

Hitachi Ops Center Administrator

10.8.2

Getting Started Guide

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

© 2019, 2022 Hitachi, Ltd. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including copying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Vantara LLC (collectively "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee may not make any other copies of the Materials. "Materials" mean text, data, photographs, graphics, audio, video and documents.

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara LLC at <https://support.hitachivantara.com/en-us/contact-us.html>.

Notice: Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi Vantara LLC.

By using this software, you agree that you are responsible for:

1. Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals; and
2. Verifying that your data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Notice on Export Controls. The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.

Hitachi and Lumada are trademarks or registered trademarks of Hitachi, Ltd., in the United States and other countries.

AI/AS/400e, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, GDPS, HyperSwap, IBM, Lotus, MVS, OS/390, PowerHA, PowerPC, RS/6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z14, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

Active Directory, ActiveX, Bing, Edge, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, the Microsoft corporate logo, the Microsoft Edge logo, MS-DOS, Outlook, PowerPoint, SharePoint, Silverlight, SmartScreen, SQL Server, Visual Basic, Visual C++, Visual Studio, Windows, the Windows logo, Windows Azure, Windows PowerShell, Windows Server, the Windows start button, and Windows Vista are registered trademarks or trademarks of Microsoft Corporation. Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

All other trademarks, service marks, and company names in this document or website are properties of their respective owners.

Copyright and license information for third-party and open source software used in Hitachi Vantara products can be found at <https://www.hitachivantara.com/en-us/company/legal.html>.

Contents

Preface.....	6
Intended Audience.....	6
Product version.....	6
Release notes.....	6
Document conventions.....	6
Conventions for storage capacity values.....	8
Accessing product documentation.....	9
Getting help.....	9
Comments.....	9
Chapter 1: Hitachi Ops Center Administrator environment.....	10
Minimum system requirements.....	10
Port requirements.....	12
Supported storage systems.....	21
Supported microcode/firmware.....	21
Supported file server.....	22
Supported fabric switches.....	22
Supported servers.....	22
Supported scalability limits.....	22
Chapter 2: Installing Ops Center Administrator.....	24
Installing Ops Center Administrator with the consolidated Ops Center preconfigured media.....	24
Installing Ops Center Administrator with the application installer.....	24
Example docker.service file for use with the application installer.....	33
Modifying the Ops Center Administrator port in virtual appliance manager	34
Installing Ops Center Administrator with stand-alone preconfigured media.....	34
Installing Hitachi Ops Center Administrator in a DHCP environment.....	34
Installing Hitachi Ops Center Administrator in a static environment.....	36
Changing the root password immediately after installation.....	39
Initial setup after installation.....	39
Changing the Elasticsearch memory setting.....	39
Changing the heap memory setting of the java process.....	40
Select a memory setting pattern.....	41

Changing the memory settings.....	42
Configuring SSO by integrating with Ops Center Common Services.....	43
Registering the Ops Center Administrator server with Ops Center.....	43
Enabling SSO with the Ops Center portal.....	45
Updating the Ops Center connection.....	46
Setting up SSL.....	46
Setting up SSL when Ops Center Administrator is running on the same server as Common Services.....	46
Generating and installing a signed SSL certificate.....	47
Installing a custom signed SSL certificate.....	48
Changing the si token authentication time-out in Ops Center Administrator.....	49
Enabling and downloading audit logs.....	49
Changing the Docker network address.....	50
Excluding directories from virus scanning.....	50
Creating Ops Center Users, User Groups, and Roles.....	50
Logging on to Ops Center Administrator.....	52
Launching the product from the Ops Center portal.....	52
Logging on through Ops Center SSO.....	52
Logging on from the Ops Center Administrator login screen.....	53
Logging on when Ops Center Administrator is not available.....	53
Chapter 3: Managing the Linux environment.....	56
Updating your Linux OS environment using Yellowdog Updater, Modified (YUM).....	56
Updating your container using Yellowdog Updater, Modified (YUM).....	56
Chapter 4: Upgrading Ops Center Administrator.....	61
Upgrading Ops Center Administrator by using the application installer.....	61
Upgrading Ops Center Administrator by using backup and restore.....	65
Chapter 5: Onboarding and configuring a storage system.....	68
Overview.....	68
Adding the first storage system.....	69
Adding a fabric switch.....	70
Adding servers	71
Chapter 6: Removing Ops Center Administrator.....	75
Removing Ops Center Administrator when using Docker.....	75
Removing Ops Center Administrator when using Podman.....	76
Appendix A: Migrating to Ops Center Administrator.....	77
Migrating host information to Ops Center Administrator.....	77

Copying server objects from Hitachi Storage Advisor Embedded to Ops
Center Administrator..... 78

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.

Intended Audience

This document is intended for system administrators, Hitachi Vantara representatives, and authorized service providers who configure and operate Virtual Storage Platform storage systems with Hitachi Ops Center Administrator.

Readers of this document should be familiar with the following:

- RAID storage systems and their basic functions.
- Volume creation and management.
- Pool creation and management.
- Parity group creation and management.

Product version

This document revision applies to Hitachi Ops Center Administrator version 10.8.2 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>.






Document conventions

This document uses the following typographic conventions:

Convention	Description
Bold	<ul style="list-style-type: none"> Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click OK. Indicates emphasized words in list items.
<i>Italic</i>	<ul style="list-style-type: none"> Indicates a document title or emphasized words in text. Indicates a variable, which is a placeholder for actual text provided by the user or for output by the system. Example: <code>pairedisplay -g group</code> <p>(For exceptions to this convention for variables, see the entry for angle brackets.)</p>
Monospace	Indicates text that is displayed on screen or entered by the user. Example: <code>pairedisplay -g oradb</code>
< > angle brackets	<p>Indicates variables in the following scenarios:</p> <ul style="list-style-type: none"> Variables are not clearly separated from the surrounding text or from other variables. Example: <code>Status-<report-name><file-version>.csv</code> Variables in headings.
[] square brackets	Indicates optional values. Example: [a b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a b } indicates that you must choose either a or b.
vertical bar	<p>Indicates that you have a choice between two or more options or arguments. Examples:</p> <p>[a b] indicates that you can choose a, b, or nothing.</p> <p>{ a b } indicates that you must choose either a or b.</p>

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

Icon	Label	Description
	Note	Calls attention to additional information.

Icon	Label	Description
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
	Important	Highlights information that is essential to the completion of a task.
	Caution	Warns the user of adverse conditions and/or consequences (for example, disruptive operations, data loss, or a system crash).
	CAUTION	Warns the user of a hazardous situation that, if not avoided, could result in major or minor injury.
	WARNING	Warns the user of a hazardous situation which, if not avoided, could result in death or serious injury.

Conventions for storage capacity values

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

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

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

Logical capacity unit	Value
1 block	512 bytes
1 cylinder	Mainframe: 870 KiB

Logical capacity unit	Value
	Open-systems <ul style="list-style-type: none"> ▪ OPEN-V: 960 KiB ▪ Others: 720 KiB
1 KiB	1,024 (2 ¹⁰) bytes
1 MiB	1,024 KiB or 1,024 ² bytes
1 GiB	1,024 MiB or 1,024 ³ bytes
1 TiB	1,024 GiB or 1,024 ⁴ bytes
1 PiB	1,024 TiB or 1,024 ⁵ bytes
1 EiB	1,024 PiB or 1,024 ⁶ bytes

Accessing product documentation

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

Getting help

The [Hitachi Vantara Support Website](https://support.hitachivantara.com/en_us/contact-us.html) 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](https://community.hitachivantara.com) is a global online community for Hitachi Vantara customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Comments

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

Thank you!


Chapter 1: 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.

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 (Docker and Podman)

Server	Minimum requirements
Hypervisor operating system	VMware® ESXi 6.0 or higher, Microsoft Hyper-V, Linux KVM <div> Note:<ul style="list-style-type: none">▪ Use the product installers when running Hyper-V or KVM.▪ Only VMware supports OVA installations.</div>
Container runtime version for installation from tar file	Docker <ul style="list-style-type: none">▪ Version 18 (minimum supported – v18.09.6)▪ Version 19 (minimum supported – v19.03.0)▪ Version 20 (minimum supported – v20.10.5) Podman Version 3.3.x
Operating system for installation from tar file Linux	Docker Linux (Except for Red Hat Enterprise Linux 8.x and Oracle Linux 8.x)

Server	Minimum requirements
	<p>Podman</p> <p>Red Hat Enterprise Linux 8.1, 8.2, and 8.4</p> <p>Oracle Linux 8.1, 8.2, and 8.4</p> <p>For details on specific supported versions of Linux, see the Compatibility matrix</p>
Access for installation from tar file	Root user
Recommended drive type	SSD or a higher performance drive type
Available disk space	<ul style="list-style-type: none"> 80 GiB under the Docker root directory (default directory: <code>/var/lib/docker</code>) 80 GiB under the Podman root directory (default directory: <code>/var/lib/container</code>) <p>In addition, temporary total of 10 GiB available space will be required for installation using the application installer. This consists of 10 GiB under <code>/var/tmp</code>.</p>
Memory	<p>16 GiB RAM</p> <div>  <p>Note: 32 GiB RAM is highly recommended for an environment where Ops Center Administrator manages 20 or more storage systems. For details, refer to: Changing the Elasticsearch memory setting (on page 39).</p> </div>
CPU	4 vCPUs
A client computer that can run a supported browser	<p>One of the following:</p> <ul style="list-style-type: none"> Google Chrome (latest version of the stable channel) Firefox ESR 91.0 or later Internet Explorer 11 or later (requires enabling the font download option) Microsoft Edge (latest version of the stable channel. Internet Explorer mode is not supported. Microsoft Edge for Linux is not supported.)

Requirements for using program products

To use Hitachi Dynamic Tiering for pools and Hitachi 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
80/tcp	Used for accessing the Ops Center Administrator UI from Ops Center Administrator clients.
443/tcp	Used for accessing the Ops Center Administrator UI from Ops Center Administrator clients.
161/tcp	Reserved.
161/udp	Reserved.
162/tcp	Reserved.
162/udp	Used for receiving SNMP traps from supported storage systems and file servers. 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.
8085/tcp	Used to manage internal services included in the container runtime.

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	80/tcp	Ops Center Administrator server

Originator		Destination	
Port number	Machine	Port number	Machine
any/tcp	Ops Center Administrator client	443/tcp	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	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ VSP 5000 series ▪ VSP E series (SVP/controller) ▪ VSP G1x00, VSP F1500 ▪ VSP G200, G/F400, G/F600, G/F800 (SVP/controller) 	<p>You can change the port number for the following models:</p> <ul style="list-style-type: none"> ▪ VSP E series ▪ VSP G200, G/F400, G/F600, G/F800 (SVP)

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
			<ul style="list-style-type: none"> VSP G/F350, G/F370, G/F700, G/F900 (SVP/controller) VSP N series (SVP/controller) 	<ul style="list-style-type: none"> VSP G/F350, G/F370, G/F700, G/F900 (SVP) VSP N series (SVP)
any/tcp	Ops Center Administrator server	1099/tcp	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> VSP 5000 series 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) 	-

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
any/tcp	Ops Center Administrator server	51100/tcp	<ul style="list-style-type: none"> VSP 5000 series VSP G1x00, VSP F1500 	<p>Unused port numbers are allocated automatically from the described range during storage system registration and a firewall is also set. The allocated ports numbers are used when starting the storage system.</p> <p>For details on how to confirm the port numbers that the SVP uses, see the documentation for the storage system.</p>
any/tcp	Ops Center Administrator server	51100-51355/tcp	<ul style="list-style-type: none"> 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) 	<p>Unused port numbers are allocated automatically from the described range during storage system registration and a firewall is also set. The allocated ports numbers are used when starting the storage system.</p> <p>For details on how to confirm the port numbers that the SVP uses, see the documentation for the storage system.</p>

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
34001-34008/ udp	Ops Center Administrator server	31001/udp	<ul style="list-style-type: none"> VSP 5000 series VSP G1x00, VSP F1500 	-
34001-34008/ udp	Ops Center Administrator server	31001-31002/ udp	<ul style="list-style-type: none"> 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) 	-
any/tcp	Ops Center Administrator server	8443/tcp	<ul style="list-style-type: none"> VSP G200, G/F400, G/F600, G/F800 (controller) in which a NAS Module is included VSP G/F350, G/F370, G/F700, G/F900 (controller) VSP N series (controller) 	This setting is required when using a NAS Manager that exists on a storage system with a built-in NAS module.

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	<ul style="list-style-type: none"> ▪ 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) 	<p>This setting is required when using SSL for Storage Navigator.</p> <p>For</p> <ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ VSP 5000 series ▪ VSP E series (SVP) ▪ VSP G1x00, F1500 	-

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
			<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> VSP 5000 series VSP G1x00, F1500 	<p>Unused port numbers are allocated automatically from the described range during storage system registration and a firewall is also set. The allocated ports numbers are used when starting the storage system.</p> <p>For details on how to confirm the port numbers used, see the documentation for your storage system.</p>
any/tcp	Ops Center Administrator client	51100-51355/tcp	<ul style="list-style-type: none"> 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) 	<p>Unused port numbers are allocated automatically from the described range during storage system registration and a firewall is also set. The allocated ports numbers are used when starting the storage system.</p> <p>For details on how to confirm the port numbers used, see the documentation for your storage system.</p>

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
any/tcp	Ops Center Administrator client	any/tcp	<ul style="list-style-type: none"> 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 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	<p>Currently, only Microsoft Active Directory is supported for LDAP authentication.</p> <p>This port number is generally used. However, a different port number might be used for an authentication server.</p>

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
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*	Fabric switch	<p>This setting is required when changing zone settings according to attaching or detaching volumes.</p> <p>This port number is generally used. However, a different port number might be used for fabric switches.</p>

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:

- 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

TLS

The supported version of TLS is 1.2.

Supported microcode/firmware

Ops Center Administrator supports the following:

- 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 83-04-2x or later.
- VSP G1x00, F1500 with microcode version 80-05-2x or later.
- VSP N series with microcode version 83-06-0x or later.



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

Supported file server

To use any new features included in a storage system firmware/microcode upgrade, you must also upgrade Ops Center Administrator.

Hitachi Ops Center Administrator supports the following file server configuration:

- **Hitachi NAS platform (HNAS) firmware version:** 13.1
- **System management unit (SMU) software:** version 13.1

Supported fabric switches

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

- Brocade: Fabric OS 7.x through 8.2.2a
- Cisco: MDS NX-OS Release 6.2(9) or later

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®

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

- [Installing Ops Center Administrator with the consolidated Ops Center preconfigured media \(on page 24\)](#)
- [Installing Ops Center Administrator with the application installer \(on page 24\)](#)
- [Installing Ops Center Administrator with stand-alone preconfigured media \(on page 34\)](#)

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 \(on page 39\)](#).

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 multiple container runtimes such as Docker and Podman to the host OS. Always use a single container runtime.
- 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 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.

For the Docker environment, run:

```
# systemctl restart docker
```

For the Podman environment, run:

```
# 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.

Verify the following:

- You have root access to the OS where you plan to install Ops Center Administrator.
- 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
```

- The OS running `firewalld` (for example, RHEL 7 or later) is configured to allow communication between containers as follows:
 - Enable communication by adding the following to the trusted zone:
 - For Docker, add `docker0`.
 - For Podman add `cni-podman0`.

- The following example is for Docker:

```
# firewall-cmd --zone=trusted --change-interface=docker0 --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.

When using Docker:

- Do not set the following service options to false:
 - `icc`: Enable inter-container communication (default true).
 - `ip-forward`: Enable `net.ipv4.ip_forward` (default true).
 - `icc`: Enable IP masquerading (default true).
 - `iptables`: Enable addition of iptables rules (default true).
- If the FORWARD chain does not contain the DOCKER chain in the iptables, restart the Docker service by running the following command:

```
# systemctl restart docker
```

- The recommended settings for using the application installer are as follows:
 - If you use the JSON-file logging driver, set the maximum log size to 50 MiB and the maximum number of files to 3.

```
--log-opt max-size=50m --log-opt max-file=3
```

- Set `ExecReload`.

```
ExecReload=/bin/kill -s HUP $MAINPID
```

- Set `Delegate` to yes.

```
Delegate=yes
```

- Set `KillMode` to process.

```
KillMode=process
```

- Set `Restart`.

```
Restart=on-failure
```

Refer to the example provided for general information about the `Docker.service` file.

When using Podman:

- 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.

- If the upgrade of Podman is suppressed, unlock the suppression temporarily before starting the installation. After completing the installation, suppress the upgrade of Podman again.
- If you cannot use YUM to install Podman because your management server is not connected to the network, you must obtain the Podman software from the OS media (ISO image or CD-ROM).

The supported version of Podman (3.3.x) is available with v8.5 of Red Hat Enterprise Linux and Oracle Linux. Therefore, regardless of the OS version that you are using, download v8.5 of the OS to get the required Podman version.

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.*
```

- The available space on the server is 100 GiB including temporary space. For details, refer to [Minimum system requirements \(on page 10\)](#).
- 16 GiB RAM



Note: Before starting the installation, note the following:

- 32 GiB RAM is highly recommended for an environment where Ops Center Administrator manages 20 or more storage systems. For details, refer to: [Changing the Elasticsearch memory setting \(on page 39\)](#).
- As a best practice, do not install Ops Center Administrator in a location running other applications.

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 host's IP:

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

- d. 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.

- e. 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: 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 `https://ip-address/vam` in the address bar.
The login credentials are `sysadmin/sysadmin`.
 - b. In the **Network** tab, enter the SNMP IP address for the storage system.
5. For Podman, suppress the upgrade of Podman to avoid unintentionally upgrading to the unsupported version.

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

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 the credentials used are sysadmin/sysadmin.
- Check your container network configuration and make sure your container runtime is working properly. Container runtime requires its network interface (`docker0` for Docker, or `cni-podman0` for Podman) to be in a trusted zone in your operating system.
- 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 setting of the HTTP server and whether the repository data which is gathered by the `reposync` command exists correctly.
- If the installation fails and an error message `iptables: No chain/target/match by that name` is output in the Ops Center Administrator installation log, uninstall Ops Center Administrator and restart the Docker service by running the command:

```
# systemctl restart docker
```

Then, retry the installation.

- Delete all Ops Center Administrator containers, images, and files and then start the installation again.
- Check the Docker or Podman logs.
- Consult the documentation of your container runtime for more information on how to do this.
- Journal entries may have additional information about the error. To view the journal log, connect to the host with the root account and run these commands:
 - Docker: `journalctl --no-pager -u docker`
 - Podman: `journalctl --no-pager -u rainier`

If the issue persists, collect the installation log which 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.

To remove files, run the command:

```
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 (use `podman` instead of `docker` depending on your container runtime):

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

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

```
[root@hid ~]# docker 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
```

For Docker, run the following to restart the service:

```
[root@hid ~]# service docker restart
Redirecting to /bin/systemctl restart docker.service
```

For Podman, run the following to restart the service:

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

If the Ops Center Administrator installation succeeded, but registering with Ops Center Common Services failed, run the **`setupcommonservice`** command after the upgraded Ops Center Administrator goes online.

Next steps

Required

- Change the root password as described in [Changing the root password immediately after installation \(on page 39\)](#).
- 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 information on using the `docker.service` file, see [Example docker.service file for use with the application installer \(on page 33\)](#).
- For more information on changing the Ops Center Administrator port number, see [Modifying the Ops Center Administrator port in virtual appliance manager \(on page 34\)](#).

Example docker.service file for use with the application installer

If you install Ops Center Administrator with the application installer, refer to the example `docker.service` file contents for location and recommended Docker settings for log rotation, Delegate, and KillMode.

This is an example of the location of recommended Docker settings for log rotation (if you use the JSON-file logging driver), Delegate and KillMode. They are set in the `/usr/lib/systemd/system/docker.service` file. This example is for CentOS and Fedora operating systems.

File path: `/usr/lib/systemd/system/docker.service`

```
[Unit]
Description=Docker Application Container Engine
Documentation=https://docs.docker.com
BindsTo=containerd.service
After=network-online.target \
    firewallld.service containerd.service
Wants=network-online.target
Requires=docker.socket

[Service]
Type=notify
ExecStart=/usr/bin/dockerd \
    --containerd=/run/containerd/containerd.sock \
    --log-opt max-size=50m --log-opt max-file=3
ExecReload=/bin/kill -s HUP $MAINPID
TimeoutSec=0
RestartSec=2
Restart=always
StartLimitBurst=3
StartLimitInterval=60s
LimitNOFILE=infinity
LimitNPROC=infinity
LimitCORE=infinity
TasksMax=infinity
Delegate=yes
KillMode=process

[Install]
WantedBy=multi-user.target
```

Modifying the Ops Center Administrator port in virtual appliance manager

You can change the port used by 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 using the IP address for your Ops Center Administrator deployment: `https://ip-address/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. In the **Network** tab, 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`.

Installing Ops Center Administrator with stand-alone preconfigured media

Use the stand-alone preconfigured media installation to install in either a static environment or in a DHCP environment.

You can also deploy the Ops Center Administrator OVA file as a VMware vSphere High Availability cluster or configure vSphere Fault Tolerance.

Installing Hitachi Ops Center Administrator in a DHCP environment

If your environment includes DHCP servers, you can use the Virtual Appliance Manager to set up your Ops Center Administrator server.

Before you begin

The initial setup of supported storage systems has been completed by an authorized service provider.

Procedure

1. From the installation media, deploy the Ops Center Administrator OVA to the ESXi host.

2. Change the VM memory size to the recommended value: 16 GiB RAM.



Note: 32 GiB RAM is highly recommended for an environment where Ops Center Administrator manages 20 or more storage systems. For details, refer to: [Changing the Elasticsearch memory setting \(on page 39\)](#).

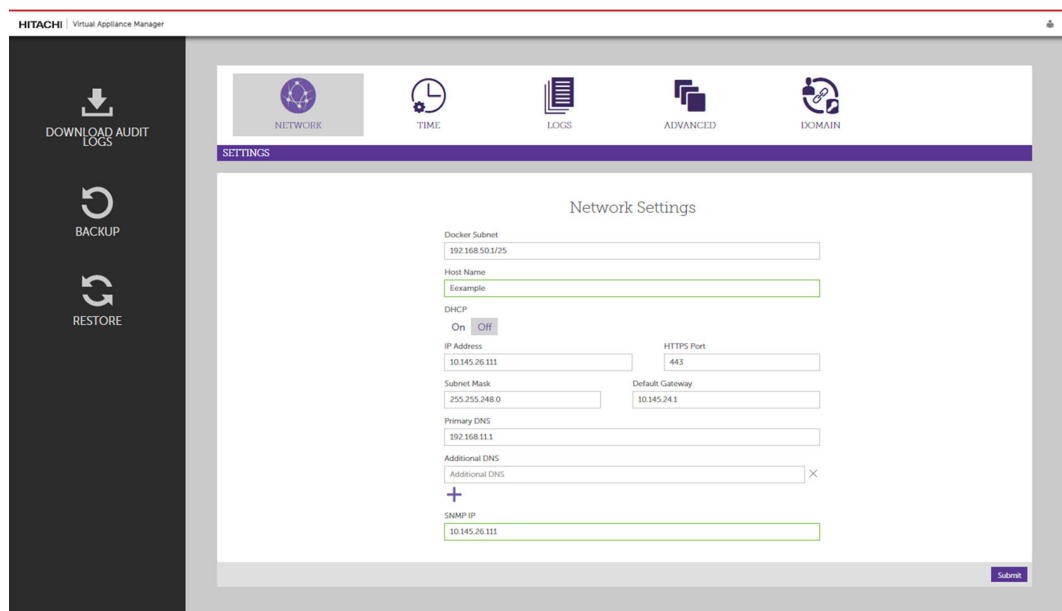
3. Start the Ops Center Administrator virtual machine.
4. In the vSphere® client, wait for the **System status** to change to **Online**.

The status is just below the banner in the virtual machine console.

```

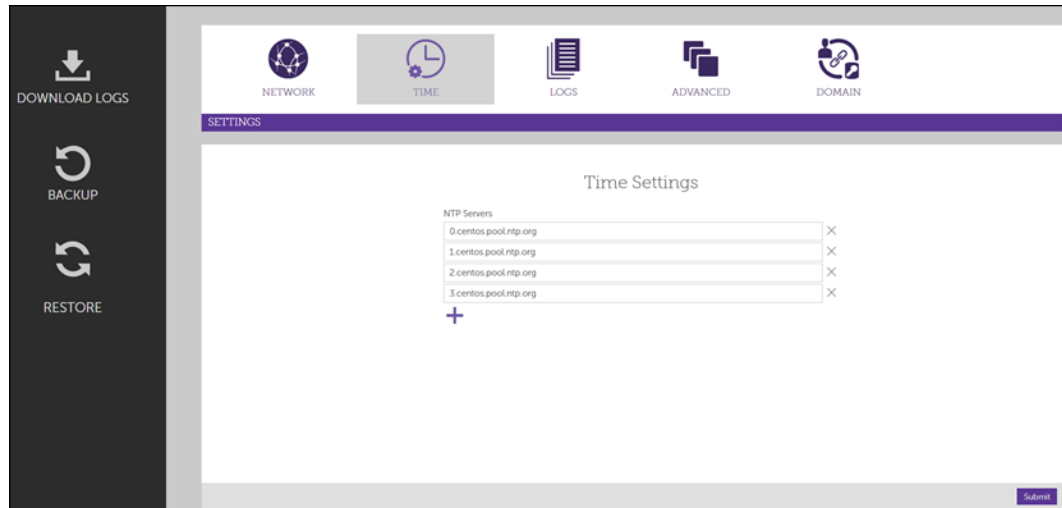
*****
***** Ops Center Administrator *****
*****
* Alt + F2 will take you to the console
* Please browse to https://172.25.64.226 for service UI
* To manage this appliance, please browse to https://172.25.64.226/vam
* In case this appliance was not able to acquire a DHCP IP address,
  please do the following:
  - In the below prompt, log on with the service account
    (provided in the accompanied manual)
  
```

5. Open a browser and enter `https://ip-address/vam` in the address bar.
The default credentials for a preconfigured media installation are:
 - User name: `service`
 - Password: `Chang3Me!`
6. Change your password.
 - a. Click **User** and select **Change password**.
 - b. Enter your new password.
7. From the Virtual Appliance Manager menu, click **Network** to configure the network settings.



- a. If your data center is using the IP address scheme 192.168.*.*, make sure you provide another IP range that is not currently used in your environment. This is the specified range used by Ops Center Administrator.
 - b. Set the host name for the virtual machine.
 - c. Set **DHCP** to On.
 - d. Click **Submit**.
8. (Optional) From the Virtual Appliance Manager menu, click **Time** and add Network Time Protocol (NTP) servers to the virtual machine.

Adding NTP servers verifies that the Ops Center Administrator servers are synchronized with the storage system environment.



- a. Click **+** to add a field for an NTP Server.
- b. Enter the host name of the NTP server.
- c. Click **Submit**.

Next steps

- Change the root password as described in [Changing the root password immediately after installation \(on page 39\)](#).
- Log in 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 for the initial log in to Ops Center Administrator.

Installing Hitachi Ops Center Administrator in a static environment

If you do not have a DHCP server, use the command-line interface to indicate the static IP address of the Ops Center Administrator server.

Procedure

1. From the installation media, deploy the Ops Center Administrator OVA to the ESXi host.
2. Change the VM memory size to the recommended value: 16 GiB RAM.



Note: 32 GiB RAM is highly recommended for an environment where Ops Center Administrator manages 20 or more storage systems. For details, refer to: [Changing the Elasticsearch memory setting \(on page 39\)](#).

3. Start the Ops Center Administrator virtual machine.
4. In the vSphere® client, wait for the **System status** to change to Online.

The status is just below the banner in the virtual machine console.

```
=====
Ops Center Administrator
=====

* Alt + F2 will take you to the console

* Please browse to https://172.25.64.226 for service UI

* To manage this appliance, please browse to https://172.25.64.226/vam

* In case this appliance was not able to acquire a DHCP IP address,
  please do the following:
  - In the below prompt, log on with the service account
    (provided in the accompanied manual)
```

5. Press **Alt + F2**.
6. Log in with the root account using the default password: 3k0\$Pe9dJyJy29HAI2mS.
7. Enter the command `ip-change`.
The Change IP Address Utility opens.
8. Enter your settings at the prompts.
9. Restart the VM to ensure that it has the IP address.
10. Open a browser and enter `https://ip-address/vam` in the address bar. The default credentials for the preconfigured media installation are:
Username: `service`
Password: `Chang3Me!`
11. Change your password.
 - a. Click **User** and select **Change password**.
 - b. Enter your new password.
12. From the menu, click **Network** to configure the network settings.

HITACHI | Virtual Appliance Manager

SETTINGS

Network Settings

Docker Subnet
192.168.50.1/25

Host Name
Example

DHCP
On ☐ Off ☒

IP Address
10.145.26.111

Subnet Mask
255.255.248.0

HTTPS Port
443

Default Gateway
10.145.24.1

Primary DNS
192.168.11.1

Additional DNS
Additional DNS

SNMP IP
10.145.26.111

Submit

- a. If your data center is using the IP address scheme 192.168.*.*, make sure you provide another IP range that is not currently used in your environment. This is the specified range used by Ops Center Administrator.
 - b. Set the host name for the virtual machine.
 - c. Set **DHCP** to **Off**.
 - d. Enter the IP address of the Ops Center Administrator server.
 - e. Click **Submit**.
13. (Optional) From the Virtual Appliance Manager menu, click **Time** and add Network Time Protocol (NTP) servers to the virtual machine.

Adding NTP servers verifies that the Ops Center Administrator servers are synchronized with the storage system environment.

SETTINGS

Time Settings

NTP Servers

- 0.centos.pool.ntp.org
- 1.centos.pool.ntp.org
- 2.centos.pool.ntp.org
- 3.centos.pool.ntp.org

+

Submit

- a. Click **+** to add a field for an NTP Server.
- b. Enter the host name of the NTP server.
- c. Click **Submit**.

Next steps

- Change the root password as described in [Changing the root password immediately after installation \(on page 39\)](#).
- Log on to Ops Center Administrator and onboard a storage system.
- Get a digitally signed SSL certificate from a trusted certificate authority (CA) by sending the CA a certificate signing request (CSR). After you obtain the signed certificate, you can import it to the server. By default, the Ops Center Administrator installation package comes with a self-signed certificate that you can use to initially log on to Ops Center Administrator.

Changing the root password immediately after installation

You must change the root password after you finish the installation.

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 with the root account using the default password:
`3kO$Pe9dJyJy29HAI2mS`
3. Run the command `passwd root`.
4. Enter the new password when prompted.

Initial setup after installation

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

- Elasticsearch memory
- SSO
- SSL
- Si token authentication time-out
- audit logging
- Docker network address
- users, groups, and roles

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

Changing the Elasticsearch memory setting

If more than 16 GiB RAM is set on the Ops Center Administrator server, change the Elasticsearch memory setting.

Procedure

1. Open the Ops Center Administrator server console:
 - For VM installations, either open an SSH connection to the VM or open the VMware console and press Alt+F2 to reach the console.
 - For physical server installations, open the command prompt.
2. Log in by using the root account.
3. If you installed using the preconfigured media, go to the next step. If you installed by using the application installer, copy the tar file `ops-center-administrator-xx.tar.gz` from the installation media to any folder, unzip it, and navigate to the unzipped folder.
4. From the command prompt, run the following command:


```
elasticsearch-memory-setting
```
5. At the prompts, enter the following:
 - a. Enter username for the service account credentials:
Enter the service account user name.
 - For Ops Center preconfigured media or application installer installations, use the `sysadmin` credentials.
 - For stand-alone preconfigured media installations, use the `service` credentials.
 - a. Enter `<users> Password:`
Enter the password for the user account.
 - b. Enter the Elasticsearch heap memory size[GiB]:
Enter half of the physical memory size. In the case of 32 GiB physical memory size, enter 16.
 - c. Ensure that the host memory size is twice as large as the specified value. Do you want to proceed? [y/n]
Enter `y`.

Ops Center Administrator automatically restarts. Wait until the user interface is accessible.
6. To confirm that the new value is applied to MEM USAGE of Elasticsearch, run the following command:


```
Docker: docker stats
```

```
Podman: podman stats
```

Changing the heap memory setting of the java process

This module covers how to change the heap memory setting of the java process on the rainier container according to the scale of the managed resources.

Select a memory setting pattern

In an environment where a large number of volumes are attached to servers, an Ops Center Administrator internal service (rainier) can stop working, and the following message is displayed:

```
Failed to get data from API. Try again.
```

Why this happens

This sometimes occurs when a large number of volumes are attached to servers. The following table provides estimated configurations for which the symptom might occur.

Average number of servers per volume	Number of volumes
1	30,000 or higher
2	12,000 or higher
4	6,000 or higher
8	3,000 or higher
16	1,500 or higher
32	800 or higher
64	400 or higher
128	200 or higher

Select a memory setting pattern

When the above conditions are met, decide on a memory setting pattern (A or B) based on the following table and follow the steps in [Changing the memory settings \(on page 42\)](#).

Average number of servers per volume	Number of volumes	Memory setting pattern
1	30,000 or higher	A
2	12,000 to 39,999	A
	40,000 or higher	B
4	6,000 to 19,999	A
	20,000 or higher	B
8	3,000 to 9,999	A
	10,000 or higher	B

Average number of servers per volume	Number of volumes	Memory settting pattern
16	1,500 to 4,999	A
	5,000 or higher	B
32	800 to 2,399	A
	2,400 or higher	B
64	400 to 1,199	A
	1,200 or higher	B
128	200 to 599	A
	600 or higher	B

Prepare additional usable physical memory based on the memory setting pattern that you selected in the table above:

- Memory setting pattern A: + 2 GiB
- Memory setting pattern B: + 6 GiB

Changing the memory settings

Change the java process memory settings by doing the following:

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 account.
3. Enter the following command in the terminal:
`/opt/rainier/bin/rainier-memory-setting`
4. At the prompts, enter the following:

- a. Enter the new java process memory size[MiB] 2048, 4096, or 8192:

Estimate the necessary memory size by referring to [Select a memory setting pattern \(on page 41\)](#).

– For memory setting pattern A: Enter 4096

– For memory setting pattern B: Enter 8192

If your configuration does not match either of these memory patterns, enter 2048, which is the default setting. You can exit from the command if the current setting is 2048.

- b. `[Entered-Memory-Size]` will be set for java process. Do you want to proceed? `[y/n]`:

Enter `y` to proceed.

- c. Restart Ops Center Administrator to reflect the new memory setting:

Do you want to restart Ops Center Administrator? `[y/n]`

Enter `y`.

Ops Center Administrator automatically restarts. Wait until the user interface is accessible.

5. To confirm that the new value is applied to MEM USAGE of the java process, run the `/opt/rainier/bin/rainier-memory-setting` command again.

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. Refer to [Registering the Ops Center Administrator server with Ops Center \(on page 43\)](#) to learn how to use the command. 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's access token.



Note: If you installed using the Ops Center OVA, Ops Center Administrator is already registered in Common Services.

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 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.

For the Docker environment, run:

```
# systemctl restart docker
```

For the Podman environment, run:

```
# 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 root.
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.

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.

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:

For the Docker environment:

```
# systemctl restart docker
```

For the Podman environment:

```
# 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 \(on page 43\)](#).

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 the user's identity 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 credentials.
2. Note the hostname of the VM (`#hostname`).
3. Run the `openssl` command and provide the Authentication sha1 or sha256, depending upon the required security. Give the Fully Qualified Domain Name for host name.

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

The system returns the message: Generating a 2048 bit RSA 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 virtual appliance manager URL in the address bar.
 For example, `https://ip-address/vam`
7. Click **Advanced**.
8. Click the **Certificate Settings** tab.
9. 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:

- Docker:

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

- Podman:

```
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.crt` file:

```
# openssl req -new -newkey rsa:2048 -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 the Ops Center Administrator virtual appliance manager UI.
6. From the **Advanced** menu, 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

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

Procedure

1. Log in to the virtual appliance manager at `https://ip-address/vam`.
 - For Ops Center preconfigured media or application installer installations, use the `sysadmin` credentials.
 - For stand-alone preconfigured media installations, use the `service` credentials.
2. Select **Advanced Option > Service Settings**.
3. Change **si.token.expirationDuration** to `6000`. The duration setting is in seconds.
4. Click **Submit**.

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

Procedure

1. Log into the virtual appliance manager at `https://ip-address/vam`.
 - For Ops Center preconfigured media or application installer installations, use the `sysadmin` credentials.
 - For stand-alone preconfigured media installations, use the `service` credentials.
2. Click **Logs** and then click **Audit Logs**.
3. To enable audit log collection, click **Enabled**. You can change the **Retention Period**.
4. To download the log, click **Download Audit Logs**.

Changing the Docker network address

By default, the Ops Center Administrator Docker uses the 192.168.50.1/25 network. If you must change the network address, do the following:

Procedure

1. Check the current setting.

```
# systemctl status docker | grep bip
```

2. Stop the Docker service.

```
# systemctl stop docker
```

3. Edit the Docker configuration file `/usr/lib/systemd/system/docker.service` and change the IP address as follows:

```
ExecStart=/usr/bin/dockerd --bip=192.168.50.0/16 \
```

4. Reload the configuration file by running the following command:

```
# systemctl daemon-reload
```

5. Start the Docker service by running the following command:

```
# systemctl start docker
```

6. Confirm that the setting has been updated:

```
# systemctl status docker | grep bip
```

Excluding directories from virus scanning

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

- `/opt/rainier`
- `/var/logs`
- Volume data directory for container runtime:
 - Docker: `/var/lib/docker/volumes`
 - Podman: `/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.

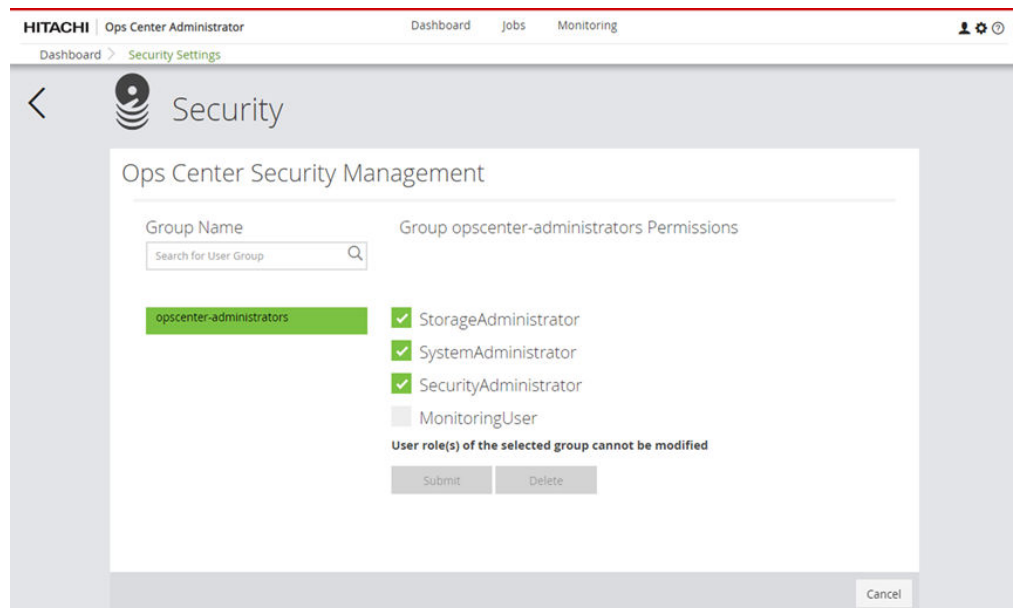
You can create users and user groups in Ops Center Common Services and assign roles to user groups in Ops Center Administrator. Role-Based Access Control (RBAC) either allows or denies users (and associated user groups) access to Ops Center Administrator based on the existing mapping between Common Services 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, 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 logging in through Ops Center SSO. Click (**Settings**) > **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, type in the user group name you created.
4. Select the desired Ops Center Administrator user roles for the user group and click **Update**.

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 \(on page 52\)](#)
- [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**.

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 documentation for your storage system.

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/9340006XXXXX/emergency.do` (where the model number is '934000' and '6XXXXX' indicates the system serial number)
- For VSP E990 storage systems, enter `https://IP-address-of-the-SVP/dev/storage/9360004XXXXX/emergency.do` (where the model number is '936000' and '4XXXXX' indicates the system serial number)
- For VSP E1090 or E1090H storage systems, enter `https://IP-address-of-the-SVP/dev/storage/9380007XXXXX/emergency.do` (where the model number is '938000' and '7XXXXX' 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/8320004XXXXX/emergency.do` (where the model number is '8320004' and '4XXXXX' 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/8340004XXXXX/emergency.do` (where the model number is '8340004' and '4XXXXX' 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/8360004XXXXX/emergency.do` (where the model number is '8360004' and '4XXXXX' indicates the system serial number)
- For VSP G/F350 storage systems, enter `https://IP-address-or-host-name-of-the-SVP/dev/storage/8820004XXXXX/emergency.do` (where the model number is '882000' and '4XXXXX' 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/8860004XXXXX/emergency.do` (where the model number is '886000' and '4XXXXX' 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 appears, click **Yes**.

7. If an Adobe Flash Player local storage area pop-up dialog box appears, 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)

Update your container using Yellowdog Updater, Modified (YUM).

Complete the following steps to use YUM to update your container:

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`.

```
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
```

2. Search for the container that requires updating:

```
docker exec -it container_id bash
```

3. Save the repository.

```
cd /etc/yum.repos.d
```

```
mv hv.repo hv.repo.old
```

```
touch hv.repo
```

4. Copy the following contents to `/etc/yum.repos.d/oracle-linux-ol7.repo`:

```
[ol7_latest]
name=Oracle Linux $releasever Latest ($basearch)
baseurl=https://yum$ociregion.$ocidomain/repo/OracleLinux/OL7/latest/
$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=1
[ol7_u0_base]
name=Oracle Linux $releasever GA installation media copy ($basearch)
baseurl=https://yum$ociregion.$ocidomain/repo/OracleLinux/OL7/0/base/
$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0
[ol7_u1_base]
name=Oracle Linux $releasever Update 1 installation media copy
($basearch)
baseurl=https://yum$ociregion.$ocidomain/repo/OracleLinux/OL7/1/base/
$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
```

```

enabled=0
[ol7_u2_base]
name=Oracle Linux $releasever Update 2 installation media copy
($basearch)
baseurl=https://yum$ociregion.$ocidomain/repo/OracleLinux/OL7/2/base/
$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0
[ol7_u3_base]
name=Oracle Linux $releasever Update 3 installation media copy
($basearch)
baseurl=https://yum$ociregion.$ocidomain/repo/OracleLinux/OL7/3/base/
$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0
[ol7_u4_base]
name=Oracle Linux $releasever Update 4 installation media copy
($basearch)
baseurl=https://yum$ociregion.$ocidomain/repo/OracleLinux/OL7/4/base/
$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0
[ol7_u5_base]
name=Oracle Linux $releasever Update 5 installation media copy
($basearch)
baseurl=https://yum$ociregion.$ocidomain/repo/OracleLinux/OL7/5/base/
$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0
[ol7_u6_base]
name=Oracle Linux $releasever Update 6 installation media copy
($basearch)
baseurl=https://yum$ociregion.$ocidomain/repo/OracleLinux/OL7/6/base/
$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0
[ol7_u7_base]
name=Oracle Linux $releasever Update 7 installation media copy
($basearch)
baseurl=https://yum$ociregion.$ocidomain/repo/OracleLinux/OL7/7/base/
$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0
[ol7_u8_base]
name=Oracle Linux $releasever Update 8 installation media copy

```

```

($basearch)
baseurl=https://yum$ociregion.$ocidomain/repo/OracleLinux/OL7/8/base/
$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0
[ol7_u9_base]
name=Oracle Linux $releasever Update 9 installation media copy
($basearch)
baseurl=https://yum$ociregion.$ocidomain/repo/OracleLinux/OL7/9/base/
$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0
[ol7_optional_latest]
name=Oracle Linux $releasever Optional Latest ($basearch)
baseurl=https://yum$ociregion.$ocidomain/repo/OracleLinux/OL7/optional/
latest/$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0
[ol7_addons]
name=Oracle Linux $releasever Add ons ($basearch)
baseurl=https://yum$ociregion.$ocidomain/repo/OracleLinux/OL7/addons/
$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0
[ol7_MODRHCK]
name=Latest RHCK with fixes from Oracle for Oracle Linux $releasever
($basearch)
baseurl=https://yum$ociregion.$ocidomain/repo/OracleLinux/OL7/MODRHCK/
$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
priority=20
enabled=0
[ol7_leapp]
name=Leapp Upgrade Utilities for Oracle Linux $releasever ($basearch)
baseurl=https://yum$ociregion.$ocidomain/repo/OracleLinux/OL7/leapp/
$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0
[ol7_latest_archive]
name=Oracle Linux $releasever Latest ($basearch) - Archive
baseurl=https://yum$ociregion.$ocidomain/repo/OracleLinux/OL7/latest/
archive/$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0

```

```
[ol7_optional_archive]
name=Oracle Linux $releasever Optional ($basearch) - Archive
baseurl=https://yum$ociregion.$ocidomain/repo/OracleLinux/OL7/optional/
archive/$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0

[ol7_security_validation]
name=Oracle Linux $releasever Update 3 ($basearch) Security Validations
baseurl=https://yum$ociregion.$ocidomain/repo/OracleLinux/OL7/security/
validation/$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0

[ol7_u8_security_validation]
name=Oracle Linux $releasever Update 8 ($basearch) Security Validations
baseurl=https://yum$ociregion.$ocidomain/repo/OracleLinux/OL7/8/
security/validation/$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0
```

5. Perform software updates.

```
yum install bind-utils
```

6. 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
```

Result

Your container is updated.

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.

- If you are upgrading from v10.x or later, you can use the application installer script as described in [Upgrading Ops Center Administrator by using the application installer \(on page 61\)](#).
- If you are moving your Ops Center Administrator instance, 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 \(on page 65\)](#).
- 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 uninstalling the older container runtime and installing a new one. Refer to [Upgrading Ops Center Administrator by using backup and restore \(on page 65\)](#) for more information.

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 script 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 Docker root directory (default directory: `/var/lib/docker`) for Docker
 - 40 GiB under the Podman root directory (default directory: `/var/lib/container`) for Podman
 - 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.
- If you also want to upgrade the container runtime version, verify the following additional prerequisites:

For Docker:

Upgrade Ops Center Administrator first and then upgrade Docker.

For Podman:

- 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.

- If the upgrade of Podman is suppressed, unlock the suppression temporarily before starting the installation. After completing the installation, suppress the upgrade of Podman again.
- If you cannot use YUM to install Podman because your management server is not connected to the network, you must obtain the Podman software from the OS media (ISO image or CD-ROM).

The supported version of Podman (3.3.x) is available with v8.5 of Red Hat Enterprise Linux and Oracle Linux. Therefore, regardless of the OS version that you are using, download v8.5 of the OS to get the required Podman version.

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 the root account.
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.
 - For Ops Center preconfigured media or application installer installations, use the `sysadmin` credentials.
 - For stand-alone preconfigured media installations, use the `service` credentials.
6. At the prompt enter `y` at the following:

```
Do you want to upgrade? [y/n]:
```

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

Ops Center Administrator begins upgrading.

7. For Podman, suppress the upgrade of Podman to avoid unintentionally upgrading to an unsupported version.

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

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 setting of the HTTP server and whether the repository data gathered by the **reposync** command exists correctly.
- Restart the Docker or Podman service, verify that the older version is running, and then retry the installation.

- Check the Docker or Podman logs.

Consult the documentation of your container runtime for more information on how to perform these actions.

- View the journal log entries to see whether there is additional error information by connecting to the host with the root account and running these commands:
 - `journalctl --no-pager`
 - `journalctl --no-pager -u docker` (Docker only)
 - `journalctl --no-pager -u rainier` (Podman only)
- 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 and download the backup file.

 - 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 uninstalling the older container runtime and installing a new one.

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, Docker, and Ops Center Administrator.
 - Use the application installer to enable maximum control of the environment. The installer must be deployed in a Docker-compatible or 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, access the virtual appliance manager at:
`https://ip-address/vam`
 - For application installer installations, use the `sysadmin` credentials.
 - For stand-alone preconfigured media installations, use the `service` credentials.
3. When the virtual appliance manager opens in the browser, click **Backup** 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 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. Refer to [Removing Ops Center Administrator \(on page 75\)](#) for more information.
 - If you used the Appliance model, the VM containing Storage Advisor or Ops Center Administrator is shut down at this time. You may want to determine a maintenance window to do this because the Ops Center Administrator product 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), uninstall the old container runtime and then install the new container runtime on the host OS.
5. Deploy the next version in the upgrade path using the method of your choice (virtual appliance or installer).
 Follow the instructions in the Getting Started content until the product is initialized and ready to use.
6. In the new instance of Ops Center Administrator, log in to the virtual appliance manager by using the default credentials.
 - For application installer installations, use the `sysadmin` credentials.
 - For stand-alone preconfigured media installations, use the `service` credentials.

7. When the virtual appliance manager opens in the browser, click **Restore**. 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.



Note: Do not cancel the restore operation. Cancellation may corrupt the Ops Center Administrator instance. The progress bar may indicate 100% completion even though the operation has not completed.

Chapter 5: Onboarding and configuring a storage system

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

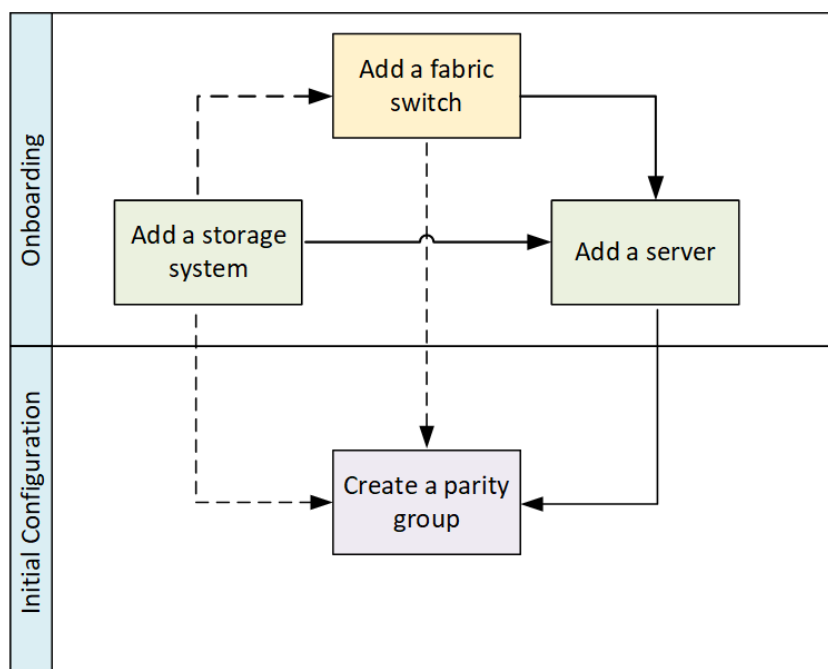
If the storage system includes NAS modules, the file storage is automatically added with the block storage

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

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.

In the following workflow, the recommended path is marked by the solid arrows. 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 the first time you start Ops Center Administrator.

Before you begin

Ops Center Administrator needs access to all resources 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.

If a storage array includes block storage and NAS modules, the file storage is automatically added with the block storage. You can then create pools and other file resources using the Ops Center Administrator interface or by using the API.

Ops Center Administrator also supports onboarding of 4-node clusters, which is a requirement for GAD Enhanced for NAS.



Note: 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 onboarded storage systems, but alert information for these storage systems is not shown in Ops Center Administrator. For Ops Center Administrator to receive alerts from onboarded storage systems, you must change the SNMP setting to SNMPv3 and add the Ops Center Administrator server as an SNMP trap destination.



Note: To get storage system 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 storage systems. To do this, see "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 the plus sign (+) to add a storage system.
2. Enter values for the following parameters in the **Onboard Storage System** window.

IP Address:

For a storage system with an SVP, enter the IP address (IPv4) of the external service processor for the storage system you want to discover.

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

Wait a while for Administrator to add the storage system. Refresh the Jobs tab 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, F1500

Adding a fabric switch

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

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:

- Servers and ports are connected according to the manufacturer's 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
 - Port Number
 - Username
 - Password
- You have the Admin role for the fabric switch.

Procedure

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

VIRTUAL FABRIC ID	FABRIC SWITCH TYPE	FABRIC SWITCH IP ADDRESS	PORT NUMBER	USERNAME	PASSWORD
Virtual Fabric Id	Fabric Switch Type	Fabric Switch IP Address	22	Username	*****

3. Enter the following information from the configuration of the switch you are adding:
 - **Virtual Fabric ID:** For Cisco switches, the VSAN ID. Not applicable to Brocade switches.
 - **Fabric Switch Type:** Select **Brocade** or **Cisco**.
 - **Fabric Switch IP Address**
To add or update a core switch, use the Management IP address of the switch or the Active CP IP address.
 - **Port Number**
 - **Username**
 - **Password**
4. Click **Submit**.

Result

A job is created 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 one server in each row.

The CSV file must have the following headings:

- For Fibre:
 - Name, OSType, WWNs (comma-separated list of WWNs).
 - Description, IPAddress and WWNsUserDefinedNames (comma-separated list of user-defined names for WWNs) are optional headings.
- For iSCSI:
 - Name, OSType, IscsiName (comma-separated list of names).
 - Description, IPAddress, ChapUser, ChapSecret and IscsiNamesUserDefinedNames (comma-separated list of user-defined names for iSCSI Names) are optional headings.

Valid OSType values are as follows:


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



Note: When you use Internet Explorer, limit the number of servers in a CSV file to 500 servers. If the browser does not work, reduce the number of servers and try again.

Procedure

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



Add Servers

CSV Import

Fibre Servers

SERVER NAME	DESCRIPTION	IP ADDRESS	OS TYPE	
Fibre_Server_Example	Example Fibre server	1.2.3.4	HP_UX	✕
<p>WWN LIST</p> <p>10:00:00:00:C9:71:C6:F4, 10:00:00:00:C9:71:C6:F4</p>				
<p>WWN USER-DEFINED NAMES</p> <p>Fibre_server1, Fibre_server2</p>				

iSCSI Servers

SERVER NAME	DESCRIPTION	IP ADDRESS	OS TYPE	CHAP USER	
iSCSI_Server_Example	Example iSCSI server	5.6.7.8	HP_UX	sysadmin	✕
<p>CHAP SECRET</p> <p>*****</p>					
<p>iSCSI LIST</p> <p>iqn.1991-05.com.microsoft:ap01vm01.ap01vm01.dom.local, iqn.1991-05.com.microsoft:ap01vm01.ap01vm01.dom.local</p>					
<p>iSCSI NAMES USER-DEFINED NAMES</p> <p>iSCSI_server1, iSCSI_server2</p>					

Cancel
Reset
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 both Fibre and iSCSI servers, use the following format:

```
Name,Description,IPAddress,OSType,WWNS,WWNsUserDefinedNames,Is
csiNames,IscsiNamesUserDefinedNames,CHAPUserName,CHAPUserSecre
t
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",,
-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
12345678901234567890123456789012345678901234567890123456789012
34567890123456789012345678901234567890123456789012345678901234
5678901234567890123456789012345678901234567890123456789012345
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
```

- Click the plus sign (+) in the table to add a row and enter the required information for Fibre Channel or iSCSI. You can add more servers by clicking the plus sign again.
- (Optionally) You can use the **WWN List** or **iSCSI List** to add/edit a server.
- (Optionally) 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.

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 \(on page 75\)](#)
- [Removing Ops Center Administrator when using Podman \(on page 76\)](#)



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 by using the following command:

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

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 remaining files, run the following commands:

```
sudo rm -rf /opt/rainier
sudo rm -rf /var/log/rainier-audit-log
sudo rm -rf /var/logs/rainier-tool
sudo rm -rf /var/logs/rainier-elastic-store
```

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 the root account.
2. Stop all containers by using the following commands:

```
systemctl stop rainier
systemctl disable rainier
```

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 remaining files, run the following commands:

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

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's 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, access the documentation site: knowledge.hitachivantara.com/Documents and then select Storage > *storage_system_type* > System Management Using Embedded Interfaces > Switching to server management that uses Storage Advisor Embedded from another management tool.

Hitachi Vantara



Corporate Headquarters

2535 Augustine Drive

Santa Clara, CA 95054 USA

HitachiVantara.com | community.HitachiVantara.com

Contact Information

USA: 1-800-446-0744

Global: 1-858-547-4526

HitachiVantara.com/contact