Description
IP Address
HP UX
CHAP USER
CHAP SECRET
user1
ISCSI LIST
ISCSI NAMES
iqn. linux-iscsi-2,eui.1234567890abCDef
ISCSI NAMES USER-DEFINED NAMES
Server1_HBA1, Server1_HBA2
Cancel
Submit

2. In the **Add Server** window, do one of the following:

   - Click the upper plus sign (**+**) to browse for the CSV file or drag the file to the plus sign. The values from the file populate the window. Example:

     ```
     name,description,ipAddress,osType,wwns,wwnsUserDefinedNames
     Esxi,ESXI
     HOST,10.30.90.200,VMWARE_EX,10:00:00:05:33:26:f7:21,Esxi_HBA_1
     Win,WINDOWS
     HOST,10.30.91.80,WIN_EX,"10:00:00:05:33:26:f7:37,10:00:00:05:3
     3:26:f7:36","HOST_HBA_1,HOST_HBA_2"
     ESXi_Cisco_1,ESXi HOST connected to Cisco
     Fabric,,VMWARE_EX,"10:00:00:05:33:26:e0:fc,10:00:00:05:33:26:e
     0:fd","Fabric_HBA_1"
     ESXi_Cisco_2,ESXi HOST connected to Cisco
     Fabric,,VMWARE_EX,"100000053326df1a,100000053326df1b",",Fabric
     _HBA_2"
     ```

   - To add Fibre, FC-NVMe, and iSCSI servers at the same time, use the following format:

     ```
     name,description,ipAddress,osType,wwns,wwnsUserDefinedNames,is
     csiNames,iscsiNamesUserDefinedNames,chapUserName,chapUserSecre
     t,hostNqns
     linux-iscsi,test dummy host,20.10.10.10,Linux,,,"iqn.
     linuxiscsi-1,iqn. linux-iscsi-2,eui.1234567890abCDef","linux-
     iscsi-HBA-1,linux-iscsi-HBA-2,linux-iscsi-HBA-3",,
     -windows-iscsi-uni-chap,test dummy
     host,20.10.10.20,Win,,,iqn.-windows-iscsi-unichap,"""host-
     HBA-1""",chapUserName,chapUserSecret
     -windows-iscsi-bi-chap,test dummy
     host,20.10.10.30,Win,,,iqn.- windows-iscsi-bichap,"""windows-
     iscsi-bi-chap-
     HBA-1""",chapUserName,chapUserSecret
     -vmware-iscsi-longest,test dummy
     host,20.10.10.40,VMWARE,,,"iqn.123456789012345678901234567890
     2345678901234567890123456789012345678901234567890123456789012
     4567890123456789012345678901234567890123456789012345678901234
     6789012345678901234567890123456789012345678901234567890123456
     789,eui.3234567890abCDef"
     ed801h,Windows,10.197.73.57,WIN,10:00:00:90:fa:b4:a8:71,"ed801
      h-HBA-1"
     ed800n,ESX
     Host,10.197.73.7,VMWARE,10:00:00:90:fa:55:85:5d,"ed800n-HBA-1"
     -linux,test dummy
     host,10.10.10.10,Linux,10:10:10:10:10:10:10:10,"ed801h-HBA-1"
     -windows,test dummy
     host,10.10.10.20,Win,10:10:10:10:10:10:10:20,"host-HBA-1"
     -vmware,test dummy
     host,10.10.10.30,VMWARE,10:10:10:10:10:10:10:30
     nvme-linux,test dummy nvme host,192.0.2.10,LINUX,
     10:10:10:10:10:10:20:10,”nvme-linux-hba-1”,,,,,nqn.test-01
     nvme-vmware,test dummy nvme host,192.0.2.20,VMWARE,
     10:10:10:10:10:10:20:20,,,,,,nqn.test-02
     nvme-vmware-ex,test dummy nvme
     host,192.0.2.30,VMWARE_EX,,,,,,,nqn.test-03
     ```

   - Click the plus sign (+) in the table to add a row and enter the required information for Fibre Channel, FC-NVMe, or iSCSI. You can add more servers by clicking the plus sign again.

- (Optional) You can use the WWN List or iSCSI List to add/edit a server.
- (Optional) You can add comma-separated user-defined names for WWNs or iSCSI names in the order they are specified.

3. Click **Submit** to add the servers.

Next steps

Create volumes and attach them to the server.

Onboarding and configuring software-defined storage

Hitachi Virtual Storage Platform One SDS Block delivers application agility and scale for new distributed workloads.

Onboarding a VSP One SDS Block storage system is the process of associating it with Ops Center Administrator. After you onboard the storage system, you can manage it from the Ops Center Administrator dashboard.

Onboarding and managing a VSP One SDS Block storage system in Ops Center Administrator requires a storage user account that has all roles (Security, Storage, Monitor, Service, and Resource). Verify that the storage username and password used to onboard a storage system in Ops Center Administrator has all the roles.

For information on onboarding block storage, see Onboarding and configuring block storage (on page 75).

Overview of onboarding a VSP One SDS Block storage system

You can onboard a VSP One SDS Block storage system in Ops Center Administrator.

You must synchronize the time between the Ops Center Administrator server and the time on the storage systems. Use NTP to synchronize the time.

Adding the first VSP One SDS Block storage system

You can manage VSP One SDS Block storage systems by onboarding them to Ops Center Administrator.

Before you begin

- Onboarding and managing a VSP One SDS Block storage system in Ops Center Administrator requires a storage user account that has all roles (Security, Storage, Monitor, Service and Resource). Verify that the storage username and password used to onboard a storage system in Ops Center Administrator has all the roles.
- Verify the representative IP address of the storage cluster.

Procedure

1. On the Ops Center Administrator dashboard, click **Add Storage Systems**.
2. Enter values for the following parameters in the **Onboard Storage System** window:

IP Address:
Enter the representative IP address of the storage cluster.

User name and password:
Log in as a user who has all roles of Security, Storage, Monitor, Service, and Resource.

3. Click **Submit**.
4. (Optional) Onboard other storage systems.

Result

The Jobs window is updated with a job called Create Storage System. If you are adding multiple storage systems, there is a job for each one.

Wait a while for Ops Center Administrator to add the storage system, then refresh the Jobs window to verify that the storage system has been onboarded.

Chapter 6: Removing Ops Center Administrator

To remove an Ops Center Administrator deployment that was installed with the application installer, you must delete any Ops Center Administrator containers, images, and files. Select one of the following procedures based on your Ops Center Administrator implementation:

- Removing Ops Center Administrator when using Docker (on page 85)
- Removing Ops Center Administrator when using Podman (on page 86)

Note: Ops Center Administrator uses `rdocker:6000` as an image repository.

Removing Ops Center Administrator when using Docker

If your installation uses Docker as the container runtime, remove Ops Center Administrator as follows:

Procedure

1. From the command prompt, log in to the OS using the root account.
2. Stop all containers and services by using the following command:

```
docker stop $(docker ps --format "{{.ID}} {{.Image}}" -a | grep "rdocker:6000/"
| awk '{ print $1 }')
systemctl stop rainier-pipe
systemctl disable rainier-pipe
```

3. Remove all containers by using the following command:

```
docker rm -fv $(docker ps --format "{{.ID}} {{.Image}}" -a | grep
"rdocker:6000/" | awk '{ print $1 }')
```

4. Remove all Docker images by using the following command:

```
docker rmi $(docker images --format "{{.ID}} {{.Repository}}" | grep
"rdocker:6000/" | awk '{ print $1 }')
```

5. Remove all Docker volumes by using the following commands:

```
docker volume rm nginx-certificates
docker volume rm nginx-certificates-override
docker volume rm nginx-confd
docker volume rm nginx-log
```

6. To remove the configuration files, run the following command:

```
/opt/rainier/bin/rainier-config-remove
```

7. To remove the remaining files, run the following commands:

```
rm -rf /opt/rainier
rm -rf /var/log/rainier-audit-log
rm -rf /var/logs/rainier-tool
rm -rf /var/logs/rainier-elastic-store
rm -rf /var/logs/rainier-logs
rm -rf /var/logs/rainier-ubi
rm -rf /var/opt/rainier-ubi
rm -f /etc/systemd/system/rainier-pipe.service
```

Removing Ops Center Administrator when using Podman

If your installation uses Podman as the container runtime, remove Ops Center Administrator as follows:

Procedure

1. From the command prompt, log in to the OS using a root user or a normal user account. If you log in as a normal user, use the **sudo** command to complete the following procedure as the root user.
2. Stop all containers and services by using the following commands:

```
systemctl stop rainier
systemctl disable rainier
systemctl stop rainier-pipe
systemctl disable rainier-pipe
```

3. Remove all containers by using the following command:

```
podman rm -fv $(podman ps --format "{{.ID}} {{.Image}}" -a | grep
"rdocker:6000/" | awk '{ print $1 }') 2>/dev/null
```

4. Remove all Podman images by using the following command:

```
podman rmi $(podman images --format "{{.ID}} {{.Repository}}" | grep
"rdocker:6000/" | awk '{ print $1 }')
```

5. Remove all Podman volumes by using the following commands:

```
podman volume rm nginx-certificates
podman volume rm nginx-certificates-override
podman volume rm nginx-confd
podman volume rm nginx-log
```

6. To remove the configuration files, run the following command:

```
/opt/rainier/bin/rainier-config-remove
```

7. To remove the remaining files, run the following commands:

```
rm -rf /opt/rainier
rm -rf /var/log/rainier-audit-log
rm -rf /var/logs/rainier-tool
rm -rf /var/logs/rainier-elastic-store
rm -rf /var/run/host-manager.sock
rm -rf /var/logs/rainier-logs
rm -rf /var/logs/rainier-ubi
rm -rf /var/opt/rainier-ubi
rm -f /etc/systemd/system/rainier.service
rm -f /etc/systemd/system/rainier-pipe.service
rm -f /etc/containers/containers.conf.d/rainier.conf
```

Note: When using Podman 4.0.x, the SELinux label of the `/var/run/podman/podman.sock` file is relabeled as `container_file_t` and the `podman.socket` service cannot be restarted, which generates an access error. Check whether there is a `container_file_t` label by running the following command:

```
ls -Z /var/run/podman/podman.sock
```

For example,

```
# ls -Z /var/run/podman/podman.sock
system_u:object_r:container_file_t:s0 /var/run/podman/podman.sock
```

If there is a `container_file_t` label, restore the original label by running the following command:

```
restorecon -F /var/run/podman/podman.sock
```

Appendix A: Migrating to Ops Center Administrator

When migrating your environment to Ops Center Administrator from another product such as Hitachi Storage Advisor Embedded, Hitachi Device Manager, or Storage Navigator, one of the key requirements is migrating host information. The following section describes how to use the Ops Center Administrator Scan Host Groups function to migrate host information when migrating from another product.

Migrating host information to Ops Center Administrator

When migrating, you must migrate host information, which can be done using the Scan Host Groups feature.

This feature enables you to automatically add servers into Ops Center Administrator from existing host groups in onboarded storage systems. (Ops Center Administrator creates or updates server objects based on host groups.) The Scan Host Group job uses host group information retrieved by using SVP and CCI.

Scan Host Groups does not change any storage configuration or related information (for example, path information). Existing information is maintained and only differential information is updated for server objects in Ops Center Administrator.

At a high level, the migration steps are as follows:

1. Install and configure Ops Center Administrator on a new server.
2. Onboard storage systems to Ops Center Administrator and temporarily manage storage systems using both products (existing product and Ops Center Administrator).
3. Migrate host information using Host Scan Groups. For details on how to use Scan Host Group as well as specifics about behavior when migrating information from different environments, see "Scanning host groups" in the *Hitachi Ops Center Administrator User Guide*.
4. As soon as you can manage the storage systems by using only Ops Center Administrator, disconnect the storage systems from the previous products.

Note: For more information about removing storage systems, see the documentation for the previous product.

Copying server objects from Hitachi Storage Advisor Embedded to Ops Center Administrator

When transitioning to Ops Center Administrator, Administrator automatically copies server information from Hitachi Storage Advisor Embedded when you onboard the storage system in Ops Center Administrator. Server object copy does not change any existing storage configuration or related information (for example, path information) and only differential information is updated for server objects in Ops Center Administrator.

Note that after you onboard the storage system and server object copy is complete, you must manage your servers by using Ops Center Administrator. You can no longer manage servers with Hitachi Storage Advisor Embedded because the provisioning function is disabled for data integrity reasons.

Server object copy results depend on the configuration of server WWNs and iSCSI names between Ops Center Administrator and Hitachi Storage Advisor Embedded for all storage systems that you onboard. This means that before you onboard any storage system, you must first ensure that the server configuration in Hitachi Storage Advisor Embedded including the server name, WWNs and iSCSI name is consistent for all storage systems you plan to onboard.

Because Ops Center Administrator server information takes priority over the information in Hitachi Storage Advisor Embedded, when server inconsistency is found, you may see different server configuration information in Ops Center Administrator than you do in Hitachi Storage Advisor Embedded.

Provisioning is reenabled for a storage system in Hitachi Storage Advisor Embedded after you remove it from Ops Center Administrator. For detailed instructions on how to onboard a storage system, see "Chapter 2: Adding a storage system" in the *Hitachi Ops Center Administrator User Guide*. If server object copy fails when onboarding, try manually refreshing the storage system.

For detailed instructions on how to switch to managing servers with Hitachi Storage Advisor Embedded, see "Switching to server management that uses Storage Advisor Embedded from another management tool" in the *Hitachi Storage Advisor Embedded User Guide*.

For detailed instructions on how to switch to managing servers with VSP One Block Administrator, see "Switching to server management that uses Hitachi VSP One Block Administrator from another management tool" in the *VSP One Block Administrator User Guide*.

Appendix B: Modifying the internal port allocated by Ops Center Administrator for host mode

When Ops Center Administrator is working in host mode, you can change the internal port number used by the container runtime by editing the `port.properties` file to avoid conflicts.

Modifying the internal port

Before proceeding the following procedure, we recommend you to create the backup of Ops Center Administrator and the `port.properties` file.

Procedure

1. Stop the services using the following command:
   ```
   # systemctl stop rainier
   ```
2. Open the `/opt/rainier/settings/port.properties` in a text editor.
3. Change the target port to the appropriate value.
4. Restart the services using the following command:
   ```
   # systemctl start rainier
   ```

Syntax rules for the port.properties file

General rules

Each line defines a key-value pair with the port name and its corresponding number.

```
<port-name>=<port-number>
```

- Do not add, remove, or comment out any lines in this file. Only modify existing values.
- Specified port numbers must be unique within the file.
- Ensure that the specified port numbers are not allocated to other programs installed on the same computer.

Range type specification

For range types, specify the starting and ending port numbers to define the range.

```
<port-name>.from=<starting-port-number>
<port-name>.to=<ending-port-number>
```

- Ensure that the range of port numbers does not overlap with any other specified ranges or individual port numbers in the file.
- Verify that the specified range of port numbers is not used by other programs on the same computer.

CLI ports

The following range type ports are allocated to the CLI container that manages the storage systems onboarded in Ops Center Administrator. These ports can be changed, but the range (width) must remain the same as the following initial settings:

```
port.internal.tcp.cli.from=21700
port.internal.tcp.cli.to=21799
port.internal.udp.cli.from=31000
port.internal.udp.cli.to=31999
port.external.udp.cli.from=33000
port.external.udp.cli.to=33999
```

When changing the range of these ports, ensure that the difference between the starting and ending port numbers remains the same as the initial settings.

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA

HitachiVantara.com/contact