FUJITSU

Fujitsu Software Infrastructure Manager V2.8.0 Infrastructure Manager for PRIMEFLEX V2.8.0

Operating Procedures

CA92344-4953-08
June 2023

Preface

Purpose

This manual describes the installation procedure and operating procedures based on usage scenes of the following operation and management software. This software manages and operates ICT devices such as servers, storages, and switches, as well as facility devices such as PDUs, in an integrated way.

- FUJITSU Software Infrastructure Manager (hereafter referred to as "ISM")
- FUJITSU Software Infrastructure Manager for PRIMEFLEX (hereafter referred to as "ISM for PRIMEFLEX")

Product Manuals

Manual Name	Description
FUJITSU Software Infrastructure Manager V2.8.0 Infrastructure Manager for PRIMEFLEX V2.8.0 First Step Guide	This manual is for those using this product for the first time. This manual summarizes the procedures for the use of this product, the product system, and licensing. In this manual, it is referred to as "First Step Guide."
FUJITSU Software Infrastructure Manager V2.8.0 Infrastructure Manager for PRIMEFLEX V2.8.0 User's Guide	This manual describes the functions of this product, the installation procedure, and procedures for operation. It allows you to quickly grasp all functions and all operations of this product. In this manual, it is referred to as "User's Guide."
FUJITSU Software Infrastructure Manager V2.8.0 Infrastructure Manager for PRIMEFLEX V2.8.0 Operating Procedures	This manual describes the installation procedure and usages for the operations of this product. In this manual, it is referred to as "Operating Procedures."
FUJITSU Software Infrastructure Manager V2.8.0 Infrastructure Manager for PRIMEFLEX V2.8.0 REST API Reference Manual	This manual describes how to use the required APIs and provides samples and parameter information for using user-created applications that integrate with this product. In this manual, it is referred to as "REST API Reference Manual."
FUJITSU Software Infrastructure Manager V2.8.0 Infrastructure Manager for PRIMEFLEX V2.8.0 Messages	This manual describes the messages that are output when using ISM or ISM for PRIMEFLEX and the actions to take for these messages. In this manual, it is referred to as "ISM Messages."
FUJITSU Software Infrastructure Manager for PRIMEFLEX V2.8.0 Messages	This manual describes the messages that are output when using ISM for PRIMEFLEX and the actions to take for these messages. In this manual, it is referred to as "ISM for PRIMEFLEX Messages."
FUJITSU Software Infrastructure Manager V2.8.0 Infrastructure Manager for PRIMEFLEX V2.8.0 Items for Profile Settings (for Profile Management)	This manual describes detailed information for the items set when creating profiles for managed devices. In this manual, it is referred to as "Items for Profile Settings (for Profile Management)."
FUJITSU Software Infrastructure Manager for PRIMEFLEX V2.8.0 Cluster Creation and Cluster Expansion Parameter List	This manual describes Cluster Definition Parameters that are used for the automatic settings in Cluster Creation and Cluster Expansion when using ISM for PRIMEFLEX. In this manual, it is referred to as "ISM for PRIMEFLEX Parameter List."
FUJITSU Software Infrastructure Manager V2.8.0	This document defines the terms that you need to understand in order to use this product. In this manual, it is referred to as "Glossary."

Manual Name	Description
Infrastructure Manager for PRIMEFLEX V2.8.0 Glossary	
FUJITSU Software Infrastructure Manager V2.8.0 Infrastructure Manager for PRIMEFLEX V2.8.0 Plug-in and Management Pack Setup Guide	This manual describes the procedures, from installation to operation as well as precautions and reference information, for the following features of Infrastructure Manager Plug-in. - Infrastructure Manager Plug-in for Microsoft System Center Operations Manager - Infrastructure Manager Plug-in for Microsoft System Center Virtual Machine Manager - Infrastructure Manager Plug-in for VMware vCenter Server - Infrastructure Manager Plug-in for VMware vCenter Server Appliance - Infrastructure Manager Management Pack for VMware vRealize Operations Manager - Infrastructure Manager Plug-in for VMware vRealize Orchestrator - Infrastructure Manager Plug-in for Microsoft Windows Admin Center In this manual, it is referred to as "ISM Plug-in/MP Setup Guide."

Together with the manuals mentioned above, you can also refer to the latest information about ISM by contacting your local Fujitsu customer service partner.

For the information about managed hardware products, refer to the manuals of the relevant hardware.

For PRIMERGY, refer to "ServerView Suite ServerBooks" or the manual pages for PRIMERGY.

https://support.ts.fujitsu.com/

Intended Readers

This manual is intended for readers who consider using the product for comprehensive management and operation of such ICT devices and possess basic knowledge about hardware, operating systems, and software.

Notation in this Manual

Notation

Keyboard

Keystrokes that represent nonprintable characters are displayed as key icons such as [Enter] or [F1]. For example, [Enter] means press the key labeled "Enter." [Ctrl]+[B] means hold down the key labeled "Ctrl" or "Control" and then press the B key.

Symbols

Items that require particular attention are indicated by the following symbols.

Point

Describes the content of an important point.

Note

Describes an item that requires your attention.

Variables: <xxx>

Represents variables that require replacement by numerical values or text strings in accordance with your usage environment.

Example: <IP address>

Abbreviation

This document may use the abbreviation for OS as shown in the following examples.

Official name	Abbreviation	
Microsoft(R) Windows Server(R) 2019 Datacenter	Windows Server 2019 Datacenter	Windows Server 2019
Microsoft(R) Windows Server(R) 2019 Standard	Windows Server 2019 Standard	
Microsoft(R) Windows Server(R) 2019 Essentials	Windows Server 2019 Essentials	
Red Hat Enterprise Linux 9.0 (for Intel64)	RHEL 9.0	Red Hat Enterprise Linux Or Linux
SUSE Linux Enterprise Server 15 SP2 (for AMD64 & Intel64)	SUSE 15 SP2(AMD64) SUSE 15 SP2(Intel64) or SLES 15 SP2(AMD64) SLES 15 SP2(Intel64)	SUSE Linux Enterprise Server Or Linux
SUSE Linux Enterprise Server 15 (for AMD64 & Intel64)	SUSE 15(AMD64) SUSE 15(Intel64) or SLES 15(AMD64) SLES 15(Intel64)	
VMware ESXi™ 7.0	VMware ESXi 7.0	VMware ESXi
VMware Virtual SAN	vSAN	
Microsoft Storage Spaces Direct	S2D	

Terms

For the major terms and abbreviations used in this manual, refer to "Glossary."

Using PDF applications (Adobe Reader, etc.)

Depending on the specifications of the PDF application you are using, issues (extra spaces and line breaks, missing spaces, line breaks, and hyphens in line breaks) may occur when you perform the following operations.

- Saving to a text file
- Copying and pasting text

High Risk Activity

The Customer acknowledges and agrees that the Product is designed, developed and manufactured as contemplated for general use, including without limitation, general office use, personal use, household use, and ordinary industrial use, but is not designed, developed and manufactured as contemplated for use accompanying fatal risks or dangers that, unless extremely high safety is secured, could lead directly to death, personal injury, severe physical damage or other loss (hereinafter "High Safety Required Use"), including without limitation, nuclear reaction control in nuclear facility, aircraft flight control, air traffic control, mass transport control, medical life support system, missile launch control in weapon system. The Customer shall not use the Product without securing the sufficient safety required for the High Safety Required Use. In addition, Fujitsu (or other affiliate's name) shall not be liable against the Customer and/or any third party for any claims or damages arising in connection with the High Safety Required Use of the Product.

To Use This Product Safely

This document contains important information required for using this product safely and correctly. Read this manual carefully before using the product. In addition, to use the product safely, the customer must understand the related products (hardware and software) before using the product. Be sure to use the product by following the precautions on the related products. Be sure to keep this manual in a safe and convenient location for quick reference during use of the product.

Modifications

The customer may not modify this software or perform reverse engineering through decompiling or disassembly.

Disclaimers

Fujitsu Limited assumes no responsibility for any claims for losses, damages or other liabilities arising from the use of this product. The contents of this document are subject to change without notice.

Trademarks

Microsoft, Windows, Windows Vista, Windows Server, Hyper-V, Active Directory, and the titles or names of other Microsoft products are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries.

Linux is a trademark or registered trademark of Linus Torvalds in the United States and other countries.

Red Hat and all trademarks and logos based on Red Hat are trademarks or registered trademarks of Red Hat, Inc. in the United States and other countries.

SUSE and the SUSE logo are trademarks or registered trademarks of SUSE LLC in the United States and other countries.

VMware, VMware logo, VMware ESXi, VMware SMP, and vMotion are trademarks or registered trademarks of VMware, Inc. in the United States and other countries.

Intel and Xeon are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java is a registered trademark of Oracle Corporation and its subsidiaries/affiliates in the United States and other countries.

Zabbix is a trademark of Zabbix LLC that is based in Republic of Latvia.

PostgreSQL is a trademark of PostgreSQL in the United States and other countries.

Apache is a trademark or registered trademark of Apache Software Foundation.

Cisco is a trademark of Cisco Systems, Inc. in the United States and other countries.

Elasticsearch is a trademark or registered trademark of Elasticsearch BV in the United States and other countries.

Xen is a trademark of XenSource, Inc.

Trend Micro and Deep Security are trademarks or registered trademarks of Trend Micro Incorporated.

Nutanix is a trademark of Nutanix, Inc. in the United States and other countries.

All other company and product names are trademarks or registered trademarks of the respective companies.

All other products are owned by their respective companies.

Copyright

Modification History

Edition	Issue Date	Modification Overview	Section	
01	August 2022	First edition	-	-
02	October 2022	Added Multi-Factor Authentication in Users and User Groups	2.3.1.1 Add users	Table "User information"

Edition	Issue Date	Modification Overview	Section	
	Modification for ISM 2.8.0.010 patch application		2.3.1.2 Edit users	"Table"
			2.3.2.1 Add user groups	Table "User group information"
			2.3.2.2 Edit user groups	"Table"
		Added the articles for expansion of PRIMERGY M6 series	6.8.1 Operation Requirements	Operation requirements for target servers
			6.8.2.8 Set up BIOS	Table "BIOS settings (PRIMERGY M6 series)"
			6.8.2.9 Create system disk (RAID1)	-
	October 2022 Major reorganization of the manual and article improvement	Modified the article for non-supported OSes	2.2.1.4 Execute Syslog forwarding	-
			6.6.1 Operation Requirements	Operation requirements for PRIMEFLEX HS/ PRIMEFLEX for VMware vSAN configuration only
			6.6.2.3 Obtain the vCSA patch file or vCSA upgrade file to be applied	-
			8.1.1 Back up ISM-VA	Deleted: "Back up ISM-VA running on VMware vSphere Hypervisor 5.5 or VMware vSphere Hypervisor 6.0"
		Changed the note for HTTPS port number	3.1.2 Register a Node Directly	Table "When [BMC] [HTTPS] is displayed in communication methods"
		Changed the note for ServerView Suite Update DVD	6.6.2.4 Import the firmware to be applied into ISM-VA	"Note"
		Added the notes and procedures for executing the manual OS installation procedure to avoid rewinding cumulative updates (S2D)	6.8.3.1 Cluster Creation procedure	"Note" in step11
			6.8.3.2 Cluster Expansion procedure	"Note" in step 8
			6.8.3.3 Manual OS Installation procedure	New addition
		Added a note for stopping and starting the TSM-SSH service	6.11 Back up Nodes or vCSA Structuring a Cluster	Table "Work flow for backup of nodes or vCSA structuring a cluster"
			6.11.3 Execute Backup	"Note"
			6.11.4.1 Start the TSM-SSH service	New addition
			6.12 Restore vCSA Structuring a Cluster	Table "Work flow for restoring vCSA structuring a cluster"
			6.12.3 Execute Restore	"Note"

Edition	Issue Date	Modification Overview	Section	
			6.12.4.3 Start the TSM-SSH service	New addition
03	November 2022 Major reorganization of the manual and article improvement	Modified the BIOS settings table for the server series	6.7.2.15 Set up BIOS	- Table "BIOS settings (PRIMERGY CX M4, CX M5 series)" - Table "BIOS settings (PRIMERGY RX M4, RX M5 series)" - Table "BIOS settings (PRIMERGY RX M6 series)"
		Added procedure to check the firmware version	6.8.2.6 Execute installation and wiring	- For Manual Discovery of nodes Added Step 5 - For Auto Discovery of nodes Added Step 4
		Modified article	6.8.2.8 Set up BIOS	Table "BIOS settings (PRIMERGY M6 series)"
		Modified procedure	6.8.2.9 Create system disk (RAID1)	Step 2: Step g in "If "MSCC SmartHBA 2100-8i" or "Adaptec SmartHBA 2100-8i" is displayed"
		Modified procedure	6.8.4.6 Set the processor compatibility of virtual machines	Changed Step 2 Added Step 6
		Added the operation for required configuration	6.8 Increase the Resources for PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI	Table "Cluster Creation or Cluster Expansion work flow"
			6.8.4.7 Set the network adapter	New addition
04	January 2023 Modification for ISM 2.8.0.020 patch application	Added the notes for Profile/Policy for each model	3.3.1 Set BIOS/ iRMC/MMB/Virtual IO with Profiles	"Note"
			3.3.4 Create a Policy to Simplify Profile Creation	"Point"
			3.3.5 Compare Assigned Profiles and Hardware Settings	"Note"
			7.1.2 Create Profile from Backup Files	"Note"
			7.1.3 Create Policy from Backup Files	"Note"
	January 2023	Updated the "Impact Analysis (VMware Virtual SAN)" screen	6.2.4 Confirm the Status of Virtual Machines/vSAN Storage	-

Edition	Issue Date	Modification Overview	Section	
	Major reorganization of the manual and article improvement	Modified the articles due to end of support for ESXi 6.0	6.6.2.12 Create scripts to execute before and after an ESXi patch/offline bundle application if needed	-
			6.7.2.8 Creating scripts to execute before and after a VMware ESXi patch application	
		Added the operation requirements when changing the network configuration of PRIMEFLEX	6.7.1 Operation Requirements	Common operation requirements for Cluster Creation and Cluster Expansion
		Modified the description of operation requirements for the target servers	6.7.1 Operation Requirements	Operation requirements for target servers
			6.8.1 Operation Requirements	
		Modified the directories for delete target	6.8.4.3 Delete unnecessary files	(2) Deleting unnecessary files of the target server
05	February 2023 Modification for ISM 2.8.0.030 patch application	Changed the description of the discovery IP address range	3.1.1 Discover Nodes in the Network and Register Nodes	Table "Discovery (When you select "Normal" for [Discovery method])"
		Added the article on node registration for PRIMERGY M7 series	3.1.1 Discover Nodes in the Network and Register Nodes	Table "Discovery (When you select "Normal" for [Discovery method])"
				Table "When selecting PRIMERGY 2/4WAY M7 or later (HTTPS) in [Discovery target]"
				Procedure 5 "Example for discovery of PRIMERGY 2/4WAY M7 or later (HTTPS)"
				"Note"
			3.1.2 Register a Node Directly	Table "[Communication methods] settings based on [Node Type] and [Model Name]"
				Table "When [HTTPS] is displayed in communication methods"
				"Note"
		Added NewHttpsPassword	3.1.1 Discover Nodes in the Network and Register Nodes	"Example for discovery of Server (iRMC/BMC +HTTPS)"
		Added the applicable type for the alarm	3.2.1.3 Set an alarm to the managed devices	Changed Step 3
			4.10.1 Set Alarms and Actions	Changed Step 2

Edition	Issue Date	Modification Overview	Section	
		Added the setting operation for Enable/Disable IPMI	3.2.4 Set Enable/Disable IPMI	New addition
		Added the article on Anomaly Detection of the physical server	4.10.4 Confirm the Current Anomaly Detection Status	"Point"
		Added a condition where restore cannot be executed, and the status of the virtual disk allocation after the ISM restoration	8.1.3 Restore ISM	"Note" Step 8: "Point"
	February 2023 Major reorganization of the manual and article improvement	Added the note for when large number of traps are received at the same time	3.2.2 Set Trap Reception for SNMP	Change in SNMP Settings
		Modified the description of requirement for MIB addition	3.2.2 Set Trap Reception for SNMP	Add MIB File
		Modified the note	3.7.5 Log In without Specifying User Name and Password	"Note"
		Added the note for when logging in to vCSA	6.6.1 Operation Requirements	"Note"
			6.7.1 Operation Requirements	"Note"
		Added the example of when setting the shared folder	6.11.2.1 Prepare a server to store backups	Step 1
		Modified the confirmation steps after the application of patch or upgrade	9.1 Apply Patches and Upgrade Programs to ISM	Modified Step 9 - 12
06	April 2023 Modification for ISM 2.8.0.040 patch application	Added the note for Manual Discovery	3.1.1 Discover Nodes in the Network and Register Nodes	"Note"
		Added the article for PRIMERGY M7 series and iRMC S6	6.7.2.10 Create a profile	"Note"
			6.7.2.12 Confirm installed storage devices	-
			6.7.2.15 Set up BIOS	Table "BIOS settings (PRIMERGY RX M7 series)"
			6.7.2.16 Confirm networks	For iRMC S6
			6.7.2.17 Register a node to ISM	"Point"
	April 2023 Major reorganization of the manual and article improvement	Updated the supported OSes and procedure	2.2.1.4 Execute Syslog forwarding	Supported OSes Step 2 - 3
		Added the note for if setting of [Assign Permission From] is "LDAP permissions"	3.7.4 Set iRMC	"Note"
		Modified the description of operation requirements for changing the PRIMEFLEX network configuration	6.7.1 Operation Requirements	Common operation requirements for Cluster Creation and Cluster Expansion
07	May 2023 Modification for ISM 2.8.0.050 patch application	Added the description of PRIMEQUEST 4000 series	2.3.4.2 Edit node groups	Table "Models in which tree structures are set between nodes"

Edition	Issue Date	Modification Overview	Section	
			3.1.1 Discover Nodes in the Network and Register Nodes	Table "Discovery (When you select "Normal" for [Discovery method])"
				Table "When selecting PRIMERGY 2/4/8WAY M7 or later, PRIMEQUEST4000 (HTTPS) in [Discovery target]"
				"Note"
			3.1.2 Register a Node Directly	Table "[Communication methods] settings based on [Node Type] and [Model Name]"
				"Note"
			3.2.4 Set Enable/Disable IPMI	-
08	June 2023 Modification for ISM 2.8.0.060 patch application	Added the article on iRMC Login	2.3.2 Manage User Groups	Added the item "iRMC Login/AVR" in the table "User group information"
			3.8 Log in Directly to iRMC from ISM	New addition
			6.16 Display iRMC AVR Screen Directly from ISM	New addition
		Added "Point" on Edit in a Batch	3.6.1 Change the Password of the Managed Nodes	"Point"
			3.6.2 Change Password of OS	"Point"
		Added the article on Prediction of Resource Fluctuations	6.3 Predict Resource Fluctuations of Cluster	New addition
		Added article on View/Switch Generations of PRIMEFLEX	6.15 View/Switch Generations of PRIMEFLEX	New addition
	June 2023 Major reorganization of the manual and article improvement	Incompatible support for upgrade to vCSA 8.0	6.7.1 Operation Requirements	Added definition to disable the alarm
		Modified description of procedure to create a profile	6.8.2.10 Create a profile	-
			6.9.2.4 Create a profile	-
		Added the requirement for target servers	6.8.4.5 Register a target server to ServerView RAID Manager	-
		Added the description of procedure to create system disk	6.9.2.9 Create system disk (RAID1)	Added Step d on if "MSCC SmartHBA 2100-8i" or "Adaptec SmartHBA 2100-8i" is displayed
		Modified the description of changes to HTML in the procedures for using video redirection with iRMC	6.8.2.15 Set up BIOS	-
			6.9.2.8 Set up BIOS	-

Edition	Issue Date	Modification Overview	Section	
			6.9.3.1 Cluster Creation procedure	-
			6.9.3.3 Manual OS Installation procedure	-

Contents

Chapter 1 Common Operations

This chapter describes the common operations for each screen on the ISM GUI.

Point

For information on starting the ISM GUI and ISM GUI settings, refer to "2.1.1 GUI" in "User's Guide."

1.1 Display the Help Screen

In ISM, there are help screens that provide a detailed description for each screen. Refer to the help screen for descriptions of the content that is displayed.

There are two ways to display the help screen. Select the appropriate procedure to display it for the screen you are on.

- Select [Help] - [Help for this screen] on the upper-right of each screen while it is displayed on the ISM GUI.
- For currently displayed screens other than the above (wizards and so on), select [ ] on the right side.

1.2 Refresh the Screen

Except for some screens, ISM retrieves information when the screens are displayed. The information on each screen will not be automatically refreshed while the screen is displayed. When you want to display the most recent information, refresh the screen.

When you select the [Refresh] button ( ), the information will be retrieved again and the screen will be refreshed.

1.3 Confirm Event Logs

If an error is displayed on the ISM "Tasks" screen, check the messages from the ISM event log.

To display the event log, from the Global Navigation Menu on the ISM GUI, select [Events] - [Events].

1.4 Upload Files Used in ISM to ISM-VA

This section describes the operations to upload files to ISM-VA using the ISM GUI.

1.4.1 Upload Files to ISM-VA

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [General].
2. From the menu on the left side of the screen, select [Upload].
3. Select the root directory from the list.
4. From the [Actions] button, select [Upload File].

   The "Upload File" screen is displayed.

   a. Select a file type.

   b. When you select "Other" for the file type, select [Upload Target Path]. If you do not select "Other" for the file type, you cannot select [Upload Target Path].

   c. Select the file to upload. Drag and drop the file to upload to the ISM GUI. Or select the [Browse] button to select the files to upload.

      If you want to upload multiple files, select the [Add] button and repeat Step a to c.
5. Select the [Apply] button.

1.4.2 Delete Files Uploaded to ISM-VA

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [General].
2. From the menu on the left side of the screen, select [Upload].
3. Select the root directory from the list.
4. Select the link of the directory or search files to display files to delete.
5. Select the checkbox for the file to delete.
6. From the [Actions] button, select [Delete File].
7. On the "Delete File" screen, confirm the file names to delete, and then select the [Delete] button.

Chapter 2 Configure the Required Settings When Installing ISM

This chapter describes operations required for ISM installation.

Perform these procedures after completing all the operations in "Chapter 3 Installation" in "User's Guide."

2.1 Configure Settings for Managing Nodes

ISM manages nodes in four tiers: data centers, floors, racks, and nodes.

This section describes how to register and remove data centers, floors, and racks.

Point

This operation can be executed only by ISM Administrators (who belong to an Administrator group and have an Administrator role).

2.1.1 Register/Delete Datacenters

Datacenter corresponds to the building layer. This layer supposes a datacenter model with multiple floors.

Register a Datacenter

Register the "Datacenter" layer showing the facility housing the datacenter.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Datacenters].

   The "Datacenter List" screen is displayed.

2. Select the  button.

   The "Register Datacenter/Floor/Rack" screen is displayed.

3. In [Object of Registration], select [Datacenter].

4. Enter the setting items, and then select the [Register] button.

   Refer to the help screen for descriptions on the setting items.

   After datacenter registration is finished, the corresponding datacenter will be displayed on the "Datacenter List" screen.

   This finishes the datacenter registration.

Delete a Datacenter

Delete a registered datacenter.

1. On the "Datacenter List" screen, select the datacenter to be deleted.

2. From the [Actions] button, select [Delete Datacenter].

   The "Delete Datacenter" screen is displayed.

   Refer to the help screen regarding things to be careful about when deleting a datacenter.

3. Confirm that the datacenter to be deleted is correct, and then select [Delete].

2.1.2 Register/Delete Floors

This layer supposes a floor space where multiple racks are located.

Point

The floor view can be displayed on the Dashboard. Also, 3D view displays 3D graphics of the floor units.

Register a floor

Register the "Floor" layer that represents the machine room in the datacenter facility.

1. Select the  button on the "Datacenter List" screen.

   The "Register Datacenter/Floor/Rack" screen is displayed.

2. In [Object of Registration], select [Floor].
3. Enter the setting items, and then select the [Register] button.

   For the setting item, [Datacenter], specify the data center registered in the "2.1.1 Register/Delete Datacenters."

   Refer to the help screen regarding other setting items.

   After floor registration is finished, the corresponding floor is displayed on the "Datacenter List" screen.

   This finishes the floor registration.

Delete a floor

Delete a registered floor.

1. On "Datacenter List" screen, select the floor to be deleted.
2. From the [Actions] button, select [Delete Floor].

   The "Delete Floor" screen is displayed.

   Refer to the help screen regarding things to be careful about when deleting a floor.

3. Confirm that the floor to be deleted is correct, and then select [Delete].

2.1.3 Register/Delete Racks

This layer supposes a server rack with multiple managed devices (nodes) mounted.

Register a rack

Register the "Rack" layer that represents the server racks on the floor.

1. Select the  button on the "Datacenter List" screen.

   The "Register Datacenter/Floor/Rack" screen is displayed.

2. In [Object of Registration], select [Rack].
3. Enter the setting items, and then select the [Register] button. For the setting items, [Datacenter] and [Floor], specify the data center and the floor registered in "2.1.1 Register/Delete Datacenters" and "2.1.2 Register/Delete Floors."

   Refer to the help screen regarding other setting items.

   After rack registration is finished, the rack will be displayed on the "Datacenter List" screen.

   This finishes the rack registration.

Delete a rack

Delete a registered rack.

1. From the Global Navigation Menu on the ISM GUI, select [Datacenter].

   The "Datacenter List" screen is displayed.

2. Select the rack to be deleted.
3. From the [Actions] button, select [Delete Rack].

   The "Delete Rack" screen is displayed.

   Refer to the help screen regarding things to be careful about when deleting a rack.

4. Confirm that the rack to be deleted is correct, and then select [Delete].

2.1.4 Locate Racks on the Floor

Locate a rack on the floor.

1. On "Datacenter List" screen, select the floor to set the rack position.

   The Details of floor screen is displayed.

2. From the [Actions] button, select [Set Rack Position].

   The "Set Rack Position" screen is displayed.

   Refer to the help screen for information on the procedure to set the rack position.

3. Select the [Add] button.

   The "Unallocated Racks" screen is displayed.

4. Select the rack to be added, and then select the [Add] button.
5. Set the position of the rack, and then select the [Apply] button.

   After locating of the rack is finished, the rack will be displayed on the Details of Floor screen.

   This finishes the locating of the rack.

2.2 Set an Alarm (ISM internal events)

By setting alarms, you can send notifications to ISM external devices when ISM detects errors or events.

When setting an alarm, it should be assigned in the following order.

1. Action settings (notification method) (Refer to "2.2.1 Execute Action Settings (notification method).")
2. Test of Action (notification method) (Refer to "2.2.2 Execute Test for Action (notification method).")
3. Alarm settings (Refer to "2.2.3 Set an Alarm to the ISM Internal Event.")

2.2.1 Execute Action Settings (notification method)

Set a notification method for communication with ISM externals.

The following are the notification methods:

- Execute an arbitrary script deployed on the external host
- Send mail
- Send/Forward SNMP traps to the external SNMP manager
- Forward/Send event messages to the external Syslog server

Point

- When executing an arbitrary script, you can specify an argument.

- When mail is sent, messages can be encrypted with S/MIME.
- Refer to the help screen for descriptions on other setting items for each screen.

Preparations are required before Action settings (notification method).

According to Action settings type (notification method), execute the following settings respectively.

- 2.2.1.1 Execute a script deployed on the external host
- 2.2.1.2 Send mail
- 2.2.1.3 Execute sending/forwarding a trap
- 2.2.1.4 Execute Syslog forwarding

2.2.1.1 Execute a script deployed on the external host

Pre-settings

Any script files to be executed must be deployed on the external host in advance.

The OSes of the external host that can be used and executable script files are as follows.

OS	Script file (file extension)
Windows	Batch file (.bat)
Azure Stack HCI	
Red Hat Enterprise Linux	Shell script (.sh)
SUSE Linux Enterprise Server	

1. Prepare a script file to use in the action setting.
2. Deploy the script file to an arbitrary directory on the OS of the host.

   If it is a shell script, set the execution privilege to the user who specifies the settings.
3. Specify the same settings as of the monitoring target OS to the OS of the external host.

   This setting is required to access to the external host from ISM and execute the script file.

   For information on the setting procedure, refer to "Appendix B Settings for Monitoring Target OS and Cloud Management Software" in "User's Guide."

Action settings

1. From the Global Navigation Menu on the ISM GUI, select [Events] - [Alarms].
2. From the menu on the left side of the screen, select [Actions].

   The "Action List" screen is displayed.
3. From the [Actions] button, select [Add].

   The "Add Action" screen is displayed.
4. Select "Execute Remote Script" in [Action Type].
5. Enter the setting items, then select the [Apply] button.

   Refer to the help screen for entering the setting items.

   After action addition is finished, the set action will be displayed on the "Action List" screen.

2.2.1.2 Send mail

Pre-settings

1. From the Global Navigation Menu on the ISM GUI, select [Events] - [Alarms].
2. From the menu on the left side of the screen, select [SMTP Server].

   The "SMTP Server Settings" screen is displayed.
3. From the [Actions] button, select [Edit].

   The "SMTP Server Settings" screen is displayed.
4. Enter the setting items, then select the [Apply] button.

   When sending encrypted mail, execute the following settings as well.
5. Prepare the personal certificate.

   Confirm that the certificate is in PEM format and that the certification and recipient mail address is encrypted.
6. Use FTP to transfer it to ISM-VA. Access the following site with FTP to store the certificate.

   `ftp://<ISM-VA IP address>/<User group name>/ftp/cert`
7. From the Console as an administrator, log in to ISM-VA.
8. Import the certificate to the ISM-VA to execute the command.

   ```
   # ismadm event import -type cert
   ```

   When executing the command, all of the certificates stored in the FTP by each user will be imported together.

Action settings

1. From the Global Navigation Menu on the ISM GUI, select [Events] - [Alarms].
2. From the menu on the left side of the screen, select [Actions].

   The "Action List" screen is displayed.
3. From the [Actions] button, select [Add].

   The "Add Action" screen is displayed.
4. Select "Send E-Mail" in [Action Type].
5. Enter the setting items, then select the [Apply] button.

   Refer to the help screen for entering the setting items.

   After the action is added, the set action is displayed on the "Action List" screen.

2.2.1.3 Execute sending/forwarding a trap

Pre-settings

1. From the Global Navigation Menu on the ISM GUI, select [Events] - [Alarms].
2. From the menu on the left side of the screen, select [SNMP Manager].

   The "SNMP Manager List" screen is displayed.
3. From the [Actions] button, select [Add].

   The "Add SNMP Manager" screen is displayed.
4. Enter the setting items, then select the [Apply] button.

Action settings

1. From the Global Navigation Menu on the ISM GUI, select [Events] - [Alarms].

2. From the menu on the left side of the screen, select [Actions].

   The "Action List" screen is displayed.

3. From the [Actions] button, select [Add].

   The "Add Action" screen is displayed.

4. Select "Send/Forward Trap" in [Action Type].

5. Enter the setting items, then select the [Apply] button.

   Refer to the help screen for entering the setting items.

   After the action is added, the set action is displayed on the "Action List" screen.

2.2.1.4 Execute Syslog forwarding

You must set the external Syslog server to be able to receive Syslog forwarding from ISM.

For the supported OSes as external Syslog servers, refer to "Support Matrix."

https://support.ts.fujitsu.com/index.asp

Select [Select a new Product] on the above site and enter "Infrastructure Manager" in [Product Search:].
Select [DOWNLOADS] and select the target operating system.
The reference procedures are subject to change without notice.

To be able to receive Syslog, log in to the external Syslog server with root privilege and change the settings according to the following procedure. This section describes the minimum settings required for reception.

The following example shows cases where Syslog forwarding is executed using the TCP 514 port. Set the appropriate values when you use UDP or different ports.

1. Execute the following command to start editing /etc/rsyslog.conf.

```
# vi /etc/rsyslog.conf
```

2. Add the following content.

   - For RHEL 7, CentOS 6, CentOS 7, SLES 12, SLES 15

```
$ModLoad imtcp
$InputTCPServerRun 514
$AllowedSender TCP,  192.168.10.10/24     *IP address of ISM
```

   - For other than the above

```
module(load="imtcp")
input(type="imtcp" port="514")
$AllowedSender TCP, 192.168.10.10/24     *IP address of ISM
```

3. After finishing editing, execute the following command and restart the rsyslog daemon.

   - For CentOS 6

```
# service rsyslog restart
```

   - For other than the above

```
# systemctl restart rsyslog
```

Action settings

1. From the Global Navigation Menu on the ISM GUI, select [Events] - [Alarms].

2. From the menu on the left side of the screen, select [Actions].

   The "Action List" screen is displayed.

3. From the [Actions] button, select [Add].

   The "Add Action" screen is displayed.

4. Select "Forward Syslog" in [Action Type].

5. Enter the setting items, then select the [Apply] button.

   Refer to the help screen for entering the setting items.

   After the action is added, the set action is displayed on the "Action List" screen.

2.2.2 Execute Test for Action (notification method)

1. From the Global Navigation Menu on the ISM GUI, select [Events] - [Alarms].
2. From the menu on the left side of the screen, select [Actions].

   The "Action List" screen is displayed.

3. From the "Action List" screen, select the action to execute a test.
4. From the [Actions] button, select [Test].

   The "Action test" screen is displayed.

5. Select the [Test] button.

   The test of the action is executed.

   Confirm that the action has been performed.

2.2.3 Set an Alarm to the ISM Internal Event

1. From the Global Navigation Menu on the ISM GUI, select [Events] - [Alarms].
2. From the menu on the left side of the screen, select [Alarms].
3. From the [Actions] button, select [Add].

   The "Add Alarm" wizard is displayed.

   When setting alarms to the errors or events in ISM, select "System" in [Applicable Type] on the "2. Target" screen in the "Add Alarm" wizard.

   Refer to the help screen for entering other setting items.

4. Confirm the contents on the "5. Confirmation" screen, and then select the [Apply] button.

   After alarm addition is finished, the set alarm will be displayed on the "Alarm List" screen.

   This finishes the alarm setting to the ISM internal event.

2.3 Configure ISM Users

By specifying a type of user group or user role at user registration, you can specify administrator users.

Point

- For information on the types of user groups or the types of user roles and their accessible range or operation privileges, refer to "2.13.1 User Management" in "User's Guide."
- Users who belong to an Administrator group and have an Administrator role are special users (ISM administrator) who can perform all the operations in ISM.

2.3.1 Manage ISM Users

The following three types of operations to manage users are available.

- 2.3.1.1 Add users
- 2.3.1.2 Edit users
- 2.3.1.3 Delete users

2.3.1.1 Add users

Point

This operation can be executed only by users with the Administrator role.

Add new users by the following procedure.

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].
2. From the menu on the left side of the screen, select [Users].
3. From the [Actions] button, select [Add].

   The information to be set when you register new users is as follows:

Table 2.1 User information

Item	Setting contents
User Name	Set a unique name to all users to be registered in ISM. The following names cannot be used: - A name starting with _ [Note] - administrator - anonymous [Note] - svimcontent [Note] [Note]: This is not displayed on the "User List" screen.
Link with ISM	You can select one of the following: - Do not set this user as a link user - Set this user as a link user
Password	Specify a user password.
Authentication Method	You can select one of the following: - Follow user group setting - Infrastructure Manager (ISM)
Multi-Factor Authentication (MFA) (ISM 2.8.0.010 or later)	You can select one of the following: - Follow user group setting - Disable Users created before ISM 2.8.0.010 are set to "Disable."
User Role	You can select one of the following: - Administrator - Operator - Monitor

Item	Setting contents
	For information on user roles, refer to "2.13.1 User Management" in "User's Guide."
Description	Freely enter a description of the user (comment) as required.
Language	Specify either Japanese or English. If you do not specify the language, English is used.
Date Format	Select the format for the date.
Time Zone	Select the time zone.

After setting the user information, select the user group the user belongs to.

2.3.1.2 Edit users

Point

For this operation, the information that can be changed differs depending on the type of user group or type of user role.

Modify the user information by the following procedure.

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].
2. From the menu on the left side of the screen, select [Users].
3. Execute one of the following:
   - Select the checkbox for the user you want to edit, and from the [Actions] button, select [Edit].
   - Select the name of the user you want to edit and when the information screen is displayed, from the [Actions] button, select [Edit].

   The information that can be modified is as follows.

User information	Administrator group		Group other than Administrator group	
	Administrator role	Operator role Monitor role	Administrator role	Operator role Monitor role
User Name	Y	Y	Y	Y
Link with ISM	Y	N	N	N
Password	Y	Y	Y	Y
Authentication Method	Y	N	Y	N
Multi-Factor Authentication (MFA) (ISM 2.8.0.010 or later)	Y	N	Y	N
User Role	Y	N	Y	N
Description	Y	N	Y	N
Language	Y	Y	Y	Y
Date Format	Y	Y	Y	Y
Time Zone	Y	Y	Y	Y
User Group	Y	N	N	N

Y: Changeable; N: Not changeable

Note

- If your system works in link with LDAP, changing any passwords does not change the passwords on the LDAP server.

- When selecting [Set this user as a link user] in link with ISM, edit the password at the same time.
- If you change the password, the previous session will be disconnected and you will be logged out.

2.3.1.3 Delete users

Point

This operation can be executed only by users with the Administrator role.

Delete any users as required by the following procedure.

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].
2. From the menu on the left side of the screen, select [Users].
3. Execute one of the following:
   - Select the checkboxes for the users you want to delete, and from the [Actions] button, select [Delete].
   - Select the name of the user you want to delete and when the information screen is displayed, from the [Actions] button, select [Delete].

2.3.2 Manage User Groups

The following types of user group management are available.

- 2.3.2.1 Add user groups
- 2.3.2.2 Edit user groups
- 2.3.2.3 Delete user groups

Point

This operation can be executed only by ISM Administrators (who belong to an Administrator group and have an Administrator role).

2.3.2.1 Add user groups

ISM administrators add new user groups by the following procedure.

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].
2. From the menu on the left side of the screen, select [User Groups].
3. From the [Actions] button, select [Add].

   The information to be set when you newly add a user group is as follows:

Table 2.2 User group information

Item	Setting contents
User Group Name	Set a unique name to all user groups to be registered in ISM. The following names cannot be used because they are used by ISM: - A name starting with __ (two half-width underbars) - Administrator - AbstractionLayer - anonymous - svimcontent

Item	Setting contents
Authentication Method	For Authentication Method for users who belong to the user group, specify one of the following: - Infrastructure Manager (ISM) The password that is used when adding a user with ISM. - Open LDAP / Microsoft Active Directory (LDAP) The password that is managed by Open LDAP or Microsoft Active Directory.
Multi-Factor Authentication (MFA) (ISM 2.8.0.010 or later)	Specify one of the following: you can set to Enable only when [Authentication Method] is "Infrastructure Manager (ISM)." - Enable Enables Multi-Factor Authentication. In addition to the user name and password, an authorization code is required to log in to ISM. - Disable Disables Multi-Factor Authentication. You can log in to ISM with a user name and password. User groups created before ISM 2.8.0.010 are set to "Disable."
iRMC Login/AVR (ISM 2.8.0.060 or later)	Specify one of the following: - Enable Enables iRMC Login and AVR. - Disable Disables iRMC Login and AVR.
Link with LDAP Groups	Specify when [Authentication Method] is "Open LDAP / Microsoft Active Directory (LDAP)." Specify when linking with users on a directory server.
Link with groups of the LDAP server	Specify one of the following: - To manage user passwords created in ISM on a directory server Do not select [Link with groups of the LDAP server]. For details, refer to "2.3.3.1 Manage user passwords created in ISM on a directory server." - To manage users and passwords on directory servers Select [Link with groups of the LDAP server]. For details, refer to "2.3.3.2 Manage users and passwords on directory servers."
LDAP groups to link with	Displayed when you select [Link with groups of the LDAP server]. When you link with users on the directory server, specify which group of which domain you will link to.
User role of the users belong to the LDAP group	Displayed when you select [Link with groups of the LDAP server]. Specify the user roles for the users to be linked.
Description	Enter a description of the user group (comment). You can freely enter any contents as required.
Managed Nodes	Create correlations between user groups and node groups as required by selecting a node group. Specify one of the following: - Nodes in the selected node group You can specify the node group to correlate with in "Node Group Name." - Manage all nodes This makes all nodes managed.

When [Nodes in the selected node group] is selected in the "Administrator" group or in [Managed Nodes], the size restriction and threshold for each usage can be specified.

Table 2.3 Setting size restriction and threshold for each usage

Utilization	Size restriction	Threshold monitoring
All user groups	Specify the total size of the files used by the user group to [Maximum size] in units of MB. The total size of the files is the total of the following files: - Repository - Archived Logs - Node Logs - Files handled with ISM-VA in FTP If the actual utilization size exceeds the specified [Maximum size], an error message is exported to the Operation Log. Even when the [Maximum size] value is exceeded, this does not affect the operations of Repository, Archived Log, and Node Log.	Specify the threshold value exporting an alert message to the Operation Log to [Warning threshold] in units of %. A warning message is exported to the Operation Log.
Repository	Specify the total size of the files imported to Repository to [Maximum size] in units of MB. If the total utilization rate of the imported files exceeds the value of the specified [Maximum size], the currently executed import to the Repository results in error and an error message is exported to the Operation Log.	You cannot specify the value.
Archived Logs	Specify the total size of Archived Log to [Maximum size] in units of MB. If the total size of the Archived Log exceeds the specified [Maximum size], newly created logs are not stored in Archived Log and an error message is exported to the Operation Log. Note that if [Maximum size] is set to the "0" default value, the occurred logs will not be archived and an error message will be exported to the Operation Log every time. The logs stored before exceeding the [Maximum size] remains stored.	Specify the threshold value exporting an alert message to the Operation Log to [Warning threshold] in units of %. A warning message is exported to the Operation Log.
Node Logs	You can specify the total size of download data and log search data to [Maximum size] in units of MB. The log search data can only be specified to the Administrator user group. If either of the total size of download data or the log search data exceeds the value specified in [Maximum Size], neither download data nor log search data are exported and an error message will be exported to the Operation Log. If the [Maximum size] of either download data, log search data or both is set to the default "0," neither data will be exported nor an error message will be exported to the Operation Log.	You can specify the threshold value that exports an alert message to the size of download data and the size of log search data, to [Warning threshold] in units of %. A warning message is exported to the Operation Log.

For information on the procedure to estimate the total size of files imported to Repository, the size of Archived Log, and the size of Node Log (data for downloads, log search data), refer to "3.2.1 Disk Resource Estimation" in "User's Guide."

Note

- Only one node group can be correlated with a user group.
- Every user who belongs to the user group can execute operations only on the nodes belonging to the node group that is correlated with that user group. They cannot access any nodes in node groups that are not correlated with their user group.
- Soon after creating a user group, execute the operations in "3.7.2 Allocation of Virtual Disks to User Groups" in "User's Guide."
- If you select "Manage all nodes," the user group, as well as the Administrator groups, you can access all the node groups and user groups. However, the repository is shared with the Administrator groups.

2.3.2.2 Edit user groups

ISM administrators edit the information on user groups with the following procedure.

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].
2. From the menu on the left side of the screen, select [User Groups].
3. Execute one of the following:
   - Select the checkbox for the user group you want to edit, and from the [Actions] button, select [Edit].
   - Select the name of the user group you want to edit and when the information screen is displayed, from the [Actions] button, select [Edit].

   The information that can be edited is as follows:

Item	Setting contents
User group name	Specify the user group name.
Authentication Method	Specify the authentication method.
Multi-Factor Authentication (MFA) (ISM 2.8.0.010 or later)	Specify the multi-factor authentication
iRMC Login/AVR (ISM 2.8.0.060 or later)	Set enable or disable iRMC Login and AVR.
Link with LDAP Groups	Set link with LDAP groups and user roles for LDAP group users.
Description	Enter a description of the user group (comment).
System volume (Administrator group only)	Specify the threshold value for outputting a warning message for the system volume in [Threshold monitoring] as a percentage with up to two decimals. The warning message is output in the Operation Log and on the GUI screen.
Setting size restriction and threshold for each usage	For details, refer to "Table 2.3 Setting size restriction and threshold for each usage" in "2.3.2.1 Add user groups."
Managed nodes	Create correlations between user groups and node groups as required by selecting a node group.

Note

- You cannot change the group names of Administrator groups.
- Only one node group can be correlated with a user group.

  Newly linking another node group to a user group to which a node group is already linked disables the existing correlation with the older node group.
- About the system volume warning messages
  - The used size of the system volume is checked every ten minutes.

- If the used size of the system volume is larger than the value of the threshold, a warning message is output.
- If the warning message displayed once is not resolved, the same message will be displayed every 24 hours.
- If the warning message displayed once is resolved, and the threshold is exceeded again, the same message is output.
- If a warning message is output, take the following countermeasures:
  - Delete unnecessary files in the repository.
  - Use the ismadm command to expand the size of the LVM volume.

2.3.2.3 Delete user groups

ISM administrators can delete any user groups with the following procedure.

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].
2. From the menu on the left side of the screen, select [User Groups].
3. Execute one of the following:
   - Select the checkboxes for the user groups you want to delete, and from the [Actions] button, select [Delete].
   - Select the name of the user group you want to delete and when the information screen is displayed, from the [Actions] button, select [Delete].

Note

- You cannot delete Administrator groups.
- You cannot delete user groups that have members.

  Before you delete a user group, delete all users who belong to the user group, or change the affiliations of all users to other user groups.
- Even if you delete user groups that are correlated with node groups, the node groups will not be deleted.
- You cannot undo deletion of a user group.
- When you delete a user group, all related data (repositories) are also deleted.

2.3.3 Link with Microsoft Active Directory or LDAP

By linking ISM with directory servers, you can integrate the management of users and passwords.

There are two ways to manage the users and passwords that are used by a directory server:

- Manage the passwords of users that were created in ISM on a directory server

  When users log in to ISM, they are authenticated using a password that is managed on the directory server. Both the ISM and directory server are operated by creating the same user name on both servers.
- Manage users and passwords on a directory server

  Users can log in to ISM using a user name and password that is managed on the directory server. You do not need to create a user in ISM.

2.3.3.1 Manage user passwords created in ISM on a directory server

The procedure is as follows.

1. Register users for operation in link with the directory server on the directory server.
2. Log in to ISM as a user who belongs to an Administrator group and has an Administrator role.
3. If the settings contain no information on the directory server, set the information for the LDAP server.
   a. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].

b. From the left side of the screen, select [LDAP Servers].

c. In [Link with Users], select "Primary" or "Secondary."

d. From the [Actions] button, select [Edit].

   The "Edit LDAP Server Settings" screen is displayed.

e. Set the LDAP server information.

For information on the settings, check with the administrator of the directory server.

Item	Setting contents
Host Name	Specify the name of the directory server. Specify one of the following: - URL or IP address - ldap://<url> or ldap://<IP address> - ldaps://<url> or ldaps://<IP address>
Port Number	Specify the port number of the directory server.
Base DN	Specify the base DN for searching accounts. This information depends on the registered contents on the directory server. Example: - For LDAP: ou=Users,ou=system - For Microsoft Active Directory: DC=company,DC=com
Search Attribute	Specify the account attribute for searching accounts. Specify one of the following fixed character strings: - For LDAP: uid - For Microsoft Active Directory: sAMAccountName
Bind DN	Specify the accounts that can be searched on the directory server. This information depends on the registered contents on the directory server. Example: - For LDAP: uid=ldap_search,ou=system - For Microsoft Active Directory: CN=ldap_search,OU=user_group,DC=company,DC=com Or ldap_search@company.com "anonymous" is not supported.
Password	Specify the password for the account you specified under Bind DN.
SSL Authentication	If you want to use SSL for the connection to the directory server, set up SSL authentication.

Set the following if you want to use SSL for the connection with the directory server.

- Specify the LDAP server name following "ldaps://."
- Specify the port number for SSL communication (Example: 636).
- Set the SSL certificate using the following.
  - Set the SSL certificate after you have uploaded it to the Administrator/ftp directory.
  - After you have set the SSL certificate, delete it since it is no longer needed.
  - Specify the URL that is in the SSL certificate as the LDAP server name.

Example procedure for setting an SSL certificate for Microsoft Active Directory

1. Select [Control Panel] - [Administrative Tools] - [Certificate Authorities].

2. Right-click the target server, and then select [Properties] - [General] - [Certification authority (CA)].
3. Select [View Certificates] to confirm the certificate.
4. Select [Details] in the dialog, and then select [Copy to File...].
5. In the certificate export wizard, select [Next], and then select "Base64 encoded X509(CER)(S)." Specify where to save the file, and then select [Done].
6. Upload the file you saved to "Administrator/ftp/."
7. Specify the file you saved above (you do not need to specify "Administrator/ftp").

4. Prepare the user groups for which you set Microsoft Active Directory or LDAP as the authentication method for ISM.
   a. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].
   b. From the menu on the left side of the screen, select [User Groups] and add a user group.

   The information to be registered is as follows.

Item	Setting contents
User Group Name	Specify any user group name.
Authentication Method	Specify "Open LDAP / Microsoft Active Directory (LDAP)."
Link with LDAP Groups	Clear the [Link with groups of the LDAP server] checkbox.

   For more information, refer to "2.3.2.1 Add user groups."

5. Add the user that you registered in the directory server in Step 1 to the ISM user group created in Step 4.
   a. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].
   b. From the menu on the left side of the screen, select [Users] and add a user.

   The information to be registered is as follows.

Item	Setting contents
User Name	Specify the names of the users you registered in Step 1.
Link with ISM	Specify when using as a user for linking.
Password	For situations when operation in link is disabled, specify a password different from that in Step 1. Note that the password you specify here is also used when you log in with FTP.
Authentication Method	Specify "Follow user group setting."
User Role	Specify the user role in ISM.
Description	Freely specify any values as required.
Language	Specify the language that is used by the user to be added.
Date Format	Specify the date format that is used by the user to be added.
Time Zone	Specify the time zone that is used by the user to be added.
User Group Name	Specify the name of the user group you prepared in Step 4.

6. Confirm that the users you registered in Step 5 are able to log in.

   Specify the following, and log in.

   - User Name

     User name registered in ISM

   - Password

     User password on the directory server

Note

If you modified the password of a user specified with bind DN on a directory server, the modifications are not reflected in the ISM settings. Modify the password in the ISM LDAP server settings.

Procedure for disabling the settings

The procedure for disabling operations in link for linked user groups and users is as follows.

The user password that was set in the operation for registration or change of the user is enabled after disabling the link.

- Disable link with users

  Execute one of the following:

  - Change the user group to which the relevant user belongs to a user group that is not linked. Edit the user information to make this change.

    a. Log in to ISM as a user who belongs to the user group that manages all nodes and has an Administrator role.

    b. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].

    c. From the left side of the screen, select [Users].

       The "User List" screen is displayed.

    d. Select a user to disable the link with, and from the [Actions] button, select [Edit].

    e. On the "Edit User Settings" screen, change the user group name to a group name it is not linked with.

  - Change the user authentication method to "Infrastructure Manager (ISM)."

    a. Log in to ISM as a user who belongs to the user group that manages all nodes and has an Administrator role.

    b. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].

    c. From the left side of the screen, select [Users].

       The "User List" screen is displayed.

    d. Select a user to disable the link with, and from the [Actions] button, select [Edit].

    e. On the "Edit User Settings" screen, select "Infrastructure Manager (ISM)" for [Authentication Method], and select the [Apply] button.

- Disable link with user groups

  1. Log in to ISM as a user who belongs to an Administrator group and has an Administrator role.
  2. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].
  3. From the left side of the screen, select [User Groups].

     The "User Group List" screen is displayed.
  4. Select the user group to disable the link with LDAP groups and from the [Actions] button, select [Edit].
  5. On the "Edit User Group Settings" screen, select "Infrastructure Manager (ISM)" for [Authentication Method], and select the [Apply] button.

2.3.3.2 Manage users and passwords on directory servers

The procedure is as follows.

1. Register groups and users for operation in link with Microsoft Active Directory on the directory server.
2. Log in to ISM as a user who belongs to an Administrator group and has an Administrator role.
3. If the settings contain no information on the directory server, set the information for the LDAP server.

   a. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].

b. From the menu on the left side of the screen, select [LDAP Servers].

c. Select the LDAP server in [Link with Groups], and from the [Actions] button, select [Edit].

   The "Edit LDAP Server Settings" screen is displayed.

d. Set the information for the LDAP server.

The linking of user accounts is supported only for Microsoft Active Directory. For information on the settings, check with the administrator of the directory server.

Item	Setting contents
LDAP Server Settings	Specify "Enable" or "Disable" for the domain.
Link with CAS	Specify "Enable" or "Disable" for CAS. - Enable: Use CAS - Disable: Do not use CAS
Host Name	Specify the name of the directory server. Specify one of the following: - URL or IP address - ldap://<url> or ldap://<IP address> - ldaps://<url> or ldaps://<IP address>
Port Number	Specify the port number of the directory server.
Base DN	Specify the base DN for searching accounts. This information depends on the registered contents on the directory server. Example: - For Microsoft Active Directory: DC=company,DC=com
Bind DN	Specify the accounts that can be searched on the directory server. This information depends on the registered contents on the directory server. Example: - For Microsoft Active Directory: ldap_search@company.com - "anonymous" is not supported.
Password	Specify the password for the account you specified under Bind DN.
SSL Certificate	Set SSL authentication for the directory server.
Host Setting	Select the checkbox to enable the settings for the directory server.

You can specify multiple host names, port numbers, SSL certificates, and host settings. If you have specified multiple items, they are used based on the active directory server, from top to bottom.

Set the following if you want to use SSL for the connection with the directory server.

- Specify the LDAP server name following "ldaps://."
- Specify the port number for SSL communication (Example: 636).
- Set the SSL certificate using the following.
  - Set the SSL certificate after you have uploaded it to the Administrator/ftp directory.
  - After you have set the SSL certificate, delete it since it is no longer needed.
  - Specify the URL that is in the SSL certificate as the LDAP server name.

Example procedure for setting an SSL certificate for Microsoft Active Directory

1. Select [Control Panel] - [Administrative Tools] - [Certificate Authorities].
2. Right-click the target server, and then select [Properties] - [General] - [Certification authority (CA)].

3. Select [View Certificates] to confirm the certificate.
4. Select [Details] in the dialog, and then select [Copy to File...].
5. In the certificate export wizard, select [Next], and then select "Base64 encoded X509(CER)(S)." Specify where to save the file, and then select [Done].
6. Upload the file you saved to "Administrator/ftp/."
7. Specify the file you saved above (you do not need to specify "Administrator/ftp").

4. Create the ISM user group that corresponds to the group on the directory server.
   a. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].
   b. From the menu on the left side of the screen, select [User Groups], and then add a user group.

   The information to be registered is as follows.

Item	Setting contents
User Group Name	Specify an arbitrary group name.
Authentication Method	Specify "Open LDAP / Microsoft Active Directory (LDAP)."
Link with LDAP Groups	Select the [Link with groups of the LDAP server] checkbox, and then specify the following. - LDAP groups to link with Specify a domain name and a group name that exists in that domain. - User role of the users belong to the LDAP group Specify a user role.

   For information other than the above, refer to "2.3.2.1 Add user groups."

5. Confirm that the users that belong to the "LDAP group to link with" registered in Step 4 are able to log in to ISM with the following:
   - User Name

     Specify the name of the directory server in "<User name>@<Domain name>" format.
   - Password

     User password on the directory server

   The "Select Login User Group" screen is displayed when the login user belongs to multiple user groups. Specify the login user group.

Point

- A user is created in ISM when you have logged in to ISM with the user on the directory server.
- Delete users that have been created in ISM when a user has been deleted from the directory server or when a user has been removed from a group.
- Even if user names are the same, users with different domains are handled as separate users.

Note

- The linking of users on a directory server is supported only for Microsoft Active Directory.
- You cannot use FTP and SSH when you have linked with a user on a directory server.
- You cannot log in to ISM with a user on a directory server that has the same name as an existing user in ISM. Change the name of the user, or delete the ISM user.

- Users are handled as follows depending on how they are specified when they log in:
  - When @Domain name is specified

    Link with Microsoft Active Directory Group user
  - When @Domain name is not specified

    Users that correspond to "2.3.3.1 Manage user passwords created in ISM on a directory server."

    Or, users that are not linked with Microsoft Active Directory or LDAP

  Upper case and lower case are not distinguished in domain names.
- The connection with the LDAP server is checked for all directory servers when you select the [Apply] or [Test] button if you have enabled the LDAP server settings.
- The connection with the LDAP server is checked for directory servers that have the checkbox selected for host settings when you select the [Apply] or [Test] button.
- If you modified the password of a user specified with bind DN on a directory server, the modifications are not reflected in the ISM settings. Modify the password in the ISM LDAP server settings.

Procedure for disabling the settings

The procedure for disabling linked user accounts on a directory server is as follows.

1. Log in to ISM as a user who belongs to an Administrator group and has an Administrator role.
2. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].
3. From the menu on the left side of the screen, select [User Groups].

   The "User Group List" screen is displayed.
4. Select a user group to disable Link with LDAP Groups, and from the [Actions] button, select [Edit].
5. On the "Edit User Group Settings" screen, from the list in [Link with LDAP Groups] - [LDAP groups to link with], select [x] next to the LDAP group name that you want to disable to delete. Select the [Apply] button.

   If you disable all LDAP groups to link with and the user group is not needed anymore, delete all users that belong to the user group, and then delete the user group.

   For details, refer to "2.3.1.3 Delete users" and "2.3.2.3 Delete user groups."

2.3.4 Manage Node Groups

The following types of node group management are available.

- 2.3.4.1 Add node groups
- 2.3.4.2 Edit node groups
- 2.3.4.3 Delete node groups

Point

This operation can be executed only by ISM Administrators (who belong to an Administrator group and have an Administrator role).

2.3.4.1 Add node groups

ISM administrators can newly add node groups with the following procedure.

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].
2. From the menu on the left side of the screen, select [Node Groups].
3. From the [Actions] button, select [Add Node Group].

Or

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Node Groups].
2. Select the  button on the "Node Group List" screen.

The information to be set when you add a new node group is as follows:

- Node Group Name

  Set a unique name to all node groups to be registered in ISM.

- Selection of Nodes to be Assigned

  Select multiple nodes for which the node group affiliation is [Unassigned].

  Note that, if you do not assign any nodes here, you can also assign them at a later stage by editing the node group.

 Note

Each node can belong to only one node group.

2.3.4.2 Edit node groups

ISM administrators can edit node groups with the following procedure.

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].
2. From the menu on the left side of the screen, select [Node Groups].
3. Execute one of the following:
   - Select the checkbox for the node group you want to edit, from the [Actions] button, select [Edit Node Group].
   - Select the name of the node group you want to edit and, when the information screen is displayed, from the [Actions] button, select [Edit Node Group].

Or

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Node Groups].
2. Select the node group from the Node Group List on the left side of the screen, from the [Actions] button, select [Edit Node Group].

The information to be set when you edit a node group is as follows:

- Node Group Name

  Set a unique name to all node groups to be registered in ISM.

- Selection of Nodes to be Newly Assigned

  Select multiple nodes for which the node group affiliation is [Unassigned].

To release or change a node assignment, follow the procedure below.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Node Groups].
2. Select the node group from the Node Group List on the left side of the screen.
3. Select a node on the right side of the screen, then select [Assign to Node Group] from the [Node Actions] button.
4. On the "Assign to Node Group" screen, select the [Select] button.
5. On the "Select Node Group" screen, select one of the following, and then select the [Select] button:
   - For disabling a node assignment: [Unassigned]
   - For changing a node assignment: [<Node group to which to assign a new>]
6. On the "Assign to Node Group" screen, select the [Apply] button.

Note

For nodes in the tree structure, only the parent node can execute [Assign to Node Group].
The child node is automatically set to the same node group as the parent node.

For nodes in the tree structure, an icon of structure path is displayed next to the node name on the "Node List" screen. Models where a tree structure is specified are as described in "Table 2.4 Models in which tree structures are set between nodes."

Table 2.4 Models in which tree structures are set between nodes

Model	Parent node	Child node	Icon
PRIMERGY BX Chassis	-	PRIMERGY BX Server BX Connection Blade	
PRIMERGY BX Server	PRIMERGY BX Chassis	-	
BX Connection Blade	PRIMERGY BX Chassis	-	
PRIMERGY CX Chassis	-	PRIMERGY CX Server	
PRIMERGY CX Server	PRIMERGY CX Chassis		
PRIMEQUEST 2000 series/3000E series	-	PRIMEQUEST Partition	
PRIMEQUEST Partition	PRIMEQUEST 2000 series/ 3000E series	PRIMEQUEST Expansion Partition	
PRIMEQUEST Expansion Partition	PRIMEQUEST Partition	-	
PRIMEQUEST 4000 series Chassis (ISM 2.8.0.050 or later)	-	PRIMEQUEST 4000 series Partition	
PRIMEQUEST 4000 series Partition (ISM 2.8.0.050 or later)	PRIMEQUEST 4000 series Chassis	-	
ETERNUS DX	-	Drive Enclosure	
Drive Enclosure	ETERNUS DX	-	
ETERNUS NR/AX/HX (Ontap) Cluster	-	ETERNUS NR/AX/HX (Ontap) Chassis	
ETERNUS NR/AX/HX (Ontap) Chassis	ETERNUS NR/AX/HX (Ontap) Cluster	External Attached Disk Shelf	
External Attached Disk Shelf	ETERNUS NR/AX/HX (Ontap) Chassis	-	
VCS Fabric	-	VDX Switch	
VDX Switch	VCS Fabric	-	

Model	Parent node	Child node	Icon
C-Fabric	-	CFX2000 series/PY CB Eth Switch 10/40Gb 18/8+2 (Fabric mode)	
CFX2000 series	C-Fabric	-	
PY CB Eth Switch 10/40 Gb 18/8+2 (Fabric mode)	C-Fabric	-	

2.3.4.3 Delete node groups

ISM administrators can delete node groups with the following procedure.

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].
2. From the menu on the left side of the screen, select [Node Groups].
3. Execute one of the following:
   - Select the checkboxes for the node groups you want to delete, from the [Actions] button, select [Delete Node Group].
   - Select the name of the node group you want to delete and, when the information screen is displayed, from the [Actions] button, select [Delete Node Group].

Or

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Node Groups].
2. Select the node group from the Node Group List on the left side of the screen, from the [Actions] button, select [Delete Node Group].

Note

You cannot delete node groups that contain any nodes. Before you delete a node group, execute one of the operations described below.

- Delete any nodes in advance
- Release any node assignments
- Assign any nodes to other node groups

Chapter 3 Register/Set/Delete a Managed Node

This chapter describes various settings such as registration/deletion of managed nodes, alarm settings for managing nodes, etc.

3.1 Register/Delete Managed Nodes

Node registration can be executed either by discovering and registering existing nodes in the network, or by directly entering the node information.

When the information registered in ISM and the information registered in the node does not match, the functionality of the ISM might be limited.

Note

If the parent node of a node with a tree structure between nodes is registered, the child node is automatically registered.
The child node is automatically set to the same node group as the parent node.

For nodes in the tree structure, an icon of structure path is displayed next to the node name on the "Node List" screen. Models where a tree structure is specified are as described in "Table 2.4 Models in which tree structures are set between nodes."

3.1.1 Discover Nodes in the Network and Register Nodes

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Node Registration].

   The "Node Registration" screen is displayed.

   Devices discovered by Auto Discovery are displayed in [Discovered Node List]. Proceed to Step 8.

   #### Point

   For target nodes by Auto Discovery, refer to "Support Matrix."

   https://support.ts.fujitsu.com/index.asp

   Select [Select a new Product] on the above site and enter "Infrastructure Manager" in [Product Search:].

   Select [DOWNLOADS] and select the target operating system.

   The reference procedures are subject to change without notice.

2. From the [Actions] button, select [Discover nodes].

   The "Discover Nodes" screen is displayed.

3. Select [Discovery method].

   Select one of the following. Screen display differs depending on your selection in [Discovery method].

   - Normal

     Execute discovery to set the discovery range by specifying the IP address range. Proceed to Step 4.

   - CSV upload

     Execute discovery to specify the CSV file in which discovery targets are specified. Proceed to Step 5.

4. When you select "Normal" in [Discovery method], set the [Discovery IP Address range] and [Discovery target], and then set the required setting items for each discovery target. After finishing all settings, select the [Execute] button.

   #### Note

   If you specify the IP address in the discovery IP address range with a different number of the third octet (for example, 10.10.0.1 - 10.10.4.255), Manual Discovery may take several hours or more to complete. To check the latest information, select the [Refresh]

button or set [Auto Refresh].
To stop Manual Discovery, select the [Cancel] button on the "Discovery Detail" screen. Note that although you cancel Manual Discovery, the discovery results up to the time of the cancellation are still displayed (ISM 2.8.0.040 or later).

Table 3.1 Discovery (When you select "Normal" for [Discovery method])

Setting items	Setting contents
Discovery IP Address range	Set the discovery range by specifying the IP address range, the FQDN, or the host name (ISM 2.8.0.030 or later). The discovery IP address range can be specified up to the third octet (ISM 2.8.0.040 or later).
Discovery target	Select from the following items: - Server (iRMC/BMC) Select when you want to discover the server or PRIMEQUEST 3800B. - PRIMERGY 2/4WAY M7 or later (HTTPS) (ISM 2.8.0.030) Select when you want to discover PRIMERGY 2/4WAY M7 series or later. - PRIMERGY 2/4/8WAY M7 or later (HTTPS) (ISM 2.8.0.040) Select when you want to discover PRIMERGY M7 series or later. - PRIMERGY 2/4/8WAY M7 or later, PRIMEQUEST4000 (HTTPS) (ISM 2.8.0.050 or later) Select when you want to discover PRIMERGY M7 series or later or PRIMEQUEST 4000 series. - PRIMERGY CX1430 M1, PRIMERGY GX (BMC + HTTPS) Select when you want to discover PRIMERGY CX1430 M1 or PRIMERGY GX. - PRIMEQUEST2000, PRIMEQUEST3000E (MMB + SSH + SNMP) Select when you want to discover PRIMEQUEST 2000 series and PRIMEQUEST 3000 series except PRIMEQUEST 3800B. - Switch, Storage, PRIMERGY BX Chassis (SSH + SNMP) Select when you want to discover storage, network switch, or PRIMERGY BX chassis. - Facility (SNMP) Select when you want to discover RackCDU, PDU, or UPS.

Table 3.2 When selecting Server (iRMC/BMC) in [Discovery target]

Setting items		Description
iRMC/BMC		-
	User Name	iRMC/BMC User Name
	Password	iRMC/BMC Password
	IPMI Port Number	iRMC/BMC Port Number (Default: 623)
	HTTPS Port Number	HTTPS Port Number (Default: 443)

Table 3.3 When selecting PRIMERGY 2/4/8WAY M7 or later, PRIMEQUEST4000 (HTTPS) in [Discovery target] (ISM 2.8.0.030 or later)

Setting items		Description
HTTPS		-
	Port Number	HTTPS Port Number (Default: 443)

Table 3.4 When selecting PRIMERGY CX1430 M1, PRIMERGY GX (BMC + HTTPS) in [Discovery target]

Setting items		Description
BMC		-
	User Name	BMC User Name
	Password	BMC Password
	Port Number	BMC Port Number (Default: 623)
HTTPS		-
	User Name	HTTPS User Name
	Password	HTTPS Password
	Port Number	HTTPS Port Number (Default: 443)

Table 3.5 When selecting PRIMEQUEST 2000, PRIMEQUEST 3000E (MMB + SSH + SNMP) in [Discovery target]

Setting items		Description
MMB		-
	User Name	MMB User Name
	Password	MMB Password
	Port Number	MMB Port Number (Default: 623)
SSH		-
	User Name	SSH User Name
	Password	SSH Password
	Port Number	SSH Port Number (Default: 22)
SNMP		-
	Version	Select SNMP Version
	Port Number	SNMP Port Number (Default: 161)
	Community	SNMP Community Name

Table 3.6 When selecting Switch, Storage, PRIMERGY BX Chassis (SSH + SNMP) in [Discovery target]

Setting items		Description
SSH		-
	User Name	SSH User Name
	Password	SSH Password
	Port Number	SSH Port Number (Default: 22)
SNMP		-
	Version	Select SNMP Version
	Port Number	SNMP Port Number (Default: 161)
	Community	SNMP Community Name

Table 3.7 When selecting Facility (SNMP) in [Discovery target]

Setting items	Description
Version	Select SNMP Version
Port Number	SNMP Port Number (Default: 161)
Community	SNMP Community Name

5. When you select "CSV upload" in [Discovery method], set the following items, and then select the [Execute] button.
   You must prepare CSV files in which the information of the discovery target nodes are provided before executing discovery.

   Table 3.8 Discovery (When you select "CSV upload" for [Discovery method])

Setting items	Setting contents
Template	Templates for the CSV file can be downloaded. You can download the CSV templates by selecting the template depending on the discovery target, and then selecting the [Download] button. Multiple templates can be selected.
File selection method	- Local Select when specifying the CSV file stored locally. - FTP Select when specifying the CSV file which is transferred to ISM with FTP.
File Path	Select the CSV file to be used for discovery.
Password encryption	- Encrypted Select when the password written in the CSV file is encrypted. For the password encryption procedures, refer to "2.4 Encryption" in "REST API Reference Manual." - Not encrypted Select when the password written in the CSV file is not encrypted.
Action after execute	Specify when you select "FTP" for [File selection method]. Select when you want to delete the CSV file after executing discovery.

   The following is an example of writing to the CSV file.

   - Example for discovery of Server (iRMC/BMC +HTTPS)

```
"IpAddress","IpmiAccount","IpmiPassword","IpmiPort","HttpsAccount","HttpsPassword","NewHttps
Password","HttpsPort"
"192.168.10.11","admin1","********","","admin1","********","",""
"192.168.10.12","admin2","********","","admin2","********","",""
```

   - Example for discovery of PRIMERGY 2/4WAY M7 or later (HTTPS) (ISM 2.8.0.030 or later)

```
"IpAddress","HttpsAccount","HttpsPassword","NewHttpsPassword","HttpsPort"
"192.168.10.11","admin1","********","********",""
"192.168.10.12","admin2","********","********",""
```

   - Example for discovery of Switch, Storage or PRIMERGY BX Chassis (SSH + SNMP)

```
"IpAddress","SshAccount","SshPassword","SnmpType","Community"
"192.168.10.21","user1","********","SnmpV1","comm1"
"192.168.10.22","user2","********","SnmpV1","comm2"
```

6. Confirm that a node is discovered and displayed in the [Discovered Node List] on the "Node Registration" screen.

   When the auto refresh setting is disabled, the discovery status is not refreshed.
   Specify the refresh period in the auto refresh settings or select the [Refresh] button to refresh the screen.

7. When the status on the [Discovery Progress] on the "Node Registration" screen is shown as [Completed], check the [Discovered Node List].

   Check the following countermeasures and perform discovery again for devices in which [Communication Result] has failed.

   You can confirm the content of an error shown in a tool tip by moving the cursor over the [] or [] icon in [Communication Result].

Communication method	Icon	Tool tip	Description/Countermeasure
PING		-	Communication successful
		Communication Failed.	Communication failure Check to see if the IP address is correct or if the network settings are appropriate.
SNMP		-	Communication successful
		Port is closed.	The specified communication port is closed Check to see if the port number is correct.
		Communication Failed.	Communication failure Check to see if the target device is correct or if the user name, password, and port number are correct.
		Authentication Failed.	(Only for SNMPv3) Authentication failure Check to see if the user name and password are correct. Communication may fail if the SNMPv3 user name or password is incorrect depending on the type of device.
		Communication method is not specified.	The user name or password is not specified. Specify the user name or password if discovering the following devices: PRIMEQUEST 2000/PRIMEQUEST 3000E/Switch/Storage/ PRIMERGY BX Chassis/Facility
		Communication is not executed.	Communication was not executed due to another communication failure Check the other tool tips for failed communication, and then check the corresponding countermeasures.
IPMI		-	Communication successful
		Port is closed.	The specified communication port is closed Check to see if the port number is correct.
		Communication Failed.	Communication failure Check to see if the target device is correct or if the user name, password, and port number are correct.
		Communication method is not specified.	The user name or password is not specified. Specify the user name or password if discovering the following devices: Server/PRIMERGY CX1430 M1/PRIMERGY GX/PRIMERGY LX/ PRIMEQUEST 2000/PRIMEQUEST 3000E
		Communication is not executed.	Communication was not executed due to another communication failure Check the other tool tips for failed communication, and then check the corresponding countermeasures.
SSH		-	Communication successful
		Port is closed.	The specified communication port is closed Check to see if the port number is correct.
		Communication Failed.	Communication failure

Communication method	Icon	Tool tip	Description/Countermeasure
			Check to see if the target device is correct or if the user name, password, and port number are correct.
		Communication method is not specified.	The user name or password is not specified. Specify the user name or password if discovering the following devices: PRIMEQUEST 2000/PRIMEQUEST 3000E/Switch/Storage/ PRIMERGY BX Chassis
		Communication is not executed.	Communication was not executed due to another communication failure Check the other tool tips for failed communication, and then check the corresponding countermeasures.
HTTPS		-	Communication successful
		Port is closed.	The specified communication port is closed Check to see if the port number is correct.
		Communication Failed.	Communication failure Check to see if the target device is correct or if the port number is correct.
		Authentication Failed.	Authentication failure Check to see if the user name and password are correct.
		Communication method is not specified.	The user name or password is not specified. Specify the user name or password if discovering the following devices: Server/PRIMERGY CX1430 M1/PRIMERGY GX
		Communication is not executed.	Communication was not executed due to another communication failure Check the other tool tips for failed communication, and then check the corresponding countermeasures.

8. Select the checkbox for the node to be registered.
9. Select the [Register discovered nodes] button.

   The "Node Registration" wizard is displayed.
10. Follow the instructions in the "Node Registration" wizard and enter the setting items.

    Refer to the help screen for descriptions on the setting items.

    - Entering node information

Table 3.9 Detailed node information

Setting items	Setting contents
Node Name	Enter the node name. The following one-byte characters cannot be used: /\:*?"<>| The following is already entered as node name by default: - When DNS name can be retrieved: DNS name - When DNS name cannot be retrieved: xxxx_yyyy The character strings displayed in xxxx, yyyy are as follows: - xxxx The following character strings are displayed according to node type: For servers: SV

Setting items	Setting contents
	For switches: SW For storages: ST For facilities: CDU or PDU or UPS - yyyy They are serial numbers for the node. When the serial numbers could not be retrieved during discovery, IP addresses are displayed. If the nodes are Ontap cluster, the cluster UUIDs are displayed instead of the serial numbers.
Chassis Name	Enter the chassis name when PRIMERGY CX is discovered. When nodes mounted on the same chassis are discovered, enter the chassis name of the node mounted on smallest number of the slots. In a case of the other nodes on the same chassis, the chassis names are automatically entered. The following one-byte characters cannot be used: /\:*?"<>| "SV_zzzz" is entered in the chassis name by default. The serial numbers of the chassis are displayed in zzzz. When the serial numbers are not collected in discovery, IP addresses are displayed.
IP address	When changing the IP address of the device, edit the IP address. Select [], enter the IP address. If editing IP address, the IP address is changed for the device when registering the node. For the target type of devices, refer to "Support Matrix." https://support.ts.fujitsu.com/index.asp Select [Select a new Product] on the above site and enter "Infrastructure Manager" in [Product Search:]. Select [DOWNLOADS] and select the target operating system. The reference procedures are subject to change without notice.
Web I/F URL	Enter the URL when you access web i/f on the node.
Description	Enter the descriptions.

- Entering communication methods

  The node required the settings for the communication method is displayed. Select [Set] for each node and enter the communication method.

11. After entering the registration information of the discovered node has been finished, select the [Register] button.
12. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes] and confirm the node registration.

    This finishes the node registration.

    After node registration is finished, the corresponding node will be displayed on the "Node List" screen.

    When receiving traps from the target nodes with SNMPv3, you must set SNMP trap reception. Refer to "Change in SNMP Settings."

    When an OS is installed on the target node, execute the following procedure.
13. On the "Node List" screen, select the target node name to select the Details of Node screen - [OS] tab.
14. Select [OS Actions] - [Edit OS Information].

    The settings on the "Edit OS Information" screen are as follows.

Table 3.10 Edit OS Information

Setting items	Setting contents
OS Type	Select OS type.
OS version	Select the OS version.
OS IP address	After setting the IP version, enter the IP address of the OS management port (IPv4/IPv6 are supported).
Domain Name	Enter domain name in FQDN format.
Account	Enter the administrator account.
Password	Enter the password of the administrator account.
OS Connection Port Number	Enter the port number for connecting to the OS. The default port is specified if you do not enter it. - For Windows: WinRM service port number (Default:5986) - For Azure Stack HCI: WinRM service port number (Default: 5986) - For Linux: SSH service port number (Default: 22)

15. After entering the OS information, select [Apply].

    This finishes OS information editing. After OS information editing is finished, the OS information on the corresponding node can be retrieved.

Note

When node registration of PRIMERGY M7 series (ISM 2.8.0.030 or later) or PRIMEQUEST 4000 series (ISM 2.8.0.050 or later) is failed to change the password or IP address, set it on the Details of Node screen of ISM after changed the settings on the device side.

3.1.2 Register a Node Directly

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Node Registration].

   The "Node Registration" screen is displayed.

2. From the [Actions] button, select [Manually register nodes].

   The "Node Manual Registration" wizard is displayed.

3. Follow the instructions in the "Node Manual Registration" wizard and enter the setting items.

   Refer to the help screen for descriptions on the setting items.

   The "1. Node Information" screen in the "Node Manual Registration" wizard displays different content for [Communication methods] depending on what is selected for [Node Type] and [Model Name].

   Refer to the following table and change the settings according to what is displayed in [Communication methods].

Table 3.11 [Communication methods] settings based on [Node Type] and [Model Name]

Node Type	Model Name	[Communication methods] Setting
server	PRIMERGY M7 series or later (ISM 2.8.0.030 or later) PRIMEQUEST 4000 series (ISM 2.8.0.050 or later)	Table 3.20 When [HTTPS] is displayed in communication methods (ISM 2.8.0.030 or later)
	PRIMERGY RX/TX series, PRIMERGY CX series (other than PRIMERGY CX1430 M1), PRIMERGY BX series (other than	Table 3.12 When [iRMC] is displayed in communication methods

Node Type	Model Name	[Communication methods] Setting
	PRIMERGY BX900 S2), PRIMEQUEST 3800B	
	PRIMERGY CX1430 M1, PRIMERGY GX	Table 3.13 When [BMC][HTTPS] is displayed in communication methods
	PRIMERGY LX	Table 3.14 When [BMC] is displayed in communication methods
	PRIMEQUEST 2000 series, PRIMEQUEST 3000 series (other than PRIMEQUEST 3800B)	Table 3.15 When [MMB][SSH][SNMP] is displayed in communication methods
	PRIMERGY BX900 S2	Table 3.16 When [SSH][SNMP] is displayed in communication methods
	Generic Server (IPMI)	Table 3.14 When [BMC] is displayed in communication methods
	Generic Server (SNMP)	Table 3.17 When [SNMP] is displayed in communication methods
	other	Table 3.18 When [iRMC/BMC][HTTPS][SSH][SNMP] is displayed in communication methods
switch	Switches with models not shown below	Table 3.16 When [SSH][SNMP] is displayed in communication methods
	Generic Switch (SNMP)	Table 3.17 When [SNMP] is displayed in communication methods
	other	Table 3.18 When [iRMC/BMC][HTTPS][SSH][SNMP] is displayed in communication methods
	SH-E514TR1, ICX6430, Generic Switch (PING)	There are no communication settings.
storage	Storage with models not shown below	Table 3.16 When [SSH][SNMP] is displayed in communication methods
	ETERNUS CS800 S7, Generic Storage (SNMP)	Table 3.17 When [SNMP] is displayed in communication methods
	ETERNUS AB/HB series	Table 3.19 When [HTTPS][SNMP] is displayed in communication methods
	other	Table 3.18 When [iRMC/BMC][HTTPS][SSH][SNMP] is displayed in communication methods
	Generic Storage (PING)	There are no communication settings.
facility	Facilities with models not shown below	Table 3.17 When [SNMP] is displayed in communication methods
	other	Table 3.18 When [iRMC/BMC][HTTPS][SSH][SNMP] is displayed in communication methods
	Generic Facility (PING)	There are no communication settings.
other	-	Table 3.18 When [iRMC/BMC][HTTPS][SSH][SNMP] is displayed in communication methods

Table 3.12 When [iRMC] is displayed in communication methods

Setting items		Description
iRMC		When not accessing the node with iRMC, clear the checkbox (Default: Selected).
	User Name	User Name of iRMC
	Password	Password of iRMC User
	IPMI Port Number	iRMC Port Number (Default: 623)
	HTTPS Port Number	HTTPS Port Number (Default: 443)

Table 3.13 When [BMC][HTTPS] is displayed in communication methods

Setting items		Description
BMC		When not accessing the node with BMC, clear the checkbox (Default: Selected).
	User Name	BMC User Name
	Password	BMC Password
	Port Number	BMC Port Number (Default: 623)
HTTPS		When not accessing the node with HTTPS, clear the checkbox (Default: Selected).
	User Name	HTTPS User Name
	Password	HTTPS Password
	Port Number	HTTPS Port Number (Default: 443) *For PRIMERGY GX2570 M5: 8080

Table 3.14 When [BMC] is displayed in communication methods

Setting items		Description
BMC		When not accessing the node with BMC, clear the checkbox (Default: Selected).
	User Name	BMC User Name
	Password	BMC Password
	Port Number	BMC Port Number (Default: 623)

Table 3.15 When [MMB][SSH][SNMP] is displayed in communication methods

Setting items		Description
MMB		When not accessing the node with MMB, clear the checkbox (Default: Selected).
	User Name	MMB User Name
	Password	MMB Password
	Port Number	MMB Port Number (Default: 623)
SSH		When not accessing the node with SNMP, clear the checkbox (Default: Selected).
	User Name	User Name of PRIMEQUEST
	Password	User Password of PRIMEQUEST
	Port Number	SSH Port Number (Default: 22)
SNMP [Note]		When not accessing the node with SNMP, clear the checkbox (Default: Selected).
	Version	SNMP Version
	Port Number	SNMP Port Number (Default: 161)
	Community	SNMP community name of PRIMEQUEST

[Note]: This is the setting item when selecting SNMPv1 or SNMPv2c for SNMP version. If you have selected SNMPv3, refer to "Table 3.21 When selecting "SNMPv3" for SNMP version."

Table 3.16 When [SSH][SNMP] is displayed in communication methods

Setting items		Description
SSH		When not accessing the node with SSH, clear the checkbox (Default: Selected).
	User Name	SSH User Name
	Password	SSH Password
	Port Number	SSH Port Number (Default: 22)
	Enable password [Note 1]	When not using the password, clear the checkbox (Default: Selected).

Setting items			Description
		Password	Enable password
SNMP [Note 2]			When not accessing the node with SNMP, clear the checkbox (Default: Selected).
	Version		SNMP Version
	Port Number		SNMP Port Number (Default: 161)
	Community		SNMP community name of the target node

[Note 1]: Displays in [Model Name] when Cisco Catalyst switch is selected.

[Note 2]: This is the setting item when selecting SNMPv1 or SNMPv2c for SNMP version. If you have selected SNMPv3, refer to "Table 3.21 When selecting "SNMPv3" for SNMP version."

Table 3.17 When [SNMP] is displayed in communication methods

Setting items		Description
SNMP [Note]		When not accessing the node with SNMP, clear the checkbox (Default: Selected).
	Version	SNMP Version
	Port Number	SNMP Port Number (Default: 161)
	Community	SNMP community name of the target node

[Note]: This is the setting item when selecting SNMPv1 or SNMPv2c for SNMP version. If you have selected SNMPv3, refer to "Table 3.21 When selecting "SNMPv3" for SNMP version."

Table 3.18 When [iRMC/BMC][HTTPS][SSH][SNMP] is displayed in communication methods

Setting items		Description
iRMC/BMC		When accessing the node with iRMC/BMC, select the checkbox (Default: Cleared).
	User Name	iRMC/BMC User Name
	Password	iRMC/BMC Password
	Port Number	iRMC/BMC Port Number (Default: 623)
HTTPS		When accessing the node with HTTPS, select the checkbox (Default: Cleared).
	User Name	HTTPS User Name
	Password	HTTPS Password
	Port Number	HTTPS Port Number (Default: 443)
SSH		When accessing the node with SSH, select the checkbox (Default: Cleared).
	User Name	SSH User Name
	Password	SSH Password
	Port Number	SSH Port Number (Default: 22)
SNMP [Note]		When accessing the node with SNMP, select the checkbox (Default: Cleared).
	Version	SNMP Version
	Port Number	SNMP Port Number (Default: 161)
	Community	SNMP community name of the node to register

[Note]: This is the setting item when selecting SNMPv1 or SNMPv2c for SNMP version. If you have selected SNMPv3, refer to "Table 3.21 When selecting "SNMPv3" for SNMP version."

Table 3.19 When [HTTPS][SNMP] is displayed in communication methods

Setting items	Description
HTTPS	When accessing the node with HTTPS, clear the checkbox (Default: Selected).

Setting items		Description
	User Name	HTTPS User Name
	Password	HTTPS Password
	Port Number	HTTPS Port Number (Default: 443)
SNMP [Note]		When accessing the node with SNMP, clear the checkbox (Default: Selected).
	Version	SNMP Version
	Port Number	SNMP Port Number (Default: 161)
	Community	SNMP community name of the target node

[Note]: ETERNUS AB/HB series only supports SNMPv2.

Table 3.20 When [HTTPS] is displayed in communication methods (ISM 2.8.0.030 or later)

Setting items		Description
Change iRMC password		When the iRMC password is not changed from the factory default, select the checkbox (Default: Cleared)
	Current Password [Note 1]	Current password of iRMC
	New Password [Note 1]	New password of iRMC
HTTPS		When you are not accessing to the node via HTTPS, clear the checkbox (Default: Selected).
	User Name	HTTPS User Name
	Password [Note 2]	HTTPS Password
	Port Number	HTTPS Port Number (Default: 443)

[Note 1]: Displays when the [Change iRMC password] checkbox is selected.

[Note 2]: When the [Change iRMC password] checkbox is selected, as same as [New Password] is displayed. You cannot edit it.

Table 3.21 When selecting "SNMPv3" for SNMP version

Setting items		Description
SNMP		When accessing the node with SNMP, select the checkbox. When not accessing the node with SNMP, clear the checkbox.
	Version	SNMP Version
	Port Number	SNMP Port Number (Default: 161)
	Engine ID	Engine ID of SNMPv3
	Context Name	Context Name of SNMPv3
	User Name	User Name of SNMPv3
	Security Level	Security Level of SNMPv3
	Authentication Protocol	Authentication Protocol of SNMPv3
	Auth Password	Authentication Password of SNMPv3 (8 characters minimum)
	Privacy Protocol	Privacy Protocol of SNMPv3
	Privacy Password	Privacy Password of SNMPv3 (8 characters minimum)

4. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes] and confirm the node registration.

   After node registration is finished, the corresponding node will be displayed on the "Node List" screen.

   It may take time to display the node list depending on the number of nodes registered in ISM.

   This finishes the node registration.

When an OS is installed on the target node, execute the following procedure.

5. On the "Node List" screen, select the target node name to select the Details of Node screen - [OS] tab.
6. Select [OS Actions] - [Edit OS Information].

   The settings on the "Edit OS Information" screen are as follows.

   Table 3.22 Edit OS Information

Setting items	Setting contents
OS Type	Select OS type.
OS version	Select the OS version.
OS IP address	After setting the IP version, enter the IP address of the OS management port (IPv4/IPv6 are supported).
Domain Name	Enter domain name in FQDN format.
Account	Enter the administrator account.
Password	Enter the password of the administrator account.
OS Connection Port Number	Enter the port number for connecting to the OS. The default port is specified if you do not enter it. - For Windows: WinRM service port number (Default: 5986) - For Azure Stack HCI: WinRM service port number (Default: 5986) - For Linux: SSH service port number (Default: 22)

7. After entering the OS information, select the [Apply] button.

   This finishes OS information editing. After OS information editing is finished, the OS information on the corresponding node can be retrieved.

Note

When node registration of PRIMERGY M7 series (ISM 2.8.0.030 or later) or PRIMEQUEST 4000 series (ISM 2.8.0.050 or later) is failed to change the password, set it on the Details of Node screen of ISM after changed the password on the device side.

3.1.3 Delete Nodes

Delete a registered node.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].

   The "Node List" screen is displayed.

   It may take time to display the node list depending on the number of nodes registered in ISM.
2. Select the node to be deleted.
3. From the [Actions] button, select [Delete Node].
4. Confirm that the node to be deleted is correct, and then select [Delete].

   After node deletion is finished, the corresponding node will be deleted from the "Node List" screen.

   This finishes node deletion.

3.2 Set up Nodes

Execute the settings to monitor each event of nodes.

3.2.1 Set an Alarm (Event of Managed Devices)

By setting alarms, you can send notifications to ISM external devices when ISM receives SNMP traps from managed devices or detects errors or events on the managed devices.

When setting an alarm, it should be assigned in the following order.

1. Action settings (notification method) (Refer to "3.2.1.1 Execute action settings (notification method).")
2. Shared Alarm Settings (Refer to "3.2.1.2 Set shared alarm settings.")
3. Alarm settings (Refer to "3.2.1.3 Set an alarm to the managed devices.")

3.2.1.1 Execute action settings (notification method)

Set a notification method for communication with ISM externals.

The following are the notification methods:

- Execute an arbitrary script deployed on the external host
- Send mail
- Send/Forward SNMP traps to the external SNMP manager
- Forward/Send event messages to the external Syslog server

Point

The action setting procedure executed in the alarm settings for the event of the managed devices is the same as the alarm settings for the ISM internal events.

For the detailed setting procedure, refer to "2.2.1 Execute Action Settings (notification method)."

3.2.1.2 Set shared alarm settings

Specify the shared settings to all set alarms.

The shared alarm settings are as follows:

- Trap Reception Restriction Period

  Prevent the continuous action execution by inhibiting reception of the same SNMP trap in the specified period when it receives the same SNMP trap from the same managed device continuously.

1. From the Global Navigation Menu on the ISM GUI, select [Events] - [Alarms].
2. From the menu on the left side of the screen, select [Shared Alarm Settings].

   The "Shared Alarm Settings" screen is displayed.
3. From the [Actions] button, select [Edit].

   The "Edit Shared Alarm Settings" screen is displayed. Refer to the help screen for entering the setting items.
4. Enter the setting items, then select the [Apply] button.

   This finishes the shared alarm settings.

3.2.1.3 Set an alarm to the managed devices

1. From the Global Navigation Menu on the ISM GUI, select [Events] - [Alarms].
2. From the menu on the left side of the screen, select [Alarms].
3. From the [Actions] button, select [Add].

   The "Add Alarm" wizard is displayed.

When setting alarms to the errors or events of the managed devices, on the "Add Alarm" wizard - "2. Target" screen - [Applicable Type], select the alarm setting target from the following:

- Nodes (for each node)

  Select the node for which you want to set alarms.

- Nodes (All Nodes) (ISM 2.8.0.030 or later)

  All nodes are subject to alarm settings.

- Nodes (Node Group) (ISM 2.8.0.030 or later)

  Select the node group for which you want to set alarms. Nodes belonging to the selected node group are subject to alarm settings.

Refer to the help screen for entering other setting items.

4. Confirm the contents on the "5. Confirmation" screen, and then select the [Apply] button.

   After alarm addition is finished, the set alarm will be displayed on the "Alarm List" screen.

   This finishes the alarm setting to the events of the managed devices.

3.2.2 Set Trap Reception for SNMP

Change in SNMP Settings

Set Trap Reception for SNMP. The default receiving settings are set as follows. Change the settings as required. When receiving traps with SNMPv3, the settings are required for each node.

- For SNMPv1/v2c
  Community: public
- For SNMPv3
  No initial settings

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [General].
2. From the menu on the left side of the screen, select [Trap Reception].

   The "Trap Reception Setting List" screen is displayed.
3. From the [Actions] button, select [Add] to add the trap reception settings.
4. Select an SNMP Version to be set, enter required information.

   When executing SNMPv3 Trap Reception Settings, select applicable nodes and set "Engine ID."

Note

When large number of traps are received at the same time, traps are processed sequentially, which may delay the reception process of intended traps such as test traps or traps for the occurrence of incident. Check the configuration of trap reception of the target device and reduce the trap reception to one trap per second.

Add MIB File

You need to get MIB files individually to import it in ISM when you monitor the hardware, such as ISM unsupported Cisco switches or HP servers, etc., that are supplied by vendors other than FUJITSU LIMITED.

1. Prepare the MIB files. Note that when the MIB file has any dependency relationship, all the target files are required.
2. Use FTP to transfer it to ISM-VA. Access ftp://<IP address of ISM-VA>/Administrator/ftp/mibs with FTP, and then store all the MIB files.
3. From the Console as an administrator, log in to ISM-VA.

4. Execute the "ismadm mib import" command.

   Executing the command causes all the MIB files stored in FTP to be imported together.

Register ignored traps

By adding traps to "List of Ignored Traps," you can prevent the same traps from being received from the same node.

1. From the Global Navigation Menu on the ISM GUI, select [Events] - [Events].
2. On the [SNMP Traps] tab, select the traps that you want to restrict trap reception for.
3. Select the [Add to List of Ignored Traps] button.

   Details on the trap added to the list of ignored traps are displayed.
4. Select the [Apply] button.

3.2.3 Set Log Collection Schedule

ISM follows the schedule set (example: every day at 23:00) and collects and accumulates Node Logs on a regular basis. You can have different settings for each node. The set schedule can be executed and log collection executed at an arbitrary time.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].

   The "Node List" screen is displayed.

   It may take time to display the node list depending on the number of nodes registered in ISM.
2. Select the node to be configured from the node list.
3. Select the [Log Collection Settings] tab.
4. In the [Log Collection Settings] tab, from the [Log Collection Settings Actions] button, select [Edit Log Collection Settings].
5. Enter the required settings on the settings screen, then select [Apply].
   - After selecting [Schedule Type], select the [Add] button and set the log collection time.
   - Select the [Enable schedule execution] checkbox. When the checkbox is cleared, the created schedule will not be executed.
   - When the node is a server, [Operating System Log] and [ServerView Suite Log] can be selected as targets for log collection when the OS information is set correctly.

     However, [Hardware Log], [ServerView Suite Log] cannot be selected depending on the server type. In this case, logs cannot be collected.

   Using the operations above, the log of the specified node will automatically be collected at the set time and accumulated in ISM.
6. When executing the log collection at an arbitrary timing according to the settings, in the [Log Collection Settings] tab, from the [Log Collection Settings Actions] button, select [Collect Logs].

   The log collection is executed. The [Collect Logs] operation will be registered as an ISM task. Select [Tasks] at the top of the Global Navigation Menu to confirm that the task has been completed.

3.2.4 Set Enable/Disable IPMI (ISM 2.8.0.030 or later)

You can set enable (to use) or disable (not to use) the IPMI protocol used to communicate with iRMC of the PRIMERGY M7 series and the PRIMEQUEST 4000 series (ISM 2.8.0.050 or later).

The default setting during node registration is Disable IPMI. If enabling the IPMI protocol, you can use Power Capping.

To enable IPMI, first enable the PRIMERGY M7 series or the PRIMEQUEST 4000 series (iRMC) setting (Enable IPMI over LAN). Then, enable IPMI in ISM.

Set Enable/Disable IPMI with the following procedure.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].

   The "Node List" screen is displayed.

2. Select the checkbox for the node that you want to set enable/disable IPMI for from the node list that is displayed.
3. From the [Actions] button, select [Enable/Disable IPMI].
4. Confirm the target node on the "Enable/Disable IPMI" screen.

   Nodes that are not IPMI setting target (unsupported nodes) are displayed in gray.
5. Set the [IPMI Mode] on the target node and select the [Apply] button.

Point

- You can also select [Enable/Disable IPMI] from the [Actions] button on the Details of Node screen that displayed after you select a target node from the [Node List] screen.
- If you display the "Enable/Disable IPMI" screen from the [Actions] button on the Details of Node screen, you will not see [Batch Settings].

3.3 Execute Settings on a Server/Install Server OS

When installing servers or adding new servers, you can set the following for a batch of multiple servers at the same time.

- Hardware settings (BIOS, iRMC, and MMB)
- OS installation
- Virtual IO settings

3.3.1 Set BIOS/iRMC/MMB/Virtual IO with Profiles

Profiles are collections of settings for node hardware or OS installation, they need to be created individually for each node.

Set up BIOS/iRMC/MMB/virtual IO of the server registered in ISM by assigning created profiles.

Point

By using policies, you can make it easy to create a profile. For details, refer to "3.3.4 Create a Policy to Simplify Profile Creation."

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
2. From the menu on the left side of the screen, select [Profile Settings] - [All Profiles].

   The "All Profiles" screen is displayed.
3. From the [Actions] button, select [Add Profile].

   The "Add Profile" wizard is displayed.
4. Follow the instructions on the "Add Profile" wizard and enter the setting items.

   Refer to the help screen for entering the setting items.

   [When setting up BIOS using policy]

   a. In the "Add Profile" wizard - "1.General Information" screen - [BIOS Policy], select the created policy.
   b. Enter the other setting items on the "1.General Information" screen, and then select the [Next] button.

      In the "2. Details" screen - [BIOS] tab, the setting values with the selected policies are automatically entered.
   c. Set the other items as required.

   [When setting up iRMC using policy]

   a. In the "Add Profile" wizard - "1.General Information" screen - [iRMC Policy], select the created policy.

b. Enter the other setting items on the "1.General Information" screen, and then select the [Next] button.

   On the "2. Details" screen - [iRMC] tab, the setting values with the selected policies are automatically entered.

c. Set the other items as required.

[When setting up MMB using policy]

a. In the "Add Profile" wizard - "1.General Information" screen - [MMB Policy], select the created policy.

b. Enter the other setting items on the "1.General Information" screen, and then select the [Next] button.

   On the "2. Details" screen - [MMB] tab, the setting values with the selected policies are automatically entered.

c. Set the other items as required.

[When setting up iRMC using Monitoring Policy]

a. In the "Add Profile" wizard - "1.General Information" screen - [Monitoring Policy], select [Enable].

b. Enter the other setting items on the "1.General Information" screen, and then select the [Next] button.

   On the "2. Details" screen - [iRMC] tab, the setting values of the selected policy are automatically entered.

c. Set the other items as necessary.

[When setting up virtual IO]

a. In the "Add Profile" wizard - "1.General Information," enter the setting items, and then select the [Next] button.

b. In the "2. Details" screen - [VirtualIO] tab, select [Settings] and follow the instructions on the wizard to enter the setting items.

5. Confirm the profile addition.

   After profile addition is complete, the corresponding profile will be displayed on the "All Profiles" screen.

   This finishes the profile creation. Next, assign the profile to a node.

6. Turn off the power to the server.

7. Select the profile to be assigned.

8. From the [Profile Actions] button, select [Assign/Reassign Profile].

   The "Profile Assignment" screen is displayed.

9. Follow the instructions on the "Profile Assignment" screen and enter the setting items.

   Refer to the help screen for entering the setting items.

   After setting the BIOS/iRMC/MMB/virtual IO, the [Status] field on the "All Profiles" screen will display [Assigned] for the corresponding server.

Point

By setting tags to nodes beforehand, you can filter the nodes by tags on the "Node List" screen. Filtering nodes makes it easier to extract target nodes.

Note

- Profile assignments for BIOS/iRMC settings may fail in some iRMC firmware versions if LDAP is enabled in the iRMC settings, and HTTP is specified as the protocol in [Web I/F URL] on the Details of Node screen. In this case, edit the node information to set HTTPS in [Web I/F URL] as the protocol. For information on editing nodes, refer to "2.2.3 Editing of Datacenters/Floors/Racks/Nodes" in "User's Guide."
- After replacing a node's system board, the BIOS/iRMC/MMB/Virtual IO settings configured in profile assignment are lost and therefore the profile should be reassigned.

- If the IP address of the iRMC with Profile for each model is changed, it is required to change the IP address of the node registered in ISM manually. If the IP address of the node registered is not changed, the ISM functions are not available for that node. For the device, the IP address changed after the server was restarted is reflected in iRMC (ISM 2.8.0.020 or later).
- Profile for each model may have the same settings as the iRMC settings. When profiles with different settings are applied with the same settings in the BIOS settings and the iRMC settings, the iRMC settings have a priority (ISM 2.8.0.020 or later).

3.3.2 Install an OS on a Server with a Profile (using PXE Boot)

Use PXE Boot to install an OS on the servers registered in ISM.

The following OSes can be installed:

- Windows Server
- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server
- VMware

1. Create a DHCP server as preparations of environment configuration before OS installation.

   For details, contact your local Fujitsu customer service partner.

2. As a preparation setting when installing the OS, import the OS image into the repository in advance.

   For the repository management, refer to "2.13.2 Repository Management" in "User's Guide."

3. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
4. From the menu on the left side of the screen, select [Profile Settings] - [All Profiles].

   The "All Profiles" screen is displayed.

5. From the [Actions] button, select [Add Profile].

   The "Add Profile" wizard is displayed.

6. Follow the instructions on the "Add Profile" wizard and enter the setting items.

   Refer to the help screen for entering the setting items.

   a. In the "Add Profile" wizard - "1.General Information" screen - [OS Type], select the OS type to be installed.
   b. Enter the other setting items on the "1.General Information" screen, and then select the [Next] button.
   c. Select the "2. Details" screen - [OS] tab to enter the setting items.
   d. Select the "2. Details" screen - [OS (for each node)] tab to enter the setting items.

   [When using a policy to set up OS]

   a. In the "Add Profile" wizard - "1.General Information" screen - [OS Policy], select the created policy.
   b. Enter the other setting items on the "1.General Information" screen, and then select the [Next] button.

      In the "2. Details" screen - [OS] tab and [OS (for each node)] tab, the setting values with the selected policies are automatically entered.

   c. Set the other items as required.

   After profile addition is complete, the corresponding profile will be displayed on the "All Profiles" screen.

7. Turn off the power to the server.
8. Select the profile to be assigned.
9. From the [Profile Actions] button, select [Assign/Reassign Profile].

   The "Profile Assignment" screen is displayed.

10. Follow the instructions on the "Profile Assignment" screen and enter the setting items.

    Refer to the help screen for entering the setting items.

    After the OS installation is complete, the [Status] field on the "All Profiles" screen will display [Assigned] for the corresponding server.

Point

By setting tags to nodes beforehand, you can filter the nodes by tags on the "Node List" screen. Filtering nodes makes it easier to extract target nodes.

3.3.3 Install an OS on a Server with a Profile (using ServerView embedded Lifecycle Management)

Use ServerView embedded Lifecycle Management (hereafter referred to as "eLCM") to install an OS on the servers registered in ISM.

The following OSes can be installed:

- Windows Server
- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server
- VMware

1. Structure a network environment on the target servers in advance.

    a. Create a network connection to the management LAN on the target servers.

    Set the LAN port that is used to install an OS on the [Profile] tab on the Details of Node screen, or in [Management LAN network port settings] of the profile settings. If it is not set, the first port of the onboard LAN is used.

    b. Prepare a DHCP server so that an OS can be installed with Profile Management.

    Enable the DHCP function in the ISM-VA or run the DHCP server in the same network segment as the target node. Execute the DHCP settings to be able to lease the appropriate IPv4 address to the LAN port for OS installation. Set the lease period to 60 minutes or longer.

    Example: Scope settings when the ISM-VA connects to 192.168.1.100/24

    - Lease range: 192.168.1.128 - 192.168.1.159
    - Lease period: eight days

2. Configure an eLCM environment on target servers in advance.

    For the procedures to configure the eLCM environment, verify it, and download eIM, refer to "ServerView embedded Lifecycle Management (eLCM) x.x for iRMC Sx Overview" (where x is the latest version.) from the following Fujitsu Manual Server site.

    https://support.ts.fujitsu.com/

    Reference procedure

    Select "Select a new Product" - [Browse For Product] and select the server that will structure the eLCM environment. Download from [Server Management Controller].

    Reference procedures are subject to change without notice.

3. Download embedded Installation Management (hereafter referred to as "eIM") to a bootable SD card on the target server.

    a. Use a profile for iRMC settings to configure the settings for the eIM download. For details on setting items, refer to "Chapter 1 BIOS/iRMC Setting Items of Profiles for PRIMERGY/PRIMEQUEST 3000B/4000E Servers" in "Items for Profile Settings (for Profile Management)."

    For the setting procedure, refer to "3.3.1 Set BIOS/iRMC/MMB/Virtual IO with Profiles."

b. Use the iRMC Web interface to download eIM to the bootable SD card on the target server.

   For the procedure to download eIM, refer to the manuals in Step 1.

4. Retrieve the information of eLCM.

   a. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].

   b. From the menu on the left side of the screen, select [Profile Assignment].

   c. Select the node name of the target node, and select the [Get Node Information] button on the "Node Information" screen.

   d. Select the [Get] button.

      Node information is retrieved.

5. Add the OS settings to the profile in Step 3a.

   a. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].

   b. From the menu on the left side of the screen, select [Profile Settings] - [All Profiles].

      The "All Profiles" screen is displayed.

   c. Select the profile in Step 3a, and then from the [Actions] button, select [Edit].

      The "Edit Profile" wizard is displayed.

   d. Follow the instructions in the "Edit Profile" wizard and enter the setting items.

      For the remaining steps, refer to Step 6 and the subsequent steps in "3.3.2 Install an OS on a Server with a Profile (using PXE Boot)."

Point

- As it takes time to retrieve node information, it is executed asynchronously.
- After the node information is retrieved, the log of message ID "10020303" is output in [Events] - [Events] - [Operation Log].

3.3.4 Create a Policy to Simplify Profile Creation

A template containing hardware settings for nodes is called a policy. When you manage a lot of nodes, you can simplify the input into the profile by setting common factors with the policy settings. You can create a policy depending on your needs and you do not have to always create a policy when creating a profile.

Here, the following procedures are described:

- Procedure for creating existing policies
- Procedure for creating a monitoring policy
- Procedure for referring to a monitoring policy from existing policies

Procedure for creating existing policies

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
2. From the menu on the left side of the screen, select [Policy Settings] - [All Policies].

   The "All Policies" screen is displayed.
3. From the [Actions] button, select [Add Policy].

   The "Add Policy" wizard is displayed.

   - When setting the BIOS policy

     On the "1. General Information" screen in the "Add Policy" wizard, select "BIOS" in the [Policy Type] field.

- When setting iRMC policy

  On the "1. General Information" screen in the "Add Policy" wizard, select "iRMC" in the [Policy Type] field.

- When setting MMB policy

  On the "1. General Information" screen in the "Add Policy" wizard, select "MMB" in the [Policy Type] field.

- When setting OS policy

  On the "1. General Information" screen in the "Add Policy" wizard, select "OS" in the [Policy Type] field.

Follow the "Add Policy" wizard and enter the other setting items.

Refer to the help screen for entering the setting items.

After the policy is added, the corresponding policy is displayed on the "All Policies" screen.

Point

On the "1. General Information" screen of the "Add Policy" wizard, you can create a policy for each model by selecting the [Select a Policy for each model] checkbox and selecting a model. Policy for each model can be set more detailed hardware settings by retrieving the setting items from the nodes (ISM 2.8.0.020 or later).

Note

Only users who belong to the Administrator group can create and edit monitoring policies.

Procedure for creating a monitoring policy

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
2. From the menu on the left side of the screen, select [Monitoring Policy Settings].

   The "Monitoring Policy" screen is displayed.
3. Select the [Edit] button.
4. Select the [Enable the monitoring policy] checkbox and enter the setting items.

   If you use the monitoring policy when registering nodes, select the [Assign the monitoring policy when registering discovered nodes.] checkbox.

   Refer to the help screen for entering the setting items.

   After the monitoring policy is edited, the results are displayed on the "Monitoring Policy" screen.

Procedure for referring to a monitoring policy from existing policies

1. Create a monitoring policy according to the procedure for creating a monitoring policy.
2. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
3. From the menu on the left side of the screen, select [Policy Settings] - [All Policies].

   The "All Policies" screen is displayed.
4. From the [Actions] button, select [Add Policy].

   The "Add Policy" wizard is displayed.

   - When setting iRMC policy

     On the "1. General Information" screen in the "Add Policy" wizard, select "iRMC" in the [Policy Type] field.
5. Select [Enable] in [Monitoring Policy].

   Follow the "Add Policy" wizard and enter the other setting items.

Refer to the help screen for entering the setting items.

After the policy is added, the corresponding policy is displayed on the "All Policies" screen.

3.3.5 Compare Assigned Profiles and Hardware Settings

After you have assigned a profile, ISM will verify the profile periodically. The user can also verify the profile at any time. The content of a profile and the BIOS/iRMC settings for a node are compared with verification of profiles. If [Verify Status] is [Mismatch], you can check for items that are different in the applicable profile, and determine whether changes were intended for node settings. You must change the status to [Match] in [Verify Status] by reassigning profiles or editing profiles to match the BIOS/iRMC settings for the server and the settings of the profile.

You can enable or disable verification of profiles by using the enable/disable commands for verification of profiles of ISM-VA Management. For details on the commands, refer to "4.24 Settings for Enabling/Disabling Verification of Profiles" in "User's Guide."

Here, the following operations are described.

- Procedures to execute the verification of profiles
- Procedures to check the items that do not match when [Verify Status] is [Mismatch]
- Procedures to change [Verify Status] back to [Match] if it is [Mismatch] (For items in which the node setting changes were not intended)
- Procedures to change [Verify Status] back to [Match] if it is [Mismatch] (For items in which the node setting changes were intended)

Procedures to execute the verification of profiles

ISM automatically verifies profiles (at approximately 24-hour intervals). You can also verify profiles at any time. The following is the procedure to verify profiles.

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
2. From the menu on the left side of the screen, select [Profile Settings] - [All Profiles].

   The "All Profiles" screen is displayed.
3. Select the profile to verify.
4. From the [Actions] button, select [Verify].

   The "Verify" screen is displayed.
5. Select [Execute].

   After the profiles are verified, [Match] or [Mismatch] is displayed in the [Verify Status] column for the applicable profile on the "All Profiles" screen.

Procedures to check the items that do not match when [Verify Status] is [Mismatch]

The following is the procedure to check for discrepancies in the applicable profile when [Mismatch] is displayed in [Verify Status].

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
2. From the menu on the left side of the screen, select [Profile Settings] - [All Profiles].

   The "All Profiles" screen is displayed.
3. Select the profile name for which [Verify Status] is [Mismatch].
4. Select the [BIOS] or [iRMC] tab.

   If there are discrepancies, the "There are differences in the profile settings." message is displayed.
5. Select "Differences from the server settings" from the pull down box below the message.

   The items that are different are displayed in red.

Procedures to change [Verify Status] back to [Match] if it is [Mismatch] (For items in which the node setting changes were not intended)

The following is the procedure to change [Verify Status] back to [Match] if [Verify Status] is [Mismatch] and there are items for which node setting changes were not intended.

1. Turn off the power to the server.
2. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
3. From the menu on the left side of the screen, select [Profile Settings] - [All Profiles].

   The "All Profiles" screen is displayed.
4. Select the profile in which to change [Verify Status] to [Match].
5. From the [Actions] button, select [Assign/Reassign Profile].

   The "Profile Assignment" screen is displayed.
6. Select the [Enable Advanced Settings] checkbox.
7. In [Assignment Mode], select "Assign profile also to unchanged portions."

   Follow the instructions on the screen, and enter the setting items.

   Refer to the help screen for entering the setting items.

   After the profile is assigned, [Match] is displayed in the [Verify Status] column for the applicable profile on the "All Profiles" screen.

Procedures to change [Verify Status] back to [Match] if it is [Mismatch] (For items in which the node setting changes were intended)

The following is the procedure to change [Verify Status] back to [Match] if [Verify Status] is [Mismatch] and there are items for which node setting changes were intended.

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
2. From the menu on the left side of the screen, select [Profile Settings] - [All Profiles].

   The "All Profiles" screen is displayed.
3. Select the profile in which to change [Verify Status] to [Match].
4. From the [Actions] button, select [Edit].
5. Follow the instructions in the "Edit Profile" wizard, and enter the correct setting items.

   After the profile is edited, [Reassignment] is displayed in [Status] for the applicable profile.
6. Select the target profile.
7. From the [Actions] button, select [Assign/Reassign Profile].

   The "Profile Assignment" screen is displayed.
8. Select the [Enable Advanced Settings] checkbox.
9. In [Assignment Mode], select "Handle profile as assigned in ISM without actually assigning it to the node."

   Follow the instructions on the screen, and enter the setting items.

   Refer to the help screen for entering the setting items.
10. Select the assigned profile.
11. From the [Actions] button, select [Verify].

    The "Verify" screen is displayed.
12. Follow the instructions on the "Verify" screen and enter the setting items.

    Refer to the help screen for entering the setting items.

    After the profile is verified, check that [Match] is displayed in the [Verify Status] column for the applicable profile.

If [Mismatch] is displayed, redo this procedure from Step 3.

Point

- To confirm the BIOS settings with verification of profiles, the backup files of the BIOS parameters must be saved on the server. Therefore, when you assign a profile, enable [Automatic BIOS Parameter Backup] in the iRMC settings for the profile.
- If the setting for [Automatic BIOS Parameter Backup] is disabled in the iRMC settings for the server or if the server does not have this setting, verification of profiles can not be executed with the latest BIOS settings. In this case, execute the verification of profiles (refer to "Procedures to execute the verification of profiles") after you have backed up the hardware settings for the BIOS (refer to "7.1.1 Backup Server Settings"). To check the existence of the [Automatic BIOS Parameter Backup] settings in the iRMC settings for the server, refer to the following manuals:
  - "ServerView Suite Remote Management iRMC S2/S3 - integrated Remote Management Controller"
  - "Fujitsu Software ServerView Suite iRMC Sx Web Interface" (Sx is the version number after S4)
- If the node is in Maintenance Mode, ISM will not execute verification of profiles. In this case, manually execute verification of profiles.
- The [Proxy Server] - [Password] item in the iRMC settings is not verified.
- If a profile has been assigned with the following settings on the "Profile Assignment" screen, [Verify Status] will be [Verify Failed]. In this case, manually execute verification of profiles.
  - [Assignment Mode]: "Handle profile as assigned in ISM without actually applying it to the node."

    [Assignment Mode] is an option that can be selected when the [Enable Advanced Settings] checkbox is selected.
  - [Status]: [Not assigned]

Note

- Verification of profiles may fail in some iRMC firmware versions if LDAP is enabled in the iRMC settings, and HTTP is specified as the protocol in [Web I/F URL] on the Details of Node screen. In this case, edit the node information to set HTTPS in [Web I/F URL] as the protocol. For information on editing nodes, refer to "2.2.3 Editing of Datacenters/Floors/Racks/Nodes" in "User's Guide."
- For the node which Profile for each model is assigned, verification of profiles is not available. For the node which Profile for each model is assigned, ISM does not verify the profiles periodically. Also, you cannot execute verification of profiles manually (ISM 2.8.0.020 or later).

3.3.6 Apply Hardware Settings When Registering Discovered Nodes

If you have previously created a policy (Monitoring Policy) that defines the settings required by ISM to monitor the target nodes, any time you automatically or manually discover and register a node, a profile referencing that policy is automatically created and assigned.

By creating a policy that can be referenced in advance, you can prevent errors and omissions in the settings required for hardware monitoring.

Point

For the procedure for creating a monitoring policy, refer to "3.3.4 Create a Policy to Simplify Profile Creation."

1. Register managed nodes.

   Execute the procedure in "3.1.1 Discover Nodes in the Network and Register Nodes" up to Step 10.
2. In the "Node Registration" wizard - "4. Monitoring/Node Group/Tag" screen, select the [Assign the monitoring policy when registering nodes] checkbox.
3. Select the [Next] button.

   If Monitoring Policy is not set or if there is no node that Monitoring Policy can be assigned to, you cannot select the checkbox.

4. In the "Node Registration" wizard - "5. Confirmation" screen, confirm the profile name, and then select the [Register] button.

   If the displayed profile name is already used, the name will be changed to a unique name and registered.

   You can check the profile name on the "Results" screen.

This finishes the procedure for applying hardware settings when registering discovered nodes.

Check the progress of the hardware setting from the "Tasks" screen.

3.4 Set up Switch/Storage

When installing or adding switches or storages, you can specify the following settings by using profiles:

- Switches

  Set the administrator password or SNMP settings for multiple nodes together.

- Storages

  Execute the RAID configuration settings or disk configuration settings.

By using Network Map, you can change the VLAN settings or Link Aggregation settings to multiple ports on multiple switches together.

3.4.1 Set up Switch/Storage with Profiles

Set RAID configuration or SNMP settings or account settings to the switch/storage registered in ISM by assigning the created profiles.

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
2. From the menu on the left side of the screen, select [Profile Settings] - [All Profiles].

   The "All Profiles" screen is displayed.
3. From the [Actions] button, select [Add Profile].

   The "Add Profile" wizard is displayed.
4. Follow the instructions on the "Add Profile" wizard and enter the setting items.

   Enter RAID configuration, SNMP settings, account and other settings for each device.

   Refer to the help screen for entering the setting items.

   After the profile is added, the corresponding profile will be displayed on the "All Profiles" screen.

   This finishes the profile creation. Next, assign the profile to a node.
5. Turn on the power to the server.
6. Select the profile to be assigned.
7. From the [Profile Actions] button, select [Assign/Reassign Profile].

   The "Profile Assignment" screen is displayed.
8. Follow the instructions on the "Profile Assignment" screen and enter the setting items.

   Refer to the help screen for entering the setting items.

   After the profile is assigned, the [Status] column of the profile will be displayed as [Assigned] on the "All Profiles" screen.

   This finishes the node profile assignment.

3.4.2 Change LAN Switch Settings from Network Map

Change the current settings of VLANs and Link Aggregations set on the LAN switch, while confirming them visually on the Network Map.

Change the VLAN settings of the LAN Switch

Change VLAN settings of LAN switch from the Network Map.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Network Map].

   The "Network Map Display" screen is displayed.

2. Select [Actions] - [Set Multiple VLANs] to enter the setting changes.
3. By LAN Switch on the Network Map, select the port to change the VLAN settings.
4. Select [Setting] on the upper-right of the screen to enter the setting changes.
5. Confirm the changes, and then select [Registration] if there are no errors.

   The settings are changed.

6. Refresh the network management information after the execution, and then confirm that the changes are applied on the Network Map.

   The [VLANs setting] operation will be registered as an ISM task. Select [Tasks] at the top of the Global Navigation Menu to confirm that the task has been completed.

   This finishes the VLAN setting changes.

Change Link Aggregation of the LAN switch

Change Link Aggregation of LAN switch from the Network Map.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Network Map].

   The "Network Map Display" screen is displayed.

2. Select [Actions] - [Set Link Aggregation].
3. Select the node to change the Link Aggregation settings, then select either of [Add], [Change] or [Delete].
4. Enter the setting change, select [Confirm].
5. Confirm the changes, and then select [Registration] if there are no errors.

   The settings are changed.

6. Refresh the network management information after the execution, and then confirm that the changes are applied on the Network Map.

   This finishes the Link Aggregation setting changes.

3.5 Create a Batch of Multiple Profiles and Allocate Them to Nodes

You can create a batch of multiple profiles by referencing an existing profile (batch duplicate) and allocate those profiles to multiple nodes when you want to configure multiple nodes to the same settings. This makes it simpler to create many profiles and apply them to nodes.

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
2. From the menu on the left side of the screen, select [Profile Settings] - [All Profiles].
   The "All Profiles" screen is displayed.
3. Select the profile to be referenced, from the [Actions] button, select [Batch Duplicate and Allocate].

   The "Batch Duplicate and Allocate Profiles" wizard is displayed.

4. Follow the instructions on the "Batch Duplicate and Allocate Profiles" wizard and enter the setting items.
5. Confirm the profile addition.

   The profiles that were selected to be allocated to the nodes in the "Batch Duplicate and Allocate Profiles" wizard will be displayed on the "All Profiles" screen.

   Next, assign the profile to a node.

6. From the menu on the left side of the screen, select [Profile Assignment].

   The "Node List" screen is displayed.

7. Select the node with the assigned profile, from the [Actions] button, select [Assign/Reassign Profile].

   The "Profile Assignment" screen is displayed.

8. Follow the instructions on the "Profile Assignment" screen and enter the setting items.

Point

The profiles created in [Batch Duplicate and Allocate] as well as the status for nodes that have been allocated will be [Reassignment].

Note

- The IP address of the OS and the computer name may overlap when [Batch Duplicate and Allocate] is executed to reference a profile that has been set on an OS. Edit the profile and change the IP address of the OS and the computer name before applying the profile.
- Virtual addresses may overlap when [Batch Duplicate and Allocate] is executed to reference a profile that has been set on a virtual IO. Edit the profile and change the virtual address before applying the profile.

3.6 Change Passwords

Change the password of the managed nodes and the password of the OS installed on the managed nodes.

Set the passwords after enabling Maintenance Mode on the target nodes.

3.6.1 Change the Password of the Managed Nodes

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].

   The "Node List" screen is displayed.

2. From Node List, select the node name of the target node.

   The Details of Node screen is displayed.

3. From the [Actions] button, select [Enable Maintenance Mode].

4. Change the password of the target node.

5. From the [Actions] button, select [Edit].

   The "Edit" screen is displayed.

   Point

   Batch editing is available to change passwords for multiple managed nodes. After selecting the target nodes on the "Node List" screen, edit them by selecting [Edit in a Batch] from the [Actions] button (ISM 2.8.0.060 or later).

6. Change the password of the communication methods to the password that was changed in Step 4.

   Change the other setting values if required.

7. Check the content of the changes, and then select the [Apply] button.

8. From [Actions] button, select [Disable Maintenance Mode].

   This finishes the password change for a managed node.

3.6.2 Change Password of OS

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].

   The "Node List" screen is displayed.

2. From Node List, select a node name of the target node.

   The Details of Node screen is displayed.

3. From the [Actions] button, select [Enable Maintenance Mode].
4. Change a password of the target OS.
5. Select the [OS] tab.
6. From the [OS Actions] button, select [Edit OS Information].

   The "Edit OS Information" screen is displayed.

   Point

   Batch editing is available to change passwords for multiple OSes. After selecting the target nodes on the "Node List" screen, edit them by selecting [Edit in a Batch] from the [Actions] button (ISM 2.8.0.060 or later).
7. Change the password to the password that was changed in Step 4.

   Change the other setting values if required.
8. Check the content of the changes, and then select the [Apply] button.
9. From [Actions] button, select [Disable Maintenance Mode].

   This finishes the password change for the OS.

3.7 Use CAS Based Single Sign-On to Log In to the Web Screen of the Server

Execute settings to log in to the web screen (iRMC screen) of the PRIMERGY server automatically (Single Sign-On) without specifying a user name and a password by using CAS (Centralized Authentication Service).

3.7.1 Set a Directory Server

Set up an LDAP server for a group link with Microsoft Active Directory.

For details, refer to "2.3.3 Link with Microsoft Active Directory or LDAP."

Note

- CAS can be used only when the directory server is Microsoft Active Directory.
- When you register certificates, specify the full computer name for the LDAP server name.

3.7.2 Set CAS Settings

Execute CAS settings to enable to log in to the iRMC screen after the login to ISM.

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].
2. From the menu on the left side of the screen, select [CAS Setting].

   The "CAS Settings" screen is displayed.
3. Select the [Set] button.

   The "CAS Settings" screen is displayed.
4. Enter the setting items.

   The information to be set is as follows:

   - CAS

     Set whether to enable or disable CAS.

- Port Number

  Set the port number to be used with CAS.

  You cannot specify 3170 for the port number.

- User Role

  Set a user role of the users who can use CAS.

Note

- After CAS has been restarted, log in to ISM again after "CAS Status" is normal in [Settings] - [Users] - [CAS Setting].

  By setting alarms for CAS restart events, you can be notified when CAS restarts. For information on the procedure for setting, refer to "2.2 Set an Alarm (ISM internal events)" and "2.2.1.2 Send mail."

- If you use CAS, set certificates in ISM. For information on the procedure for setting, refer to "4.7 Certificate Activation" in "User's Guide." If you use CAS on ISM in which certificates were set before ISM 2.4.0, set the certificates again.

3.7.3 Set CAS Users

Set users who can use CAS as follows.

1. Setting of the user group to which the user belongs

   - Managed Nodes

     Set "Manage all nodes."

   - Authentication Method

     Set "Open LDAP/Microsoft Active Directory (LDAP)."

   For user group settings, refer to the following.

   - "2.3.2.1 Add user groups"
   - "2.3.2.2 Edit user groups"

2. User Settings

   - Directory server

     Set the user in the directory server (LDAP server) that was set in "2.3.3.2 Manage users and passwords on directory servers."

   - ISM

     a. User Name

        Set a user name existing in the directory server set in "2.3.3 Link with Microsoft Active Directory or LDAP."

     b. Authentication Method

        Set "Follow user group setting."

     c. User Group

        Set the name of the user group set in 1 above.

     d. User Role

        The following are user roles set in "3.7.2 Set CAS Settings" and user roles that can use CAS.

        Table 3.23 User roles that can use CAS

User roles specified in CAS Settings	User roles that can use CAS
Administrator	Administrator
Operator	Administrator

User roles specified in CAS Settings	User roles that can use CAS
	Operator
Monitor	Administrator
	Operator
	Monitor

For details on user settings, refer to the following.

- "2.3.1.1 Add users"
- "2.3.1.2 Edit users"

Note

Users who belong to the user groups other than the user group whose setting item [Managed Nodes] is "Manage all nodes" cannot use CAS.

3.7.4 Set iRMC

Set CAS information set in "3.7.2 Set CAS Settings" in iRMC.

Set the following in [Setting] - [User Management] - [Centralized Authentication Service (CAS)] of iRMC in which CAS is used.

- CAS Support

  Select "Enable CAS"

- Server

  Set the IP address of ISM.

- Network Port

  Set the port number set in "3.7.2 Set CAS Settings."

- Login Page Display

  It is recommended that you select the [Always display Login Page] checkbox.

  Displays behaviors when selected.

  - At the automatic login to the web screen of iRMC after the login to ISM, the screen to select "Login" or "CAS login" is displayed.
    - If you select "Login," you can log in by specifying a user account of iRMC.
    - If you select "CAS login," you can log in automatically.

- Redfish role

  For the servers that have the [Redfish Role] setting item, select items other than "No Access."

  If you select "No Access," you cannot use automatic login that was enabled by selecting "CAS login" on the iRMC web screen.

Note

- If you clear the [Always display Login Page] checkbox, you cannot log in to the web screen of iRMC unless you log in to ISM. In that case, enter the URL of the login screen in the web browser manually.

  URL example for the login screen: https://<IP address of iRMC>/login

- Do not give privileges exceeding the required range to the user privilege of iRMC using CAS.
- If the setting in [Settings] - [User Management] - [Central Authentication Service (CAS)] - [Assign Permissions From] of iRMC is "LDAP permissions," set "(userPrincipalName=%s)" in [Settings] - [User Management] - [Lightweight Directory Access Protocol (LDAP)] - [Access Configuration] - [User Login Search filter] of iRMC.

3.7.5 Log In without Specifying User Name and Password

Log in to the web screen of iRMC without specifying a user name and a password with the following procedure.

1. Log in to ISM.
2. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].

   The "Node List" screen is displayed.
3. Select the target node name from the node list.

   The Details of Node screen is displayed.
4. Select the URL of [Web I/F URL] on the Details of Node screen.

   The login screen of iRMC is displayed.
5. Select "CAS login."

Note

If you select "CAS login" on the web screen of iRMC without logging in to ISM, the ISM login screen will be displayed.
After the login to ISM, iRMC screen is not displayed. On the Details of Node screen of ISM GUI, select the URL in the [Web I/F URL] to display the iRMC screen.

3.8 Log in Directly to iRMC from ISM (ISM 2.8.0.060 or later)

To display the iRMC Web interface from ISM, the existing procedure is to register the IP address of the iRMC in the [Web I/F URL] in the Details of Node screen and select that URL. However, this procedure requires a login operation.

This section describes the iRMC login procedure, which displays the iRMC Web interface directly without executing the login operation to iRMC.

Note

You need to disable your pop-up blocker. Allow pop-ups for the ISM URLs in your web browser.

3.8.1 Set Relay Route

A relay route is set when there is a router between the management terminal and the monitored node, and access from the management terminal to the iRMC is restricted by a firewall.

If the management terminal and ISM-VA are in the same network or if there is no firewall setting, there is no need to set the relay route.

For the feature of the relay route, refer to " 2.3.7.1 Web interface screen display with iRMC Login " in "Use's Guide."

By setting the relay route according to the following procedure, the iRMC login via the relay route can be executed.

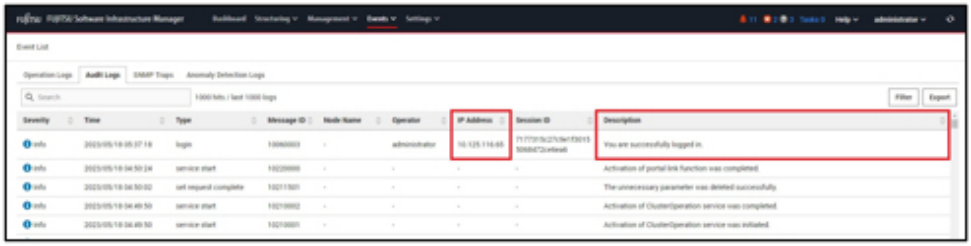
1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].
2. From the menu on the left side of the screen, select [Relay Route Settings].
3. Select the [Set] button.

4. Set the IP address of the management terminal to any unconfigured relay route number.

Point

- The IP address of the management terminal to be set as the relay route may not be the IP address of the management terminal itself, depending on the settings of the router between the management terminal and the monitoring node. You can check the IP address to be set by following the procedure below.

  1. From the Global Navigation Menu on the ISM GUI, select [Events] - [Events].
  2. Select [Audit Logs] tab and check the IP address in the [IP Address] that displays in the line of "You are successfully logged in." in [Description].



- If multiple IP addresses display "You are successfully logged in." is displayed, you have logged into ISM-VA from multiple management terminals.
  Set the IP address by identifying the management terminal to which the relay route should be set.

5. Install the client certificate for the relay route which is issued by ISM-VA on the management terminal with the relay route is set.

   For details on how to create and install the client certificate for the relay route, refer to "4.29 Creation of client certificate for relay route" in "User's Guide."

3.8.2 Log in to iRMC from ISM

The iRMC login procedure is described below.

The [Login] button is displayed only for nodes that allow iRMC login.

Note

The "Destination IP Address " in the pull-down box displayed when the [Login] button is selected indicates the IP address of the last iRMC that any user connected to using a relay route. Since only one user can use a relay route at the same time, when sharing a relay route with other users, make sure that no other users are using the relay route beforehand. If the relay route is used at the same time, the connection of the first user is disconnected and the connection used later becomes valid.

Enable iRMC login

Enable iRMC login for a user group.

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].
2. From the menu on the left side of the screen, select [User Groups].
3. Select the target user group, and then from the [Actions] button, select [Edit].
4. Select [Enable] in [iRMC Login/AVR].

Log in to iRMC from Node List

Execute iRMC login by selecting the [Login] button of the node list.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].

   The "Node List" screen is displayed.
2. In the [iRMC Login] of the target node, select the [Login] button.

   If multiple relay routes are set, the relay route number is displayed in a pull-down box when the [Login] button is selected.

   The iRMC screen is displayed in a separate web browser window.

Log in to iRMC from the Details of Node screen

Execute iRMC login by selecting the [Login] button on the Details of Node screen.

1. In the [iRMC Login] on the Details of Node screen, select the [Login] button.

   If multiple relay routes are set, the relay route number is displayed in a pull-down box when the [Login] button is selected.

   The iRMC screen is displayed in a separate web browser window.

Point

If a relay route is set, you may be prompted to select a certificate before the iRMC screen displays in a separate window.

Chapter 4 Confirm the Status of a Managed Node

This chapter describes the procedure to check information such as the status of managed nodes or resources, or logs.

4.1 Operate Dashboard

The Dashboard displays widgets that show various information about status, logs etc. The user can select a widget to refer to information according to their needs.

Refer to the help screen for the procedure to select a widget to show on the Dashboard.

4.2 Confirm the Position of a Node

If you specified the settings for the mounting positions of nodes in racks, you can confirm them on the "Rack View" screen of the GUI.

If you did not specify the settings for the mounting positions in racks, the nodes are displayed as "Not Mounted."

The "3D View" can be used to confirm positions of the floors, racks, and position of the devices within racks as three-dimensional images.

Check the mounting position of a node with Rack View

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Datacenters].

   The "Datacenter List" screen is displayed.

2. Select the target rack and check the position of a node.

Check the Status of a node with 3D View

Check the positions of the rack and devices, and status or power consumption and inlet air temperature of them with 3D View.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [3D View].

   The "3D View" screen is displayed.

2. Execute the following operations depending on your purpose:

   - When switching the floor to display

     a. Select floor display part in the Floor summary on the upper-left of the "3D View" screen.

        The "Select Floor" screen is displayed.

     b. Select the floor to check, and then select the [Apply] button.

        The floor display switches.

   - When switching the information to display

     Select the information to display with the button to switch the display information on the bottom right of the "3D View" screen.

     With 3D View, the following display information can be confirmed:

     - Status
     - Alarm Status
     - Air Inlet Temperature
     - Power consumption

   This finishes the confirmation of the node status with 3D View.

Point

When you want to display Power Consumption status in the display information, you must set the threshold values for [NodePowerConsumption] from the Details of Node screen - [Monitoring] tab for the managed device in advance.

4.3 Confirm the Status of a Node

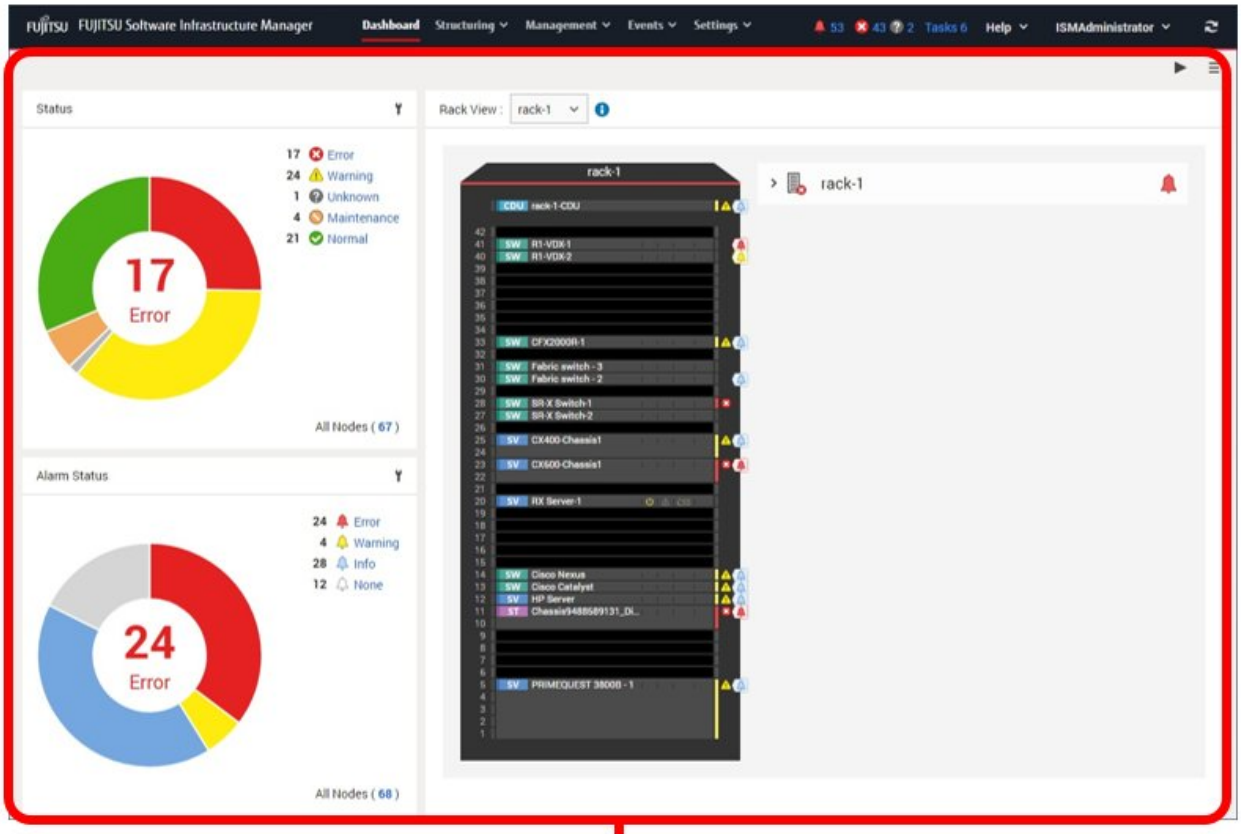
The node status can be checked in the [Status] widget on the Dashboard or on the "Node List" screen.

1. From the Global Navigation Menu on the ISM GUI, select [Dashboard].

   The "Dashboard" screen is displayed.

2. In the [Status] widget, confirm the status of the node.

   Refer to the help screen for detailed descriptions regarding the [Status] widget.



[Dashboard] screen

3. In the [Status] widget, select the status to check (Error, Warning, Maintenance, Normal, and Unknown).

   The nodes with the target status will be displayed on the "Node list" screen.

   It may take time to display the node list depending on the number of nodes registered in ISM.

   Refer to the help screen for descriptions of the content displayed.

   This finishes the node status display.

4.4 Display the Node Notification Information

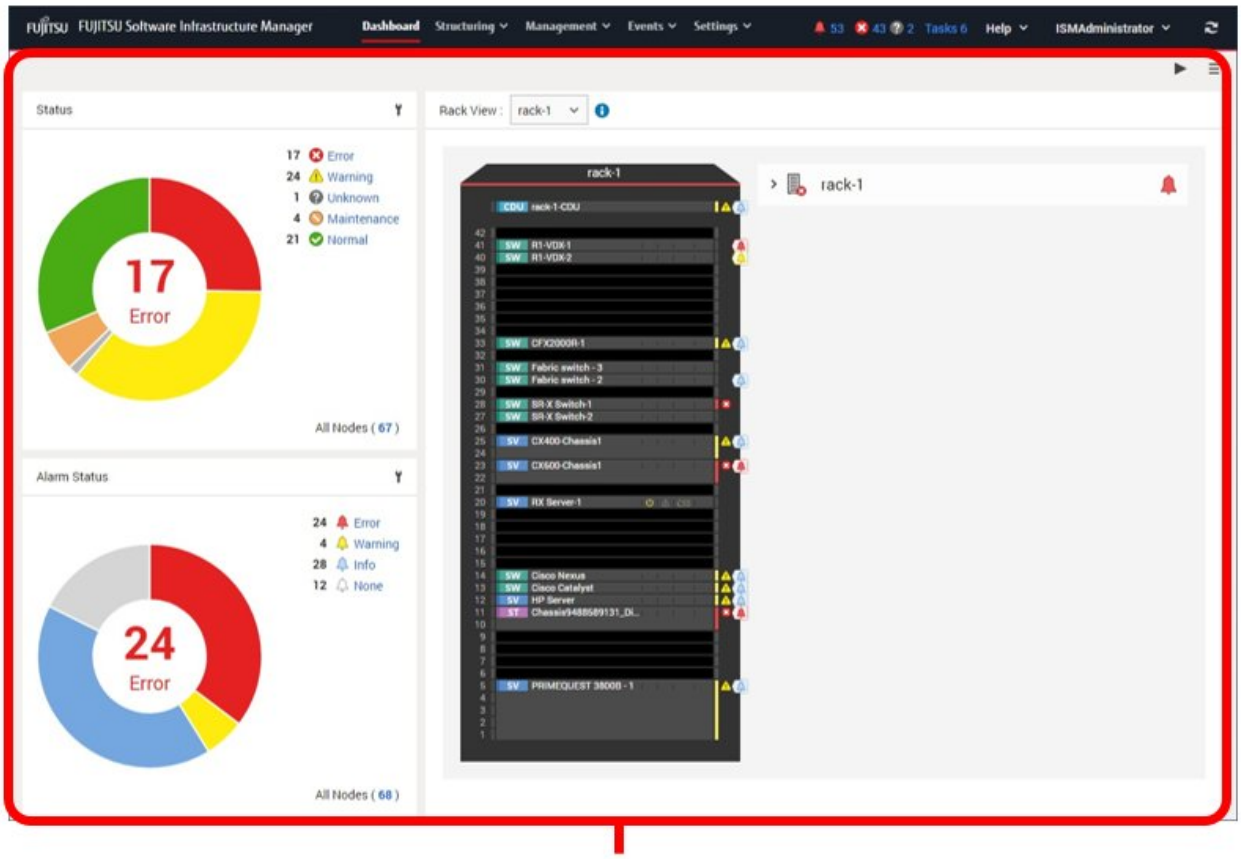
The node status, as well as whether an event has occurred on the node can be checked using either the [Alarm Status] widget on the Dashboard or by checking the "Node List" screen.

1. From the Global Navigation Menu on the ISM GUI, select [Dashboard].

   The "Dashboard" screen is displayed.

2. In the [Alarm Status] widget, check the alarm.

   Refer to the help screen for descriptions regarding the [Alarm Status] widget.



[Dashboard] screen

3. In the [Alarm Status] widget, select the status to check (Error, Warning, Info, and None).

   The nodes with the alarm status will be displayed on the "Node list" screen.

   It may take time to display the node list depending on the number of nodes registered in ISM.

   Refer to the help screen for descriptions of the content displayed.

   This finishes the display of the node notification information.

4.5 Display Monitoring History in a Graph

On the ISM GUI, the history of monitoring items accumulated with Monitoring can be displayed in a graph. The graph display allows the user to easily grasp transitions and tendencies in the history of the monitored items. There are two ways to display, one is displaying a graph for each node and the other is displaying graphs for multiple nodes on the [Monitoring History] widget on the Dashboard.

4.5.1 Display Monitoring History in a Graph for each Node

Displays the history of monitoring items in a graph for each node.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].

   The "Node List" screen is displayed.

2. Select the node name of the target node.

3. Select the [Monitoring] tab.
4. Select the [Graph] button for the monitoring item to display in a graph.

   The "Monitoring Item Graph" screen is displayed and the graph will be displayed.

Display multiple graphs piled together

On the "Monitoring Item Graph" screen, multiple graphs can be displayed on top of one another.

Compare with other periods

From the [Compare with other periods] tab, graphs for the multiple periods of the same monitoring item can be displayed on top of one another. You can add 5 periods at a maximum and can display 6 graphs on top of one another. By putting the graphs of multiple periods together, you can compare and grasp the tendency by time or by day.

The procedure is as follows.

1. From the [Compare with other periods] tab, select the [Add display period] button.
2. Select the period to display in the graph.

   Multiple graphs are displayed on top of one another.

Compare with other item

From the [Compare with other item] tab, graphs for the multiple items of the same node can be displayed on top of one another. You can add one item at a maximum and can display two graphs on top of one another. By putting the graphs of other items together, you can grasp the correlation between the items.

The procedure is as follows.

1. From the [Compare with other item] tab, select the [Add display item] button.
2. Select items to compare and the start date and time for graph display.

   Multiple graphs are displayed on top of one another.

4.5.2 Display Monitoring History of Multiple Nodes in a Graph

Displays the monitoring history of multiple nodes in a graph.

1. From the Global Navigation Menu on the ISM GUI, select [Dashboard].
2. Select [Add Widget].
3. Select [Monitoring History], and then select the [Add] button.
4. Follow the "Widget settings" wizard, select nodes and monitoring items to display on the widget.

   The [Monitoring History] widget is added to the Dashboard.

Point

- If you add the [Monitoring History] widget, the pull down menu to specify the period is displayed on the upper right of the Dashboard screen. From this pull down menu, you can change the periods to display on the [Monitoring History] widget.
- In the pull down menu for specifying the period, you can only change the periods to display on the [Monitoring History] widget. If you specify the period from this menu, widgets other than [Monitoring History] will not be affected.

4.6 Confirm the Firmware Version

Displays the firmware version of the servers registered in ISM.

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Firmware/Driver].

   The "Node List" screen is displayed.

2. Select the node name of the target device and retrieve node information from the "Node Information" screen - [Get Node Information].

   Execute it for the same number of the node to confirm the firmware version.

   On the "Node List" screen, the firmware version of the server will be displayed in the [Current Version] column.

   This finishes the check of the firmware version of the server.

Point

- As it takes time to retrieve node information, it is executed asynchronously.
- When node information is retrieved, the log of message ID "10020303" is output in [Events] - [Events] - [Operation Log].
- By setting tags to nodes beforehand, you can filter the nodes by tags on the "Node List" screen. Filtering nodes makes it easier to extract target nodes.

4.7 Display Node Logs

Display the logs collected from the managed node lined up in a time series. By specifying the requirements of the managed node, Severity, Category (Hardware, operating system) etc., the logs displayed can be narrowed down.

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Log Collection].
2. From the menu on the left side of the screen, select [Node Log Search].

   The "Node Log List" screen is displayed.
3. To narrow down the displayed node logs, select the [Filter] button.

   The "Filter" screen is displayed.
4. Enter the filter requirements on the "Filter" screen, and then select the [Filter] button.

   Refer to the help screen for entering the filter requirements.

   The filtered node logs will be displayed on the "Node Log List" screen.

   This finishes the node logs display.

4.8 Download Archived Logs

The Archived Logs collected from the managed node can be downloaded.

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Log Collection].
2. From the menu on the left side of the screen, select the [Log Management] - [Archived Log] tab.
3. Select the checkbox for the node whose Archived Logs should be downloaded.
4. From the [Actions] button, select [Create Download Files].

   The "Create Download Files of Archived Log" screen is displayed.
5. Enter the setting items, then select the [Apply] button.

   Refer to the help screen for entering the setting items.

   The download file is created.
6. Select the [Download] button in the download file items.

   The download file created in Step 5 will be downloaded to the console.

   This finishes the download of the Archived Logs.

4.9 Filter Nodes with Detailed Information

Nodes can be filtered with the detailed information of managed nodes so that only nodes that have specific information are displayed.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].

2. Select the button.

   The "Filter" screen is displayed.

3. Specify filter items. When you want to filter for all items, specify the filter conditions in [All Items] field. When you want to filter for an individual item, specify filtering conditions in the field of applicable filtering items.

   Point

   If specified multiple statuses in [Status] and [Alarm Status], search with OR condition will be executed. If multiple items other than [Status] and [Alarm Status] are specified, or multiple conditions delimited by a space are specified for one item, search with AND condition will be executed. Upper case and lower case are not distinguished.

4. Select the [Filter] button.

   On the "Node List" screen, nodes which have been filtered with the specified items are displayed.

   If [Status], [Alarm Status], or [Boot Type] is specified as a filter condition, the specified status button or pull down box at the top of the "Node List" screen becomes selected.

4.10 Detect Nodes that are not Behaving Normal

You can detect servers that are not behaving normally (anomalies) using Anomaly Detection. Execute Anomaly Detection with the following procedures.

- 4.10.1 Set Alarms and Actions
- 4.10.2 Enable the CPU Utilization Prediction Setting
- 4.10.3 Start Anomaly Detection
- 4.10.4 Confirm the Current Anomaly Detection Status
- 4.10.5 Confirm Anomaly Detection Event Notifications
- 4.10.6 Confirm Anomaly Detection History
- 4.10.7 Stop Anomaly Detection
- 4.10.8 Disable the CPU Utilization Prediction Setting

4.10.1 Set Alarms and Actions

You can set notifications to ISM external devices for alarms using the action and alarm settings for events for when an anomaly is detected and when an anomaly has recovered. If you do not need notifications for alarms, this procedure is not required.

1. Set the action.

   For the setting procedure for actions, refer to "3.2.1.1 Execute action settings (notification method)."

2. Add the alarm.

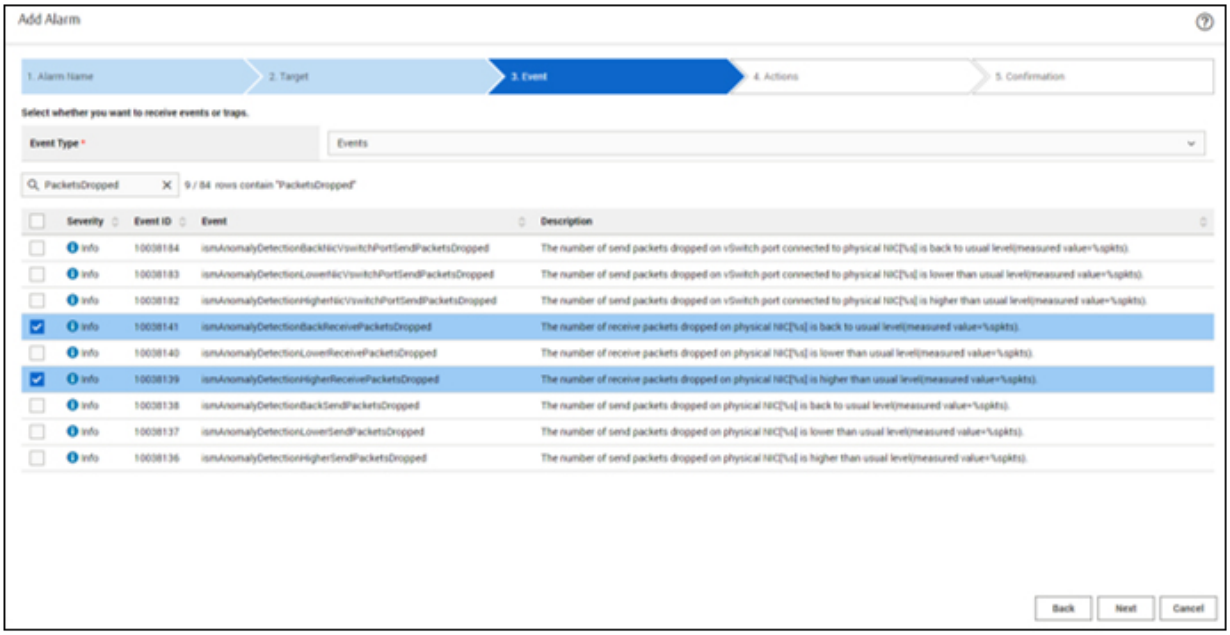
   For the setting procedure for alarms, refer to "3.2.1.3 Set an alarm to the managed devices." Select the following in the "Add Alarm" wizard.

   Select "Nodes (for each node)", "Nodes (All Nodes)" (ISM 2.8.0.030 or later), or "Nodes (Node Group)" (ISM 2.8.0.030 or later) in [Applicable Type] on the "2. Target" screen to select an alarm setting target node.

Select "Events" in [Event Type] on the "3. Event" screen, and then select the event for the alarm notification from Event ID that starts with "ismAnomalyDetection" for the event type.

In the following example, the detection and recovery for "Receive packets dropped (higher than usual level)" on the physical NIC are set.

Figure 4.1 Example of selecting an event in "Add Alarm"



4.10.2 Enable the CPU Utilization Prediction Setting

This setting predicts a rise in CPU usage and enables/disables the date and time prediction exceeding a certain value for detecting anomalies. If you do not want to make a prediction, this step is not necessary.

Use the following procedure to enable the CPU Utilization Prediction setting.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].

   The "Node List" screen is displayed.

2. From the [Actions] button, select [Set CPU Utilization Prediction].

   The "Set CPU Utilization Prediction" screen is displayed.

3. In [CPU Utilization Prediction], select "Enable."

4. Select the [Apply] button.

Point

- The CPU Utilization Prediction setting is applied to all nodes running Anomaly Detection of the virtual platform. It is also applied if you start Anomaly Detection first and enable the CPU Utilization Prediction setting later.
- When you enable the CPU Utilization Prediction setting, the prediction occurs after the prediction data is created. For more details on prediction data, see "2.3.6 Anomaly Detection" in "User's Guide."

4.10.3 Start Anomaly Detection

Start Anomaly Detection using the following procedure.

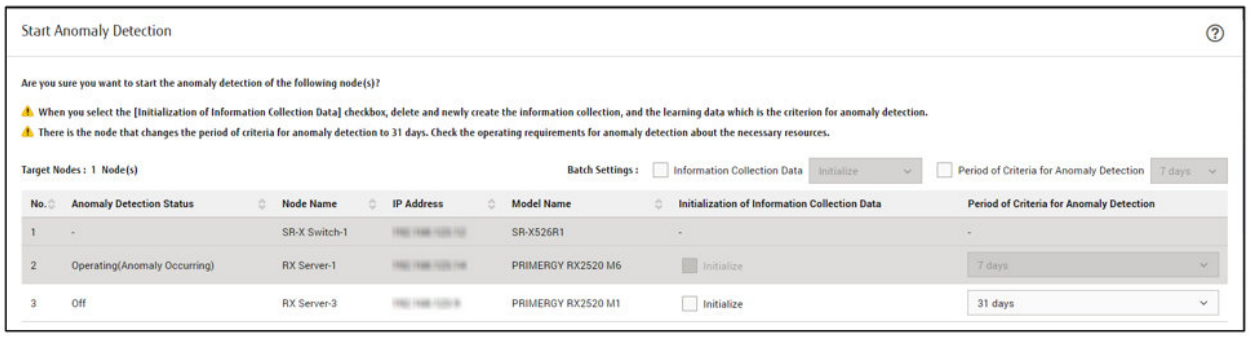
1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].

   The "Node List" screen is displayed.

2. Select the checkbox for the node that you want to start Anomaly Detection for from the node list that is displayed.
3. From the [Actions] button, select [Start Anomaly Detection].
4. Confirm the target node on the "Start Anomaly Detection" screen.

   Nodes that Anomaly Detection will not be started for (nodes that are not supported or nodes in which Anomaly Detection is already started) are displayed in gray.

   Figure 4.2 "Start Anomaly Detection" screen



Point

If you want to initialize the information collection data, select [Initialization of Information Collection Data].

For details, refer to "2.3.6.2 Starting and stopping Anomaly Detection" in "User's Guide."

5. Select the [Period of Criteria for Anomaly Detection].
6. Confirm the target nodes for starting Anomaly Detection, and then select the [Yes] button.
7. Confirm the "Results" screen.

Point

- If starting Anomaly Detection for one node, select the target node from the "Node List" screen, select the [Anomaly Detection] tab on the Details of Node screen, and from the [Anomaly Detection Action] button, select [Start Anomaly Detection].
- After Anomaly Detection is started, learning data is created, and then the anomaly analysis is started (about two and a half days at least). In addition, when the CPU Utilization Prediction setting is enabled, the prediction will start three weeks after the start of Anomaly Detection.

Note

- If performing maintenance on a node, stop Anomaly Detection. Behavior as a result of maintenance tasks may be considered not normal by Anomaly Detection. The status for maintenance tasks could also be considered as normal in the learning data and decrease the accuracy of Anomaly Detection.
- Additional resources are required if you set the period of criteria for anomaly detection as [31 days]. For more information, refer to "2.3.6.1 Operation requirements" in "User's Guide."

4.10.4 Confirm the Current Anomaly Detection Status

[Anomaly Detection Status] is not "Off" for nodes for which Anomaly Detection is started.

Perform the required action for the status that is displayed.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].

   The "Node List" screen is displayed.

2. Select the target node, and then select the [Anomaly Detection] tab.

3. Check [Anomaly Detection Status].

4. Take action according to the status that is displayed.

   Refer to "2.3.6.4 Anomaly Detection statuses" in "User's Guide."

Point

- Collection (when learning data is created) is the standard for the normal range used to determine an anomaly. Conduct normal operations during collection (when learning data is created) to gather information that is closer to actual operations.
- Learning data is updated every 12 hours for the virtual platform, every 24 hours for the physical server (ISM 2.8.0.030 or later). You can get higher accuracy for determining behavior that is not normal by consistently using Anomaly Detection.

4.10.5 Confirm Anomaly Detection Event Notifications

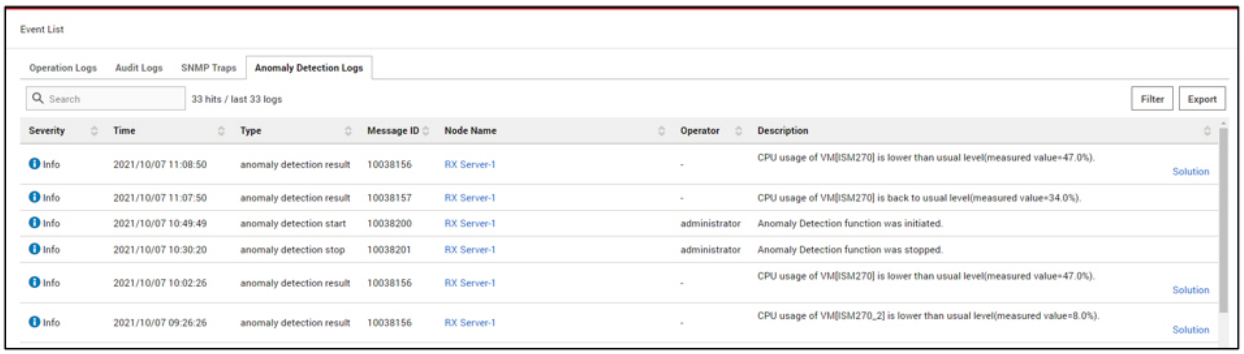
Notifications are made for events for anomaly detection results when behavior that is not normal is detected (anomaly detection) or when normal behavior is recovered for nodes in which Anomaly Detection is started. When alarm notification is set for the corresponding event, the action that has been set (mail notification, etc.) is performed.

Check Anomaly Detection events with the following procedure.

1. From the Global Navigation Menu on the ISM GUI, select [Events] - [Events].

   The "Event List" screen is displayed.

2. Select the [Anomaly Detection Logs] tab.



3. Check the events that were notified.

   Notification is made for events such as when Anomaly Detection is started or stopped, an anomaly is detected, and when normal behavior is recovered.

4. In the [Description] column, select [Solution].

   The "Solution" screen is displayed.

Point

If checking Anomaly Detection events for one node, select the target node from the "Node List" screen, select the [Properties] tab on the Details of Node screen, and then select the number for [Anomaly Detection Log].

4.10.6 Confirm Anomaly Detection History

Check the history for Anomaly Detection with the following procedure.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].

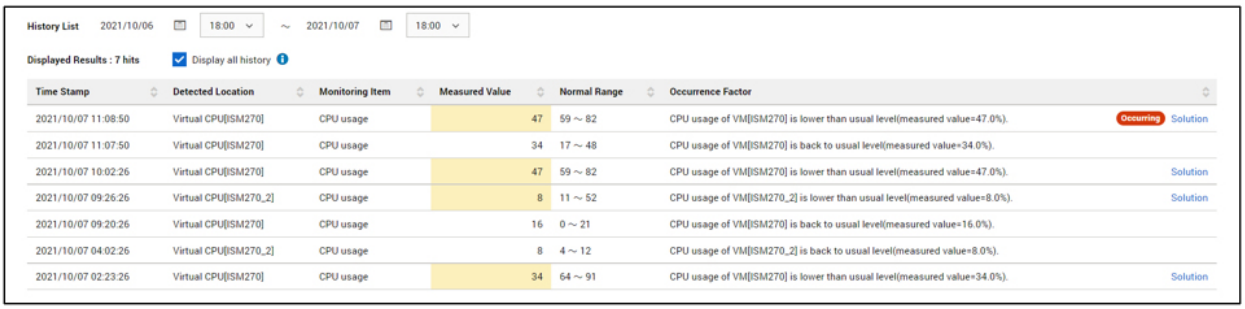
   The "Node List" screen is displayed.

2. Select the target node, and then select the [Anomaly Detection] tab.

3. In the [History List], specify the period that you want to display.

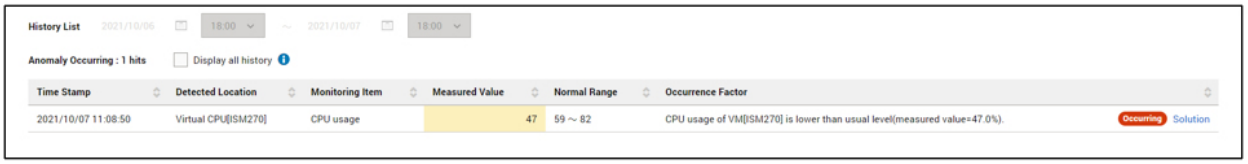
   - To check the history of any period

     Select the [Display all history] checkbox, and then select the start date/time and end date/time.



   - To check the history of all periods

     Clear the [Display all history] checkbox.

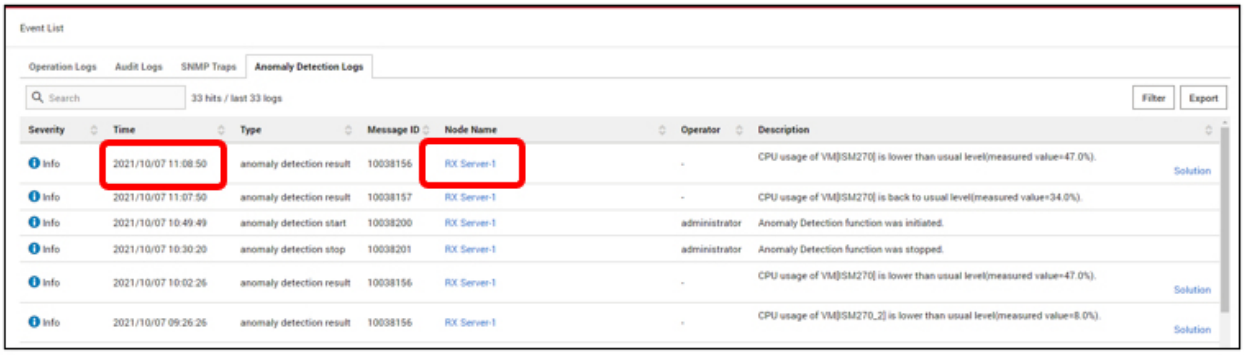


Checking Anomaly Detection history for a node that corresponds to an anomaly detection result event

To check for Anomaly Detection events, refer to "4.10.5 Confirm Anomaly Detection Event Notifications."

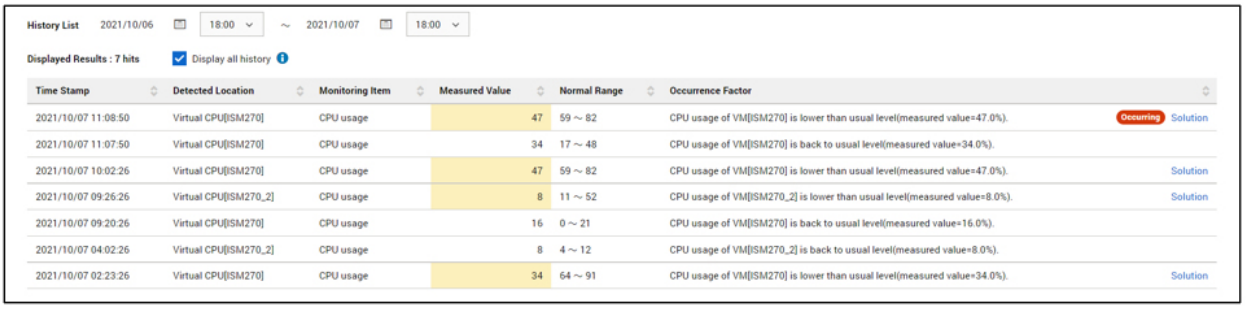
1. Record the date of the event you want to confirm on the "Event List" and select the node name.

   In the following example, the recorded date for the event is "2021/10/7 11:08:50," and the selected node name is "RX Server-1."



   On the Details of Node screen for the node you selected, the [Anomaly Detection] tab is displayed.

2. In [History List], specify the times you recorded in Step 1.



4.10.7 Stop Anomaly Detection

Stop Anomaly Detection using the following procedure for nodes that no longer need Anomaly Detection.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].

   The "Node List" screen is displayed.

2. Select the checkbox for the node that you want to stop Anomaly Detection for from the node list that is displayed.
3. From the [Actions] button, select [Stop Anomaly Detection].
4. Confirm the target node on the "Stop Anomaly Detection" screen.

   Nodes that Anomaly Detection will not be stopped for (nodes that are not supported or nodes in which Anomaly Detection is already stopped) are displayed in gray.

5. Confirm the target nodes for stopping Anomaly Detection, and then select the [Yes] button.
6. Confirm the "Results" screen.

Point

If stopping Anomaly Detection for one node, select the target node from the "Node List" screen, select the [Anomaly Detection] tab on the Details of Node screen, and from the [Anomaly Detection Action] button, select [Stop Anomaly Detection].

4.10.8 Disable the CPU Utilization Prediction Setting

Use the following procedure to disable the CPU Utilization Prediction setting.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].

   The "Node List" screen is displayed.

2. From the [Actions] button, select [Set CPU Utilization Prediction].

   The "Set CPU Utilization Prediction" screen is displayed.

3. In [CPU Utilization Prediction], select "Disable."
4. Select the [Apply] button.

Note

If you disable the CPU Utilization Prediction setting, the prediction data created is deleted. Therefore, even if you enable the CPU Utilization Prediction setting again, a three-week period is required to start the prediction in order to create new prediction data.

For more details on prediction data, see "2.3.6 Anomaly Detection" in "User's Guide."

Point

It is possible to continue to use Anomaly Detection and only disable the CPU Utilization Prediction setting.

Chapter 5 Identify Managed Nodes in Error

This chapter describes the procedure to identify the managed nodes on which some errors occur and the procedure to collect the maintenance data in such cases.

5.1 Confirm Nodes that have an Error

By displaying only the monitoring target nodes where an error occurred, it becomes easy to check the information of error nodes.

ISM does not refresh the status of the nodes on the screen in real time. In order to display the current status of the node, select the [Refresh] button to refresh the screen.

1. From the Global Navigation Menu on the ISM GUI, select [Dashboard].
2. In the [Status] widget, select [Error] on the right side of .

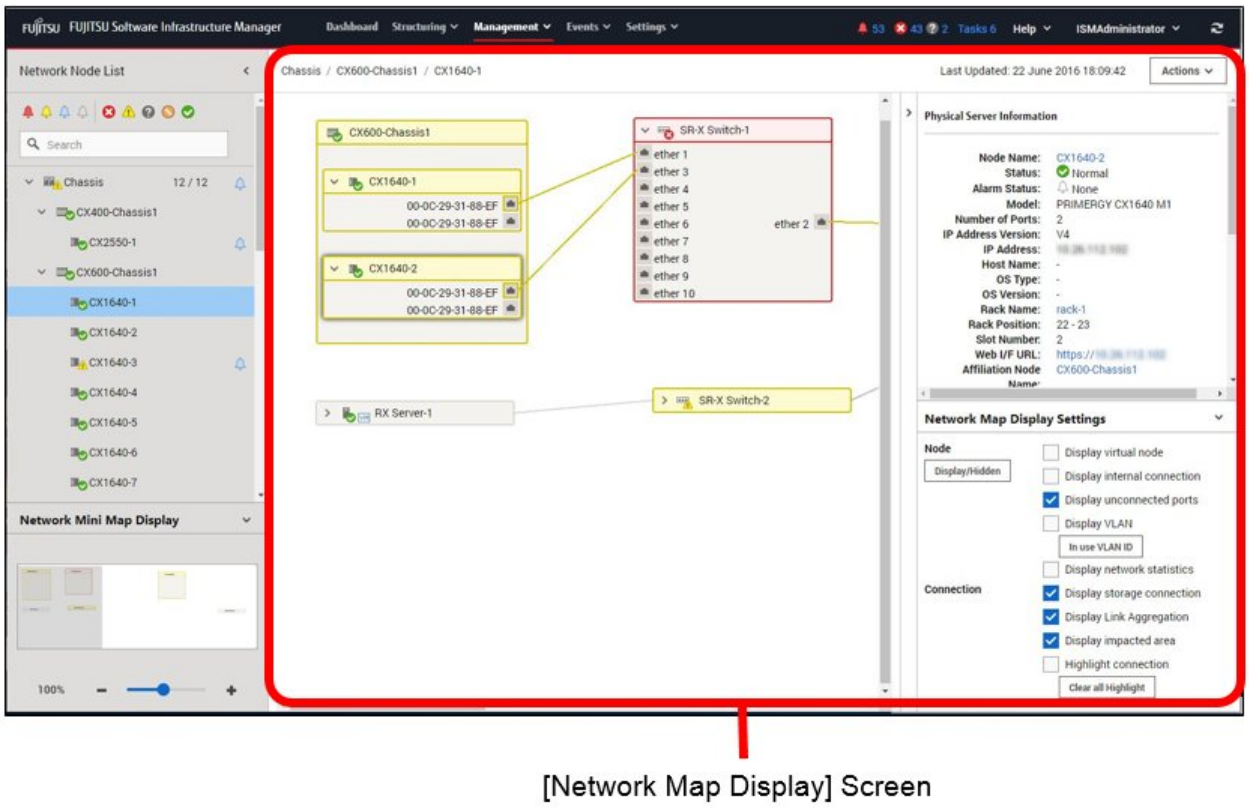
   Only the nodes where an error has occurred are displayed.
3. Check the status for the error nodes displayed.

5.2 Confirm the Error Location/Affected Area on the Network

You can graphically check the error location on the network and its affected area with the Network Map.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Network Map].

   The "Network Map Display" screen is displayed.



[Network Map Display] Screen

   Check the node indicated in red. The node where an error occurs turns red.
2. On the "Network Map Display Settings" pane displayed on the lower right on the Network Map, select the [Display impacted area] checkbox to display the status of the impacted area.

   The connection in the affected area, the port frame or the node frame is displayed in yellow.

When virtual networks are configured, the virtual machines within the affected area, the virtual switches, the virtual routers and the virtual connections are also displayed in yellow.

This finishes the check for error locations on the network and its affected area.

5.3 Collect Logs of Managed Nodes

You can collect and accumulate node logs at any time.

The following is the procedure for using the GUI to collect logs.

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Log Collection].
2. From the [Log Collection] menu, select [Log Collection Settings].
3. Select the checkboxes for the nodes from which to collect logs. By selecting the checkboxes for multiple nodes, you can set the same contents at the same time.
4. From the [Actions] button, select [Collect Logs].

   The "Result" screen is displayed. Take a memo of the detailed task number that is displayed on this screen.
5. From the top of the Global Navigation Menu, select [Tasks] and check the processing status.

   Under Task Type, [Collecting Node Log] is displayed.

   For the Task ID, confirm the detailed task number that you took a memo of on the "Result" screen.

Point

Manual log collection can be executed using the same operations for the screens displayed in the following procedures.

- From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Log Collection] to execute either of the following:
  - Select [Log Management] on the Log Collection menu.
  - Select [Node Log Search] on the Log Collection menu.
- From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes] to execute either of the following:
  - From the [Column Display] field in the node list, select [Log Collection Settings].
  - From the node list, select [Node Name] of the node, and then select the [Log Collection Settings] tab.

Note

- Although cancel of manual log collection can be executed from the [Tasks] from the top of the Global Navigation Menu, the cancel cannot be completed until the log collection is completed if log collection is being executed.
- Each time you execute a manual log collection, this is added to the number of retained generations for Archived Logs. Note that repeatedly executing this operation several times eventually deletes logs from the past that exceed the setting for the number of retained generations. Moreover, if manual log collection results in an error, it is not added to the number of generations count.
- For log collection executed for nodes where logs are currently being deleted, it will be suspended until log deletion has been completed, then after log deletion has been completed it will be executed.

5.4 Collect Logs for Clusters in PRIMEFLEX for VMware vSAN

This section describes the procedure for collecting logs for a cluster for PRIMEFLEX for VMware vSAN.

5.4.1 Operation requirements

The following requirements must be met to use Batch Collection of vSAN Logs.

- ISM for PRIMEFLEX operation environment
  - All servers in the target cluster are registered in ISM
  - The target cluster is registered in the cloud management software
  - The virtual disks in the Administrator user group must have sufficient free space.
    Estimated required free space: Approximately 6Gbyte in a 4-node configuration (More space may be required depending on the vm-support and vc-support log sizes.)
- Cluster configuration and operating status
  - Allow SSH access to the vCenter Server Appliance
- Cloud management software registration status
  - A local user is not used for the registration account information for the cloud management software
  - Use a user that has administrator privileges for the registration account information for the cloud management software

You can get information from cloud management software if the conditions match the above.

For details on getting information from cloud management software, refer to "2.13.6.2 Retrieving information from cloud management software" in "User's Guide."

5.4.2 Batch collect vSAN logs

1. From the Console as an administrator, log in to ISM-VA.
2. Execute the cluster name check command to confirm the name of the cluster for which you want to collect vSAN logs.

   Example: Results for checking the cluster name (If there were three clusters configured)

```
# ismadm cluster logcollect -listcluster
Cluster List:
 TestCluster62vSanTrue             VMware
 Cluster-1                         VMware
 S2DCluster                        Hyper-V
```

   Under "Cluster List:", <Cluster Name> and <Cluster Type> are displayed on separate lines. Confirm the cluster name (For example, "TestCluster62vSanTrue") of the cluster for which you want to collect logs.

3. Execute the start command for Batch Collection of vSAN Logs.

   Set the required information for the command options.

   Example: Collecting logs as log files "clusterlog_20191111_TestCluster62vSanTrue.zip" in the directory "/Administrator/ftp" for the cluster in "TestCluster62vSanTrue"

```
# ismadm cluster logcollect -collect -dir /Administrator/ftp -file
clusterlog_20191111_TestCluster62vSanTrue.zip
```

4. At the command prompt, specify the cluster name from Step 2 and the zip password (If necessary).

   Example: The cluster name is "TestCluster62vSanTrue" and the zip password is "Himitsu".

```
# ismadm cluster logcollect -collect -dir /Administrator/ftp -file
clusterlog_20191111_TestCluster62vSanTrue.zip
ClusterName:                    .... cluster name
TestCluster62vSanTrue
Password:                        .... zip password
Himitsu
```

5. Confirm the message and enter "Y" to execute it.

```
TestCluster62vSanTrue Collect Start?(Y/N)
Y                               .... enter "Y" to execute
```

6. Check the collection status and wait for the log batch collection to complete.

   The log collection runs in the background. Therefore, check that the collection status check command changes "Status (vSAN log collection status)" to "Complete".

   It may take some time for the log collection to complete.

   Example: Checking the collection status of the cluster "TestCluster62vSanTrue" while running Batch Collection of vSAN Logs.

```
# ismadm cluster logcollect -status
ClusterName:                    ... Enter cluster name to check collection status (Example:
"TestCluster62vSanTrue")
TestCluster62vSanTrue
ClusterName:TestCluster62vSanTrue
Directory:/Administrator/ftp      ... Destination directory name
FileName:clusterlog_20191111_TestCluster62vSanTrue.zip
Status:Collecting               ... vSAN log collection status(Wait for it to become "Complete")
CollectStartTime:2019/11/11 12:33:40   ... Collection start time
CollectEndTime:                         ... Collection end time
CheckSum:                                ... Checksum value
[CmsStatus]                              ... CMS related log collection status
Collecting:VcSupport
Wait:RVC
[NodeStatus]                            ... Log collection status for each node
Complete:PRIMERGY1
Collecting:PRIMERGY2
Wait:PRIMERGY3
```

   Example: Checking the collection status of a cluster that has never executed Batch Collection of vSAN Logs

```
# ismadm cluster logcollect -status
ClusterName:
TestCluster62vSanTrue
'TestCluster62vSanTrue' is not collecting.     ... Display as "'Cluster name'is not collecting."
```

7. Check the output log file.

   Check that the specified directory contains log files and the resulting information files. The collection results can be confirmed in the information file of the collection results.

   If you started the log collection in the example in Step 3, the following files are created in the directory "/Administrator/ftp".

   - clusterlog_20191111_TestCluster62vSanTrue.zip (Log file)
   - clusterlog_20191111_TestCluster62vSanTrue.Result (Collection results information file)

   Example: Contents of the collection results information file

```
ClusterName:TestCluster62vSanTrue
Directory:/Administrator/ftp
FileName:clusterlog_20191111_TestCluster62vSanTrue.zip
Status:Complete                ... Collection complete
CollectStartTime:2019/11/11 12:33:40
CollectEndTime:2019/11/11 13:33:40
CheckSum:xxxxxxxxxxxxxxx
[CmsStatus]                    ... Successful collection of vc-support and RVC commands
Complete:VcSupport
Complete:RVC
[NodeStatus]                   ... PRIMERGY1, PRIMERGY3 node collected successfully, PRIMERGY2
node collected error
Complete:PRIMERGY1
Error:PRIMERGY2
Complete:PRIMERGY3
```

8. Retrieve the log file with FTP.

9. Delete the log file.

   After getting the log files, delete them to increase the virtual disk space for the Administrator user group.

Chapter 6 Other Functions to Manage/Operate Nodes

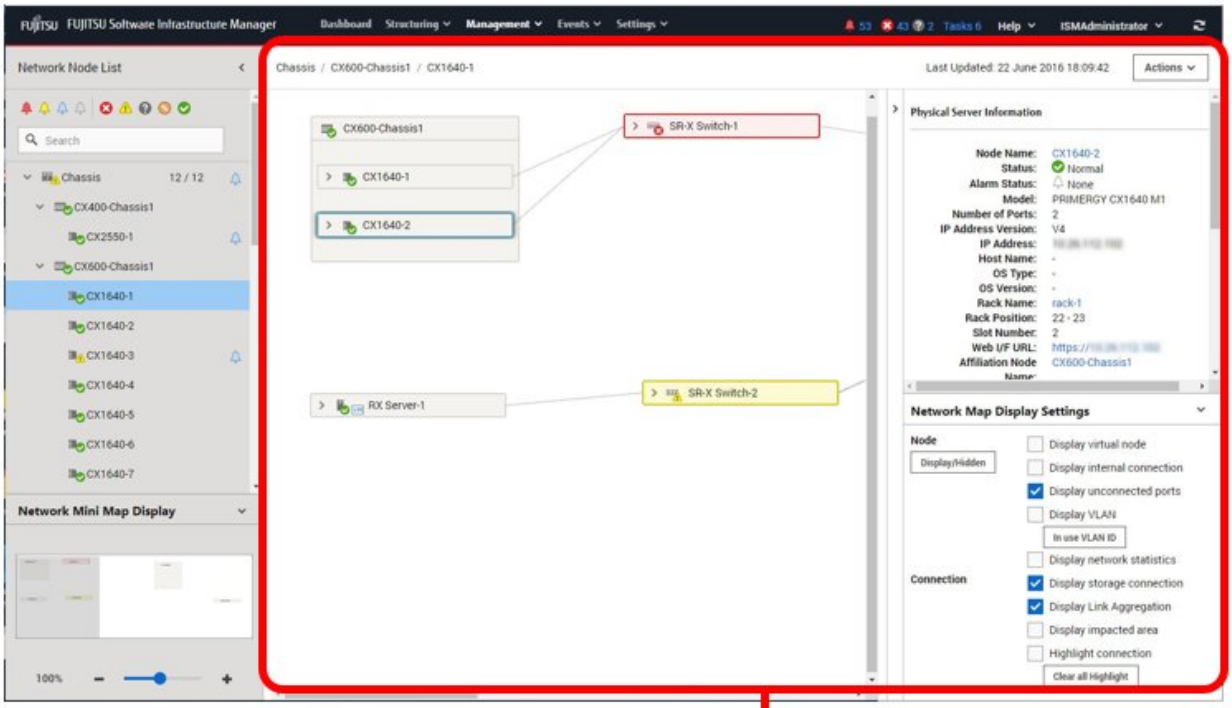
This chapter describes various operations for each node.

6.1 Set up Network Map

The Network Map displays the physical connections of LAN cables among managed nodes. If LLDP (Link Layer Discovery Protocol) of the network port on a managed node is enabled, ISM retrieves the relationship between the nodes and displays the connections on the Network Map. However, when a managed node does not support LLDP or is not enabled, the connections are not displayed automatically. In that case, you can manually set up connections between respective nodes.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Network Map].

   The "Network Map Display" screen is displayed.



[Network Map Display] Screen

2. From the [Actions] button, select [Update network information], and then select the [Update Network Information] button.
3. From the [Actions] button, select [Edit Connection].
4. Select the node name of the node to be connected.

   The network port "  " is displayed.
5. Select the two ports to be connected and select the [Add] button.

   The added connections are displayed in green.
6. Repeat Step 3 to 5 as many times as the number of the connections you want to add.
7. On the "Network Map Display" screen, select the [Save] button.
8. On the "Edit Connections Saved" screen, confirm the contents of the connections set up, then select the [Save] button.

   The added connections are displayed in gray.

This finishes the procedure of network connection set up.

6.2 Display Virtual/Machines Virtual Resources Information

You can confirm the information of virtual machines and virtual switches running on managed servers or virtual resources (storage pool (cluster)) configuring them to link with the cloud management software.

Execute the settings to display information on the virtual machines or virtual resources on ISM.

6.2.1 Register a Cloud Management Software

The following is the operation procedure for registering new cloud management software.

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [General].
2. From the menu on the left side of the screen, select [Cloud Management Software].

   The "Cloud Management Software List" screen is displayed.
3. From the [Actions] button, select [Register].

   The "Register Cloud Management Software" screen is displayed.
4. Enter the information required for registration.

   Refer to the help screen for entering the setting items.
5. Select the [Register] button or the [Test] button.

   Selecting the [Register] button displays the cloud management software that was set on the "Cloud Management Software List" screen.

   Selecting the [Test] button displays the "Cloud Management Software Test" screen. The following shows how to operate the "Cloud Management Software Test" screen.

   a. Select "When the test is successful, then register the cloud management software." or "Execute only the test."

   b. Select the [Apply] button.

      If you selected "When the test is successful, then register the cloud management software.", the cloud management software that was set on the "Cloud Management Software List" screen is displayed when the test is successful.

      If you selected "Execute only the test.", the "Register Cloud Management Software" screen is displayed when the test is successful. To register the cloud management software, select the [Register] button.

   This finishes the registration of the cloud management software.

Point

The [Test] button is enabled when you select "VMware vCenter Server" or "System Center" for [Type].

Note

It may take some time for the test to complete. Do not close the screen until the test completes. If you closed the screen, execute the test again.

6.2.2 Confirm Information for Virtual Machines on Managed Servers

Retrieve the information for cloud management software in order to display the information of virtual machines.

Point

You must register the managed servers as nodes and set their OS information in ISM in advance.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].

   The "Node List" screen is displayed.

2. Select the nodes that are managed with the cloud management software.

   The Details of Node screen is displayed.

3. From the [Actions] button, select [Get Node Information].

   The node information is retrieved. Execute the following after the node information is retrieved.

4. From the Global Navigation Menu on the ISM GUI, select [Settings] - [General].

5. From the menu on the left side of the screen, select [Cloud Management Software].

   The "Cloud Management Software List" screen is displayed.

6. Retrieve information using one of the following procedures:

   - If retrieving information from all cloud management software, select the [Get Cloud Management Software Info] button and then select the [Run] button.
   - If limiting the items to retrieve, select the target cloud management software. From the [Actions] button, select [Get Info] -the [Run] button.

   Execute the following after the cloud management software information is retrieved.

7. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].

   The "Node List" screen is displayed.

8. Select the node that you retrieved the node information for in Step 3.

   The Details of Node screen is displayed.

9. Confirm the virtual machine information according to the following procedures:

   - If you want to confirm the list of virtual machines registered on the node and the information on the CPU, memories and so on that are allocated to each virtual machine, select the [Virtual Machines] tab.
   - If you want to confirm the power status of the virtual machine, the information on the virtual adapter, or the connection status between the virtual switches, from the [Properties] tab, select [Network] - "Map" to display the Network Map.

     Select the virtual machine that you want to confirm its information with the Network Map and confirm the virtual machine information.

6.2.3 Confirm the Status of a Virtual Resource

By adding the information display screen (the widget) for virtual resource management on the ISM Dashboard, the details of the target resource information can be displayed to check directly from the Dashboard.

The resource information can also be checked from the Details of Node screen.

Check the status of virtual resource from ISM Dashboard

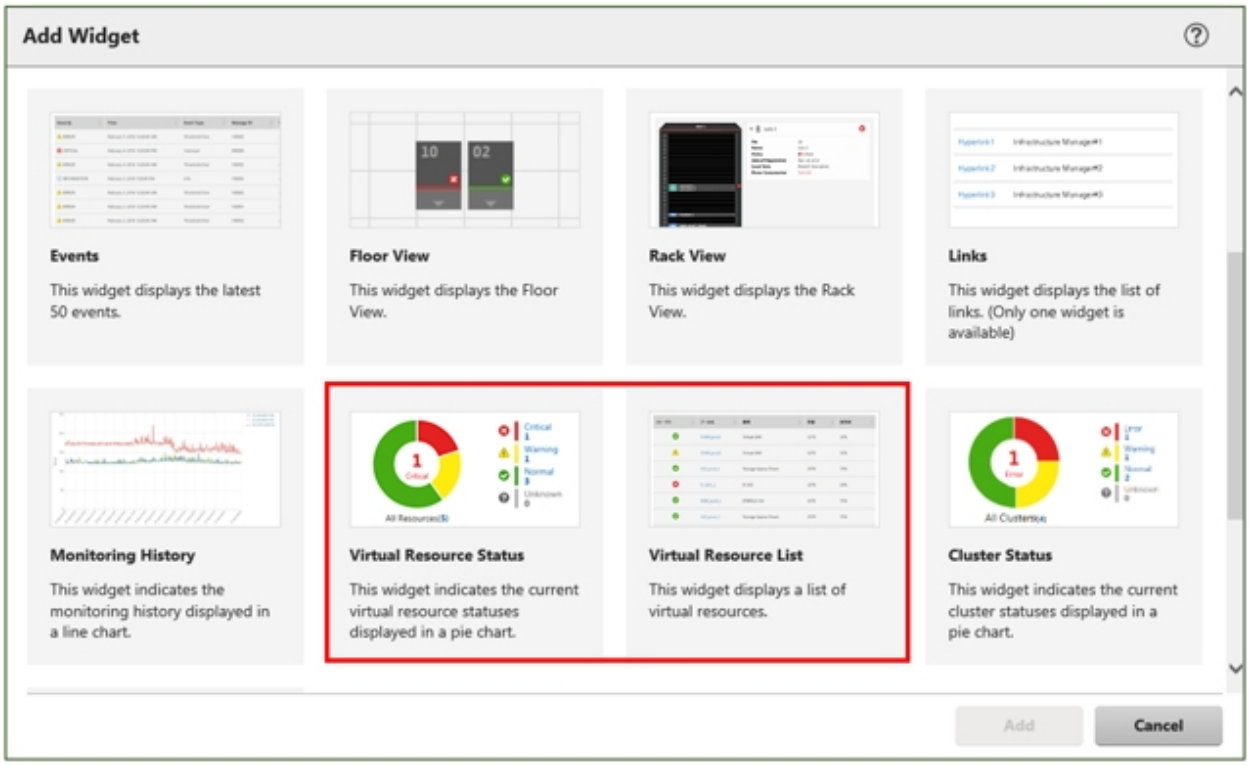
1. From the Global Navigation Menu on the ISM GUI, select [Dashboard].

   The "Dashboard" screen is displayed.

2. From the [☰] button on the upper right of the screen, select [Add Widget].

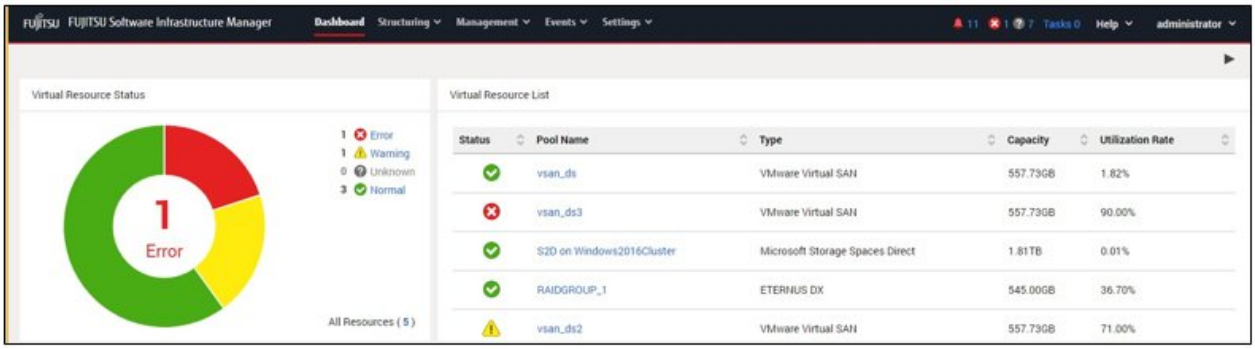
   The "Add Widget" screen is displayed.

[Virtual Resource Status] and [Virtual Resource List] are the display widgets for virtual resources.



3. Select either [Virtual Resource Status] or [Virtual Resource List], then select the [Add] button.

   The selected widget is displayed on the Dashboard.

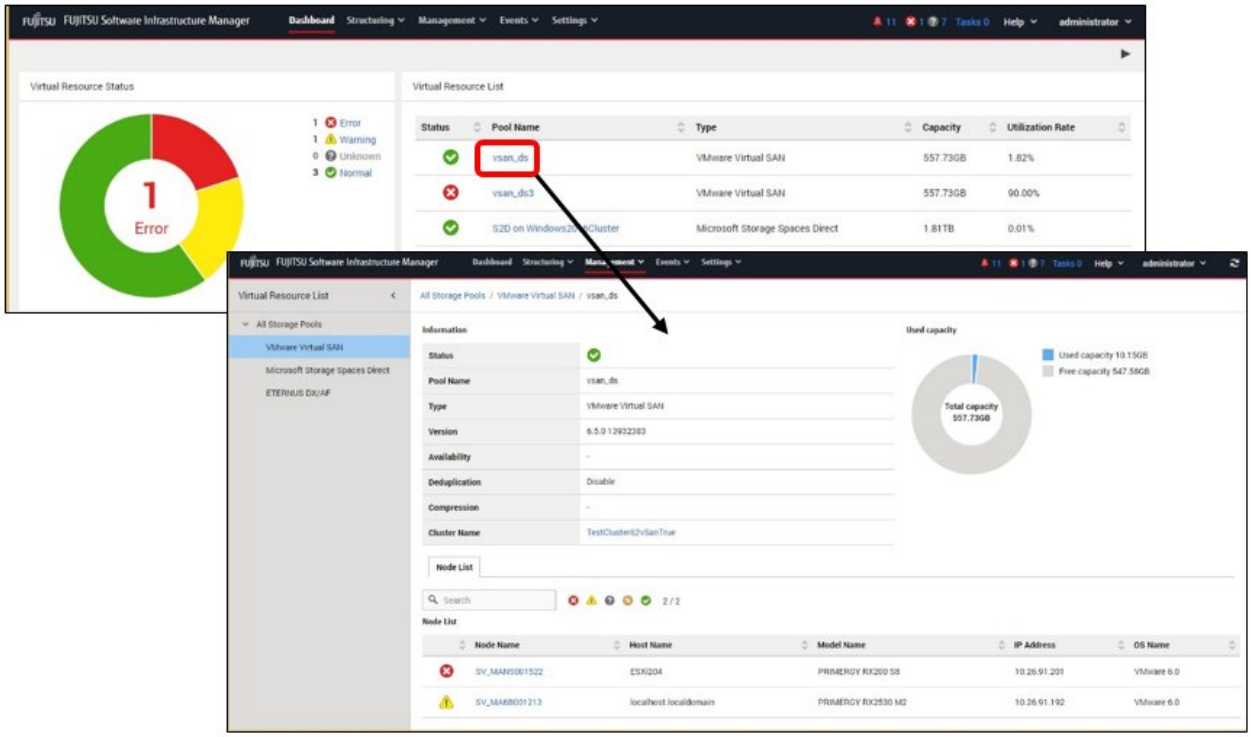


4. Select the pool name in the [Virtual Resource List] widget, or select the status to check (Error, Warning, Unknown, Normal) in the [Virtual Resource Status] widget.

   If you select a pool name, the detailed pool information will be displayed.

   When a status is specified, the list of the target status is displayed.

Refer to the help screen for descriptions of the content displayed.

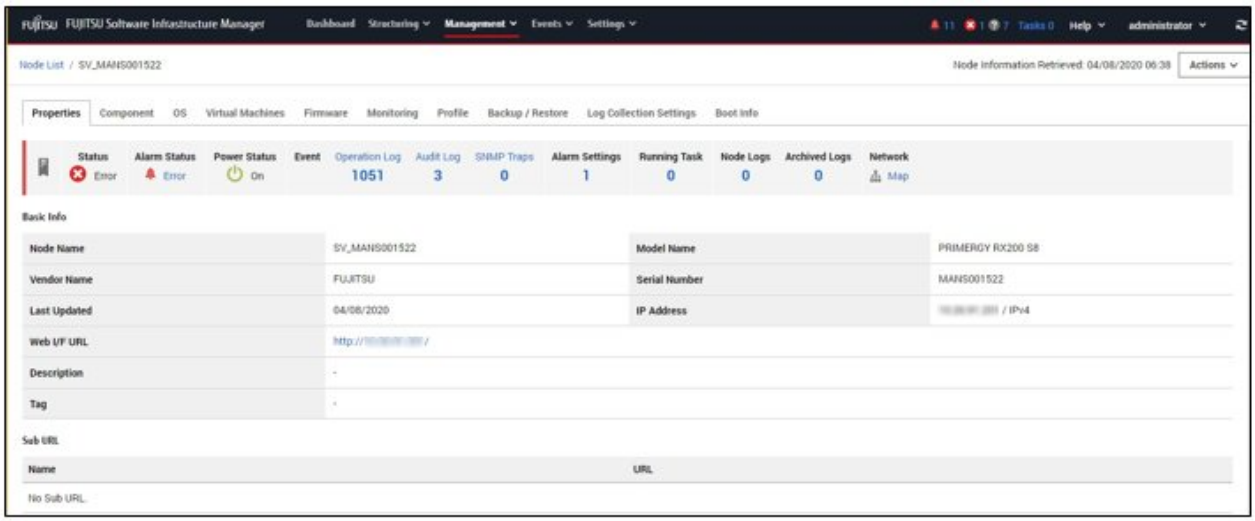


Check the resource information from the Details of Node screen

By embedding the virtual resource management information into the Details of Node screen, they link with each other.

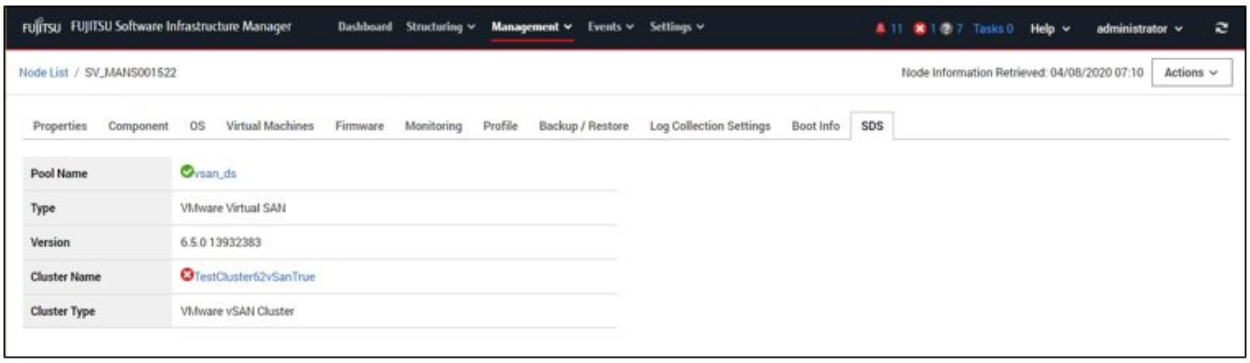
1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes] to select the node name on the "Node List" screen.

   The Details of Node screen is displayed.



2. Select the [SDS] tab.

   The storage pool information related to the node is displayed.



   When selecting [Pool Name], the details of the virtual resource screen is displayed.

6.2.4 Confirm the Status of Virtual Machines/vSAN Storage

You can see the configuration of the physical disks for the vSAN storage used by virtual machines, the read and write latency values, and I/O latency status for the virtual disks.

Display virtual machines and vSAN storage statuses

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Virtual Resource], and then select "VMware Virtual SAN" on the "Virtual Resource List" screen.
2. Execute one of the following tasks.
   - Select the storage pool, from the [Actions] button, select [Impact Analysis(VMware Virtual SAN)].
   - Select the storage pool to display the information for the storage pool. From the [Actions] button, select [Impact Analysis(VMware Virtual SAN)].

   The "Impact Analysis (VMware Virtual SAN)" screen is displayed.

Confirm the configuration of virtual machines, servers, and vSAN storage

1. Select the dot for the virtual machine that you want to confirm.
2. In the configuration view area on the left side of the screen, confirm the physical disks (cache disks and capacity disks) in the vSAN that the virtual machine is configuring and the servers that make up the physical disks.

   The physical disks (cache disks and capacity disks) in the vSAN that the virtual machine configures and the servers that make up the physical disks are displayed as dots.
   You can also select the dots for the servers, cache disks, and capacity disks, and confirm them as well.

Point

Virtual machines are represented as the following dots.

Status	Dot on the ISM GUI	Description
Error	(Red)	Virtual machine disk latency has occurred (I/O latency threshold exceeded). Possible causes include degraded disk performance or data congestion.
Unknown	(Gray)	Disk latency information for the virtual machine cannot be obtained.

Status	Dot on the ISM GUI	Description
Normal	(Green)	The virtual machine is operating normally.

Confirm the information for virtual machines, servers, and vSAN storage

1. Select the dot for the virtual machine that you want to confirm.
2. In the detail information display area on the right side of the screen, confirm the virtual machine name, I/O latency status, I/O latency threshold (ms), write latency value (ms), and read latency value (ms).
3. Refer to the detail information display area to confirm lists of affected server names, cache disk names, capacity disk names.

   You can also select the dot (impact dot) for the servers, cache disks, and capacity disks, and confirm them as well.

   - Selecting a server

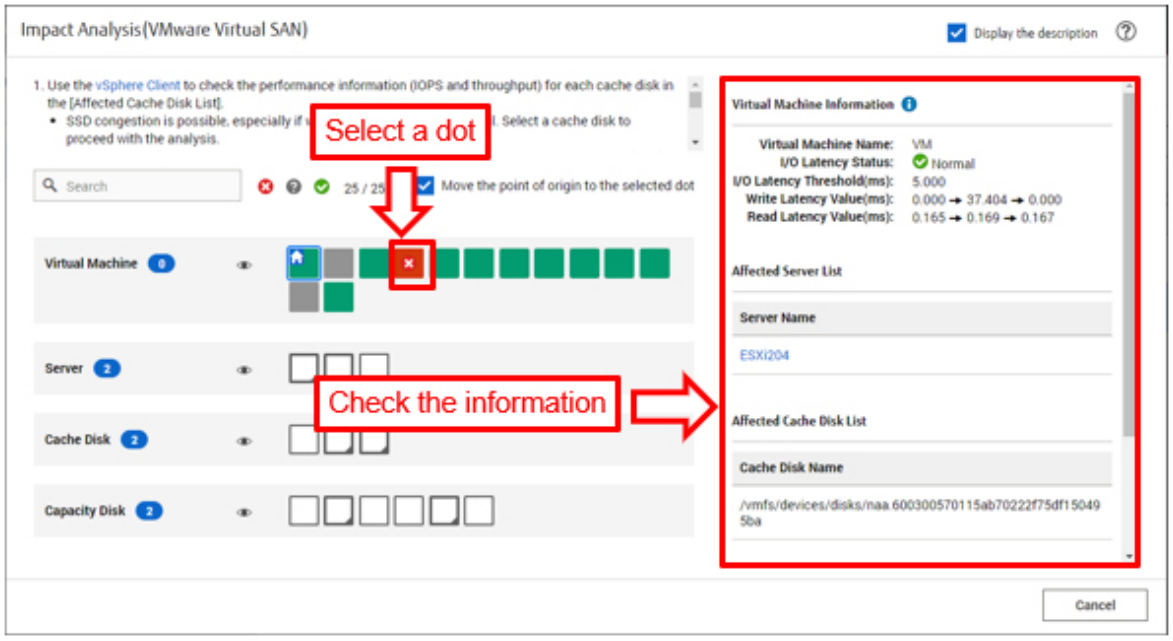
     Confirm server names, OS types, and lists of affected virtual machine names, cache disk names, capacity disk names.

   - Selecting a cache disk

     Confirm cache disk names, disk types, affected server names, and lists of affected virtual machines and capacity disks.

   - Selecting a capacity disk

     Confirm capacity disk names, disk types, affected server names, and lists of affected virtual machines and cache disks.



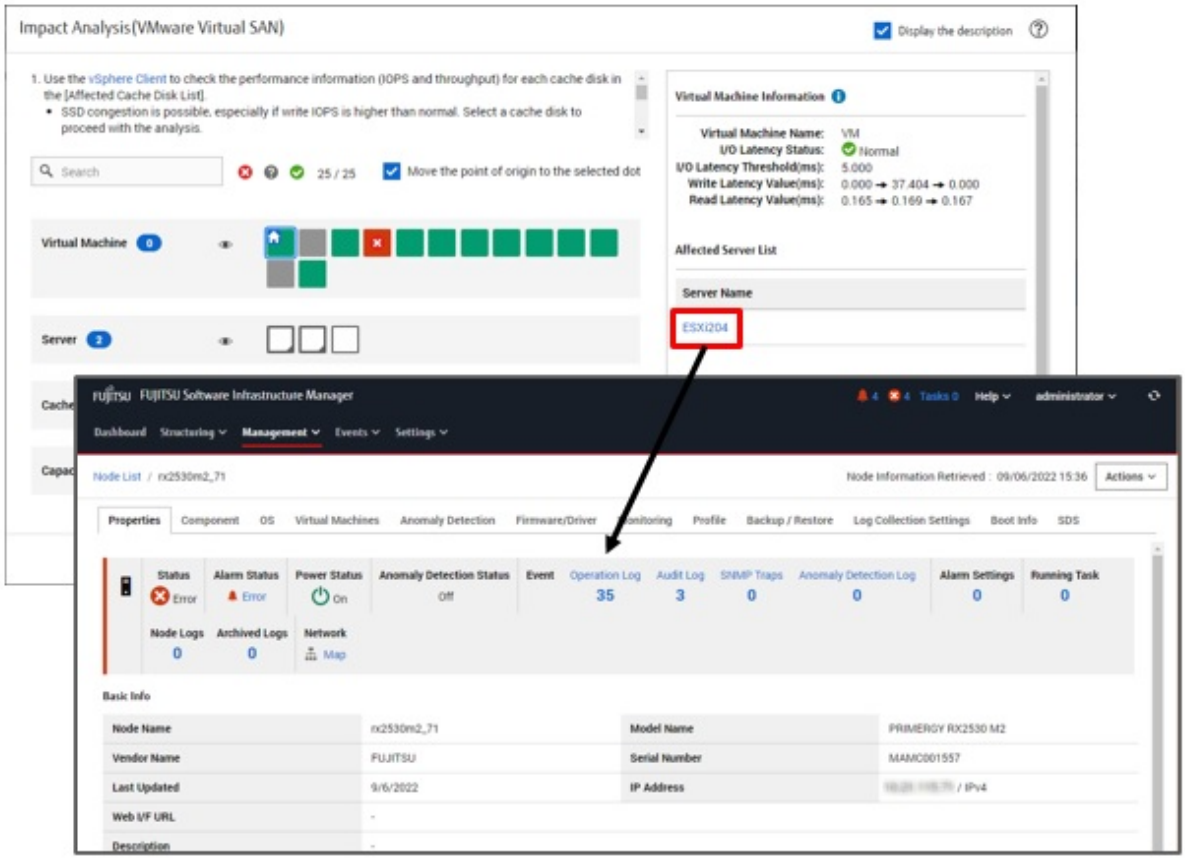
Point

You can filter the dots when many dots are displayed.

You can filter the content that is displayed by entering the conditions into the "Filter." Dots that do not fit the conditions of the entered text turn grey and cannot be selected.

You can also filter the dots by specified status using the status filter icons in the upper part of the screen.

Select the link for the server name in [Server Name] to confirm the information registered for that server.



Point

- Select the dot for a virtual machine that has the "Error" status displayed on the "Impact Analysis (VMware Virtual SAN)" screen to check the affected servers, cache disks, and capacity disks.
- Use a vSphere Client to confirm the performance information (IOPS and throughput) for each cache disk in the [Affected Cache Disk List].

  SSD congestion can occur, especially if write IOPS is higher than normal. Select a cache disk to proceed with the analysis.
- Use a vSphere Client to confirm the performance information (IOPS and throughput) for each capacity disk in the [Affected Capacity Disk List].

  I/O congestion can occur, especially if the write/read IOPS is higher than normal. Select a capacity disk to proceed with the analysis.
- Use a vSphere Client to confirm the performance information (CPU and memory usage) for each server in the [Affected Server List].

  If the CPU utilization is above 90%, there may be CPU conflicts. Select a server to proceed with the analysis.

6.3 Predict Resource Fluctuations of Cluster (ISM 2.8.0.060 or later)

Prediction of Resource Fluctuations can predict when the cluster will run out of resources. Prediction of Resource Fluctuations can be executed as following procedures:

- 6.3.1 Execute Prediction of Resource Fluctuations
- 6.3.2 Display Prediction of Resource Fluctuations Result

6.3.1 Execute Prediction of Resource Fluctuations

Prediction of Resource Fluctuations collects the historical resource health information of vSAN cluster from the vCenter Server and displays the resource utilization prediction up to one year later in a graph. The following steps are required.

Point

The cloud management software must have already been registered in ISM to retrieve the cluster information.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster].

   The "Cluster List" screen is displayed.

2. From the Cluster list, select the cluster for which you want to predict the resource fluctuations.

   The [Cluster Info] tab is displayed.

3. Select the [Prediction of Resource Fluctuations] tab.

   The "Prediction of Resource Fluctuations" screen is displayed.

4. From the [Prediction of Resource Fluctuations Actions] button, select [Prediction of Resource Fluctuations].

   The "Prediction of Resource Fluctuations" wizard is displayed.

5. Follow the "Prediction of Resource Fluctuations" wizard to enter the settings.

   Refer to the help screen for entering the setting items.

6. Select the [Execute] button in the "Prediction of Resource Fluctuations" wizard.

   Prediction of Resource Fluctuations is executed.

   The results are added as a result list in "History List" on the [Prediction of Resource Fluctuations] tab.

6.3.2 Display Prediction of Resource Fluctuations Result

To display the results of Prediction of Resource Fluctuations executed in "6.3.1 Execute Prediction of Resource Fluctuations", execute the following procedure.

1. Confirm that the [Result] button is displayed in the "History List."

   Point

   The [Result] button will not display until "Prediction of Resource Fluctuations" has been successfully executed.

2. Select the [Result] button.

   The "Result of Prediction of Resource Fluctuations" screen is displayed. Refer to the help screen for the detail of the result screen.

6.4 Update the Firmware/Driver of the Node

You can use the following to update the firmware/driver of the nodes registered in ISM.

- Imported firmware data
- ServerView embedded Lifecycle Management

Note

The reference procedures on the Fujitsu manual site described in the following procedures are subject to change without notice.

6.4.1 Update Firmware Using Imported Firmware Data

Use imported firmware data to update the firmware of a node registered in ISM.

Preparation must be made if using Offline Update. For details, refer to "Required preparations for using Offline Update" in "2.6.3 Firmware/Driver Update" in "User's Guide."

1. If the firmware to be updated is not imported yet, the firmware must first be imported. If it is already imported, proceed to Step 7.
2. Download the firmware data released on the Fujitsu web site.

   http://support.ts.fujitsu.com
3. Store the downloaded file in an arbitrary folder.

   If the downloaded file is compressed, decompress the file in the folder.
4. Compress the folder in which the downloaded files are stored.
5. Import the firmware.
   a. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Firmware/Driver].
   b. Select [Import] in the menu on the left side of the screen.
   c. On the [Import Data List] tab, from the [Actions] button, select [Import Firmware].
   d. On the "Import Firmware" screen, select [Local] in the [File selection method].
   e. Select the [Browse] button in [File Path], and select the .zip file that was created in Step 4.
   f. Follow the instructions on the "Import Firmware" screen, and enter the [Type], [Model Name], and [Version] and then select the [Apply] button.
   g. Select [Task Details: <Task ID>] on the upper-left of the "Result" screen, or select [Tasks] on the top of the Global Navigation Menu.

      The Task list is displayed on the "Tasks" screen. Confirm that task is "Success."
6. Confirm that the firmware has been imported.
   a. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Firmware/Driver].
   b. Select [Import] in the menu on the left side of the screen.
   c. Select the [Firmware Data] tab on the "Import" screen.

      Confirm that the imported firmware is displayed on the list screen.
7. Select the target firmware.

   Point

   You should set the port used in [PXE Boot Port] on the [Firmware/Driver] tab on the Details of Node screen in the following cases.

   - Offline Update for the server
   - The port used for PXE boot for Offline Update is not the first port of the on-board

   a. From the menu on the left side of the screen, select [Update].
   b. From the [Update Mode:] column on the "Node List" screen, select [Online Update] or [Offline Update].
   c. Select the checkbox for the firmware you want to perform the firmware update for.

      When a firmware with a higher version than the current one is imported, the version of that firmware is displayed in [Latest (Online)] or [Latest (Offline)]. When a firmware with a higher version than the current one is not imported you cannot select the checkbox.

d. From the [Actions] button, select [Update Firmware/Driver].

   The "Update Firmware/Driver" wizard is displayed.

8. Start the firmware update.

   Follow the instructions on the "Update Firmware/Driver" wizard and enter the setting items.

   Refer to the help screen for entering the setting items.

   After starting the firmware update, the operations are registered as an ISM task.

   Confirm the current status of the task on the "Tasks" screen.

   Select [Tasks] on the top of the Global Navigation Menu to display a list of the tasks on the "Tasks" screen.

   Note

   You can cancel tasks that are being executed from the "Task Details" screen from the task that was registered. However, you cannot cancel the task after "Updating firmware." is displayed in the subtask message. If you attempt to do this, the task will fail to cancel.

9. If you update the BIOS and PCI cards with online firmware update, reboot the target server.

10. Confirm that the firmware version of the target server has been updated.

    a. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Firmware/Driver].

       The "Node List" screen is displayed.

    b. Select the node name for which the firmware was updated.

       The "Node Information" screen is displayed.

    c. Select the [Get Node Information] button.

       Node information is retrieved, and the version is displayed in [Current Version] on the "Node List" screen after the update.

    This finishes the server firmware update.

Point

By setting tags to nodes beforehand, you can filter the nodes by tags on the "Node List" screen. Filtering nodes makes it easier to extract target nodes.

6.4.2 Offline Update Firmware Using ServerView embedded Lifecycle Management

Use ServerView embedded Lifecycle Management (hereafter referred to as "eLCM") to update the firmware of a node registered in ISM.

The firmware update procedure involves using firmware data from the Repository Server or the Fujitsu website, or using firmware data imported into ISM.

6.4.2.1 Update using firmware data from a Repository Server

You can update firmware using firmware data from the Fujitsu website, however this section describes the procedure using firmware data from the Repository Server.

1. Check the environment of the Repository Server.

   For the procedure to check the environment of a Repository Server, refer to "ServerView Repository Server - Installation and User Guide" on the Fujitsu manual site below.

   https://support.ts.fujitsu.com/

   Reference procedure

Select "Select a new Product" - [Product Search]. Enter "Repository Server" and select [Continue].
Download from [Documentation] - [Setup Guide].

2. Structure the eLCM environment on the node.

   For details, refer to "ServerView embedded Lifecycle Management (eLCM) x.x for iRMC Sx Overview" (where x is the latest version.) on the Fujitsu manual site below.

   https://support.ts.fujitsu.com/

   Reference procedure

   Select "Select a new Product" - [Browse For Product] and select the server that you want to update.
   Download from [Server Management Controller].

3. Set the Repository Server information (URL settings) to the iRMC of the target server when using a Repository Server.

   a. Use a web browser to connect to iRMC on the node.

   b. Select [Services] on the [Settings] tab.

   c. Select [Update and Deployment].

   d. Enter the URL of the Repository Server in [Repository Location] for the [Update] item, and select the [Apply] button.

4. Select the target server on the ISM GUI.

   a. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].

   b. From [Column Display:] on the "Node List" screen, select [Firmware/Driver].

   c. From [Update Mode:], select [eLCM Offline Update].

   d. Select the checkbox for the firmware you want to perform the firmware update for.

   e. From the [Actions] button, select [Update Firmware/Driver].

      The "Update Firmware/Driver" wizard is displayed.

5. Start the firmware update.

   Follow the instructions in the "Update Firmware/Driver" wizard and enter the setting items.

   Refer to the help screen for entering the setting items.

   After starting the firmware update, the operations are registered as an ISM task.

   Confirm the current status of the task on the "Tasks" screen.

   Select [Tasks] on the top of the Global Navigation Menu to display a list of the tasks on the "Tasks" screen.

   Note

   You can cancel tasks that are being executed from the "Task Details" screen from the task that was registered. However, you cannot cancel the task after "Updating firmware. (eLCM Offline)" is displayed in the subtask message. If you attempt to do this, the task will fail to cancel.

6. Confirm that the firmware version of the target server has been updated.

   a. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Firmware/Driver].

      The "Node List" screen is displayed.

   b. Confirm the firmware version is displayed in [Current Version].

   This finishes the node firmware update.

6.4.2.2 Update using firmware data imported into ISM

This is an update procedure that uses firmware data imported into ISM and eLCM.

Preparations (For updating a PCI card)

Import the eLCM Offline Update (SimpleUpdate) tool when updating the PCI card for the target node.

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Firmware/Driver].
2. On the "Firmware Tool" screen, check that the eLCM Offline Update (SimpleUpdate) tool has been imported.

   If the eLCM Offline Update tool is imported, this procedure is not required.

   If the eLCM Offline Update tool is not imported, execute this procedure.
3. From the ServerView Suite DVD, obtain the eLCM Offline Update (SimpleUpdate) tool.
   a. Go to the following directory on the ServerView Suite Update DVD.

      Firmware/Tools/UpdateManagerExpress/xx.xx.xx.xx (where x is the version number.)

   b. Copy the [xx.xx.xx.xx] folder to an arbitrary folder.

   c. Compress the folder you copied to zip format.
4. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Firmware/Driver].
5. Select [Import] in the menu on the left side of the screen.
6. Select the [Firmware Tool] tab.
7. From the [Actions] button, select [Import].

   The "Firmware Tool Import" screen is displayed.
8. Select [Local] in the [File selection method].
9. Select the [Browse] button in [File Path], and select the .zip file that was created in Step 3.
10. Select the [Apply] button.
11. Confirm that the imported firmware tool is displayed on the list screen.

Update Firmware

1. Set to skip SSL/TLS certificate validation during updates to the iRMC of the target node.
   a. Use a web browser to connect to iRMC on the node.

   b. Select [Services] on the [Settings] tab.

   c. Select [Update and Deployment].

   d. Select the [Skip SSL/TLS certificate verification] checkbox for the [Update] item and select the [Apply] button.
2. Structure the eLCM environment on the node.

   For details, refer to "ServerView embedded Lifecycle Management (eLCM) x.x for iRMC Sx Overview" (where x is the latest version.) on the Fujitsu manual site below.

   https://support.ts.fujitsu.com/

   Reference procedure

   Select "Select a new Product" - [Browse For Product] and select the server that you want to update.
   Download from [Server Management Controller].
3. Perform Step 1 to 6 in "6.4.1 Update Firmware Using Imported Firmware Data" to import the firmware data into ISM.
4. Select target firmware on the ISM GUI.
   a. From the menu on the left side of the screen, select [Update].

   b. From the [Update Mode:] column on the "Node List" screen, select [eLCM Offline Update(Simple Update)].

c. Select the checkbox for the firmware you want to perform the firmware update for.

   You cannot check the firmware if it is older than the current version or if the firmware data corresponding to this update method has not been imported.

d. From the [Actions] button, select [Update Firmware/Driver].

   The "Update Firmware/Driver" wizard is displayed.

5. Start the firmware update.

   Follow the instructions on the "Update Firmware/Driver" wizard and enter the setting items.

   Refer to the help screen for entering the setting items.

   After starting the firmware update, the operations will be registered as an ISM task.

   Confirm the current status of the task on the "Tasks" screen.

   Select [Tasks] on the top of the Global Navigation Menu to display a list of the tasks on the "Tasks" screen.

   If you specify "Start the update on next boot," the firmware update process is scheduled for the target node when the task completes successfully. The update process runs when the target node is turned off. After turning on the target node, execute "Get Node Information" from the Details of Node screen.

   Note

   You can cancel tasks that are being executed from the "Task Details" screen from the task that was registered. However, you cannot cancel the task after "Updating firmware. (eLCM Offline)" is displayed in the subtask message. If you attempt to do this, the task will fail to cancel.

This finishes the node firmware update.

6.4.3 Online Update Firmware/Driver Using ServerView embedded Lifecycle Management

You can update firmware using data from the Fujitsu website, however this section describes the procedure using data from a Repository Server.

Note

eLCM Online Update supports target nodes with the Windows OS only.

Preparation

1. Execute Steps 1 to 3 in "6.4.2.1 Update using firmware data from a Repository Server" to structure the Repository Server and eLCM environment for the target node.
2. Check that ServerView PrimeUp and ServerView Agents or ServerView Agentless Service (a ServerView Suite product) is installed on the target node.

   For details about ServerView Agents and ServerView Agentless Service, refer to "ServerView-Agenten Vx.xx (Windows Server xxxx / xxxx / xxxx / xxxx)" (where x is the latest version and the target Windows Server version) on the Fujitsu manual site below.

   https://support.ts.fujitsu.com/

   Reference procedure

   Select "Select a new Product" - [Product Search], enter "Agents," and then select [Continue].
   Download from [Documentation] - [Setup Guide].

Update the driver

1. Enable the firmware/driver information displayed in the target node list.

   If the information is displayed, the following procedure is not necessary.

   a. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].

   b. Select the target node, and then select the [Firmware/Driver] tab.

   c. In "eLCM Online Info Retrieval," change the setting to [Enable].

      Select the [Set] button to change the setting.

   d. From the [Actions] button, select [Get Node Information].

   e. Confirm that the firmware/driver information is displayed in the list.

2. From the [Firmware/Driver Actions] button, select [Update Firmware/Driver].

   The "Update Firmware/Driver" wizard is displayed.

3. Select the checkbox for the firmware/driver you want to perform the update for.

   If there are firmware/drivers that can be updated, the latest version is listed in [Latest (eLCM Online)].

   If there are no firmware/drivers to update, a "-" is displayed in both the [FW/Driver Name] and [Latest (eLCM Online)] columns or a "-" is displayed in the [Latest (eLCM Online)] column and it cannot be selected.

4. Select the [Next] button.

5. From the [Update Mode:] column, select [eLCM Online].

6. Select the [Next] button, follow the instructions on the "Update Firmware/Driver" wizard and enter the setting items to start the update.

   Refer to the help screen for entering the setting items.

   After starting the firmware update, the operations will be registered as an ISM task.

   Confirm the current status of the task on the "Tasks" screen.

   Select [Tasks] on the top of the Global Navigation Menu to display a list of the tasks on the "Tasks" screen.

   Note

   You can cancel tasks that are being executed from the "Task Details" screen from the task that was registered. However, you cannot cancel the task after "Updating firmware. (eLCM Online)" is displayed in the subtask message. If you attempt to do this, the task will fail to cancel.

   This finishes the node firmware update.

6.5 Execute Power Capping

In ISM, specifying the upper limit of power consumption by each rack enables you to curb the power consumption of mounted devices.

The upper limit of the power consumption is configured by each Power Capping Policy (definitions according to the operational pattern).

Power Capping Policy operates two types of custom definitions, one definition for schedule operation, and one definition for the minimum power consumption operation (Minimum), by switching the four types in total.

In order to use power capping, you must set [Add Power Capping Setting] (the node information for the power capping target and definition for Power Capping Policy) beforehand to enable Power Capping Policy.

Note

The power capping settings are managed by each rack. You must review the power capping settings (node power settings, the upper limit value for Power Capping Policy) related to each rack when:

- Adding a node to the rack
- Removing a node from the rack
- Moving a node to another rack

6.5.1 Confirm the Current Power Capping Status

Confirm the power capping status of the target rack.

1. On the "Datacenter List" screen, select the rack that you want to confirm the power capping setting status for.
2. Confirm the contents in the power capping setting status displayed on the upper right of the rack details screen.

Table 6.1 Power capping status

Power capping status	Description
Not set Power Capping	Power capping has not been set up.
Stopped Power Capping	Power capping has been set up but all Power Capping Policies are disabled. To enable it, from the [Actions] button, select [Enable/Disable Power Capping Policy].
Power Capping	Power capping has been set up and at least one Power Capping Policy is enabled.
Updating Power Capping	The power capping settings are being updated.
Difference in Power Capping	A node was added or deleted after the power capping was set up. You must enter the node power settings of the added device and to review the upper limit of the Power Capping Policy.

6.5.2 Add/change the Power Capping Settings of the Rack

Register or edit the power capping definitions of the target rack.

1. On the "Datacenter List" screen, select the rack that you want to add or edit the power capping settings for.
2. From the [Actions] button, select the following:
   - When adding a new power capping setting: [Add Power Capping Setting]
   - When editing a set power capping setting: [Edit Power Capping Setting]

The displayed content as well as the settings are displayed below.

Rack power consumption column

The current power capping status value is displayed.

Table 6.2 Rack power consumption column

Item	Description
Current status	Displays the latest status of the power capping settings.
It is currently enabled policy	Displays the policy that has been enabled in [Enable/Disable Power Capping Policy].
Max power consumption	Displays the total maximum power consumption value currently entered in the node power settings.
Fixed power	Displays the entered total fixed power value (the total maximum power value of devices not using power capping).
Power consumption	The current total power consumption of the devices capable of power capping (mainly servers) and the maximum power consumption of devices that does not use power capping.

[Settings by nodes] tab

Enter the settings value of the nodes using power capping.

Table 6.3 [Settings by nodes] tab

Item	Description
Node type	Type of each node.
Node Name	Name of each node.
Fixed power	Use the maximum power consumption value entered as a fixed value. Check when handling it as a fixed power. For the devices that ISM cannot retrieve the power consumption value, this will be enabled automatically.
Max power consumption	Enter the maximum power consumption value as specification in catalogs. When calculating internally, it is used as the possible range of node power capping. For devices where power capping cannot be used, it is calculated using appropriate fixed power values.
Power consumption	Displays the current power consumption value retrieved from the nodes.
Business Priority	- Low When the power reaches the upper power value, it becomes the target for power capping. - Middle When capping the power for Low devices is not enough, it will be the power capping target. - High When capping the power for Low and Middle devices is not enough, it will be the power capping target. - Critical Out of target for power capping. However, when minimum policy is enabled power capping will be used.

[Power Capping Policy] tab

Register the setting values for the three types of Power Capping Policies.

For the upper limit power consumption target, upper limit values for two types of custom policies, upper limit value for schedule policy as well as schedule can be set.

Table 6.4 [Power Capping Policy] tab

Item		Description
Power Capping Policy		
	Custom 1,2	Operation will be executed with the set upper limit value specified for power consumption.
	Schedule	When schedule policy is enabled, it is operated using the specified upper limit value during the duration of the schedule (day, time).
	Minimum	Operations will be executed using minimal power consumption, including devices whose business priority is Critical.
Displayed value		
	Upper Value	Enter the upper limit target value for each policy.
	Fixed Value	The total value of the maximum power consumption of the devices that are out of target for power capping.
	Enabled/Disabled	Displays the status of the Power Capping Policy.
Setting details of schedule		

Item		Description
	All day	Select when not specifying operating time.
	Specify Time	Select when setting the start time and completion time. - Start Time Set the time to start using scheduled power capping. Set the value in the ISM-VA time zone. - End Time Set the time to complete operating scheduled power capping. Set the value in the ISM-VA time zone.
	Day of the week	Check the day when scheduled power capping is operated. Multiple days can be selected.

Note

The upper limit value is the power capping target value. Whereas the capping is normally executed to make sure that the power consumption is lower than the upper limit, when the upper limit is set low it may exceed the power consumption.

Point

When setting it as in the example below, it will be scheduled from Sunday 23:00 to Monday 5:00 in the ISM-VA time zone.

Setting Example:

- Start Time: 23:00
- End Time: 5:00
- Day of the week: Sunday

6.5.3 Enable the Power Capping Policy of the Racks

Enable the Power Capping Policy for the applicable racks.

1. On the "Datacenters List" screen, select the rack that you want to enable Power Capping Policy for.
2. From the [Actions] button, select [Enable/Disable Power Capping Policy].
3. In the row of the Power Capping Policy you want to enable, set [Enable/Disable] - [After Change] to [Enable], then select [Apply].

   The displayed content is as follows.

Table 6.5 The displayed content in the "Enable/Disable Power Capping Policy" screen

Item	Description
Policy Name	Name of the Power Capping Policy. There are four types: custom 1, custom 2, schedule, and minimum.
Upper Value	The upper limit target value entered for each policy in the power capping settings.
Fixed Value	The total value of the maximum power consumption of the devices that are out of target for power capping.
Enabled/Disabled	Displays the status of the Power Capping Policy.

Note

- Whereas all Power Capping policies are enabled independently, when the minimum is set it is executed with the highest priority. In this case, it will be operated with the minimum power consumption also for devices where the business priority in [Setting by nodes] in the power capping settings is Critical.
- When multiple Power Capping Policies other than minimum are enabled, the policy with the lowest upper power consumption limit value will be executed.

6.5.4 Delete Power Capping Settings for Racks

Delete all power capping settings information for the rack.

1. On the "Datacenters List" screen, select the rack that you want to delete the power capping settings for.
2. From the [Actions] button, select [Delete Power Capping Setting].
3. Confirm that it is the rack that the settings should be deleted for, then select the [Delete] button.

6.6 Confirm the Traffic Status of the Network

Network Map displays the traffic status for virtual adapters of the virtual machines running on the monitoring target hosts. This section describes the procedures to check traffic status with Packet Analysis of Virtual Network.

Execute Packet Analysis of Virtual Network with the following procedures.

- 6.6.1 Set Virtual Adapter Threshold
- 6.6.2 Confirm Notifications
- 6.6.3 Confirm the Traffic for Virtual Adapters
- 6.6.4 Start Packet Analysis
- 6.6.5 Confirm the Status of Packet Analysis
- 6.6.6 Confirm the Results for Packet Analysis
- 6.6.7 Stop Packet Analysis

Note

To use this function, you must log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.

6.6.1 Set Virtual Adapter Threshold

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Network Map].

   The "Network Map Display" screen is displayed.
2. From the [Actions] button, select [Setting Virtual Adapter Threshold].
3. Select the monitoring target node and the virtual adapter for the virtual machine.
4. Select the [Setting Monitor] button.

Point

If you select [Setting Virtual Adapter Threshold] with a node, virtual machine or virtual adapter selected on Network Map, the status will be the one where the target virtual adapter is selected.

5. Select "Enable" from Enable/Disable for [Monitor] and after setting the threshold values for the item that you want to enable threshold judgment, select the [Reflection] button. Set the threshold values in the range from 0.001 to 100 percent.

Point

- When you enable [Monitor], monitoring the virtual adapters and retrieving performance statistics information are started.
- When you disable [Monitor], monitoring the virtual adapters and retrieving performance statistics information are stopped.
- When you enter threshold values, the threshold judgment for the items that you entered is enabled.
- When you clear threshold values, the threshold judgment is disabled.
- For threshold values, Warning Threshold and Critical Threshold can be set. However, you can only set one on them.

Note

- Up to 1,000 virtual adapters can be monitored. Set the number of virtual machines within the range of the total number of virtual machines that you set as resources assigned for ISM-VA. For details, refer to "Using Packet Analysis for a virtual network" in "1.3.1 Requirements for Hypervisor to Run ISM-VA (Virtual Machines)" in "User's Guide."
- You can check the number of adapters being monitored currently from "Monitoring Virtual Adapter" displayed on the upper side of the "Setting Virtual Adapter Threshold" screen.

6.6.2 Confirm Notifications

If the number of virtual adapters exceeds the threshold value set for virtual adapters, an event will occur.

The following message will be displayed on [Events] - [Operation Log].

Event ID	Message
30030112	The upper warning threshold value was exceeded at the virtual adapter 'virtual adapter name' of the virtual machine 'virtual machine name'. The monitoring item 'monitoring item name' with value 'measured value' exceeded threshold 'value set by user'.
50030114	The upper abnormal limit threshold value was exceeded at the virtual adapter 'virtual adapter name' of the virtual machine 'virtual machine name'. The monitoring item 'monitoring item name' with value 'measured value' exceeded threshold 'value set by user'.

The following are set for the monitoring item name.

- Transmit Error Rate
- Transmit Drop Rate
- Received Error Rate
- Received Drop Rate

6.6.3 Confirm the Traffic for Virtual Adapters

1. Select the node that was notified of in the event in "6.6.2 Confirm Notifications."
2. Select the "Network" - "Map" on the Details of Node screen.

3. Select the virtual adapter name that you want to check the traffic for. Otherwise, select the highlighted virtual adapter name.

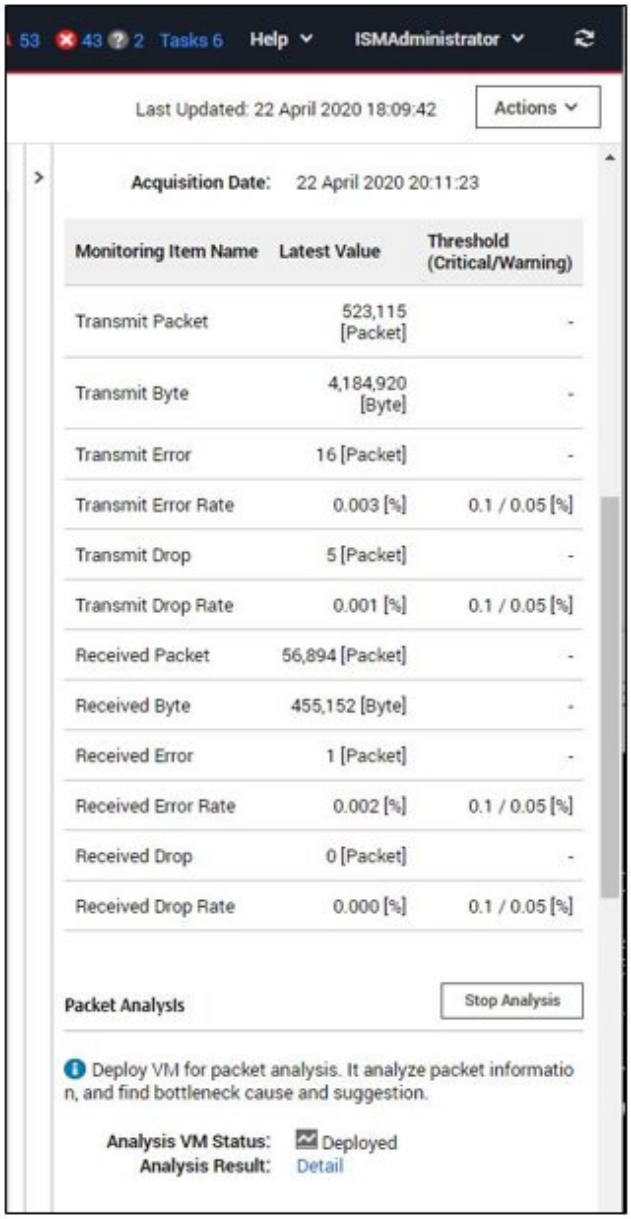
4. Scroll the bar downward on the [Virtual Adapter Information] window displayed in the right pane to see [Traffic Information].
   By selecting the [Graph] button located on the right of the information, you can check the transition of the monitored data in a graph.

Point

- For OpenStack, [Process information] (CPU utilization rate of the virtual adapter) is displayed in [Virtual Adapter Information].

- If you select a virtual machine that has a virtual adapter which is set for monitoring, [CPU Information] (vCPU utilization range of the VM) is displayed in [Virtual Machine Information]. If you select vCPU ID, [Process Information] (CPU utilization rate of the process) is displayed. If you select [CPU core ID], [Physical CPU Information] (Physical CPU utilization rate) is displayed.

Figure 6.1 [Virtual Adapter Information] window



6.6.4 Start Packet Analysis

If the cause of performance degradation cannot be identified even by completing up to the traffic check, execute the packet analysis of the monitoring target host where the event is occurring.

Deploy Analysis VM for the monitoring target host hypervisor where the performance failure is occurring.

6.6.4.1 Obtain Analysis VM

To obtain Analysis VM of virtual network, contact your local Fujitsu service partner.

Note

The Analysis VM image used varies according to the type of hypervisor (VMware, OpenStack).

6.6.4.2 Import Analysis VM

Deploy an Analysis VM image on ISM-VA according to the following procedure. If you have already deployed it in ISM-VA, ignore this procedure.

Deploy the Analysis VM image in the file transfer area "/Administrator/ftp" in ISM-VA using the FTP client or the file upload function.

For details, refer to "2.1.2 FTP Access" in "User's Guide" or "1.4.1 Upload Files to ISM-VA."

You can also import Analysis VM when you input parameters in "6.6.4.3 Start Packet Analysis." In this case, a unique identification character string is attached to the beginning of the file name.

Example: PKTANALYZ110_VMWARE.vmdk
File name after importing
563654e8-2f95-4c89-96b3-eece9772d179-PKTANALYZ110_VMWARE.vmdk

6.6.4.3 Start Packet Analysis

1. Select the virtual network adapter to execute Packet Analysis from [Virtual Adapter].
2. Select the [Start Analysis] button for Packet Analysis displayed in the right pane of the screen.
3. Enter the parameters.

Table 6.6 Analysis VM IP Address Settings

Item	Description
IP Version*	Select the IP version.
DHCP*	Select whether to enable or disable DHCP. **For OpenStack, if IPv6 is selected for the IP Version, DHCP is automatically enabled.
IP address*	Specification is required if DHCP is disabled.
Prefix (when IPv6 is specified)* Subnet Mask (when IPv4 is specified)*	Specification is required if DHCP is disabled.
Default Gateway	Specification is required if DHCP is disabled. **VMware will be shown only.
NTP server IP Address	Specify the NTP server with the IP address. **It is recommended to specify an NTP server IP address to avoid time lag.

*: Required setting item

Table 6.7 Analysis VM Deploy Settings (VMware)

Item	Description
Analysis VM Name*	Specify the Analysis VM name.
Analysis VM Image Filename*	Specify vmdk file of Analysis VM.
Analysis VM ovf Filename*	Specify ovf file of Analysis VM.
Datastore Name*	Specify the data store name.
Folder Name	Specify the folder name of vCenter that manages Analysis VM.
Virtual Switch Type Connected to Management Port*	Select the type of virtual switch for the connection destination (standard virtual switch/virtual distributed switch) of the management port.

Item	Description
Virtual Switch Name*	Specify the name of switch that can communicate with ISM.
Network Label/Port Group*	Specify the network label that can communicate with ISM or a port group name.

*: Required setting item

Table 6.8 Analysis VM Deploy Settings (OpenStack)

Item	Description
Analysis VM Name*	Specify the Analysis VM name.
Analysis VM Image Filename*	Specify qcow2 file of Analysis VM.
Security Group*	Specify the security group name that has SSH permission to be applied to Analysis VM.
Project Name*	Specify the project name in which the Analysis VM belongs.
Network Name*	Specify the network that can be communicated with ISM.
Floating IP Address Setting*	Select if you use a floating IP address.
Floating IP Address*	Specify the floating IP address. **This item is required if you use a floating IP address.

*: Required setting item

Note

- If the condition been improved after addressing the cause as a result of checking the packet analysis outcome, it is recommended that you stop the packet analysis in order to reduce the processing load and usage of disk space.
- Once the packet analysis is started, do not delete or change the node OS account or cloud management software settings. If you delete or change them, you will not be able to retrieve Packet Analysis information. Also, you will not be able to remove Analysis VM from ISM.
- Resources must be obtained in advance because Analysis VM will be deployed on the monitoring target host hypervisor.

  For details, refer to "1.3 System Requirements" in "User's Guide."
- When Analysis VM is deployed, packet mirror settings will be executed on the monitoring target host automatically. Packet Analysis analyzes only the header information for the packets that have been captured by mirroring. Also, the captured information is not stored.
- During the execution of Packet Analysis, the performance of service VM may be degraded due to the high workload node CPU because the resources on the monitoring target host are depleted from analyzing packets. Keep this in mind before use.
- For VMware, the virtual adapter to be analyzed must be connected to the virtual distributed switch.
- For OpenStack, SSH must be authenticated in a security group applied to Analysis VM.

6.6.5 Confirm the Status of Packet Analysis

Check Operation Log to see if Packet Analysis has been started. Also, you can check the current Packet Analysis status list by selecting [Packet analysis of virtual network] from the [Actions] button.

The main messages output in Operation Log are as follows.

Event ID	Message	Action
10030037	Packet Analysis setting was completed (Analysis VM: analysis virtual machine name)	Start Analysis is completed successfully. Check the result of Packet Analysis.
50035216	An error has occurred while deploying of packet analysis. Analysis virtual machine (analysis virtual	Specify the correct input parameter and execute again. Or check the status of the cloud management software.

Event ID	Message	Action
	machine name) deploying was failed. (Error message)	Take action according to the output (Error message).
50035217	An error has occurred while deploying of packet analysis. Analysis virtual machine (analysis virtual machine name) setting was failed. (Error message)	Specify the correct input parameter and execute again. Or check the status of the cloud management software. Take action according to the output (Error message).

6.6.6 Confirm the Results for Packet Analysis

Check the bottleneck Analysis Cause, Analysis Reason, and Analysis Suggestion. Also, check the result of Packet Analysis.

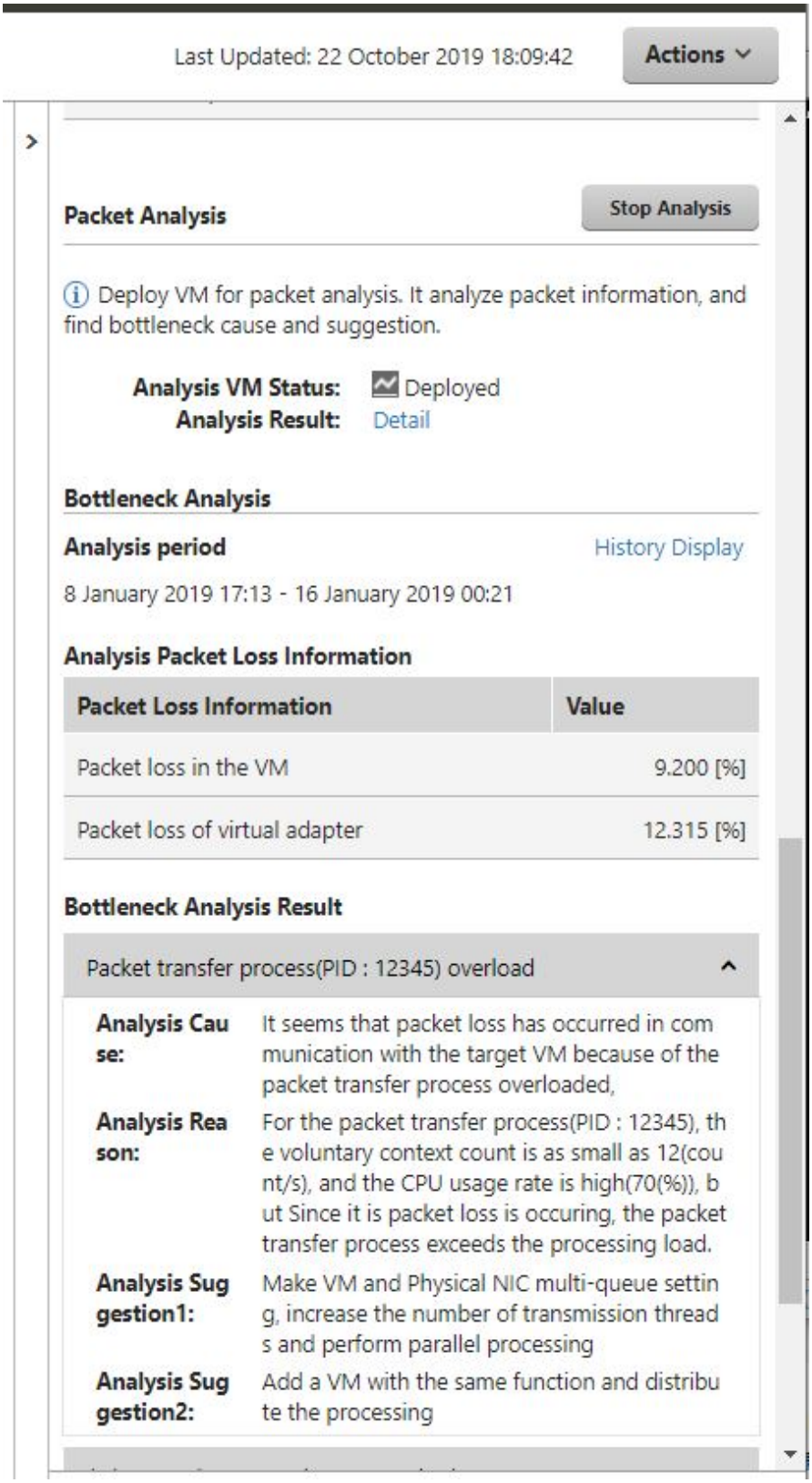
Point

To check the packet analysis results, select "Detail" and check the information approximately ten minutes after packet analysis has started.

The following items are displayed as [Bottleneck Analysis]. Consider the countermeasures, referring to the description.

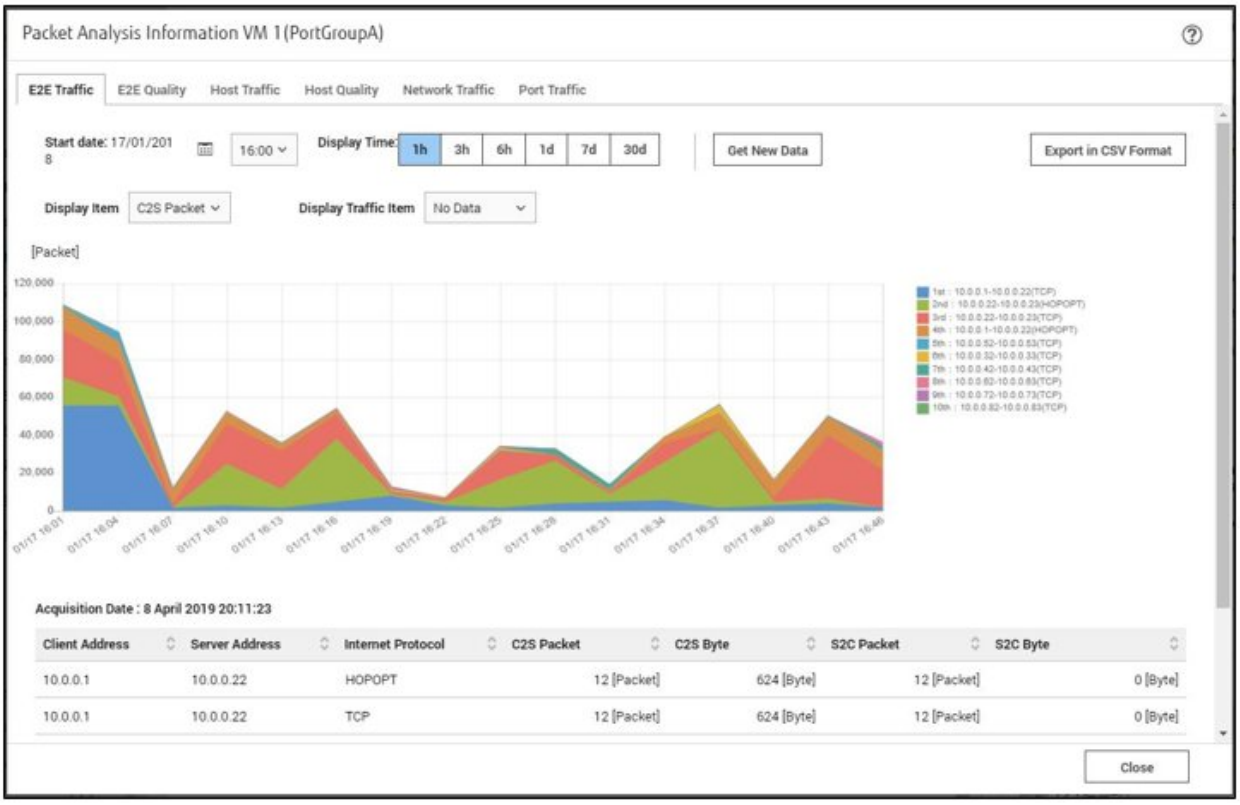
- [Analysis period]
- [Analysis Packet Loss Information]
- [Bottleneck Analysis Result] (Analysis Cause, Analysis Reason, and Analysis Suggestion)

Figure 6.2 Bottleneck analysis result



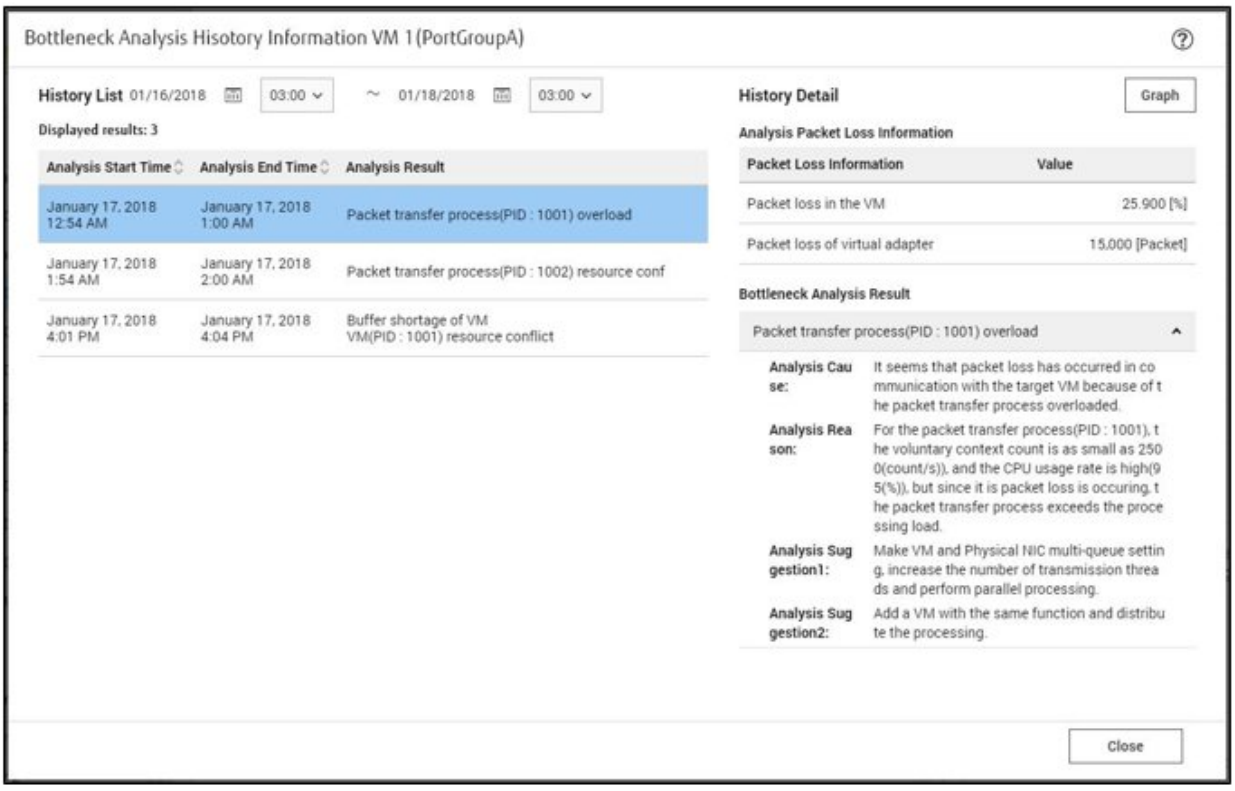
Select "Detail" and check the result of [Packet Analysis].

Figure 6.3 Packet Analysis Result



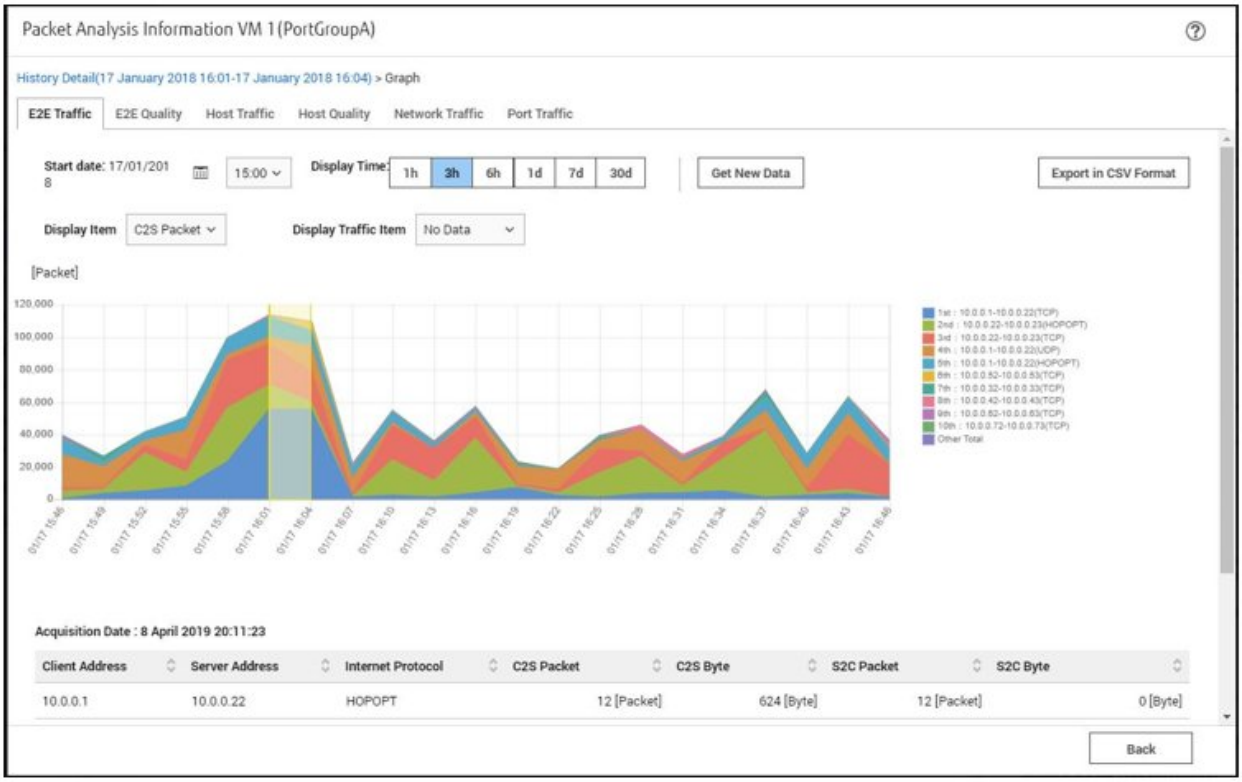
With [Bottleneck Analysis], you can check the past bottleneck analysis results by selecting [History Display].

Figure 6.4 Bottleneck Analysis History



Select the [Graph] button to display bottleneck analysis results including the selected bottleneck analysis information period. The target period is highlighted in yellow on the graph.

Figure 6.5 Packet analysis result (includes the previous bottleneck analysis period)



6.6.7 Stop Packet Analysis

Select "Virtual Adapter" for which Packet Analysis is executed and select the [Stop Analysis] button for Packet Analysis displayed in the [Virtual Adapter Information] in the right side of the screen. Or from the [Actions] button, select [Packet analysis of virtual network], and then select the [Stop Analysis] button in the analysis settings.

Analysis VM is deleted from the hypervisor.

6.7 Execute Rolling Update on the PRIMEFLEX System

This section describes the procedure to execute Rolling Update for firmware and ESXi patches, ESXi Offline bundle, and vCSA patches, and vCSA upgrades with the function in ISM for PRIMEFLEX after having taken virtualized platforms for PRIMEFLEX HS/PRIMEFLEX for VMware vSAN or PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI into operation.

This function can be used only when the ISM Operation Mode is "Advanced for PRIMEFLEX."

Rolling Update is executed according to the following work flow.

Table 6.9 PRIMEFLEX HS/PRIMEFLEX for VMware vSAN Rolling Update work flow

Rolling Update procedure		Tasks
1	Preparations	- Obtaining the firmware data to be applied - Obtaining the ESXi patch/offline bundle file to be applied - Obtaining the vCSA patches or vCSA upgrade files to be applied - Importing the firmware data to be applied into ISM-VA

Rolling Update procedure		Tasks
		- Deleting scripts that are executed before and after the application of old ESXi patches/offline bundle and ESXi patches/offline bundle - Uploading the ESXi patch/offline bundle file to ISM-VA - Uploading the vCSA patch file to be applied to the datastore - Mounting the vCSA patch to be applied to vCSA - Uploading the vCSA upgrade file to be applied to ISM-VA - Selecting nodes on which to execute firmware updates - Selecting temporary nodes for virtual machines - Creating scripts to execute before and after an ESXi patch/offline bundle application
2	Execute Rolling Update	
3	Follow-up Processing	- Confirming firmware updates - Confirming the ESXi version - Confirming the script execution results - Confirming the vCSA version - Updating the OS information - Updating the cloud management software information - Unmounting the applied vCSA patch from vCSA - Deletion of the existing vCSA - Confirming and migrating vCLS virtual machine datastores - Deleting unnecessary files

Table 6.10 PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI Rolling Update work flow

Rolling Update procedure		Tasks
1	Preparations	- Obtaining the firmware data to be applied - Importing the firmware data to be applied into ISM-VA - Selecting nodes on which to execute firmware updates - Selecting temporary nodes for virtual machines
2	Execute Rolling Update	
3	Follow-up processing	- Confirming firmware updates - Changing verify status for profiles that are mismatch to match

6.7.1 Operation Requirements

To use Rolling Update, the following operation requirements must be met.

- Common operation requirements for all configurations
- Operation requirements for PRIMEFLEX HS/PRIMEFLEX for VMware vSAN configuration only
- Operation requirements for PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI configuration only

Common operation requirements for all configurations

Operation requirements for target clusters

- Virtual Resource Management pre-settings have been executed.

  For details, refer to "3.8 Pre-Settings for Managing Virtual Resources/Clusters" in "User's Guide."

- At least one ADVM must be running for configurations that link with Active Directory.
- The network configuration must be the same as the environment that has been structured with PRIMEFLEX HS, PRIMEFLEX for VMware vSAN, PRIMEFLEX for Microsoft Storage Spaces Direct, or PRIMEFLEX for Microsoft Azure Stack HCI installation service.
- The time settings must synchronize with the NTP server.
- When updating firmware, upload/import the firmware data to ISM in advance.

  Use the latest firmware data that is already registered in ISM to apply firmware data.

- When migrating virtual machines on other nodes, make sure to specify temporary nodes that have enough resources (CPU performance, memory capacity, and so on) to operate the virtual machines as temporary nodes and that have no virtual machines that are turned on.

  Rolling Update temporarily migrates the virtual machine operating on the node to be updated to a temporary node. After restarting the node that was updated, the virtual machine is migrated back from the temporary node to the node that was updated.
  Set temporary nodes from the "Rolling Update" wizard - the "3. Temporary Node" screen - [Temporary Node].

- The number of IP addresses allocated by the DHCP server/router is set to be three times or more the number of servers for Offline Update of firmware.

Operation requirements for target servers

- Update target nodes must be turned on.

  You can check if nodes are turned on with the following procedure.

  1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster] to display the "Cluster List" screen.
  2. From the [<Target cluster>] - [Node List] tab, select the name of the update target nodes to display Details of Node screen.
  3. Check the power status from the [Property] tab - "Power Status."

Note

- If the virtual machines that cannot be migrated to other nodes due to reasons related to system configurations or cluster settings are running, Rolling Update will fail.

  Example: For PRIMEFLEX for Microsoft Storage Spaces Direct configurations, ISM-VA can only be migrated between management and workload servers.

  You can avoid migrating virtual machines with one of the following procedures:

  - Stop virtual machines that cannot be migrated to another node manually before executing Rolling Update.
  - Set nodes that are running virtual machines that cannot be migrated to another node so that they are not rebooted in the "Rolling Update" wizard.

  For Offline Update, shut down the update target node. Do not specify nodes that are running virtual machines that cannot be migrated to another node as update target nodes.

- Rolling Update migrates virtual machines that are running to other nodes when they are restarted even if there are virtual machines that must not be migrated due to license-related issues. Be sure not to migrate virtual machines that would cause a licensing violation.

  You can avoid migrating virtual machines with one of the following procedures:

  - Stop the virtual machines that must not be migrated to another node manually before executing Rolling Update.

- Set nodes that are running virtual machines that must not be migrated to another node so that they are not rebooted in the "Rolling Update" wizard.

For Offline Update, shut down the update target node. Do not specify nodes with virtual machines that must not be migrated due to licensing issues and do not specify nodes that are running as update target nodes.

- If using an ADVM in a PRIMEFLEX configuration and Offline Update, do not update the target nodes that are running ADVM#1 and ADVM#2 at the same time.

  You must execute Rolling Update for the nodes that are running ADVM#1 and ADVM#2 separately.

  Example: Procedure to update all nodes running ADVM#1 and ADVM#2 in two separate instances with Rolling Update

  1. Manually stop ADVM#2.
  2. Select all the update target nodes except for the node that is running ADVM#1.
  3. Execute Rolling Update.
  4. Manually start ADVM#2.
  5. Manually stop ADVM#1.
  6. Select the update target node that was running ADVM#1.
  7. Execute Rolling Update.
  8. Manually start ADVM#1.

Operation requirements for PRIMEFLEX HS/PRIMEFLEX for VMware vSAN configuration only

Operation requirements for target clusters

- Use the administrator of the vCenter Single Sign-On domain for your cloud management software registration account information.
- There are no errors in the statuses of clusters and nodes.

  The statuses of clusters and nodes are checked at the beginning of processing. If an error has occurred, Rolling Update is not executed, since data integrity cannot be guaranteed.

  Before executing Rolling Update, check the statuses of clusters and nodes for any errors.

  - Clusters

    For vCSA 6.5 and earlier (Flash):

    1. Log in to vCSA with vSphere Web Client.
    2. From the "Top" screen, from the [Home] tab check that there are no warnings or error icons in the cluster names in the [Hosts and Clusters] navigation menu.

    For vCSA 6.7 or later (HTML5):

    1. Log in to vCSA with vSphere Client.
    2. From the "Top" screen, check that there are no warnings or error icons in the cluster names in the [Shortcuts] - [Hosts and Clusters] navigation menu.

  - Nodes

    Log in to ISM and check that the status of the update target node in the [Management] - [Nodes] - the "Node List" screen is "Normal."

- Use four or more normal nodes for the configuration.

  You cannot use Rolling Update for the configuration of three or less nodes.

- The vCSA of PRIMEFLEX must be registered in the cloud management software of ISM.

- The automation level must be set to "Automatic."

  When the VMware Distributed Resource Scheduler (hereafter referred to as "DRS") is on, you can set the automation level of VMware DRS with the following procedure, however, if you set the automation level to other than "Automatic" it may finish with an error. Make sure to set the automation level to "Automatic." When DRS is enabled, you do not need to prepare a temporary node.

  For vCSA 6.5 and earlier (Flash):

  1. Log in to vCSA with vSphere Web Client.
  2. From the "Top" screen, set the automation level of DRS from the [Home] tab - [Hosts and Clusters] - [<Cluster Name>] - [Settings] - [Service] - [vSphere DRS] - [Edit].

  For vCSA 6.7 or later (HTML5):

  1. Log in to vCSA with vSphere Client.
  2. From the "Top" screen, set the automation level of VMware DRS from [Shortcuts] - [Hosts and Clusters] - [<Cluster Name>] - [Configure] - [Service] - [vSphere DRS] - [Edit].

- There is enough free space on the vSAN data store.

  Even if you set one node in Maintenance Mode, you must be able to secure 30% or more of vSAN data store.

- Set Health errors to disabled in the alarm definitions.

  Set the ESXi host in Maintenance Mode because the update target nodes are rebooted during Rolling Update. In this case, the following Health errors may occur:

  - For vSAN 6.5 environment (VMware ESXi 6.5) to vSAN 7.0 U1 environment (VMware ESXi 7.0 U1)
    - Virtual SAN Health alarm, "Virtual SAN Disk Balance"
    - Virtual SAN Health service alarm, "General health summary"
    - Virtual SAN Health alarm, "Cluster Health"
  - For vSAN 7.0 U2 environment (VMware ESXi 7.0 U2) or later
    - vSAN cluster alarm 'vSAN disk balance'
    - vSAN health service alarm for Overall Health Summary
  - For vSAN7.0 U3 environment (VMware ESXi 7.0 U3) or later
    - vSAN cluster alarm "vSAN disk balance"
    - vSAN health service alarm, "Overall Health Summary "
    - vSAN hardware compatibility, "vSAN HCL DB up-to-date"
    - vSAN hardware compatibility, "vSAN HCL DB Auto Update"
    - vSAN build recommendation, "vSAN release catalog up-to-date"
    - vSAN build recommendation, "vSAN build recommendation engine"
    - "vSAN Support Insight"

  Set the above health errors to disabled in the alarm definition. You can set the alarm definition with the following procedure.

  - For vSAN 6.5 environment (VMware ESXi 6.5) or later (Flash)

    From the "Top" screen, select [Inventories] - [Hosts and Clusters] - [<vCSA Name>] - [Monitor] - [Issues] - [Alarm Definitions]

  - For vSAN 6.7 environment (VMware ESXi 6.7) or later (HTML5)

    From the "Top" screen, select [Inventories] - [Hosts and Clusters] - [<vCSA Name>] - [Configure] - [Alarm Definitions]

  After executing Rolling Update, reverse the alarm definition if necessary.

Point

- If you do not set these Health errors to disabled with the alarm definition and a Health error occurs, Rolling Update ends in an error before completion.
- If you reverse the alarm definition after executing Rolling Update, these Health errors may occur. Take action, referring to the following KB:

  https://kb.vmware.com/s/article/2144278

- For vCSA 7.0 U1 or later, the status of vSphere Cluster Service (vCLS) must be normal.

  Confirm the vSphere Cluster Service (vCLS) status with the following procedure.

  1. Log in to vCSA with vSphere Client.
  2. From the "Top" screen, select [Shortcuts] - [Hosts and Clusters] - [<Cluster name>] - [VMs] - [Virtual Machines].
  3. Check [<vCLS name>] - [Status] for [Name].

     - For vCSA 7.0U2 and earlier:

       <vCLS name> is displayed as "vCLS (n)" (n is a number).

     - For vCSA 7.0U3 or later:

       <vCLS name> is displayed as "vCLS-XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX" (X is a 16 digit number).

     Check that [Status] is "Normal."

  4. Repeat Step 2 to 3 for all vCLS virtual machines.

Point

Depending on the user type that logs in to vCSA, vSphere Cluster Service (vCLS) may not be displayed.
Use the administrator for the vCenter Single Sign-On domain to perform vSphere Cluster Service (vCLS) -related operations.

- For vCSA 7.0 U1 or later, the vCLS virtual machine must exist on the vSAN datastore.

  Confirm the datastore in which the vCLS virtual machine is placed with the following procedure.

  1. Log in to vCSA with vSphere Client.
  2. From the "Top" screen, select [Shortcuts] - [Hosts and Clusters] - [<Cluster name>] - [VMs] - [Virtual Machines] - [<vCLS name>].

     - For vCSA 7.0U2 and earlier:

       <vCLS name> is displayed as "vCLS (n)" (n is a number).

     - For vCSA 7.0U3 or later:

       <vCLS name> is displayed as "vCLS-XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX" (X is a 16 digit number).

  3. Check that [Data Store] - [Name] is the vSAN datastore name.

     To confirm the vSAN datastore name, use the ISM GUI to check Cluster Definition Parameters for the target cluster in the [Cluster Details] - [Storage Pool] tab under [Storage Pool Name].

     If it is not the vSAN datastore name, perform "Procedure for migrating to the vSAN datastore" in "6.7.4.9 Confirm and migrate the vCLS virtual machine datastore."

  4. Repeat Step 2 to 3 for all vCLS virtual machines.

Operation requirements for applying a vCSA patch

- SSH login for vCSA must be enabled.

  You can check if SSH login is enabled with the following procedure.

  1. Log in to VMware Appliance Management as the root user.
  2. You can check "Enabled" in [Access] - [Access Settings] - [SSH Login].

  You can start the SSH service with the following procedure.

  1. Log in to VMware Appliance Management as the root user.
  2. Select the [Access] - [Access Settings] - [EDIT] button.
  3. On the "Edit Access Settings" screen, enable [Enable SSH Login] and select the [OK] button.
- For vCSA 7.0 U1 or later, the user in the cloud management software must be a vCenter Server single sign-on administrator user.
- When applying a patch to a vCenter Server Appliance, update the vCenter Server Appliance before applying the patch.

  Example: If you are applying the vCSA 7.0U2c patch to vCSA 7.0

  Apply the patches in the following order.
  Update 7.0 to 7.0U2, then apply the 7.0U2c patch (a patch cannot be applied directly, such as 7.0 to 7.0U2c)

Operation requirements for applying a vCSA upgrade

- SSH login for vCSA must be enabled.
- DRS must be off.
- The user in the cloud management software must be a vCenter Server single sign-on administrator user.
- vCSA exists in the target cluster.
- Cluster Definition Parameters have been set.
- The version of vDS for the vCSA you are using must be supported.

  Confirm that the version is supported by referring to the following URL.

  https://kb.vmware.com/s/article/52826

  If the version is not supported, upgrade to a version of vDS that is supported by vCSA in advance.

  The version of vDS can be checked with the following procedure.

  For vCSA 6.5 and earlier (Flash):

  1. Log in to vCSA with vSphere Web Client.
  2. From the "Top" screen, select the [Home] tab - [Inventories] - [Networking] - [<vDS switch name>].
  3. Select the [Summary] tab - [Version].
  4. Repeat Step 2 to 3 for all vDS.

  For vCSA 6.7 or later (HTML5):

  1. Log in to vCSA with vSphere Client.
  2. From the "Top" screen, select [Shortcuts] - [Inventories] - [Networking] - [<vDS switch name>].
  3. Select the [Summary] tab - [Version].
  4. Repeat Step 2 to 3 for all vDS.
- The type of the vCSA version and the cloud management software are the same.
- When upgrading vCenter Server Appliance, update the vCenter Server Appliance before applying the upgrade.

  Example: If you are upgrading vCSA 6.7 to vCSA 7.0U2c

Apply the upgrade in the following order.
Update 6.7 to 7.0U2, then upgrade to 7.0 U2c (an upgrade cannot be applied directly, such as 6.7 to 7.0 U2c)

Operation requirements for applying an ESXi patch/Offline bundle

- If using an ADVM in a PRIMEFLEX configuration, DRS must be off.
- If using an ADVM in a PRIMEFLEX configuration, select the node that is executing ADVM#1 or ADVM#2 as the temporary node.

  Migrate ADVM#1 or ADVM#2 executing on the node selected as the temporary node to the node executing ADVM#1 or ADVM#2 that is not selected as the temporary node.

Note

- Since the Health check of vSAN is enabled, the following warning may be displayed. Health errors and countermeasures are as follows:
  - When the hardware compatibility check results in an error, refer to the following web site and update the HCL DB (Hardware Compatibility List Database) to the latest version, and then check that the error display has disappeared.

    https://kb.vmware.com/kb/2109870

    The latest HCL DB data can be obtained from the following URL:

    http://partnerweb.vmware.com/service/vsan/all.json
  - When the performance service check results in an error, set the performance service on to avoid the error. If you enable the performance service, you must design the capacity of the capacity devices with consideration of the maximum capacity of 255 GB of the database.

    https://kb.vmware.com/kb/2144403

    When the performance service is not used in the customer's environment, from the "Top" screen - [Home] tab - [Inventories] - [Host and Clusters], select [<Cluster Name>] - [Summary] - [Reset To Green] for the target warning to clear the warning.
  - If [Network] - [MTU Check (ping for largest packet size)] is in an error, the alert warning may be issued in error. If there are no errors in the network configuration and the ESXi host, the alert warning can be avoid by taking the following countermeasures:
    - Disable the alarm in vSAN Health Alarm "MTU Check (ping for larger packet size)" in the alarm definition.
    - Delete an event for "Warning" from the screen to specify the trigger.
  - If [Cluster] - [Virtual SAN Disk Balance] is in an error, you can normalize the Virtual SAN Disk Balance by executing "Rebalance Disks" manually. Also, when the utilization rate of the capacity device reaches to 80%, vSAN will re-valance the cluster until the utilization rate of the capacity device becomes lower than the threshold value.
- When the ESXi host is set in Maintenance Mode to reboot the update target nodes during Rolling Update, the following Health errors may occur:
  - Disk format version

  When you apply the ESXi offline bundle, "Disk format version" may be changed. The alert warning can be disabled by taking action as described on the following web site:

  https://kb.vmware.com/s/article/2145267
  - Disable the alarm with "Disk format version" in the alarm definition.
- When applying the vCSA upgrade and ESXi patch/offline bundle, confirm that the combination of the versions to be applied is supported by referring to the following URL.

  Never upgrade to a version that is not supported, as this may damage the environment.

  https://www.vmware.com/resources/compatibility/sim/interop_matrix.php

  Example: For ESXi 6.7 U3, vCSA 6.7 or later is required.
- For vCSA 7.0 U2 or later, do not use local users to log in to vCSA.

Operation requirements for PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI configuration only

Operation requirements for target clusters

- There are no errors in the statuses of clusters and nodes.

  The statuses of clusters and nodes are checked at the beginning of processing. If an error has occurred, Rolling Update is not executed, since data integrity cannot be guaranteed.

  Before executing Rolling Update, check the statuses of clusters and nodes for any errors.

  - Clusters

    Access the cluster representative IP (cluster access point) using remote desktop connection, open the Failover Cluster Manager and check that there are no warnings or errors in the [<Cluster name>] cluster events and that the Health status of [<Cluster name>] - [Storage] - [Pool] - [<Pool name>] - [Virtual Disk] is "Normal."

  - Nodes

    Log in to ISM and check that the status of the update target node in the [Management] - [Nodes] - the "Node List" screen is "Normal."

- The "Health Status" of the virtual disk must be normal.

  In the Failover Cluster Manager, select [Storage] - [Pool] - [Pool Name], and then select [Virtual Disk] at the bottom of the screen to confirm the "Health Status" of the virtual disk.

- Use three or more normal nodes for the configuration.

  You cannot use Rolling Update for the configuration of two or less of nodes.

- The target Microsoft Failover Cluster must be registered in the cloud management software of ISM.

  System Center can be registered, but it is not used with Rolling Update.

- Virtual machines must be high availability virtual machines.

  Virtual machine migration is supported only for high availability machines. A high availability virtual machine can be configured by selecting a virtual machine and a common storage as the storage location for the virtual hard disk. To check if the virtual machine is a high availability virtual machine, from Failover Cluster Manager, select [Roles] - [<Virtual Machine Name>] and check the [Resources] tab at the bottom of the screen to confirm that the memory area is "Cluster virtual disk (Vdisk)."

Note

- Since the ADVM is created in the local disk (other than Storage Spaces Direct), Live Migration cannot be used. Therefore, when you restart the node that contains ADVM, shut down the ADVM in advance.
- If a CPU Internal Error (CPU IERR) or other error occurs during the execution of the Rolling Update, all virtual machines may fail over.

6.7.2 Preparations

This section describes the preparations required before executing Rolling Update.

Use the following procedure for the preparations.

6.7.2.1 Obtain the firmware data to be applied

For information on the procedure to obtain firmware data for Offline Update, refer to "6.4 Update the Firmware/Driver of the Node" and "2.13.2 Repository Management" in "User's Guide."

Also, for supported firmware, refer to "2.12.4 Rolling Update" in "User's Guide."

6.7.2.2 Obtain the ESXi patch file/offline bundle file to be applied

Download the ESXi patch file/offline bundle file from the VMware web site.

6.7.2.3 Obtain the vCSA patch file or vCSA upgrade file to be applied

Download the vCSA patch file or vCSA upgrade file from the VMware web site.

Table 6.11 File name for each applicable file to vCSA

File Type	File Name
vCSA patch	An iso file that has "-patch-FP" attached to the end of the file name Example: VMware-vCenter-Server-Appliance-<product_version>-<build_number>-patch-FP.iso
vCSA upgrade	iso files other than the above

- Example: When vCSA patches are used for an update (vCSA upgrades cannot be used.)

  Version up from vCSA6.7 Update1 to vCSA6.7 Update3

  Version up from vCSA6.7 Update1 to vCSA6.7 Update2a

  Version up from vCSA6.7 to vCSA6.7 Update2a

- Example: When vCSA upgrades are used for an update (vCSA patches cannot be used.)

  Version up from vCSA6.5 to vCSA6.7

  Version up from vCSA6.5 Update1 to vCSA6.7 Update2a

Note

If you upgrade to vCSA 7.0 Update2, the vSAN build recommendation alarm "vSAN Build Recommendation Engine Health" will occur and Rolling Update will fail. Therefore, before performing Rolling Update, use the procedure on the following site.

https://kb.vmware.com/s/article/83813

6.7.2.4 Import the firmware to be applied into ISM-VA

For information on the procedure to import the firmware data to ISM-VA, refer to "6.4 Update the Firmware/Driver of the Node" and "2.13.2 Repository Management" in "User's Guide."

Also, for supported firmware, refer to "2.12.4 Rolling Update" in "User's Guide."

Add ISM-VA virtual disks if necessary. For information on the procedure to add virtual disks, refer to "3.7 Allocation of Virtual Disks" in "User's Guide."

Note

- For Intel LAN cards, the identifier eTrack-ID is displayed in the current version.

  The eTrack-ID is the firmware version displayed on the iRMC web interface.

  Compare the current version with the imported firmware version to determine what to update.

  - When the firmware is imported from the ServerView Suite Update DVD (12.19.07 or later)

    Format: eTrack-ID before the firmware is applied - eTrack-ID after the firmware is applied (Firmware version of the firmware file)

    If the eTrack-ID before the firmware is applied matches the current version, it will be updated.

  - When the firmware is downloaded from the public site or when the firmware is imported from the ServerView Suite Update DVD (earlier than 12.19.07) or when the imported firmware is earlier than ISM 2.6.0.020

    Format: (Imported firmware version (The firmware does not contain an eTrack-ID))

    It will be updated regardless of the current version.

- To update the firmware for PSAS CP403i / PSAS CP400i, import the version of the ServerView Suite Update DVD that contains the firmware other than the ServerView Suite Update DVD V13.

6.7.2.5 Delete previously used scripts

Use the following procedure to delete old scripts that are executed before and after the application of ESXi patches/offline bundle and ESXi patches/offline bundle when using Rolling Update.

(1) Delete old ESXi patches

Execute for ISM-VA. If you are using ESXi patches that you uploaded to ISM-VA the last time you used Rolling Update, this procedure is not required.

1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. Delete any files that are no longer needed by checking the following items and referring to "1.4.2 Delete Files Uploaded to ISM-VA."

Item	Value
Root Directory	Administrator/ftp
Directory Name	Administrator/ftp/ClusterOperation/ESXi/patch
File	Old ESXi patch files

(2) Delete old ESXi offline bundles

Execute for ISM-VA. If you are using an ESXi offline bundle that you uploaded to ISM-VA the last time you used Rolling Update, this procedure is not required.

1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. Delete any files that are no longer needed by checking the following items and referring to "1.4.2 Delete Files Uploaded to ISM-VA."

Item	Value
Root Directory	Administrator/ftp
Directory Name	Administrator/ftp/ClusterOperation/ESXi/offlinebundle
File	Old ESXi offline bundle

(3) Delete old scripts that are executed before and after the application of ESXi patches/offline bundles

Execute for ISM-VA. If you are using scripts that are executed before and after the application of ESXi patches/offline bundles that you uploaded to ISM-VA the last time you used Rolling Update, this procedure is not required.

1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. Delete any files that are no longer needed by checking the following items and referring to "1.4.2 Delete Files Uploaded to ISM-VA."

Item	Value
Root Directory	Administrator/ftp
Directory Name	Administrator/ftp/ClusterOperation/ESXi/script
File	Old scripts that are executed before and after the application of ESXi patches/offline bundles

6.7.2.6 Upload the ESXi patch file/offline bundle file to be applied to ISM-VA

Upload the ESXi patch file/offline bundle file by checking the following items and referring to "1.4.1 Upload Files to ISM-VA."

Add ISM-VA virtual disks if necessary. For information on the procedure to add virtual disks, refer to "3.7 Allocation of Virtual Disks" in "User's Guide."

Table 6.12 ESXi patch to be uploaded and the directory

Item	Value
Root Directory	Administrator/ftp

Item	Value
File Type	Other
Upload Target Path	Administrator/ftp/ClusterOperation/ESXi/patch
File	ESXi patch file Example: ESXi650-201704001.zip

Table 6.13 ESXi offline bundle to be uploaded and the directory

Item	Value
Root Directory	Administrator/ftp
File Type	Other
Upload Target Path	Administrator/ftp/ClusterOperation/ESXi/offlinebundle
File	ESXi offline bundle file Example: VMware-ESXi-6.7.0-13473784-Fujitsu-v470-1-offline_bundle.zip

Note

Do not decompress the uploaded ESXi patch file/offline bundle file (zip file). If you decompress the file, Rolling Update ends with an error.

6.7.2.7 Upload the vCSA patch file to be applied to the datastore

This operation is required when you apply a vCSA patch.

Use the following procedure to upload the vCSA patch to the datastore of the host on which vCSA is running.

1. Create a folder to store the vCSA patch file with the following procedure.

   For vCSA 6.5 and earlier (Flash):

   a. Log in to vCSA with vSphere Web Client.

   b. From the "Top" screen, select the [Home] tab - [Storages] - [vsanDatastore] - [Files] tab.

   c. Select [Create a new folder] to create a folder for storing the vCSA patch.

   d. Confirmed the [<Created folder>].

   Point

   The created folder name is displayed with the following two types of names from the vSphere Web Client.

   - Name
   - Friendly name

   The name you entered when you created the folder can be confirmed with "Friendly name."

   Record the value displayed in "Name" that is correlated to the "Friendly name."

   For vCSA 6.7 or later (HTML5):

   a. Log in to vCSA with vSphere Client.

   b. From the "Top" screen, select [Shortcuts] - [Storages] - [vsanDatastore] - [Files] tab.

   c. Select [Create a new folder] to create a folder for storing the vCSA patch.

   d. Confirm the [<Created folder>].

Point

- For vCSA 6.7U3 and earlier:

  The created folder name is displayed with the following two types of names from the vSphere Client.

  - Name

  - Friendly name

  The name you entered when you created the folder can be confirmed with "Friendly name."

  Record the value displayed in "Name" that is correlated to the "Friendly name."

- For vCSA 7.0 or later:

  Record the value displayed in the "Path" column after the folder is created.

2. Log in to ESXi of the host on which vCSA is running with Host Client.
3. From the "Top" screen, select the [Navigator] - [Storage] - [Datastores] tab - [vsanDatastore], and then select [Datastore browser].

   The "Datastore browser" screen is displayed.
4. Select the folder name with the same value as "Name" or "Path" confirmed in Step d.
5. Select [Upload] to upload the vCSA patch.

6.7.2.8 Mount the vCSA patch to be applied to vCSA

This operation is required when you apply a vCSA patch.

Use the following procedure to mount the vCSA patch to the vCSA.

For vCSA 6.5 and earlier (Flash)

1. Log in to vCSA with vSphere Web Client.
2. From the "Top" screen, select the [Home] tab - [Inventories] - [Hosts and Clusters] - [<vCSA name>] - [Configure].
3. Select [Configure] - [Hardware of Virtual Machine] - [Edit].
4. On [Edit Settings], select the [Virtual Hardware] tab - [CD/DVD drive 1] - [Datastore ISO File], and then select the [Connected] checkbox.
5. Select [CD/DVD Drive 1] - [CD/DVD Media] - [Reference] to mount vCSA patch.

For vCSA 6.7 and later (HTML5)

1. Log in to vCSA with the vSphere Client.
2. From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters] - [<vCSA name>] - [Summary].
3. Select [Summary] - [Hardware of Virtual Machine] - [Edit Settings].
4. On [Edit Settings], select the [Virtual Hardware] tab - [CD/DVD drive 1] - [Datastore ISO File], and then select the [Connected] checkbox.
5. Select [CD/DVD Drive 1] - [CD/DVD Media] - [Reference] to mount vCSA patch.

6.7.2.9 Upload the vCSA upgrade to be applied to ISM-VA

This operation is required when you apply a vCSA upgrade.

Upload the vCSA upgrade by checking the following items and referring to "1.4.1 Upload Files to ISM-VA."

Add ISM-VA virtual disks if necessary. For information on the procedure to add virtual disks, refer to "3.7 Allocation of Virtual Disks" in "User's Guide."

Table 6.14 Uploading a vCSA upgrade file and directory

Item	Value
Root Directory	Administrator/ftp
File Type	Other
Upload Target Path	Administrator/ftp/ClusterOperation/vCSA
File	vCSA upgrade file Example: VMware-VCSA-all-6.7.0-10244745.iso

6.7.2.10 Select nodes on which to execute firmware updates

When you select nodes, refer to "6.7.1 Operation Requirements," and select nodes that meet the operation requirements.

6.7.2.11 Select temporary nodes for virtual machines

When you select temporary nodes, refer to "6.7.1 Operation Requirements," and select temporary nodes that meet the operation requirements.

Point

When DRS is enabled in a PRIMEFLEX HS/PRIMEFLEX for VMware vSAN configuration, you do not need to prepare a temporary node. DRS can be checked with the following procedure.

For vCSA 6.5 and earlier (Flash):

1. Log in to vCSA with vSphere Web Client.
2. From the "Top" screen, check it from the [Home] tab - [Hosts and Clusters] - [<Cluster Name>] - [Settings] - [Service] - [vSphere DRS].

For vCSA 6.7 or later (HTML5):

1. Log in to vCSA with vSphere Client.
2. From the "Top" screen, check it from [Shortcuts] - [Hosts and Clusters] - [<Cluster Name>] - [Configure] - [Service] - [vSphere DRS].

6.7.2.12 Create scripts to execute before and after an ESXi patch/offline bundle application if needed

There may be some restrictions or precautions for an ESXi patch file or offline bundle file. For details, contact your local Fujitsu customer service partner. By creating a script, the countermeasures for precautions can be taken while Rolling Update is executing.

You can execute these scripts at the following timing.

- Before the ESXi patch/offline bundle application
- At the ESXi patch/offline bundle application
- After the ESXi patch/offline bundle application

Note

- "At the ESXi patch/offline bundle application" means immediately after executing the command and before restarting ESXi.

  "After the ESXi patch/offline bundle application" means after both executing the command and ESXi has been restarted.
- Rolling Update will fail if the script does not finish within the specified time (720 seconds). If an error is displayed on the ISM "Tasks" screen, check the ISM event log. Confirm the message by referring to "ISM for PRIMEFLEX Messages" and take action.

Each script name is fixed. The script names differ depending on when they are executed.

Script name [Note]	When to be executed
pre_script.sh	To be executed before the ESXi patch/offline bundle application
post01_script.sh	To be executed at the ESXi patch/offline bundle application
post02_script.sh	To be executed after the ESXi patch/offline bundle application

[Note]: Only shell (bash) format is supported for scripts.

Point

- You can detect errors by using "exit 1" to terminate the script.
- To be able to check the results of the script in the follow-up processing, add the process for outputting the log into a file in the script on ESXi.

Refer to the following samples to create scripts.

Example for creating a script to execute before the ESXi patch/offline bundle application

The example script is for the following processes required to apply the ESXi patch/offline bundle:

- Removing tools
- Removing drivers
- Changing the driver settings

```
#!/usr/bin/sh

### Tool removal ###
echo "Tool removal Start" >> /scratch/log/pre_script.log
toolName=`(esxcli software vib list | grep storcli)`
if [ $? = 0 ]; then
    echo ${toolName} >> /scratch/log/pre_script.log
    toolName=`(echo ${toolName} | cut -f 1 -d ' ')`
    cmd="esxcli software vib remove -n ${toolName}"
    echo ${cmd} >> /scratch/log/pre_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
echo "Tool removal End" >> /scratch/log/pre_script.log

### Driver removal ###
echo "Driver removal Start" >> /scratch/log/pre_script.log
driver1=`(esxcli software vib list | grep "OEM.500")`
if [ $? = 0 ]; then
    echo ${driver1} >> /scratch/log/pre_script.log
    driver1Name=`(echo ${driver1} | cut -f 1 -d ' ')`
    cmd="esxcli software vib remove -n \"${driverName1}\""
    echo ${cmd} >> /scratch/log/pre_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi

fi
echo "Driver removal End" >> /scratch/log/pre_script.log

### Driver settings ###
```

```
echo "Driver settings Start" >> /scratch/log/pre_script.log
driver2=`(esxcli system module list | grep lsi_mr3)`
if [ $? = 0 ]; then
    echo ${driver2} >> /scratch/log/pre_script.log
    cmd="esxcli system module set -e true -m lsi_mr3"
    echo ${cmd} >> /scratch/log/pre_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
driver3=`(esxcli system module list | grep lsi_msgpt3)`
if [ $? = 0 ]; then
    echo ${driver3} >> /scratch/log/pre_script.log
    cmd="esxcli system module set -e true -m lsi_msgpt3"
    echo ${cmd} >> /scratch/log/pre_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
echo "Driver settings End" >> /scratch/log/pre_script.log

echo "pre_script End" >> /scratch/log/pre_script.log
exit 0
```

Example for creating a script to execute at ESXi patch/offline bundle application

The example script is for executing the countermeasures for the precautions for operation and maintenance for ESXi 6.7:

- Script for replacing an Inbox driver when applying the patch "ESXi670-201905001" or later to the ESXi structured with a custom image of v470-1

```
#!/usr/bin/sh

#### parameter settings ####
EffectiveValue='VMware-ESXi-6.7.0-13473784-Fujitsu-v470-1-offline_bundle.zip -n lsi-mr3 -n lsi-
msgpt3'

### Execution command ###
cmd="esxcli software vib install --dry-run -d /var/tmp/RollingUpdatePatch/${EffectiveValue}"
echo ${cmd} >> /scratch/log/post01_script.log
eval ${cmd}
if [ $? != 0 ]; then
    exit 1
fi

cmd="esxcli software vib install -d /var/tmp/RollingUpdatePatch/${EffectiveValue}"
echo ${cmd} >> /scratch/log/post01_script.log
eval ${cmd}
if [ $? != 0 ]; then
    exit 1
fi

echo "post01_script End" >> /scratch/log/post01_script.log
exit 0
```

Example for creating a script to execute after the ESXi patch/offline bundle application

The example script is for executing the following countermeasures for restrictions and precautions after the ESXi patch offline bundle is applied:

- Restricting power management settings
- Updating an igbn driver

- Setting a temporary area

```
#!/usr/bin/sh

#### parameter settings ####
PowerValue="High Performance"
DriverFile="<driver file name to apply>"
TemporaryName="scratch"
### Execution command ###
# Power Policy
echo "Power Policy Start" >> /scratch/log/post02_script.log
CurrentValue=`esxcli system settings advanced list --option=/Power/CpuPolicy | grep '   String
Value: High Performance'`
if [ $? != 0 ]; then
    cmd='esxcli system settings advanced set --option=/Power/CpuPolicy --string-value="High
Performance"'
    echo ${cmd} >> /scratch/log/post02_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
echo "Power Policy End" >> /scratch/log/post02_script.log

# Update Driver
echo "Update Driver Start" >> /scratch/log/post02_script.log
cmd="esxcli software vib install -d /var/tmp/RollingUpdatePatch/${DriverFile}"
echo ${cmd} >> /scratch/log/post02_script.log
eval ${cmd}
if [ $? != 0 ]; then
    exit 1
fi
echo "Update Driver End" >> /scratch/log/post02_script.log

# Temporary
echo "Temporary Start" >> /scratch/log/post02_script.log
TmpSetting=`(vim-cmd hostsvc/advopt/view ScratchConfig.ConfiguredScratchLocation | grep
"value")`
TmpDir=`(echo ${TmpSetting} | cut -f 2 -d '"')`
if [ ${#TmpDir} = 0 ]; then
    cmd="mkdir /var/tmp/${TemporaryName}"
    echo ${cmd} >> /scratch/log/post02_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
    cmd="vim-cmd hostsvc/advopt/update ScratchConfig.ConfiguredScratchLocation string /var/tmp/
${TemporaryName}"
    echo ${cmd} >> /scratch/log/post02_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
echo "Temporary End" >> /scratch/log/post02_script.log

echo "post02_script End" >> /scratch/log/post02_script.log
exit 0
```

Point

The first line of the script must contain the following.

```
#!/usr/bin/sh
```

Note

Do not include an instruction to restart the target node in the script. A reboot always occurs after a script is executed.

Upload script files by checking the following items and referring to "1.4.1 Upload Files to ISM-VA."

Table 6.15 A script to be uploaded and the directory

Item	Value
Root Directory	Administrator/ftp
File Type	Other
Upload Target Path	Administrator/ftp/ClusterOperation/ESXi/script
File	- To upload a script that is to be executed before the ESXi patch/offline bundle application pre_script.sh - To upload a script that is to be executed at the ESXi patch/offline bundle application post01_script.sh - To upload a script that is to be executed after the ESXi patch/offline bundle application post02_script.sh

Point

Upload the offline bundle that is used in the post script to ISM-VA according to the procedure in "6.7.2.6 Upload the ESXi patch file/offline bundle file to be applied to ISM-VA." If you have any files other than the offline bundle to upload, upload the files by checking the following items and referring to "1.4.1 Upload Files to ISM-VA."

Item	Value
Root Directory	Administrator/ftp
File Type	Other
Upload Target Path	Administrator/ftp/ClusterOperation/ESXi/other
File	Other files

6.7.3 Execute Rolling Update

By executing Rolling Update, you can apply rolling update to the firmware, the ESXi patch/offline bundle, vCSA patch, and vCSA upgrade files on the virtualized platform.

Before executing Rolling Update, make sure to check the operation requirements in "6.7.1 Operation Requirements."

This section describes the procedure for executing Rolling Update of ISM for PRIMEFLEX.

Point

Before executing Rolling Update, execute the following "Information retrieval from cloud management software" and "Refreshment of the cluster information":

- Execute information retrieval from cloud management software

  Retrieve information from the cloud management software on ISM GUI to update the contents of the display.

  For details, refer to "2.13.6.2 Retrieving information from cloud management software" in "User's Guide."

  1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [General].
  2. From the menu on the left side of the screen, select [Cloud Management Software].

     The "Cloud Management Software List" screen is displayed.
  3. Select the [Get Cloud Management Software Info] button, and then select the [Run] button.

     When retrieving the information is completed, the log of message ID "10021503" is output in [Events] - [Events] - [Operation Log].

- Refresh cluster information

  Retrieve the information of the virtualized platform on the ISM GUI and update the displayed information.

  For details, refer to "2.12.1.3 Refreshing cluster information" in "User's Guide."

  1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster].

     The "Cluster List" screen is displayed.
  2. From the [Actions] button, select [Refresh Cluster Information].
  3. Check that the update of the cluster information has become "Complete."

Do not execute Rolling Update while other ISM for PRIMEFLEX functions are being executed. Rolling Update will fail. Check the ISM event log. Confirm the message by referring to "ISM for PRIMEFLEX Messages" and take action.

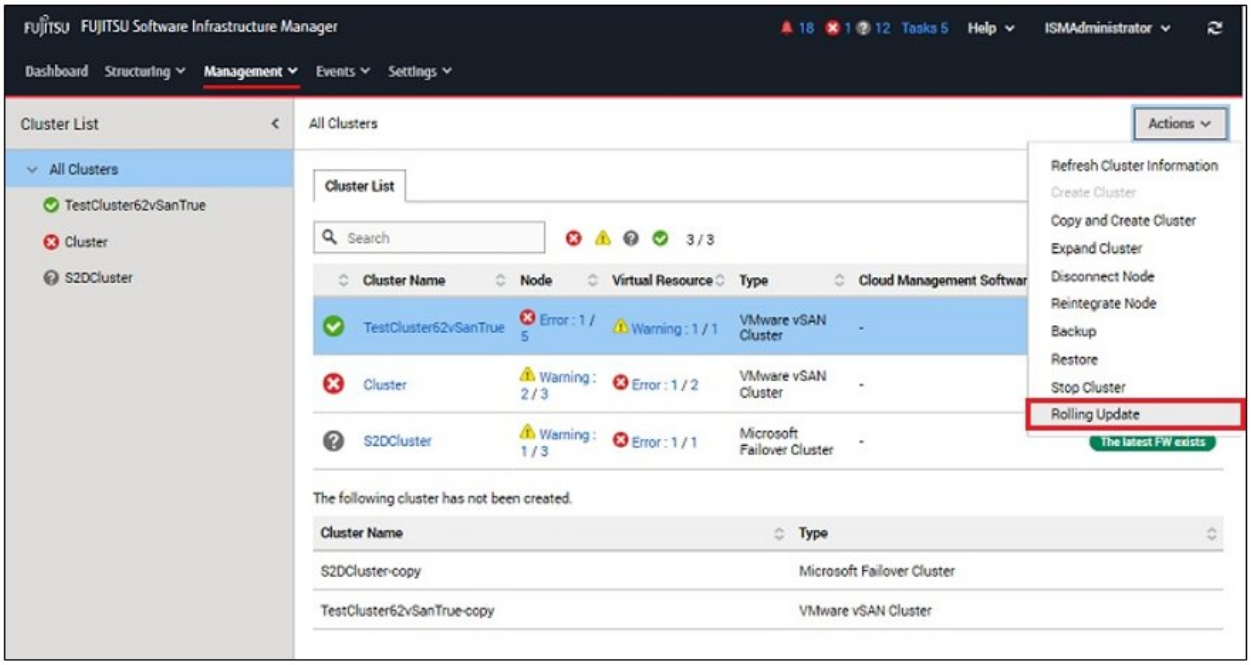
For ISM for PRIMEFLEX functions, refer to "2.12 Functions of ISM for PRIMEFLEX" in "User's Guide."

1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster].

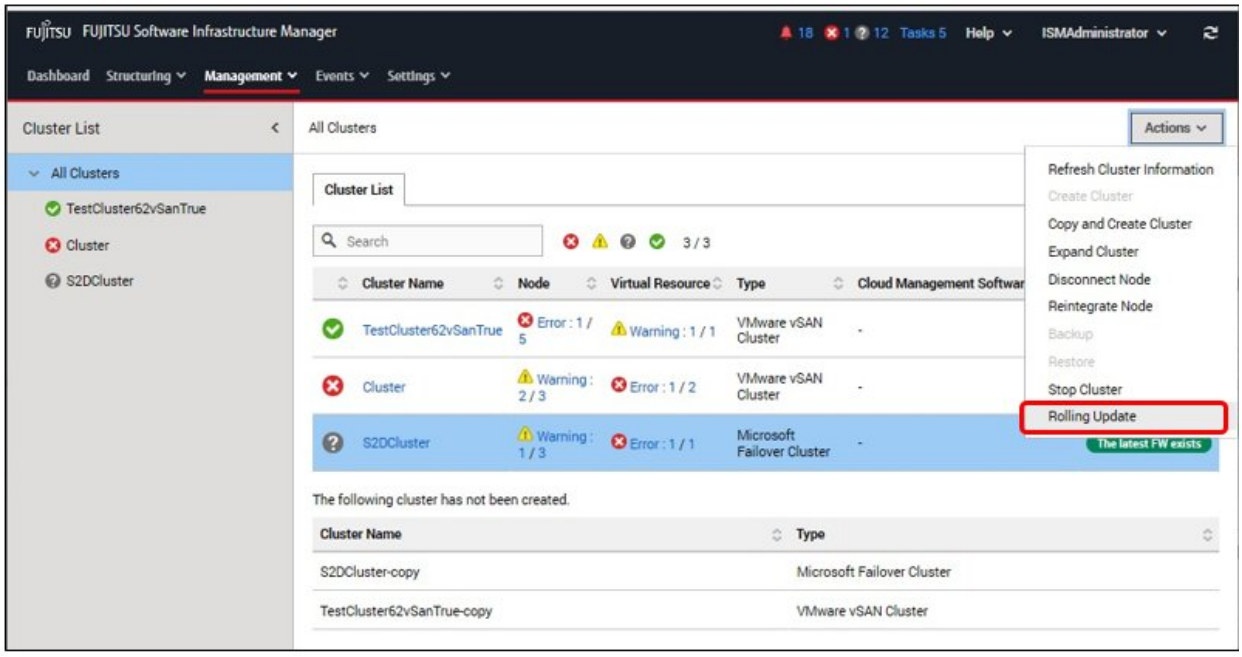
   The "Cluster List" screen is displayed.

3. Select [<Target Cluster>], from the [Actions] button, select [Rolling Update].

   For PRIMEFLEX HS/PRIMEFLEX for VMware vSAN



   For PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI



   The "Rolling Update" wizard is displayed.

   Select an operation option using the following procedure.

Point

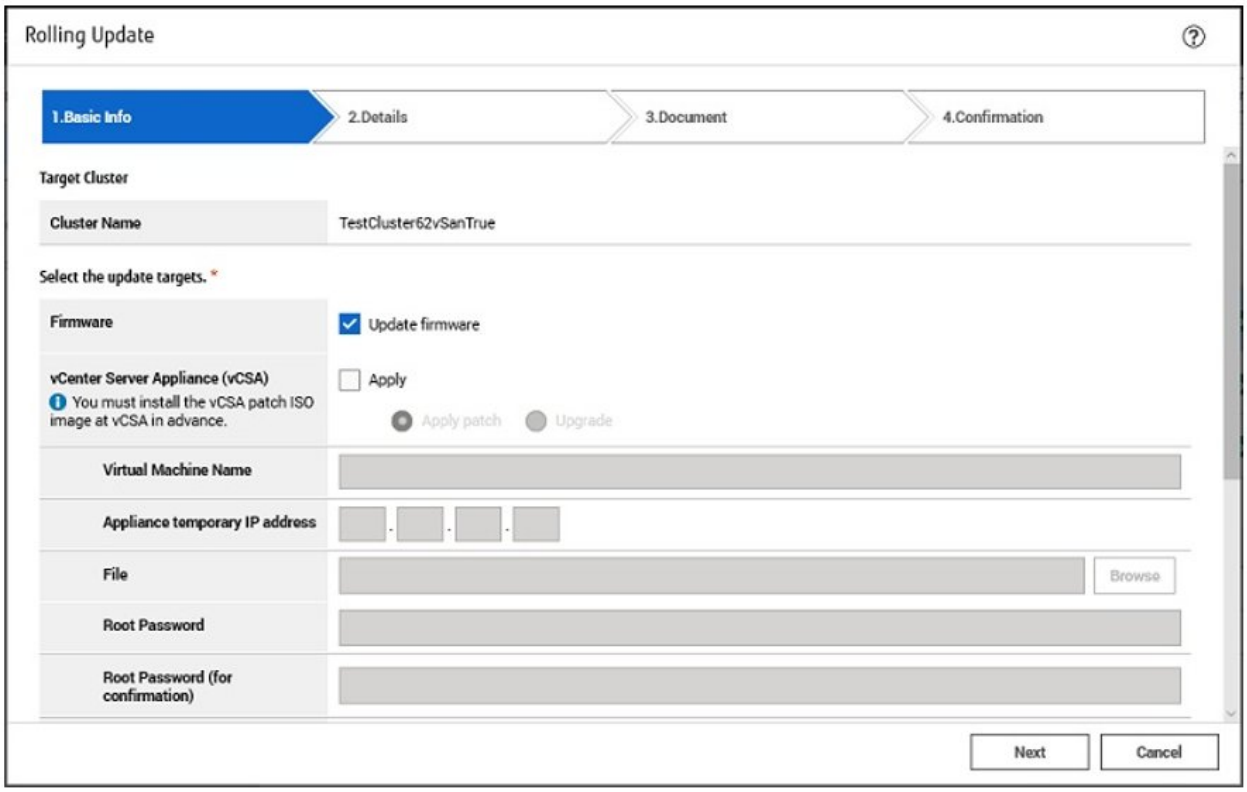
Only for the clusters whose Update Status of the "Cluster List" screen is [The latest FW exists], Rolling Update can be executed.

If the execution conditions are not satisfied, the following "Result" screen is displayed. Read the message and take action to satisfy the execution conditions, and then execute again. For details on the execution conditions, refer to "6.7.1 Operation Requirements."

4. Set the basic information from the "1. Basic Info" screen for Rolling Update execution, and select the [Next] button.

   If executing again, select the [Next] button to proceed to Step 5 if no settings are required.

   For PRIMEFLEX HS/PRIMEFLEX for VMware vSAN



Point

- If you select [VMware ESXi] for the update target, all nodes will be the target nodes. If there are the virtual machines that are running and cannot be migrated to other nodes due to reasons related to system configurations or cluster settings, stop the virtual machines manually.

- If you select [vCenter Server Appliance (vCSA)] - [Upgrade] for the update target, enter the items as follows.
  - Specify an existing vCSA virtual machine name for the virtual machine name.

    The vCSA virtual machine name after the upgrade is <existing vCSA virtual machine name>-new.
  - Specify the same network IP address as the existing vCSA for the temporary IP address of the appliance.
  - Specify the root password of the existing vCSA for the root password.

    This is the same password as the upgraded vCSA.

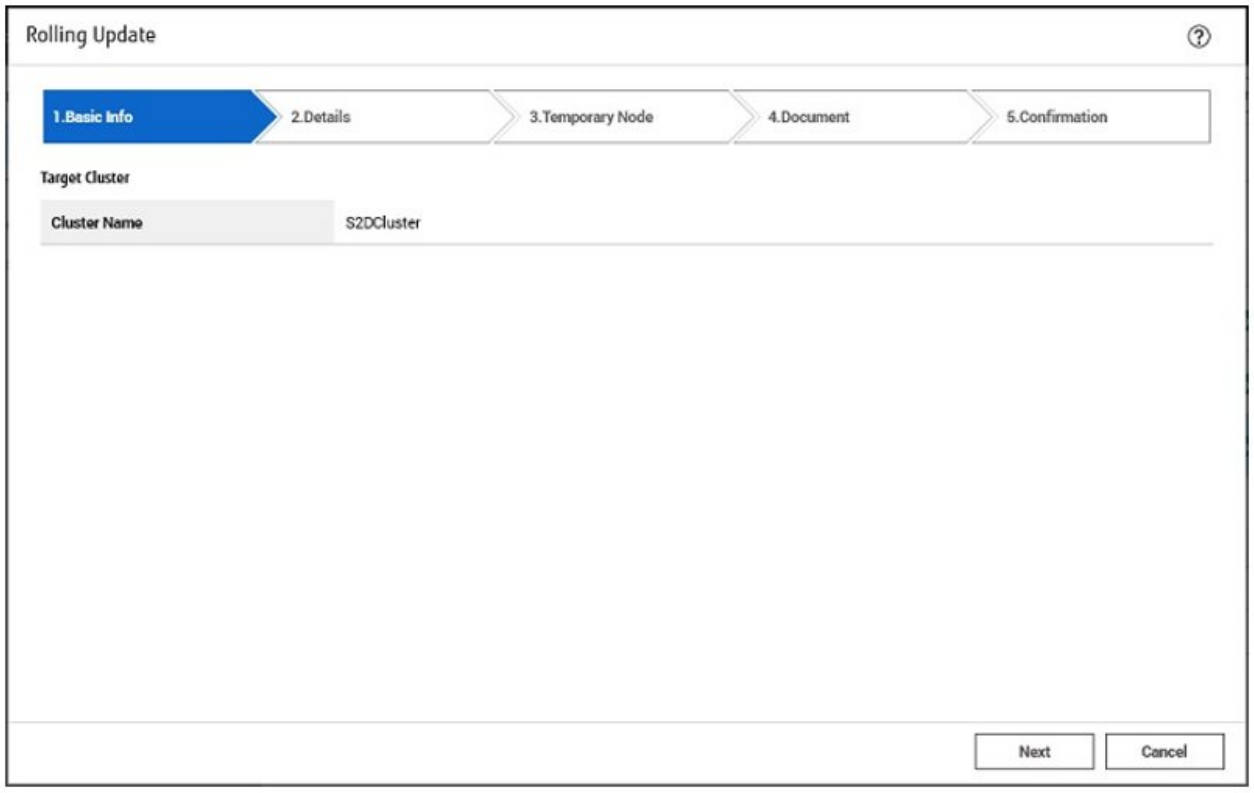
Note

- Local account users are not carried over after vCSA upgrades. You must add local user accounts as in "6.7.4.4 Confirm the vCSA version."

  https://kb.vmware.com/s/article/78148
- If you are applying a patch or upgrading to vCSA 7.0 U1 or later from vCSA 7.0 or earlier, select [vCenter Server Appliance (vCSA)] only and do not select [Firmware] or [VMware ESXi] for update target.

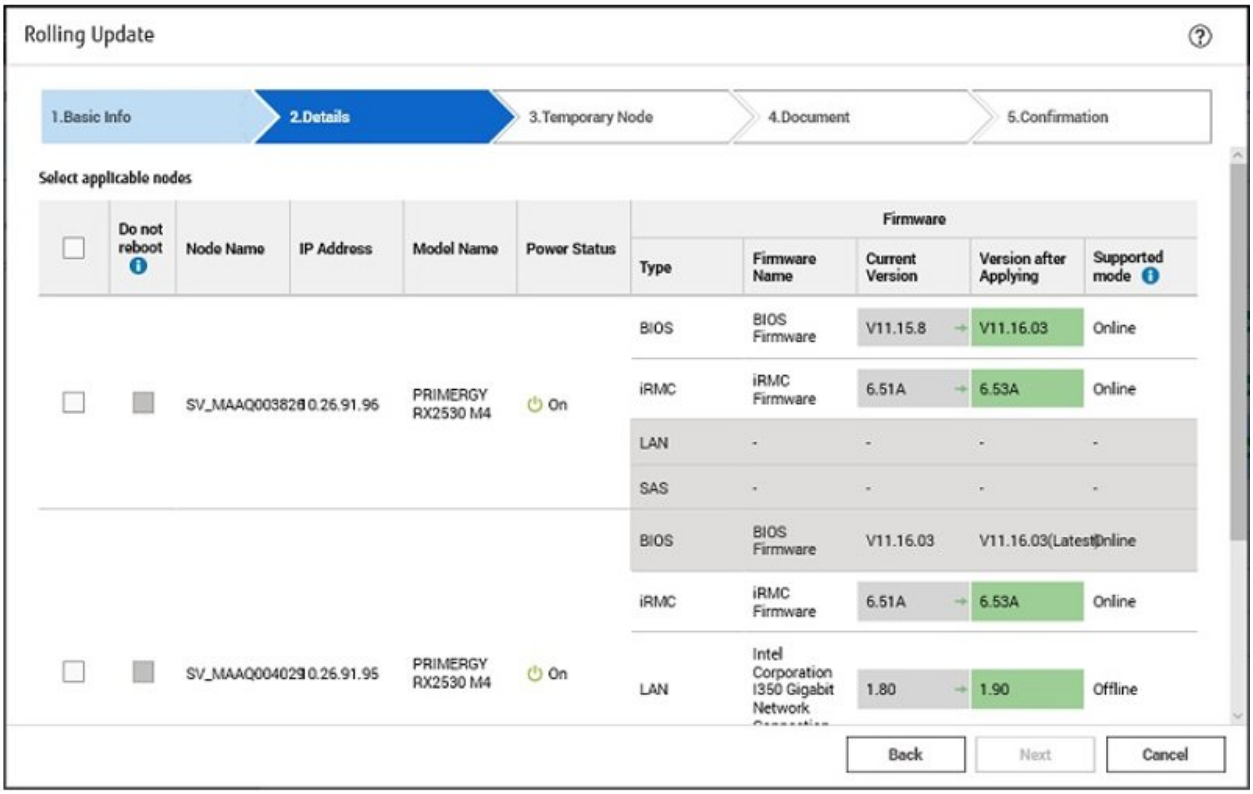
  If you are applying a patch or upgrading to vCSA 7.0 U1 or later from vCSA 7.0 or earlier, the procedure described in "6.7.4.9 Confirm and migrate the vCLS virtual machine datastore" is required. If you select anything other than [vCenter Server Appliance (vCSA)] for the update target before performing this procedure, the vCLS virtual machine migration to the temporary node will fail with an error and Rolling Update will fail.

For PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI



5. From the "2. Details" screen, select the applicable nodes and select the [Do not reboot] checkbox if required, and select the [Next] button.

   If executing again, select the [Next] button to proceed to Step 6 if settings of applicable nodes and the [Do not reboot] checkbox are not required.



Point

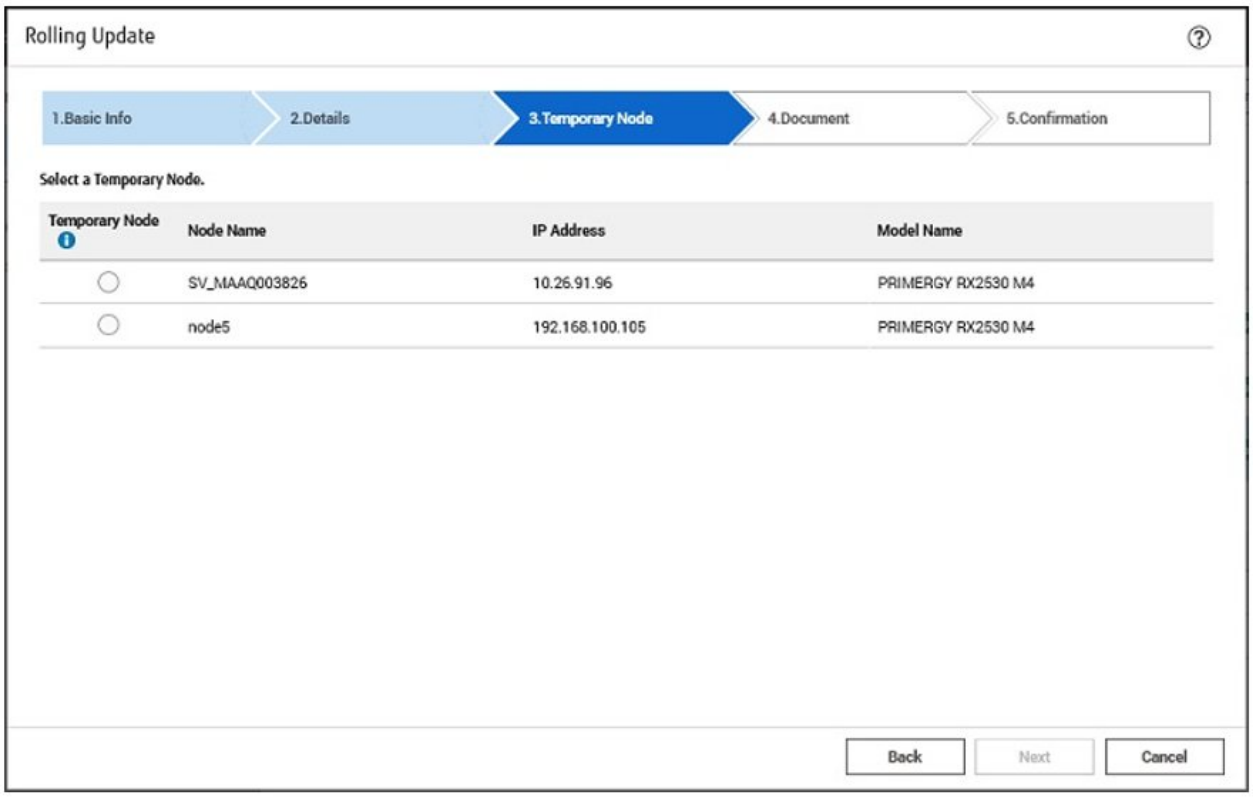
When the target cluster is PRIMEFLEX HS/PRIMEFLEX for VMware vSAN, the "2. Details" screen is not displayed if you do not select [Firmware] for the update target on the "1. Basic Info" screen. Proceed to Step 6.

Note

- Firmware updates of iRMC does not require restarting of the nodes. You can set not to reboot nodes by selecting the [Do not reboot] checkbox for the applicable nodes for the firmware update, which are selected on the "2. Details" screen.
- For firmware updates for BIOS, clear the [Do not reboot] checkbox for the applicable nodes for firmware update, which are selected on the "2. Details" screen. If there are some nodes that must not be rebooted, select the [Do not reboot] checkbox, and then reboot manually after executing Rolling Update.

6. Select the temporary node on the "3. Temporary Node" screen, and select the [Next] button.

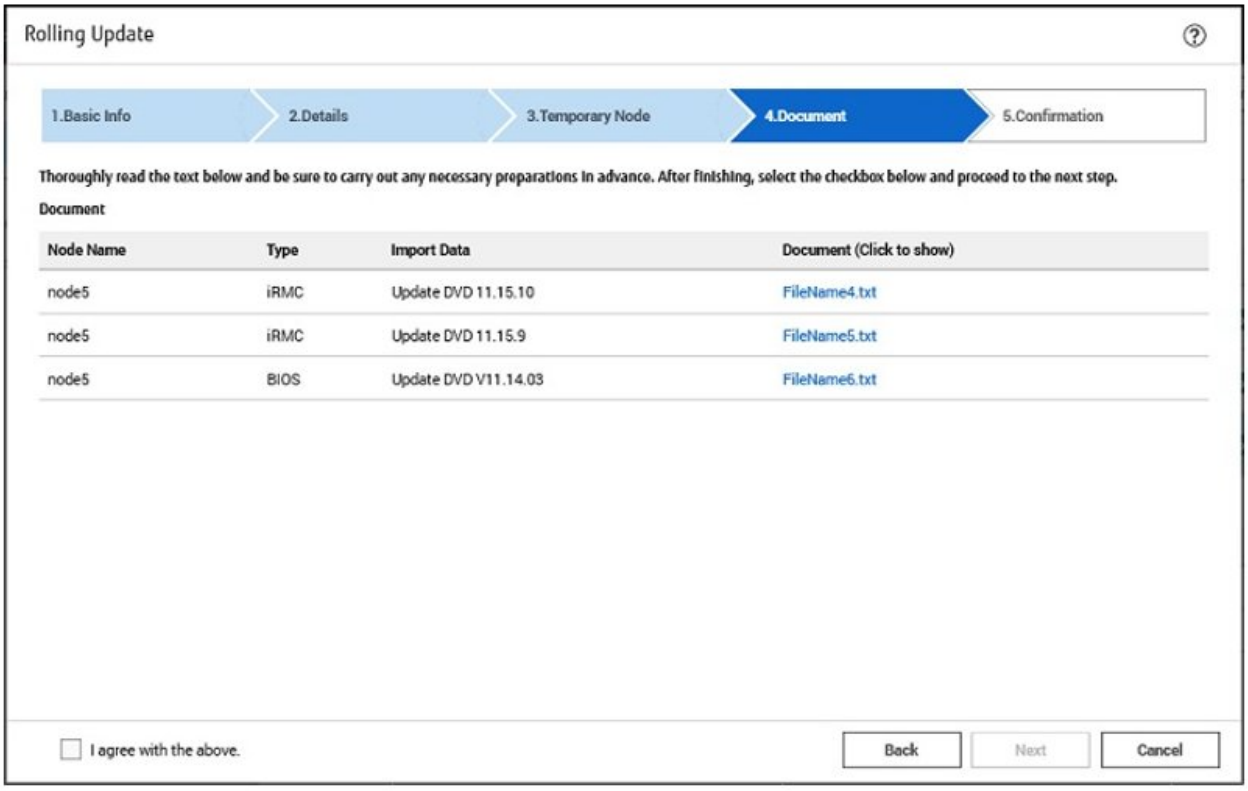
   If executing again, select the [Next] button to proceed to Step 7 if re-selection of the temporary node is not required.



Point

When the target cluster is PRIMEFLEX HS/PRIMEFLEX for VMware vSAN, the "3. Temporary Node" screen is not displayed if DRS is ON. Proceed to Step 7. You can check the DRS status, ON or OFF, from the "1. Basic Info" screen in Step 4.

7. On the "3. Document" or "4. Document" screen, check the document of the firmware to apply, and select the [Next] button.

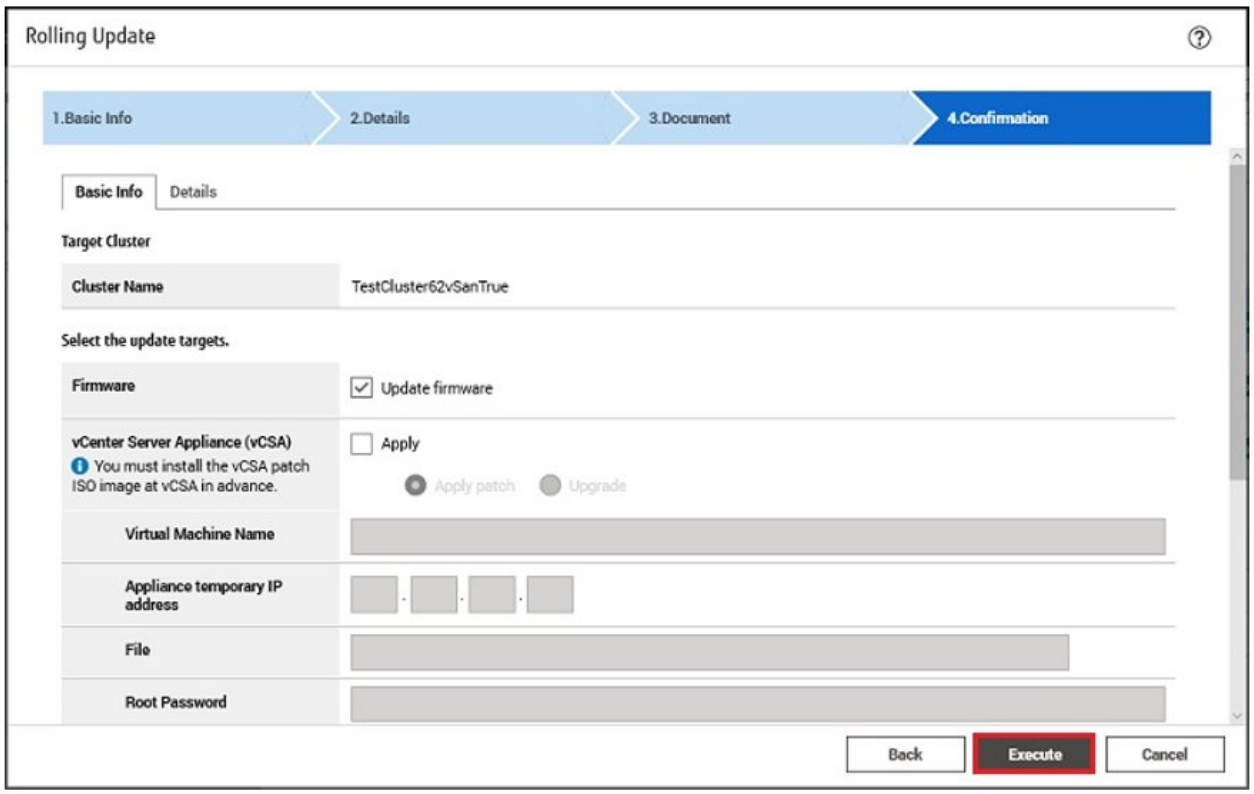


Point

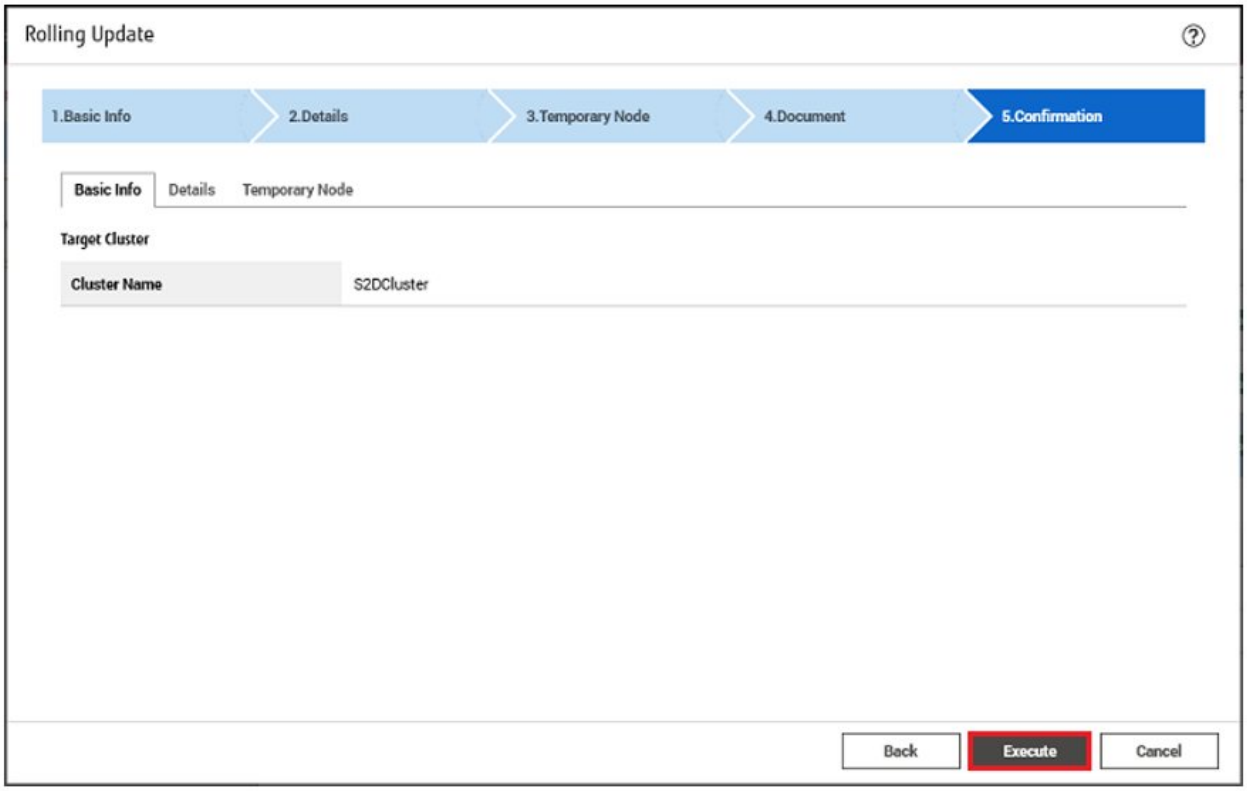
When the target cluster is PRIMEFLEX HS/PRIMEFLEX for VMware vSAN, the "3. Document" screen is not displayed if you do not select [Firmware] for the update target on the "1. Basic Info" screen. Proceed to Step 8.

8. Check the parameters on the "4. Confirmation" or "5. Confirmation" screen, then select the [Execute] button.

   For PRIMEFLEX HS/PRIMEFLEX for VMware vSAN

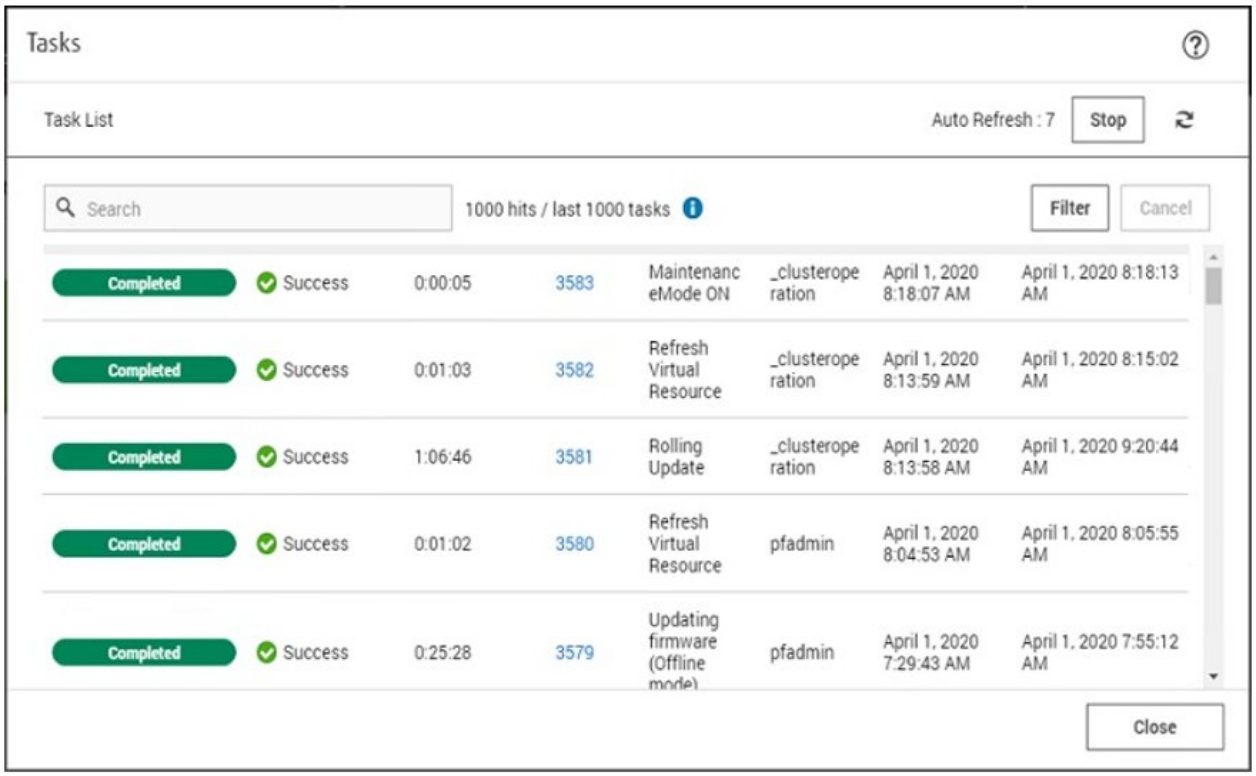


   For PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI



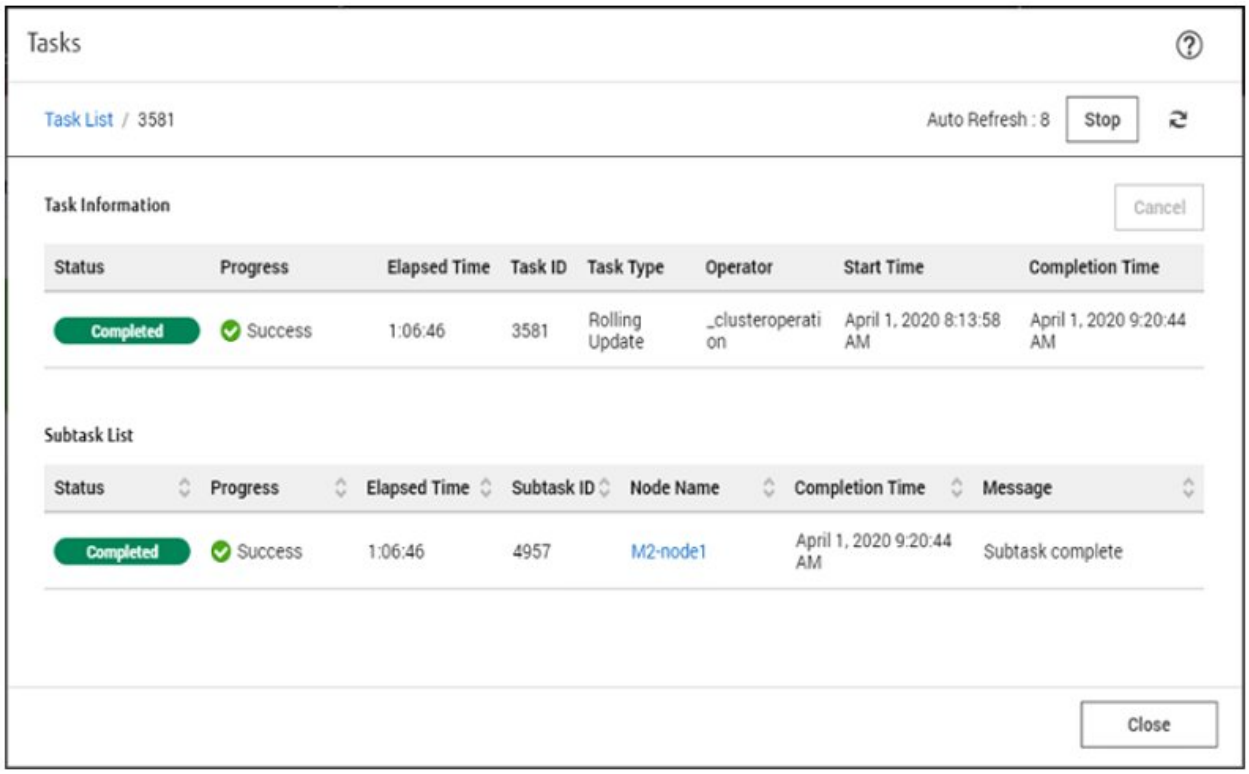
   The execution of Rolling Update is registered as an ISM task.

On the "Tasks" screen, which is displayed when you select [Tasks] on the top of the Global Navigation Menu, tasks whose Task Type is "Rolling Update" are Rolling Update tasks.



Point

If you select [Task ID] for "Rolling Update" from the "Tasks" screen, the "Tasks" screen for "Rolling Update" is displayed. On this screen, the subtask list is displayed and you can confirm the status of the task by checking the message.



9. Check that the status of "Rolling Update" has become "Completed."

Note

Notes on common operation requirements for all configurations

- If an error is displayed on the ISM "Tasks" screen, check the ISM event log. Confirm the message by referring to "ISM for PRIMEFLEX Messages" and take action.

  After the error is resolved, execute Rolling Update again.

- If the BIOS Rolling Update finishes with an error during execution, the target node may be in a state where it is waiting for a restart. If the job is executed again in this state, it may end with an error. To check that the target node is waiting for a reboot, check if the update has been executed with the following procedure. When the update has not been executed, restart manually to complete the update. If updated, no countermeasures are required.

  1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
  2. From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster] to display the "Cluster List" screen.
  3. From [<Target cluster>] - [Node List] tab, select the name of the target nodes to display Details of Node screen.
  4. In the [Firmware/Driver] tab, select the [Actions] button - [Get Node Information].

     The firmware information is refreshed.
  5. Check [Current Version] of the node to be updated and check that the firmware has not been applied.

- Even when there are some nodes on which Update Firmware of Firmware Management ends in an error, if the status of the cluster is normal, any node updated normally will reboot and the firmware will be applied.

- If you set the target nodes for firmware updates to reboot in the "Rolling Update" wizard, the nodes will be rebooted after the firmware update. When the reboot of the nodes starts, the nodes will be disconnected temporarily and the status of the cluster will

be "Error." However, the status of the cluster will return to normal after the reboot is complete. Rolling Update checks the status of the cluster after rebooting and if the status of the cluster is not normal, it ends with an error.

However, in a PRIMEFLEX HS/PRIMEFLEX for VMware vSAN configuration, it may take over six hours until the cluster returns to the normal status depending on when it is updated. When the status of the cluster does not return to normal, execute the test again with the following procedure, and check that the status has returned to normal.

For vCSA 6.5 and earlier (Flash):

1. Log in to vCSA with vSphere Web Client.
2. From the "Top" screen, select [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Monitor] - [vSAN] - [Health], and execute the test again.

For vCSA 6.7 or later (HTML5)

1. Log in to vCSA with vSphere Client.
2. From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Monitor] - [vSAN] - [Health [Note]], and execute the test again.

   [Note]: In vCSA 7.0 or later, [Skyline Health] is displayed.

If the status does not return to normal even after re-testing, collect maintenance data and contact your local Fujitsu customer service partner.

- If the following message is displayed and the process ends with an error, the firmware updates may have succeeded.

```
50215410: Failed to execute Rolling Update. An error occurred during verification of the
Rolling Update task. (Cluster status is abnormal; cluster name = xxxx; cluster status =
YELLOW; detail code = E201003)
```

Use the following procedure to check the results. If the firmware has been updated successfully, no countermeasures are required.

1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster] to display the "Cluster List" screen.
3. From [<Target cluster>] - [Node List] tab, select the name of the target nodes to display Details of Node screen.
4. In the [Firmware/Driver] tab, select the [Actions] button - [Get Node Information].

   The firmware information is refreshed.
5. Check [Current Version] of the node to be updated and check that the firmware has been applied.

- When the network connection cannot be established during node reboot, if ISM retrieves information from this node at this time, it may not be able to retrieve the status and other information and an alarm may be detected. After completion, if an alarm (Warning/Error) is displayed on the [Management] - [Nodes] - "Node List" screen, check the Operation Log of the node. It is not an error if a log fails to retrieve the status or other information. Cancel the alarm. The following message may be displayed in the ISM event log, but you can ignore it.

```
Acquisition of Cloud Management Software information failed. Cloud Management Software
information that was not included in the target or did not exist was specified.
(Message ID: 50170511)
```

- On the "Tasks" screen, a task for "Refresh Virtual Resource" may output the following message and end in an error, but you can ignore it.

```
HTTPError Catched. ServerConnectionError ResponceMessage: (50975051 : An internal error that
cannot be caught has occurred.)
```

Notes on PRIMEFLEX HS/PRIMEFLEX for VMware vSAN configurations

- Even when there are some nodes whose ESXi patch/offline bundle application failed, if the cluster status is normal, any node that successfully completed ESXi patch/offline bundle application process will reboot and the ESXi patch/offline bundle will be applied.

- If you have applied an ESXi patch/offline bundle, update the version of the vSAN disk format if necessary.

  Example: When you execute Cluster Expansion after executing ESXi patch file/offline bundle file application

- If an error is displayed on the ISM "Tasks" screen after you have applied an ESXi patch/offline bundle file, refer to "6.7.4.2 Confirm the ESXi version" and "6.7.4.3 Confirm the execution results of the scripts" to confirm the ESXi version and the execution results of the script.

  If the ESXi version is the version that you have applied the patch/offline bundle to and the execution results of the script are successful, remove ESXi from the update targets and execute Rolling Update again.

- If an error is displayed on the ISM "Tasks" screen after you have applied a vCSA patch or vCSA upgrade, refer to "6.7.4.4 Confirm the vCSA version" to confirm the vCSA version.

  If the vCSA version is the version that you have applied the patch or vCSA upgrade to, remove vCSA from the update targets and execute Rolling Update again. If a vCSA patch is applied or a vCSA upgrade is performed separately, no action is required.

- Rolling Update reboots the updated node by setting the ESXi host to VMware Maintenance Mode. If setting Maintenance Mode fails, set the VMware Maintenance Mode multiple times until successful. Therefore, it may take more than eight hours to complete setting up VMware Maintenance Mode.
  The failure to configure Maintenance Mode can be confirmed by the following error message from the "MaintenanceMode ON" task list on the "Tasks" screen in ISM.

```
HTTPError Catched. OperationError ResponceMessage: (50976211 : Execution failed. Execution of
maintenancemodeon is not capable under this condition. (maintenancemodeon
com.vmware.vim25.Timedout Operation timed out.))
```

Notes on PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI configurations

- If a warning is displayed in the cluster event of [<Cluster name>] of the Failover Cluster Manager after completing Rolling Update, check the event ID and the event details. If the following content is included, it is only a temporary warning and is not an error. Execute [Resetting of the latest event] in the right pane.

Event ID	Details of Event
5120	Cluster Shared Volume 'Volume1'('Cluster virtual disk (Vdisk)') is no longer available on this node because of 'STATUS_DEVICE_NOT_CONNECTED (c000009d)'. All I/O will temporarily be queued until a path to the volume is reestablished.

6.7.4 Follow-up Processing

This section describes the follow-up processing required after executing Rolling Update of ISM for PRIMEFLEX.

6.7.4.1 Confirm Firmware Update

Confirm the Firmware Update with the following procedure.

1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Firmware/Driver].
3. From the menu on the left side of the screen, select [Update].

   Check the displayed "Node List" screen.

   a. From the displayed "Node List" screen, check the current version of the node to be updated and check that firmware has been applied.

      If all firmware except for the nodes for which the [Do not reboot] checkbox is selected have been applied, proceed to Step 4.

   b. For nodes that firmware has not been applied except for the nodes for which the [Do not reboot] checkbox is selected, refer to "Appendix F Troubleshooting" in "User's Guide" and solve the error.

      After that, execute one of the following operations.

      - From the "Rolling Update" wizard, change the settings, and then restart Rolling Update.

- From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Firmware/Driver].

  From the menu on the left side of the screen, select [Update].

  From the displayed "Node List" screen, select the target firmware and from the [Actions] button, select [Update Firmware/Driver].

4. From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster], and check the displayed "Cluster List" screen. If there are any errors in the status of the cluster or the status of the nodes that configure the cluster, collect maintenance data and contact your local Fujitsu customer service partner.

   Note

   In a PRIMEFLEX HS/PRIMEFLEX for VMware vSAN configuration, if you reverse the alarm definition after executing Rolling Update, these Health errors may occur. Take action, referring to the following KB:

   - Virtual SAN Disk Balance

     https://kb.vmware.com/s/article/2144278

5. Log in to the iRMC and confirm that any errors are not output in the System Event Log.

6.7.4.2 Confirm the ESXi version

Use the following procedure to confirm the ESXi version.

For vCSA 6.5 and earlier (Flash)

1. Log in to vCSA with the vSphere Web Client.
2. From the "Top" screen, select the [Home] tab - [Inventories] - [Hosts and Clusters], and then select [<Cluster name>] - [<Host name>] - [Summary].

   The ESXi version is displayed in "Hypervisor."
3. Confirm that the version matches the version of the ESXi patch/offline bundle that you set in Step 4 in "6.7.3 Execute Rolling Update."

   If the application of the ESXi patch/offline bundle fails, refer to "3.3 Action Examples for when a Rolling Update Error Occurs" in "ISM for PRIMEFLEX Messages" and take action. If the error is not resolved, collect maintenance data for ISM and contact your local Fujitsu customer service partner.

   No countermeasures are required if the ESXi patch/Offline bundle is applied successfully.

For vCSA 6.7 or later (HTML5)

1. Log in to vCSA with the vSphere Client.
2. From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters], and then select [<Cluster name>] - [<Host name>] - [Summary].

   The ESXi version is displayed in "Hypervisor."
3. Confirm that the version matches the version of the ESXi patch/offline bundle that you set in Step 4 in "6.7.3 Execute Rolling Update."

   If the application of the ESXi patch/offline bundle fails, refer to "3.3 Action Examples for when a Rolling Update Error Occurs" in "ISM for PRIMEFLEX Messages" and take action. If the error is not resolved, collect maintenance data for ISM and contact your local Fujitsu customer service partner.

   No countermeasures are required if the ESXi patch/Offline bundle is applied successfully.

Note

If you cannot confirm that the ESXi version has been updated after the ESXi patch/offline bundle has been applied, the ESXi patch file that was specified in the "Rolling Update" wizard may be incorrect. Check if the ESXi patch/offline bundle file is correct and execute Rolling Update again.

6.7.4.3 Confirm the execution results of the scripts

Confirm the execution results of the scripts that were created in "6.7.2.12 Create scripts to execute before and after an ESXi patch/offline bundle application if needed" with the output log.

The following messages are output in the log file when the scripts have been executed successfully.

The following message is output for the script that is executed before application in (Example: /scratch/log/pre_script.log).

```
pre_script End
```

The following message is output for the script that is executed at application in (Example: /scratch/log/post01_script.log).

```
post01_script End
```

The following message is output for the script that is executed after application in (Example: /scratch/log/post02_script.log).

```
post02_script End
```

If the script execution failed, check the script logs and take action. After resolving the error, execute the content of the script manually. For details, contact your local Fujitsu customer service partner.

6.7.4.4 Confirm the vCSA version

Use the following procedure to confirm the vCSA version.

For vCSA 6.5 and earlier (Flash)

1. Log in to vCSA with vSphere Web Client.
2. From the "Top" screen, select the [Home] tab - [Inventories] - [Hosts and Clusters].
3. On the screen that is displayed, select vCenter Server, and then select the [Summary] tab.

   The version is displayed in "Version Information."
4. Confirm that the version matches the version of the vCSA patch file or vCSA upgrade file that you set in Step 4 in "6.7.3 Execute Rolling Update."

   If the application of the vCSA patch or vCSA upgrade fails, refer to "3.3 Action Examples for when a Rolling Update Error Occurs" - "Action example 18" and "Action example 19" in "ISM for PRIMEFLEX Messages" and take action. If the error is not resolved, collect maintenance data for ISM and contact your local Fujitsu customer service partner.
5. If you have upgraded vCSA, add local account users with the following procedure.
   a. Log in to vCSA with vSphere Web Client.
   b. From the "Top" screen, select the [Home] tab - [Inventories] - [Hosts and Clusters] - [<Name of the vCSA>] - [Permissions].
   c. Confirm the name of the local account user.

      The local account users listed are not actually inherited, so add them as follows.
   d. Connect to vCSA with the root user via SSH.
   e. Execute the following command.

```
Command>localaccounts.user.add --role admin --username <User name confirmed in Step c> --
password
Enter password:<Password>
```

```
Reenter password: <Password>
Command>
```

f. Execute Step 5a to 5e for all local user accounts.

For vCSA 6.7 or later (HTML5)

1. Log in to vCSA with the vSphere Client.
2. From the "Top" screen, select the [Shortcuts] tab - [Inventories] - [Hosts and Clusters].
3. On the screen that is displayed, select vCenter Server, and then select the [Summary] tab.

   The version is displayed in "Version Information."
4. Confirm that the version matches the version of the vCSA patch file or vCSA upgrade file that you set in Step 4 in "6.7.3 Execute Rolling Update."

   If the application of the vCSA patch or vCSA upgrade fails, refer to "3.3 Action Examples for when a Rolling Update Error Occurs" - "Action example 18" and "Action example 19" in "ISM for PRIMEFLEX Messages" and take action. If the error is not resolved, collect maintenance data for ISM and contact your local Fujitsu customer service partner.
5. If you have upgraded vCSA, add local account users with the following procedure.

   a. Log in to vCSA with vSphere Client.

   b. From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters] - [<Name of the vCSA>] - [Permissions].

   c. Confirm the name of the local account user.

      The local account users listed are not actually inherited, so add them as follows.

   d. Connect to vCSA with the root user via SSH.

   e. Execute the following command.

```
Command>localaccounts.user.add --role admin --username <User name confirmed in Step c> --
password
Enter password:<Password>
Reenter password: <Password>
Command>
```

   f. Execute Step 5a to 5e for all local user accounts.

Point

- The password policy has changed from vCSA 7.0 U2, so your previous password may not be usable. Change the password and add the local account user.
- Check the web browsers that support vSphere Web Client/vSphere Client at the web sites below.
  - vCSA 6.5

    https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.upgrade.doc/GUID-F6D456D7-C559-439D-8F34-4FCF533B7B42.html
  - vCSA 6.7

    https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vcenter.install.doc/GUID-EC80836B-BE02-4CB2-9F40-15928AFB6E20.html
  - vCSA 7.0

    https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vcenter.install.doc/GUID-EC80836B-BE02-4CB2-9F40-15928AFB6E20.html

6.7.4.5 Update OS information

This operation is required after you have applied the ESXi offline bundle.

Use the following procedure to update the OS Information.

On the ISM GUI, update the OS information to refresh the display contents.

For details, refer to "2.2.1.5 Registration of node OS information" in "User's Guide."

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].

   The "Node List" screen is displayed.

2. Select the target node name and select the [OS] tab.

3. From the [OS Actions] button, select [Edit OS Information].

   If [Auto] is selected in [OS Version], Step 4 is not required. Proceed to Step 5.

4. Enter the information in [OS Version] and then select the [Apply] button.

5. From the [Actions] button, select [Get Node Information].

   If the node information retrieval is complete, the log for message ID "10020303" is output in [Events] - [Events] - [Operation Log].

6. Select the [Refresh] button to refresh the display content of the [OS] tab.

7. From the [OS] tab, check [Version] under [Information from OS] to confirm that the version is the ESXi patch/offline bundle that was set in Step 4 in "6.7.3 Execute Rolling Update."

   If the application of the ESXi patch/offline bundle fails, refer to "3.3 Action Examples for when a Rolling Update Error Occurs" in "ISM for PRIMEFLEX Messages" and take action. If the error is not resolved, collect maintenance data for ISM and contact your local Fujitsu customer service partner.

   No countermeasures are required if the ESXi patch/offline bundle is applied successfully.

6.7.4.6 Update cloud management software information

This operation is required after you have applied a vCSA upgrade.

Use the following procedure to update the cloud management software information.

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [General].

2. From the menu on the left side of the screen, select [Cloud Management Software].

   The "Cloud Management Software List" screen is displayed.

3. Select the cloud management software where the vCSA has been upgraded, and then from the [Actions] button, select [Edit].

4. On the "Edit Cloud Management Software information" screen, update to the version of the cloud management software where the vCSA has been upgraded, and then enter the password.

5. Select the [Register] button.

   The "Cloud Management Software List" screen is displayed. The edited cloud management software [Type] is updated.

6.7.4.7 Unmount the applied vCSA patch from vCSA

This operation is required after you have applied a vCSA patch.

Use the following procedure to unmount the vCSA patch from vCSA.

For vCSA 6.5 and earlier (Flash)

1. Log in to vCSA with vSphere Web Client.

2. From the "Top" screen, select the [Home] tab - [Inventories] - [Hosts and Clusters] - [<Name of the vCSA>] - [Configure].

3. Select [Configure] - [Virtual Hardware] - [Edit].

4. On the displayed "Edit Settings" screen, select the [Virtual Hardware] tab - [CD/DVD drive 1] - [Datastore ISO File], and then clear the [connected] checkbox.

For vCSA 6.7 or later (HTML5)

1. Log in to vCSA with the vSphere Client.
2. From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters] - [<Name of the vCSA>] - [Configure].
3. Select [Summary] - [Virtual Hardware] - [Edit Settings].
4. On the displayed "Edit Settings" screen, select the [Virtual Hardware] tab - [CD/DVD drive 1] - [Datastore ISO File], and then clear the [connected] checkbox.
5. If it does not unmount in Step 4, restart vCSA.

6.7.4.8 Deletion of the existing vCSA

Delete the existing vCSA if necessary after you have applied a vCSA upgrade.

For vCSA 6.5 and earlier (Flash)

1. Log in to vCSA with vSphere Web Client.
2. From the "Top" screen, select the [Home] tab - [Inventories] - [Hosts and Clusters].
3. On the screen that is displayed, select the virtual machine for vCSA, and then select [<Virtual machine name>] - [Delete from Disk].
4. On the displayed "Confirm Delete" screen, select the [Yes] button.
5. Confirm that "Completed" is displayed for the status of [Delete virtual machine] displayed in [Recent Tasks].

For vCSA 6.7 or later (HTML5)

1. Log in to vCSA with the vSphere Client.
2. From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters].
3. On the screen that is displayed, select the virtual machine for vCSA, and then select [<Virtual machine name>] - [Delete from Disk].
4. On the displayed "Confirm Delete" screen, select the [Yes] button.
5. Confirm that "Completed" is displayed for the status of [Delete virtual machine] displayed in [Recent Tasks].

6.7.4.9 Confirm and migrate the vCLS virtual machine datastore

This operation is required after you have applied a patch or updated to vCSA 7.0 U1 or later.

Applying a patch or updating vCSA to 7.0 U1 or later enables the vSphere Cluster Service (vCLS) and creates a vCLS virtual machine on the cluster. A maximum of three vCLS virtual machines are created in a cluster.

If this vCLS virtual machine was created in the local datastore, it must be migrated to the vSAN datastore.

Perform this on all target clusters.

Point

Depending on the user type that logs in to vCSA, vSphere Cluster Service (vCLS) may not be displayed.
Use the administrator for the vCenter Single Sign-On domain to perform vSphere Cluster Service (vCLS) -related operations.

Procedure to confirm the datastore in which the vCLS virtual machine is placed

Confirm the datastore in which the vCLS virtual machine is placed.

1. Log in to vCSA with vSphere Client.

2. From the "Top" screen, select [Shortcuts] - [Hosts and Clusters] - [<Cluster name>] - [VMs] - [Virtual Machines] - [<vCLS name>].

   - For vCSA 7.0U2 and earlier:

     <vCLS name> is displayed as "vCLS (n)" (n is a number).

   - For vCSA 7.0U3 or later:

     <vCLS name> is displayed as "vCLS-XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX" (X is a 16 digit number).

3. Check that [Data Store] - [Name] is the vSAN datastore name.

   To confirm the vSAN datastore name, use the ISM GUI to check Cluster Definition Parameters for the target cluster in the [Cluster Details] - [Storage Pool] tab under [Storage Pool Name].

   If it is not the vSAN datastore name, perform "Procedure for migrating to the vSAN datastore."

4. Repeat Step 2 to 3 for all vCLS virtual machines.

Procedure for migrating to the vSAN datastore

Migrate the vCLS virtual machine to the vSAN datastore.

For vCSA 7.0U2 and earlier

1. Log in to vCSA with vSphere Client.
2. From the "Top" screen, select [Shortcuts] - [Hosts and Clusters] - [<Cluster name>] - [VMs] - [Virtual Machines] - [<vCLS name>].
3. Select [ACTIONS] - [Migrate].

   A confirmation screen is displayed.

4. Select [YES] on the confirmation screen.

   The "Migrate" screen is displayed.

5. Select "Change storage only" in [1 Select migration type], then select the [NEXT] button.
6. Select the vSAN data store in [2 Select storage] and select the [NEXT] button.

   You can view the vSAN datastore in "vSAN" in [Type].

7. Use [3 Ready to complete] to check the settings and select the [FINISH] button.

For vCSA 7.0U3 or later

1. Log in to vCSA with vSphere Client.
2. From the "Top" screen, select [Shortcuts] - [Hosts and Clusters] - [<Cluster name>].
3. Select [Configure] - [vSphere Cluster Service] - [Datastores] - [ADD].

   The "Add datastores" screen is displayed.

4. On the "Add datastores" screen, select a vSAN datastore and select [ADD].

6.7.4.10 Deleting unnecessary files

Delete unnecessary files with the following procedure after completing Rolling Update.

(1) Delete ESXi patches

Execute for ISM-VA.

1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. Delete any files that are no longer needed by checking the following items and referring to "1.4.2 Delete Files Uploaded to ISM-VA."

Item	Value
Root Directory	Administrator/ftp

Item	Value
Directory Name	Administrator/ftp/ClusterOperation/ESXi/patch
File Name	ESXi patch files in "6.7.2.6 Upload the ESXi patch file/offline bundle file to be applied to ISM-VA."

(2) Delete ESXi offline bundles

Execute for ISM-VA.

1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. Delete any files that are no longer needed by checking the following items and referring to "1.4.2 Delete Files Uploaded to ISM-VA."

Item	Value
Root Directory	Administrator/ftp
Directory Name	Administrator/ftp/ClusterOperation/ESXi/offlinebundle
File Name	ESXi offline bundle in "6.7.2.6 Upload the ESXi patch file/offline bundle file to be applied to ISM-VA."

(3) Delete scripts that are executed before and after the application of ESXi patches/offline bundles

Execute for ISM-VA.

1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. Delete any files that are no longer needed by checking the following items and referring to "1.4.2 Delete Files Uploaded to ISM-VA."

Item	Value
Root Directory	Administrator/ftp
Directory Name	Administrator/ftp/ClusterOperation/ESXi/script
File Name	Script that is executed before and after the application of ESXi patches/offline bundles in "6.7.2.12 Create scripts to execute before and after an ESXi patch/offline bundle application if needed."

6.7.4.11 Changing [Verify Status] for profiles that are [Mismatch] to [Match] (For iRMC S5 firmware versions updated to 3.37P or later)

When the firmware version for iRMC S5 is updated to 3.37P or later using Rolling Update, the profile verification status is mismatch because the profile content and the node settings are different.

Refer to "Procedures to change [Verify Status] back to [Match] if it is [Mismatch] (For items in which the node setting changes were intended)" in "3.3.5 Compare Assigned Profiles and Hardware Settings."

Refer to "4.5.3 Details - [iRMC] tab" in "ISM for PRIMEFLEX Parameter List" for editing profiles.

6.8 Increase the Resources for PRIMEFLEX HS/PRIMEFLEX for VMware vSAN

You can execute Cluster Creation or Cluster Expansion to increase the resources for PRIMEFLEX HS/PRIMEFLEX for VMware vSAN.

This function can be used only when the ISM Operation Mode is "Advanced for PRIMEFLEX."

Servers for creating a new cluster or servers for expanding a cluster will hereafter be referred to as "target servers."

Cluster Creation or Cluster Expansion is executed according to the following work flow.

Table 6.16 Cluster Creation or Cluster Expansion work flow

Cluster Creation or Cluster Expansion procedure		Tasks
1	Preparations	- Setting VMware EVC for vCenter Server

Cluster Creation or Cluster Expansion procedure		Tasks
		- Creating ADVM certificates - Registering host records in DNS - DHCP settings - Importing ServerView Installation Manager that is provided with the ServerView Suite DVD, and the ISO image of the OS installation media to ISM-VA - Deleting scripts that are executed before and after the application of old VMware ESXi patches and VMware ESXi patches - Upload of the VMware ESXi patch file - Creating scripts to execute before and after a VMware ESXi patch application - Upload of VMware SMIS Provider - Creating profiles - Creating and editing Cluster Definition Parameters - Confirming storage devices - Installation and Wiring - Setting the IP address of iRMC - BIOS settings - Confirming networks - Registering nodes in ISM
2	Execute Cluster Creation or Cluster Expansion	
3	Follow-up Processing	- Confirming resources - Confirming the script execution results - Restrictions/Precautions for VMware vSphere - Confirming and migrating vCLS virtual machine datastores - Registering in ServerView RAID Manager - Deleting unnecessary files - Confirming the settings for VMware EVC mode

6.8.1 Operation Requirements

To use Cluster Creation or Cluster Expansion, the following requirements must be met.

- Common operation requirements for Cluster Creation and Cluster Expansion
- Operation requirements for Cluster Creation
- Operation requirements for Cluster Expansion

Common operation requirements for Cluster Creation and Cluster Expansion

Operation requirements for existing clusters

- The cluster must be the PRIMEFLEX for VMware vSAN cluster
- That the DNS and NTP are all running normally and can be used

- That the time settings synchronize with the NTP server
- That the Active Directory is operating normally and can be used when you are using an Active Directory already configured in your environment, or are using a configuration with an ADVM dedicated to PRIMEFLEX HS/PRIMEFLEX for VMware vSAN
- That the information of the DNS server is registered in ISM-VA
- That the existing cluster is operating normally
- That you register the target server in AD in advance when configuring an AD that already exists in your environment, since registering a computer in AD is restricted by policies etc.
- That the following files of PRIMEFLEX HS/PRIMEFLEX for VMware vSAN installation service in ADVM#1 and ADVM#2 exist when configuring ADVM dedicated to PRIMEFLEX HS/PRIMEFLEX for VMware vSAN:
  - c:\FISCRB\PowerShellScript\fis_advm_ftp_put.ps1
  - c:\FISCRB\PowerShellScript\FIS_JOB_ADVM_SET_DNS_ZONE.ps1
- The following network configuration on vCenter should not be changed from the environment that has been structured with PRIMEFLEX HS/PRIMEFLEX for VMware vSAN installation service (changes effect on the behavior of Cluster Creation/ Expansion):
  - Virtual distributed switch for management
  - Name and uplink port of Virtual distributed switch for workload

  To check the name of the virtual distributed switch, select inventory in the vSphere Client and select the network from the inventory tree displayed. After the structure of PRIMEFLEX HS/PRIMEFLEX for VMware vSAN installation service, the virtual distributed switch displays on vCenter with the following name:
  - Virtual distributed switch for management: vSwitch1 (for PRIMERGY CX series of PRIMEFLEX HS model, vSwitch0 is displayed)
  - Virtual distributed switch for workload: vSwitch0 (for PRIMERGY CX series of PRIMEFLEX HS model, vSwitch1 is displayed)
- NetBIOS domain name is not used for the Active Directory domain name
- Use the administrator of the vCenter Single Sign-On domain for your cloud management software registration account information

Operation requirements for target servers

- That the physical NIC of the target server using the storage network is 10 GbE or 25 GbE
- That the port of the physical switch using the storage network is 10 GbE or 25 GbE
- The power of the target server is off

  The following is an operation requirement when executing Cluster Creation or Cluster Expansion again with the OS installation completed using profile assignment:
  - The power of the target server is on

  To check if the OS installation has been completed, use the following procedure.
  1. At the top of the Global Navigation Menu on the ISM GUI, select [Tasks].
  2. From the cluster list on the "Tasks" screen, select the task ID whose task type is "Assigning profile."
  3. Check that all the results of the tasks in the subtask list have become "Success."
- That the storage configuration is appropriate for the environment

  For details, refer to "6.8.2.12 Confirm installed storage devices."
- The OS information has not been registered for the target server

  The target server is excluded from the selection of target nodes if the OS information has been registered.
- A profile has been created for the target server with Profile Management of ISM

- The computer name of the target servers which you specify in the profile must be unique among all nodes managed by ISM.

  Check if the computer name is unique by comparing with the following conditions:

  - Upper case characters and lower case characters are not distinguished
  - Domain name is excluded

- The IP address of the OS of the target servers which you specify in the profile must be unique among all IP addresses of the OS of the nodes managed by ISM
- The profile has not been applied to the target server

  The target server is excluded from the selection of target nodes if the profile has been applied.

- On the "3. Cluster Details" screen in the "Create Cluster" wizard or "Create Cluster Definition Parameters" wizard, [Function] tab - [vSAN Settings] - [Add disks to storage] is "Manual"
- In a Hybrid configuration, on the "3. Cluster Details" screen in the "Create Cluster" wizard or "Create Cluster Definition Parameters" wizard, [Function] tab - [vSAN Settings] - [Deduplication and compression] is "Disable"
- IPv4 address for the management network port group is the same as the profile setting ([Details] - [OS (for each node)] tab - [Network] - [DHCP] - [IP address]).
- The network information is displayed on iRMC

  For details, refer to "6.8.2.16 Confirm networks."

Operation requirements for Cluster Creation

Operation requirements for existing clusters

- There is one or more existing clusters
- The version of the vCSA of the existing cluster is the same or later than the version of the ESXi of the cluster to be created

Operation requirements for target servers

- The type of the target servers must be the same
- There are three or more target servers
- On the "2. Basic Information" screen in the "Create Cluster" wizard, the name in [Cluster Name] must be 15 characters or less
- On the "3. Cluster Details" screen in the "Create Cluster" wizard, [Storage Pool Name] in the [Storage Pool] tab does not overlap the [Storage Pool Name] of an existing cluster
- On the "3. Cluster Details" screen in the "Create Cluster" wizard, [Port Group Name] in the [Network] tab does not overlap the [Port Group Name] of an existing cluster when creating a new vDS
- If you specify the same vDS name as the vDS name of an existing cluster, vmnic of the vDS of the existing cluster is not LAG (Link Aggregation) configured
- If you specify the same vDS name as the vDS name of an existing cluster, there must be two vmnics for the servers configuring the existing cluster for each vDS
- All the VMware ESXi installation media is the same on the servers for creating a new cluster
- If you apply the VMware ESXi patch, VMware ESXi patch version and VMware ESXi installation media version must be the same

  Also, the VMware ESXi patch build number must be newer than the VMware ESXi installation media build number.

- vCSA and VMware ESXi versions are supported

  For the latest information on products supported by Cluster Creation, refer to "Support Matrix."

  https://support.ts.fujitsu.com/index.asp

  Select [Select a new Product] on the above site and enter "Infrastructure Manager" in [Product Search:].

  Select [DOWNLOADS] and select the target operating system.

The reference procedures are subject to change without notice.

Operation requirements for Cluster Expansion

Operation requirements for existing clusters

- If [Deduplication and compression] is enabled in an All Flash configured environment, set [Add disks to storage] to "Manual."

  If [Add disks to storage] is set to "Automatic," a "vSAN cluster configuration consistency" vSAN health error may occur after executing Cluster Expansion.

  For details, refer to the "Note" in "6.8.2.11 Create and edit Cluster Definition Parameters."

- Cluster Management pre-settings have been executed for the cluster to be expanded

  For settings of Cluster Management, refer to "3.8 Pre-Settings for Managing Virtual Resources/Clusters" in "User's Guide."

- All the VMware ESXi in the existing cluster for cluster expansion have the same version build number

- All vSAN disks in the existing cluster for cluster expansion are the same version

  Confirm this with the following procedure.

  For vCSA 6.5 and earlier (Flash)

  1. Log in to vCSA with vSphere Web Client.
  2. From the "Top" screen, select the [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Monitor] - [vSAN] - [Physical Disk] to display the disk of the target server.

  For vCSA 6.7 or later (HTML5)

  1. Log in to vCSA with vSphere Client.
  2. From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Monitor] - [vSAN] - [Physical Disk] to display the disk of the target server.

  For vCSA 7.0U3 or later

  1. Log in to vCSA with vSphere Client.
  2. From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Configure] - [vSAN] - [Disk Management] - [<Host name>] - [VIEW DISKS] and move the cursor over [disk format version] to display it.

- There are no "disk format version" vSAN health errors

  Confirm this with the following procedure.

  For vCSA 6.5 and earlier (Flash)

  1. Log in to vCSA with vSphere Web Client.
  2. From the "Top" screen, select the [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Monitor] - [vSAN] - [Health] to execute the test again.

  For vCSA 6.7 or later (HTML5)

  1. Log in to vCSA with vSphere Client.
  2. From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Monitor] - [vSAN] - [Health [Note]] to execute the test again.

     [Note]: In vCSA 7.0 or later, it is displayed as [Skyline Health].

- vmnic of the vDS of the existing cluster is not LAG (Link Aggregation) configured

  Confirm this with the following procedure.

  For vCSA 6.5 and earlier (Flash)

  1. Log in to vCSA with vSphere Web Client.
  2. From the "Top" screen, select the [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [<Host name>] - [Configure] - [Networking] - [Virtual switches] - [Distributed Switch] to confirm that the LAG settings are disabled.

For vCSA 6.7 or later (HTML5)

1. Log in to vCSA with vSphere Client.
2. From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [<Host name>] - [Configure] - [Networking] - [Virtual switches] - [Distributed Switch] to confirm that the LAG settings are disabled.

- There must be two vmnics for the servers configuring the existing cluster for each vDS

  Confirm this with the following procedure.

  For vCSA 6.5 and earlier (Flash)

  1. Log in to vCSA with vSphere Web Client.
  2. From the "Top" screen, select the [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [<Host name>] - [Configure] - [Networking] - [Virtual switches] - [Distributed Switch] to confirm that there are two vmnics.

  For vCSA 6.7 or later (HTML5)

  1. Log in to vCSA with vSphere Client.
  2. From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [<Host name>] - [Configure] - [Networking] - [Virtual switches] - [Distributed Switch] to confirm that there are two vmnics.

- The device for the vSAN (vMotion) traffic of the VMkernel adapter in the server configuring the existing cluster must be vmk1 (vmk2)

  Confirm this with the following procedure.

  For vCSA 6.5 and earlier (Flash)

  1. Log in to vCSA with vSphere Web Client.
  2. From the "Top" screen, select the [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [<Host name>] - [Configure] - [Networking] - [VMkernel adapters] to confirm that [vmk1(vmk2)] is vSAN (vMotion).

  For vCSA 6.7 or later (HTML5)

  1. Log in to vCSA with vSphere Client.
  2. From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [<Host name>] - [Configure] - [Networking] - [VMkernel adapters] to confirm that [vmk1(vmk2)] is vSAN (vMotion).

- For vCSA 7.0 U1 or later, the status of vSphere Cluster Service (vCLS) must be normal.

  Confirm the vSphere Cluster Service (vCLS) status with the following procedure.

  1. Log in to vCSA with vSphere Client.
  2. From the "Top" screen, select [Shortcuts] - [Hosts and Clusters] - [<Cluster name>] - [VMs] - [Virtual Machines].
  3. Check [<vCLS name>] - [Status] for [Name].

     - For vCSA 7.0U2 and earlier:

       <vCLS name> is displayed as "vCLS (n)" (n is a number).

     - For vCSA 7.0U3 or later:

       <vCLS name> is displayed as "vCLS-XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX" (X is a 16 digit number).

     Check that [Status] is "Normal."

  4. Repeat Step 2 to 3 for all vCLS virtual machines.

Point

Depending on the user type that logs in to vCSA, vSphere Cluster Service (vCLS) may not be displayed.
Use the administrator for the vCenter Single Sign-On domain to perform vSphere Cluster Service (vCLS) -related operations.

- For vCSA 7.0 U1 or later, the vCLS virtual machine must exist on the vSAN datastore.

  Confirm the datastore in which the vCLS virtual machine is placed with the following procedure.

  1. Log in to vCSA with vSphere Client.
  2. From the "Top" screen, select [Shortcuts] - [Hosts and Clusters] - [<Cluster name>] - [VMs] - [Virtual Machines] - [<vCLS name>].

     - For vCSA 7.0U2 and earlier:

       <vCLS name> is displayed as "vCLS (n)" (n is a number).

     - For vCSA 7.0U3 or later:

       <vCLS name> is displayed as "vCLS-XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX" (X is a 16 digit number).

  3. Check that [Data Store] - [Name] is the vSAN datastore name.

     To confirm the vSAN datastore name, use the ISM GUI to check Cluster Definition Parameters for the target cluster in the [Cluster Details] - [Storage Pool] tab under [Storage Pool Name].

     If it is not the vSAN datastore name, perform "Procedure for migrating to the vSAN datastore" in "6.8.4.4 Confirm and migrate the vCLS virtual machine datastore."

  4. Repeat Step 2 to 3 for all vCLS virtual machines.

Operation requirements for target servers

- The target server must be the same or a successor to a server that is configured in an existing cluster

  For the detailed information, refer to "Support Matrix" ([Details of ISM for PRIMEFLEX] sheet).
  https://support.ts.fujitsu.com/index.asp

  Select [Select a new Product] on the above site and enter "Infrastructure Manager" in [Product Search:].
  Select [DOWNLOADS] and select the target operating system.
  The reference procedures are subject to change without notice.

- Cluster Definition Parameters have been set

  For details, refer to "6.8.2.11 Create and edit Cluster Definition Parameters."

- VMware ESXi patch version is the same as the VMware ESXi build number of the existing cluster for cluster expansion
- VMware ESXi installation media is the following
  - If there are multiple target servers, all the VMware ESXi installation media is the same
  - If you do not apply the VMware ESXi patch, the VMware ESXi patch version is the same as the VMware ESXi build number of the existing cluster for cluster expansion
  - If you apply the VMware ESXi patch, the VMware ESXi patch version is the same as the VMware ESXi version of the existing cluster for cluster expansion

Point

- You must confirm that the resources have increased after executing Cluster Expansion. Confirm the current vSAN storage capacity before executing Cluster Expansion in advance. For the procedure to confirm, refer to "6.8.4.1 Confirm resources."
- Confirm that the VMware ESXi versions, build numbers, and vSAN disk format versions are supported by referring to the following URL.

  https://kb.vmware.com/s/article/2150753

Note

For vCSA 7.0 U2 or later, do not use local users to log in to vCSA.

6.8.2 Preparations

This section describes the preparations required before cluster creation or cluster expansion.

6.8.2.1 Set up VMware EVC for vCenter Server

This operation is required to use Cluster Expansion. This is not required to use Cluster Creation.

This operation is required to add a successor server to PRIMEFLEX.

You can maintain the compatibility of vMotion on all hosts in a cluster when you use the EVC (Enhanced vMotion Compatibility) function of VMware.

Note

- To set VMware EVC mode, you may need to stop virtual machines in the vSAN cluster even if the servers configuring the cluster are the same.

  If an ADVM in a PRIMEFLEX configuration must be stopped, set VMware EVC mode with a user that has administrator privileges and is not a domain user.

- Confirm the vCSA and ESXi version being used and whether the set CPU generations are supported by referring to the following URL.

  If the CPU generations are not supported, upgrade the version to a vCSA and ESXi version that supports the CPU generations in advance.

  https://kb.vmware.com/s/article/1003212

  https://kb.vmware.com/s/article/1005764

  Example: vCSA 6.5 or later and ESXi 6.5 or later is required for the PRIMERGY M2 series (Intel (R) "Broadwell" Generation).

Set VMware EVC according to the following procedure.

For vCSA 6.5 and earlier (Flash)

1. Log in to vCSA with vSphere Web Client.
2. From the "Top" screen, select the [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Configure] - [Configuration] - [VMware EVC] - [Edit the EVC configuration of the cluster].
3. On the screen to change the EVC mode, select the [Enable EVC for Intel(R) Hosts] checkbox in [Select EVC Mode], and select [VMware EVC Mode].

   Table 6.17 VMware EVC mode settings

Server with the oldest generation in your PRIMEFLEX environment	Setting Value
PRIMERGY M2 series	Intel (R) "Broadwell" Generation
PRIMERGY M4 series	Intel (R) "Skylake" Generation
PRIMERGY M5 series	Intel (R) "Cascade Lake" Generation

4. Select the [OK] button.

For vCSA 6.7 or later (HTML5)

1. Log in to vCSA with vSphere Client.

2. From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Configure] - [Configuration] - [VMware EVC] - [Edit the EVC configuration of the cluster].

3. On the screen to change the EVC mode, select the [Enable EVC for Intel(R) Hosts] checkbox in [Select EVC Mode], and select [VMware EVC Mode].

   Table 6.18 VMware EVC mode settings

Server with the oldest generation in your PRIMEFLEX environment	Setting Value
PRIMERGY M2 series	Intel (R) "Broadwell" Generation
PRIMERGY M4 series	Intel (R) "Skylake" Generation
PRIMERGY M5 series	Intel (R) "Cascade Lake" Generation

4. Select the [OK] button.

For vCSA 7.0U3 or later

1. Log in to vCSA with vSphere Client.

2. From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Configure] - [Configuration] - [VMware EVC] - [Edit the EVC configuration of the cluster].

3. On the screen to change the EVC mode, select the [Enable EVC for Intel(R) Hosts] checkbox, and select [CPU Mode].

   Table 6.19 VMware EVC mode settings

Server with the oldest generation in your PRIMEFLEX environment	Setting Value
PRIMERGY M2 series	Intel (R) "Broadwell" Generation
PRIMERGY M4 series	Intel (R) "Skylake" Generation
PRIMERGY M5 series	Intel (R) "Cascade Lake" Generation

4. Select the [OK] button.

6.8.2.2 Create ADVM certificates

This setting is required when configuring an ADVM dedicated to PRIMEFLEX HS/PRIMEFLEX for VMware vSAN when Cluster Creation or Cluster Expansion is used. Execute it only one time the first time. This is not required if you are using AD of your environment or will not use link with Active Directory.

Certificate registration is required because Cluster Creation or Cluster Expansion sets ADVM from ISM with SSL encrypted communication.

For ADVM#1 and ADVM#2, follow the following operations flow and register certificates for SSL communication and execute the settings to permit communication.

You can use Cluster Creation or Cluster Expansion without using SSL encrypted communication. In this case, this setting is not required. Proceed to "6.8.2.3 Register host records in DNS."

Note

- If using Cluster Creation or Cluster Expansion without using SSL encrypted communication, settings are specified using http communication, creating a risk that setting parameters are intercepted among other security risks. If you cannot accept this security risk, follow this procedure and register certificates.
- Enter the following items under the [Cluster Details] - [DNS Information] - [WinRM Service Port Number] of Cluster Definition Parameters depending on usage of SSL encryption communication.

Use of SSL encrypted communication	Setting contents	Description
Use SSL encrypted communication	- Set "HTTPS" to [Communication Method] - Enter the [Port Number]	Set the communication between ADVM and WinRM to SSL communication.
Do not use SSL encrypted communication	- Set "HTTP" to [Communication Method]. - Enter the [Port Number]	Set the communication between ADVM and WinRM not to use SSL communication.

For details on Cluster Definition Parameters, refer to "Chapter 3 Parameter List for Cluster Definition Parameters Settings" in "ISM for PRIMEFLEX Parameter List."

- If an error message is displayed and you cannot connect while using remote desktop connection, the cause may be one of the errors described at the following link. From the Hypervisor console screen, use a shared folder to transfer and apply the latest update program on the destination of remote desktop connection.

  https://support.microsoft.com/en-us/help/4093492/credssp-updates-for-cve-2018-0886-march-13-2018

- 6.8.2.2.1 Confirm WinRM service startup
- 6.8.2.2.2 Set up WinRM service
- 6.8.2.2.3 Open the port of the firewall
- 6.8.2.2.4 Change the Windows PowerShell script execution policy

6.8.2.2.1 Confirm WinRM service startup

From ADVM#1, open command prompt with administrator privilege and execute the following command to check the startup of the WinRM service.

```
>sc query winrm
```

Check the results below and check that STATE is RUNNING.

```
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

If WinRM service is not started, execute the following command to start the WinRM service.

```
>sc start winrm
```

Execute the command above for confirmation again to check that the "STATE" is "RUNNING."

Note

- Depending on the environment, the WinRM service may not start automatically. Set the WinRM service to automatic startup (auto) or to delayed automatic startup (delayed-auto).

  The following is an example of when setting up automatic startup.

  ```
  >sc config winrm start=auto
  ```

- Do the same startup checking for ADVM#2 to WinRM service, replacing ADVM#1 with ADVM#2 in the description.

6.8.2.2.2 Set up WinRM service

(1) WinRM service settings

Since Basic authentication is not permitted in the initial setup, you must set up "Basic authentication permission."

Basic authentication communication is encrypted by https communication.

From ADVM#1, open the command prompt with administrator privilege and execute the following command.

```
>winrm quickconfig
```

If "WinRM service is already running on this computer." is displayed, this means that setup is already completed. Proceed to "Basic authentication permission."

If "WinRM is not set up to permit remote access to this computer for administration purposes." is displayed, this means that the WinRM service is running, but remote access is not permitted, so enter "y."

```
WinRM is not set up to permit remote access to this computer for administration purposes.
You must change the following settings. Configure "LocalAccountTokenFilterPolicy" to give remote
administrator privilege to local users.
Do you want to change it [y/n]? y
```

The following message is displayed.

```
WinRM was updated for remote management.

LocalAccountTokenFilterPolicy was configured to give remote administrator privilege to local users
```

Execute the command above for confirmation again to check that the message "WinRM Service is already running on this computer" is displayed.

Basic authentication permission

Execute the following command in command prompt and check the settings of WinRM service.

```
> winrm get winrm/config
```

Check the following results. If [Config] - [Client] - [Auth] - [Basic] is false, proceed to the procedure below. If it is true the settings have already been completed, then proceed to "(2) https communication settings."

```
Config
    MaxEnvelopeSizekb = 150
    MaxTimeoutms = 60000
    MaxBatchItems = 20
    MaxProviderRequests = 25
    Client
        NetworkDelayms = 5000
        URLPrefix = wsman
        AllowUnencrypted = false
        Auth
            Basic = false
            Digest = true
            Kerberos = true
            Negotiate = true
            Certificate = true
        DefaultPorts
            HTTP = 80
            HTTPS = 443
(Below is omitted)
```

Execute the following command.

```
>winrm set winrm/config/service/Auth @{Basic="true"}
```

Execute the command above for confirmation again to check that [Config] - [Client] - [Auth] - [Basic] is "true."

(2) https communication settings

To use https communication you must set up a certification. Certificates can be created from the management terminal.

Preparations for required tools

There are two tools required for creating certificates.

- .NET Framework 4.5 (Download site)

  https://www.microsoft.com/en-us/download/details.aspx?id=30653

- Windows Software Development Kit (Download site)

  https://developer.microsoft.com/en-us/windows/downloads/windows-10-sdk

Note

- Install the above tool to the management terminal.
- Download the .NET Framework 4.5 in the URL above in the same language that is set for the management terminal used to create certificates.
- The Windows Software Development Kit works for Windows 8.1, Windows Server 2012 and later OS versions. Install the appropriate Windows Software Development Kit if installing other OSes.
- When using Windows 10 SDK on a platform other than Windows 10, Universal CRT must be installed (Refer to KB2999226 "https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows"). To avoid errors occurring during the setup, make sure to install the latest recommended update programs and patches from Microsoft Update before installing Windows SDK.

(3) Creating certificates

Use the tool to create certificates (makecert.exe) and the tool to create files to replace personal information (pvk2pfx.exe) to create the following three files from the management terminal:

- CER file (certificate)
- PVK file (private key file)
- PFX file (service certificate)

Create two certificates for ADVM#1 and ADVM#2.

(3-1) Creating certificate and private key file

Open the command prompt (administrator) on the management terminal and execute the following command.

```
>makecert.exe -r -pe -n "CN=<ADVM#1 server name>" -e <expiration date for the certificate (mm/dd/
yyyy)> -eku 1.3.6.1.5.5.7.3.1 -ss My -sr localMachine -sky exchange <ADVM#1 computer name>.cer -
sv <file name of the private key>.pvk
```

The following is a command example where the target ADVM#1 server name is "192.168.10.10," the certificate expiration date is March 30, 2018, the computer name for ADVM#1, and the file name of the private key are "ADVM1."

```
>makecert.exe -r -pe -n "CN=192.168.10.10" -e 03/30/2018 -eku 1.3.6.1.5.5.7.3.1 -ss My -sr
localMachine -sky exchange ADVM1.cer -sv ADVM1.pvk
```

As you will be required to enter the password to be set to the certificate twice in the process, enter it correctly. If an error occurs, perform the same process to execute the command above again.

Execute the following command to check the creation of <ADVM#1 computer name>.cer and <file name of the private key>.pvk.

```
>dir
```

(3-2) Creating service certificates

Open the command prompt (administrator) on the management terminal and execute the following command.

```
>pvk2pfx.exe -pvk <file name of the private key>.pvk -spc <ADVM#1 computer name>.cer -pfx
<ADVM#1 computer name>.pfx
```

The following is a command example when you set the file name of the private key and the ADVM#1 computer name to "ADVM1."

Execution example:

```
>pvk2pfx.exe -pvk ADVM1.pvk -spc ADVM1.cer -pfx ADVM1.pfx
```

You will be required to enter the password set in (3-1) during the process, then enter it accordingly.

Execute the following command to check the creation of <ADVM#1 computer name>.pfx.

```
>dir
```

(4) Registering certificates and service certificates

Upload the certificate and service certificate created by the management terminal to ADVM#1.

Start certificate snap-in and register the certificate created in (3).

1. Execute mmc.exe on ADVM#1.
2. Select [File] - [Add and Delete Snap-in].
3. From [Snap-in that can be used], select "Certificate" and select [Add].
4. Select "Computer Account," then select [Next], [Complete] in order.
5. Select [OK].

(5) Registering SSL certificate

Execute the following procedures from certificate snap-in on ADVM#1.

1. Register a route certificate device trusted by the <ADVM#1 computer name>.cer

   [Console Root] - [Certificate (local computer)] - right-click on [Trusted Root Certification Authorities]. From [All tasks] - [Import], select <ADVM#1 computer name>.cer and close the "Certificate Import Wizard" screen.

2. Check that <ADVM#1 computer name>.cer could be registered in [Trusted Root Certification Authorities].

   Select [Console Root] > [Certificate (local computer)] > [Trusted Root Certification Authorities] > [Certificates] in order and check that both [Issued to] and [Issued by] shows the server name specified in CN and that "Purpose" is set to "Server authentication." If not, execute Step 1 in (5) again.

3. Register <ADVM#1 computer name>.pfx as personal.

   [Console root] - [Certificate (local computer)] - right-click on [Personal]. From [All tasks] - [Import], select the <ADVM#1 computer name>.pfx file and close the "Certificate Import Wizard" screen. Though you will be requested to enter private key password during the process, enter nothing and select the [Next] button with the part blank.

   Note

   When selecting <ADVM#1 computer name>.pfx file, you must specify it from the pull-down box.

4. Check that the <ADVM#1 computer name>.pfx is registered as [Personal].

   Select [Console Root] - [Certificate (local computer)] - [Personal] - [Certificate] in order and check that both [Issued to] and [Issued by] shows the server name specified in CN and that "Purpose" is set to "Server authentication." If not, execute Step 3 in (5) again.

(6) Registering the thumb print in the WinRM service certificate

(6-1) Checking thumb print (Thumbprint)

The following is the procedure if the certificate is saved to LocalMachine\my.

1. Open PowerShell from the ADVM#1 command prompt.

2. Check thumb print. Execute the following command.

```
>ls cert:LocalMachine\my
```

It will be displayed as follows.

```
PS C:\Windows\system32> ls cert:LocalMachine\my

Directory: Microsoft.PowerShell.Security\Certificate::LocalMachine\my
Thumbprint                                Subject
----------                                -------
1C3E462623BAF91A5459171BD187163D23F10DD9  CN=192.168.10.10
```

(6-2) Registering the thumbprint in the WinRM listener certificate

Finish PowerShell and execute the following script. A space is required between 'HTTPS' and '@'.

```
>winrm create winrm/config/listener?Address=*+Transport=HTTPS @{Hostname="<CN name set when
creating certificate>";CertificateThumbprint="<Thumbprint of the created certificate>"}
```

(6-3) Registering check of WinRM listener

Execute the following command.

```
>winrm get winrm/config/listener?Address=*+Transport=HTTPS
```

If command results like the displayed below are returned, the WinRM listener is registered. If it does not return, redo it from "(6-2) Registering the thumbprint in the WinRM listener certificate."

```
Listener
    Address = *
    Transport = HTTPS
    Port = 5986
    Hostname = 192.168.10.10
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint = 1C3E462623BAF91A5459171BD187163D23F10DD9
    ListeningOn = 192.168.10.10, 127.0.0.1, ::1, 2001:258:8402:200:bd8a:1c1:c50d:8704,
fe80::5efe:192.168.10.10%13, fe80::bd8a:1c1:c50d:8704%12
```

Note

Execute the procedures of (1), (4) through (6) in "6.8.2.2.2 Set up WinRM service," replacing ADVM#1 to ADVM#2.

6.8.2.2.3 Open the port of the firewall

To enable the WinRM service to receive requests, you must open the port set in WinRM listener. The default port for https communication is 5986.

1. Open Windows PowerShell with administrator privilege from the ADVM#1.
2. Execute commands as is shown below.

```
>New-NetFirewallRule -DisplayName <Firewall rule name> -Action Allow -Direction Inbound -Enabled
True -Protocol TCP -LocalPort <Port number>
```

Example: Set "WinRM" as the name for a rule that opens port number 5986.

```
>New-NetFirewallRule -DisplayName WinRM -Action Allow -Direction Inbound -Enabled True -Protocol
TCP -LocalPort 5986
```

3. Execute the following command to check the firewall settings.

```
Show-NetFirewallRule | ?{$_.LocalPort -match <Port number>}
```

Example: Check the firewall settings for port number 5986.

```
Show-NetFirewallRule | ?{$_.LocalPort -match 5986}
```

If command results like the displayed below are returned, the firewall is opened.

```
$_ | Get-NetFirewallPortFilter
Protocol : TCP
LocalPort : 5986
RemotePort : Any
IcmpType : Any
DynamicTarget : Any

$_ | Get-NetFirewallPortFilter
Protocol : TCP
LocalPort : 5986
RemotePort : Any
IcmpType : Any
DynamicTarget : Any
```

Note

- The firewall settings differ depending on the environment (OS version and so on).
- Execute "6.8.2.2.3 Open the port of the firewall" to ADVM#2 as well, replacing ADVM#1 to ADVM#2.

6.8.2.2.4 Change the Windows PowerShell script execution policy

Open Windows PowerShell with administrator privilege from ADVM#1 and execute the following command to check the PowerShell script execution policy settings.

```
> get-executionpolicy
```

When you check the command results, if it is "RemoteSigned," the settings have been completed. Proceed to "6.8.2.3 Register host records in DNS" or "6.8.2.4 Set up DHCP."

If it is not "RemoteSigned," follow the procedure below.

1. Execute the following command.

   ```
   > set-executionpolicy remotesigned
   ```

2. If the following message is displayed, enter [Y] and click the [Enter] key.

   ```
   Updating the execution policy
   The execution policy is useful for preventing the execution of untrusted scripts. If you change
   the execution policy, as is explained in the about_Execution_Policies
   topic in (http://go.microsoft.com/fwlink/?LinkID=135170)
   you might be exposed to various security risks. Do you want to update the execution policy? [Y]
   Yes(Y) [N] No(N) [S] Stop(S) [?] Help (Default is "Y"): Y
   ```

3. Execute the command above for confirmation again to check that the result is "RemoteSigned."

Note

Execute "6.8.2.2.4 Change the Windows PowerShell script execution policy" to ADVM#2 as well, replacing ADVM#1 to ADVM#2.

6.8.2.3 Register host records in DNS

This section is required only when you use DNS servers already setup in your environment. Before executing Cluster Creation or Cluster Expansion, make sure that name resolution is possible for the OS of the target servers used for DNS forward lookup zones and reverse lookup zones.

Execute for all target servers.

Figure 6.6 Example for registration of forward lookup zones

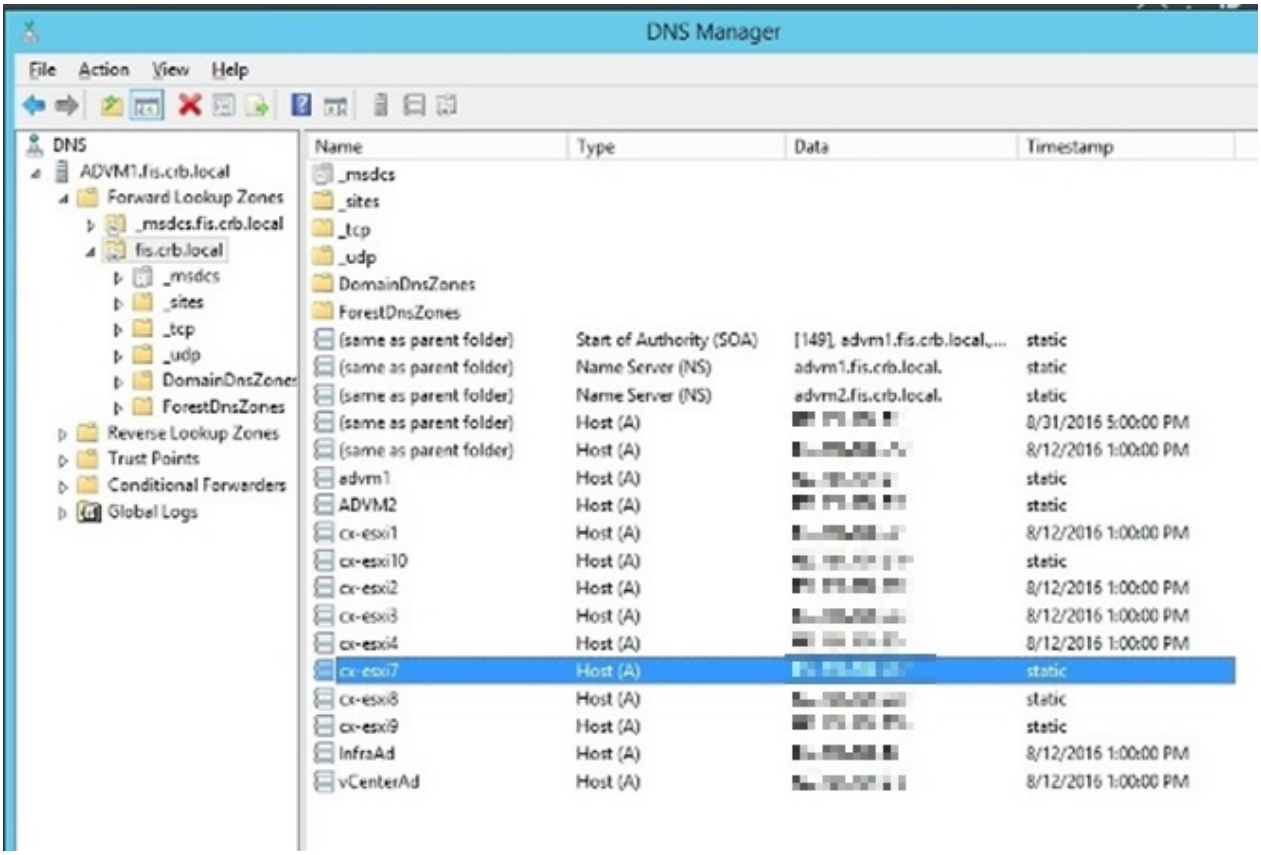
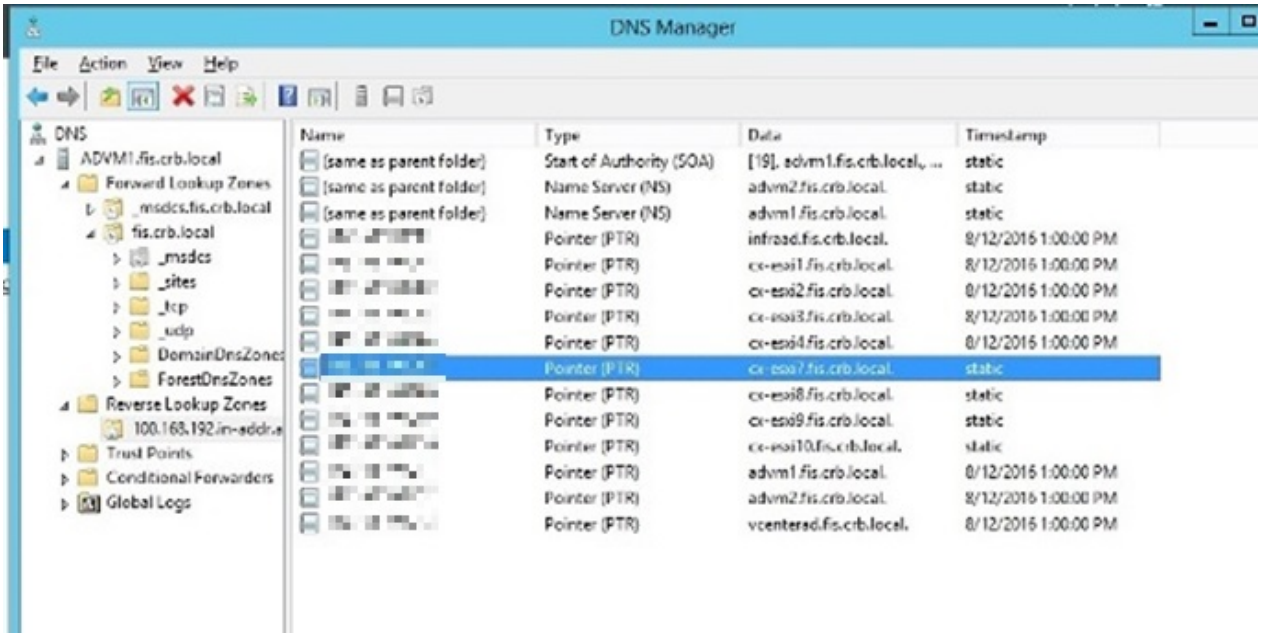


Figure 6.7 Example for registration of reverse lookup zones



6.8.2.4 Set up DHCP

For Cluster Creation or Cluster Expansion, execute OS installation by using profile assignment. To execute OS installation with profile assignment, a DHCP server is required.

Although ISM-VA has a DHCP server function internally, you can also prepare an external DHCP server for ISM-VA. If you are going to use an internal DHCP server, set it up with reference to "4.15 ISM-VA Internal DHCP Server" in "User's Guide."

Set it so that multiple leases are possible for all target servers.

Note

- Confirm that any DHCP services to be used are started.
- If you have multiple DHCP servers running within the same network, they may not always function properly. Stop any DHCP services that are not in use.
- Set lease periods so that they do not expire while any work is in progress.
- Since the management network is made redundant in the configuration of this product, IP addresses are leased to two ports. Make the settings so that there are always two IP addresses that can be leased for a node.
- Check whether the settings are for internal or external DHCP of ISM, and modify them according to the same DHCP that you are using. For information on the procedure to modify the settings, refer to "4.15.4 Switch of DHCP Servers" in "User's Guide."

6.8.2.5 Import ServerView Installation Manager provided with the ServerView Suite DVD, and the ISO image of the OS installation media to ISM-VA

Import ServerView Installation Manager (hereafter referred to as "SVIM") that is provided with ServerView Suite DVD, and the OS installation media into ISM.

- Import ServerView Installation Manager

  Import the applicable ServerView Installation Manager for the target server.

- Import OS installation media

  Import the same version of the OS installation media as VMware ESXi in the existing cluster.

For information on import operations, refer to "2.13.2 Repository Management" in "User's Guide."

For the support version, refer to "3.2 Profiles for VMware ESXi" in "Items for Profile Settings (for Profile Management)."

Add ISM-VA virtual disks if necessary. For information on the procedure to add virtual disks, refer to "3.7 Allocation of Virtual Disks" in "User's Guide."

Note

Import the following items for the OS installation media if using Cluster Expansion. If you import the incorrect item, Cluster Expansion ends with an error.

- If you do not apply the VMware ESXi patch, the build number of the same version as VMware ESXi in the existing cluster
- If you apply the VMware ESXi patch, the same version as VMware ESXi in the existing cluster

6.8.2.6 Delete scripts that are executed before

Use the following procedure to delete old VMware ESXi patches and scripts that were executed before and after the application of VMware ESXi patches when using Cluster Creation or Cluster Expansion.

(1) Delete old VMware ESXi patches

If you are using VMware ESXi patches that you uploaded to ISM-VA the last time you used Cluster Creation or Cluster Expansion, this procedure is not required.

1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. Delete any files that are no longer needed by checking the following items and referring to "1.4.2 Delete Files Uploaded to ISM-VA."

Item	Value
Root Directory	Administrator/ftp
Directory Name	Administrator/ftp/kickstart
File	Old VMware ESXi patch files

(2) Delete old scripts that were executed before and after the application of VMware ESXi patches

Execute for ISM-VA. If you are using scripts that are executed before and after the application of VMware ESXi patches that you uploaded to ISM-VA the last time you used Cluster Creation or Cluster Expansion, this procedure is not required.

1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. Delete any files that are no longer needed by checking the following items and referring to "1.4.2 Delete Files Uploaded to ISM-VA."

Item	Value
Root Directory	Administrator/ftp
Directory Name	Administrator/ftp/ClusterOperation/ESXi/script
File	Old scripts that are executed before and after the application of VMware ESXi patches

6.8.2.7 Upload the VMware ESXi patch file

Execute this when you want to apply the VMware ESXi patch by using Cluster Creation or Cluster Expansion. When you upload the VMware ESXi patch file, the patch application process will be executed.

Execute the operations depending on your environment so that the build number of the version of VMware ESXi of the new cluster is the same version as that of the existing cluster when using Cluster Expansion.

Add ISM-VA virtual disks if necessary. For information on the procedure to add virtual disks, refer to "3.7 Allocation of Virtual Disks" in "User's Guide."

Note

- There should be only one VMware ESXi patch file. If you upload multiple files, Cluster Creation or Cluster Expansion ends with an error.
- Do not decompress the uploaded VMware ESXi patch file (zip file). If you decompress the file, Cluster Creation or Cluster Expansion ends with an error.

Upload the VMware ESXi patch file, checking the following items and referring to "1.4.1 Upload Files to ISM-VA."

Item	Value
Root Directory	Administrator/ftp
File Type	File for cluster management
Upload Target Path	Administrator/ftp/kickstart
File	VMware ESXi patch file [Note] Example: ESXi650-201704001.zip

[Note]: Upload the VMware ESXi patch file without renaming it.

6.8.2.8 Creating scripts to execute before and after a VMware ESXi patch application

There may be some restrictions or precautions for a VMware ESXi patch file. For details, contact your local Fujitsu customer service partner. By creating a script, the countermeasures for precautions can be taken while Cluster Creation or Cluster Expansion is executing.

You can execute a script at the following timing.

- Before the VMware ESXi patch application
- At the VMware ESXi patch application
- After the VMware ESXi patch application

Note

- "At the VMware ESXi patch application" means immediately after executing the command and before restarting ESXi.

  After the VMware ESXi patch application means after both executing the command and ESXi has been restarted.

- Cluster Creation or Cluster Expansion will fail if the script does not finish within the specified time (720 seconds). If an error is displayed on the ISM "Tasks" screen, check the ISM event log. Confirm the message by referring to "ISM for PRIMEFLEX Messages" and take action.

Each script name is fixed. The script names differ depending on when they are executed.

Script name [Note]	When to be executed
pre_script.sh	To be executed before the VMware ESXi patch application
post01_script.sh	To be executed at the VMware ESXi patch application
post02_script.sh	To be executed after the VMware ESXi patch application

[Note]: Only shell (bash) format is supported for scripts.

Point

- You can detect errors by using "exit 1" to terminate the script.
- To be able to check the execution results of the script in the follow-up processing, add the process for outputting the log into a file in the script on ESXi.
- If the Cluster Creation or Cluster Expansion task ends with an error, you must execute Cluster Creation or Cluster Expansion again. Create a script so that the task does not end with an error even if you execute it again. The following samples are created so that the task does not end in an error even if the script is executed again.

Refer to the following samples to create scripts.

Example for creating a script to execute before the VMware ESXi patch application

The example script is for the following processes required to apply the ESXi patch:

- Removing tools
- Removing drivers
- Changing the driver settings

```
#!/usr/bin/sh

### Tool removal ###
echo "Tool removal Start" >> /scratch/log/pre_script.log
toolName=`(esxcli software vib list | grep storcli)`
if [ $? = 0 ]; then
    echo ${toolName} >> /scratch/log/pre_script.log
```

```
    toolName=`(echo ${toolName} | cut -f 1 -d ' ')`
    cmd="esxcli software vib remove -n ${toolName}"
    echo ${cmd} >> /scratch/log/pre_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
echo "Tool removal End" >> /scratch/log/pre_script.log

### Driver removal ###
echo "Driver removal Start" >> /scratch/log/pre_script.log
driver1=`(esxcli software vib list | grep "OEM.500")`
if [ $? = 0 ]; then
    echo ${driver1} >> /scratch/log/pre_script.log
    driver1Name=`(echo ${driver1} | cut -f 1 -d ' ')`
    cmd="esxcli software vib remove -n \"${driverName1}\""
    echo ${cmd} >> /scratch/log/pre_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
echo "Driver removal End" >> /scratch/log/pre_script.log

### Driver settings ###
echo "Driver settings Start" >> /scratch/log/pre_script.log
driver2=`(esxcli system module list | grep lsi_mr3)`
if [ $? = 0 ]; then
    echo ${driver2} >> /scratch/log/pre_script.log
    cmd="esxcli system module set -e true -m lsi_mr3"
    echo ${cmd} >> /scratch/log/pre_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
driver3=`(esxcli system module list | grep lsi_msgpt3)`
if [ $? = 0 ]; then
    echo ${driver3} >> /scratch/log/pre_script.log
    cmd="esxcli system module set -e true -m lsi_msgpt3"
    echo ${cmd} >> /scratch/log/pre_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
echo "Driver settings End" >> /scratch/log/pre_script.log

echo "pre_script End" >> /scratch/log/pre_script.log
exit 0
```

Example for creating a script to execute at the VMware ESXi patch application

The example script is for executing the countermeasures for the precautions for operation and maintenance for ESXi 6.7:

- Script for replacing an Inbox driver when applying the patch "ESXi670-201905001" or later to the ESXi structured with a custom image of v470-1

```
#!/usr/bin/sh

#### parameter settings ####
EffectiveValue='VMware-ESXi-6.7.0-13473784-Fujitsu-v470-1-offline_bundle.zip -n lsi-mr3 -n lsi-
msgpt3'
```

```
### Execution command ###
cmd="esxcli software vib install --dry-run -d /var/tmp/SvrExpScriptDir/${EffectiveValue}"
echo ${cmd} >> /scratch/log/post01_script.log
eval ${cmd}
if [ $? != 0 ]; then
    exit 1
fi

cmd="esxcli software vib install -d /var/tmp/SvrExpScriptDir/${EffectiveValue}"
echo ${cmd} >> /scratch/log/post01_script.log
eval ${cmd}
if [ $? != 0 ]; then
    exit 1
fi

echo "post01_script End" >> /scratch/log/post01_script.log
exit 0
```

Example for creating a script to execute after the VMware ESXi patch application

The example script is for executing the following countermeasures for restrictions and precautions after the ESXi patch is applied:

- Restricting power management settings
- Updating an igbn driver
- Setting a temporary area

```
#!/usr/bin/sh

#### parameter settings ####
PowerValue="High Performance"
DriverFile="<driver file name to apply>"
TemporaryName="scratch"
### Execution command ###
# Power Policy
echo "Power Policy Start" >> /scratch/log/post02_script.log
CurrentValue=`esxcli system settings advanced list --option=/Power/CpuPolicy | grep '   String
Value: High Performance'`
if [ $? != 0 ]; then
    cmd='esxcli system settings advanced set --option=/Power/CpuPolicy --string-value="High
Performance"'
    echo ${cmd} >> /scratch/log/post02_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
echo "Power Policy End" >> /scratch/log/post02_script.log

# Update Driver
echo "Update Driver Start" >> /scratch/log/post02_script.log
cmd="esxcli software vib install -d /var/tmp/SvrExpScriptDir/${DriverFile}"
echo ${cmd} >> /scratch/log/post02_script.log
eval ${cmd}
if [ $? != 0 ]; then
    exit 1
fi
echo "Update Driver End" >> /scratch/log/post02_script.log

# Temporary
echo "Temporary Start" >> /scratch/log/post02_script.log
TmpSetting=`(vim-cmd hostsvc/advopt/view ScratchConfig.ConfiguredScratchLocation | grep
"value")`
```

```
TmpDir=`(echo ${TmpSetting} | cut -f 2 -d '"')`
if [ ${#TmpDir} = 0 ]; then
    cmd="mkdir /var/tmp/${TemporaryName}"
    echo ${cmd} >> /scratch/log/post02_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
    cmd="vim-cmd hostsvc/advopt/update ScratchConfig.ConfiguredScratchLocation string /var/tmp/
${TemporaryName}"
    echo ${cmd} >> /scratch/log/post02_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
echo "Temporary End" >> /scratch/log/post02_script.log

echo "post02_script End" >> /scratch/log/post02_script.log
exit 0
```

Point

The first line of the script must contain the following.

```
#!/usr/bin/sh
```

Note

Do not include an instruction to restart the target node in the script. A reboot always occurs after a script is executed.

Upload script files by checking the following items and referring to "1.4.1 Upload Files to ISM-VA."

To upload a script and directory

Table 6.20 A script to be uploaded and the directory

Item	Value
Root Directory	Administrator/ftp
File Type	Other
Upload Target Path	Administrator/ftp/ClusterOperation/ESXi/script
File	- To upload a script that is to be executed before the VMware ESXi patch application pre_script.sh - To upload a script that is to be executed at the VMware ESXi patch application post01_script.sh - To upload a script that is to be executed after the VMware ESXi patch application post02_script.sh

Point

Upload an offline bundle that is used in the post script to ISM-VA according to the procedure in "6.8.2.7 Upload the VMware ESXi patch file." If you have any files other than the offline bundle to upload, upload the files by checking the following items and referring to "1.4.1 Upload Files to ISM-VA."

Item	Value
Root Directory	Administrator/ftp
File Type	Other
Upload Target Path	Administrator/ftp/ClusterOperation/ESXi/other
File	Other files

6.8.2.9 Upload VMware SMIS provider

This is a required operation when the target servers are PRIMERGY M4 series or VMware ESXi 6.5.

When you upload VMware SMIS Provider, the application processing will be executed.

For the VMware SMIS Provider file upload, use the offline bundle in the decompressed files of the downloaded compressed file (zip file).

- Example of the compressed file downloaded (zip file):

  VMware_MR_SAS_Providers-00.63.V0.05.zip

- Example of the offline bundle:

  VMW-ESX-5.5.0-lsiprovider-500.04.V0.63-0005-offline_bundle-5240997.zip

Add ISM-VA virtual disks if necessary. For information on the procedure to add virtual disks, refer to "3.7 Allocation of Virtual Disks" in "User's Guide."

Note

- VMware SMIS Provider offline bundle should be only one. If you upload multiple files, Cluster Creation or Cluster Expansion ends with an error.
- Do not decompress the uploaded offline bundle (zip file) of the VMware SMIS Provider. If you decompress the file, Cluster Creation or Cluster Expansion ends with an error.

Upload the offline bundle of the VMware SMIS Provider, checking the following items and referring to "1.4.1 Upload Files to ISM-VA."

Item	Value
Root Directory	Administrator/ftp
File Type	File for cluster management
Upload Target Path	Administrator/ftp/kickstart
File	Offline bundle of the VMware SMIS Provider [Note] Example: VMW-ESX-5.5.0-lsiprovider-500.04.V0.63-0005-offline_bundle-5240997.zip

[Note]: Upload the Offline bundle file name of the VMware SMIS Provider without renaming it.

6.8.2.10 Create a profile

Use ISM Profile Management to create the profiles for target servers.

To create a profile, refer to "3.3 Execute Settings on a Server/Install Server OS."

For the detailed profile setting values, refer to "Chapter 4 Parameter List for Profile Settings" in "ISM for PRIMEFLEX Parameter List."

- When using Cluster Creation

  If the target server is the same as the server in the existing cluster environment, copy and create from the existing profile.
  If the target server is different from the server in the existing cluster environment, create a new profile.

- When using Cluster Expansion

  - If the target server is the same as the server in the existing cluster environment, create and copy from the existing profile.
    If you add a successor server, create a new profile.

  - If the target server is the same as the server in the existing cluster environment, create and copy from the existing profile or policy, and assign a profile again. For this operation refer to "Procedures to change [Verify Status] back to [Match] if it is [Mismatch] (For items in which the node setting changes were intended)" in "3.3.5 Compare Assigned Profiles and Hardware Settings."

  - If you are updating ESXi in the existing cluster environment, create the OS policy that specifies the version of the install media you plan to deploy, and then create a new profile.
    For the creation procedure, refer to "3.3 Execute Settings on a Server/Install Server OS."

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
2. To create a new profile, from the [Actions] button, select [Add Profile].
   To copy and create a profile, select the duplication source from existing profile, and select [Duplicate Profile] from the [Actions] button.
3. Set each item.

Point

Refer to "2.4.3 OS Installation Settings" in "User's Guide" to perform the preparation tasks required when installing an OS.

Note

- Do not check the following items:
  - In the [OS] tab, [Network] - [Setup]

    This item is not required to be set because the VM standard network is not used.

  - In the [OS] tab, [Register to Cloud Management Software]

    This item is not required to be set because existing cloud management software is used.

  - In the [OS (for each node)] tab, [DHCP]

    This item is not required to be set because the fixed IP address is used for the management LAN.

- There is no problem if the following item is selected.

  This is because it is automatically set by Cluster Creation and Cluster Expansion.

  - In the [OS] tab, [Execute Script after Installation]

    If this item is set in the OS policy, make sure that the following settings are configured. If the values are different, Cluster Creation and Cluster Expansion will end in an error.

    - In the [OS] tab, [Execute Script after Installation]: Enabled
    - In the [OS] tab, [The directory of Script]: kickstart
    - In the [OS] tab, [Script to Execute]: ESXi_Setting.sh

- Set the following items so that they do not overlap:
  - In the [OS (for each node)] tab, [IP Address]
  - In the [OS (for each node)] tab, [Network] - [DHCP] - [Get Computer Name from DNS Server] - [Computer Name]

- Set the following in the [OS] tab - [Management LAN network port settings] items. This item must be set because there are multiple onboard LANs and the network port that is used for the management LAN must be specified.
  - Check [Network port specification]
  - For [Method to specify], select [MAC Address].
  - For [MAC Address], specify the MAC address of a port with 10 Gbps or higher communication available

    For the PRIMERGY M6 series/PRIMERGY M7 series (ISM 2.8.0.040 or later), specify the MAC address of the port on the PCI card.
- For PRIMERGY M2 series, do not check the following items. This item is not required to be set because there is only one onboard LAN and the port for the management LAN is not required to be set.
  - In the [OS] tab, [Network port specification]
- Specify the items that were imported in "6.8.2.5 Import ServerView Installation Manager provided with the ServerView Suite DVD, and the ISO image of the OS installation media to ISM-VA" for the following items when using Cluster Expansion. If you specify different items, Cluster Expansion ends with an error.
  - In the [OS] tab, [Installation Image] - [Type of Installation Media]
- For the latest information on products supported by Cluster Creation or Cluster Expansion, refer to "Support Matrix."

  https://support.ts.fujitsu.com/index.asp

  Select [Select a new Product] on the above site and enter "Infrastructure Manager" in [Product Search:].

  Select [DOWNLOADS] and select the target operating system.

  The reference procedures are subject to change without notice.

6.8.2.11 Create and edit Cluster Definition Parameters

This operation is required to use Cluster Expansion. This is not required to use Cluster Creation.

Use the ISM GUI to create and edit Cluster Definition Parameters as required.

Create Cluster Definition Parameters for the cluster to be expanded. If there are multiple clusters to expand, create the parameters for all the clusters. You do not need to create Cluster Definition Parameters for the servers for expanding a cluster. Set these when executing Cluster Expansion.

If Cluster Definition Parameters are already created, check the contents. If the contents require modifications, edit them.

From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster] - [<Target Cluster>] - [Cluster Definition Parameters] tab.

- To create a new parameter

  From the [Parameter Actions] button, select [Create].
- To edit a current parameter

  From the [Parameter Actions] button, select [Edit].

Point

- For the operation of creating and editing Cluster Definition Parameters, refer to the online help.
- For details on Cluster Definition Parameters, refer to "Chapter 3 Parameter List for Cluster Definition Parameters Settings" in "ISM for PRIMEFLEX Parameter List."
- Edit the Cluster Definition Parameters if there are setting items for which Cluster Definition Parameters are not set after the ISM upgrade. In addition, some items in ISM GUI are input automatically. Check if the setting values are correct.

Note

- If Cluster Definition Parameters are already created, you must change them. Edit Cluster Definition Parameters. Manual setting is recommended for adding disks to storage rather than using VMware. Also, deduplication and compression are valid settings when the storage configuration is All-Flash.

Setting item	Current setting value	New setting value
Cluster Details - the [Function] tab - [vSAN Settings] - [Add Disks to Storage]	Automatic	Manual
Cluster Details - [Function] tab - [vSAN Settings] - [Deduplication and Compression] [Note]	Enable	Disable

[Note]: Change this setting item when the storage configuration is Hybrid. If the storage configuration is All-Flash, you do not need to change the setting.

If you change the Cluster Definition Parameters, change the settings for the target cluster with the following procedure.

You can change the settings for both disk addition to the storage, and deduplication and compression at the same time.

- Setting procedure for the target cluster when changing the setting for disk addition to storage from "Automatic" to "Manual"

  For vCSA 6.5 and earlier (Flash)

  1. Log in to vCSA with vSphere Web Client.
  2. From the "Top" screen, select the [Home] tab - [Inventories] - [Hosts and Clusters], and then select [<Cluster name>] - [Configure] - [vSAN] - [General] - [vSAN is Turned ON] - [Edit].

     The "Edit vSAN settings" screen is displayed.
  3. Set [Add disks to storage] to "Manual," and then select the [OK] button.

  For vCSA 6.7 or later (HTML5)

  1. Log in to vCSA with vSphere Client.
  2. From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters], and then select [<Cluster name>] - [Configure] - [vSAN] - [Services] - [Deduplication and compression] - [Edit].

     The " vSAN Services" screen is displayed.
  3. Set [Add disks to storage] to "Manual," and then select the [APPLY] button.

- Setting procedure for the target cluster when changing the setting for deduplication and compression from "Enabled" to "Disabled"

  For vCSA 6.5 and earlier (Flash)

  1. Log in to vCSA with vSphere Web Client.
  2. From the "Top" screen, select [Home] tab - [Inventories] - [Hosts and Clusters], and then select [<Cluster name>] - [Configure] - [vSAN] - [General] - [vSAN is Turned ON] - [Edit].

     The "Edit vSAN settings" screen is displayed.
  3. Set [Service] - [Deduplication and compression] to "Disabled," and then select the [OK] button.

  For vCSA 6.7 to vCSA 7.0 U1 (HTML5)

  1. Log in to vCSA with vSphere Client.
  2. From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters], and then select [<Cluster name>] - [Configure] - [vSAN] - [Services] - [Deduplication and compression] - [Edit].

     The "vSAN Services" screen is displayed.
  3. Set [Service] - [Deduplication and compression] to "Disabled," and then select the [APPLY] button.

  For vCSA 7.0 U2 or later

  1. Log in to vCSA with vSphere Client.

2. From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters], and then select [<Cluster name>] - [Configure] - [vSAN] - [Services] - [Data Services] - [Edit].

   The "vSAN Services" screen is displayed.

3. Set [Space efficiency] to "None," and then select the [Apply] button.

- If Rolling Update is being executed or has ended with an error, do not create or edit Cluster Definition Parameters. Creating and editing Cluster Definition Parameters will fail.

6.8.2.12 Confirm installed storage devices

Confirm the storage devices installed on the target server. Verify that your storage device meets the operation requirements for your storage configuration.

- For PRIMEFLEX HS:
  - The conditions that should be met for the storage configuration you are using

Storage configuration	Configuration for each disk group	
	Type	Number of disks
Hybrid	Cache device: SSD	1
	Capacity device: HDD	Up to 7
All Flash	Cache device: SSD	1
	Capacity device: SSD [Note]	Up to 7

[Note]: Disk space must not be 160 - 210 GB or 320 - 420 GB

  - The maximum number of disk groups is as follows:

Type	Maximum number of disk groups
PRIMERGY RX2530 M2	2
PRIMERGY RX2540 M2	4
PRIMERGY CX2550 M2	1

- For PRIMEFLEX for VMware vSAN:
  - The conditions that should be met for the storage configuration you are using

Storage configuration	Configuration for each disk group		Configuration for each SAS controller card
	Type	Number of disks	
Hybrid	Cache device: SSD	1	Must have at least one SSD, and the number of HDDs must be at least the number of SSDs
	Capacity device: HDD	Up to 7	
All Flash	Cache device: SSD	1	The two types of SSD (for cache and capacity) have two or one type of disk capacity - For two types of disk space Cache devices must be the lesser of the two types of SSDs (when the number of SSDs is the same, the smaller the disk capacity) - For a single type of disk space Cache device must have one SSD for cache
	Capacity device: SSD	Up to 7	

  - No more than five cache devices

- The maximum number of disk groups is as follows

Type	Maximum number of disk groups
PRIMERGY RX2530 M4	3
PRIMERGY RX2540 M4	5
PRIMERGY CX2560 M4	2
PRIMERGY RX2530 M5	3
PRIMERGY RX2540 M5	5
PRIMERGY CX2560 M5	2
PRIMERGY RX4770 M5	4
PRIMERGY RX2530 M6	4
PRIMERGY RX2540 M6	5
PRIMERGY RX2530 M7 (ISM 2.8.0.040 or later)	5
PRIMERGY RX2540 M7 (ISM 2.8.0.040 or later)	5

6.8.2.13 Execute installation and wiring

Install a target server at its physical location and connect the cables. For details, refer to the "Operating Manual" of the target server. Execute the settings for your network switches as appropriate, referring to the manual for the switches.

Point

Only one ISM network interface can be defined. If creating a new cluster in a network other than the current one, set the router and set it so that communication is possible between each network. For the network configuration, refer to "1.2 Configuration" in "User's Guide."

Execute for all target servers.

The order of the operations differs depending on the node discovery method at the node registration in the ISM.

- For Manual Discovery of nodes

  Execute the operations in the following procedures.

  1. "6.8.2.14 Set the IP address of iRMC."
  2. "6.8.2.15 Set up BIOS"
  3. "Node registration using Manual Discovery" in "6.8.2.17 Register a node to ISM"
  4. "6.8.3 Execute Cluster Creation or Cluster Expansion"

- For Auto Discovery of nodes

  Execute the operations in the following procedures.

  1. "Node registration using Auto Discovery" in "6.8.2.17 Register a node to ISM"
  2. "6.8.2.15 Set up BIOS"
  3. "6.8.3 Execute Cluster Creation or Cluster Expansion"

6.8.2.14 Set the IP address of iRMC

When you register a target server by using Manual Discovery, set a static IP address for the iRMC.

Boot the BIOS of the target server, and on the "BIOS setup" screen, set a static IP address. To execute this operation, you must execute "6.8.2.13 Execute installation and wiring." Moreover, to display and operate the "BIOS setup" screen, connect a display and keyboard to the target server.

For information on booting the BIOS and setting the IP address for the iRMC, refer to the "BIOS Setup Utility Reference Manual" for the target server.

Set for all target servers.

Also, execute "6.8.2.15 Set up BIOS" as well as setting of the IP address.

You can obtain the "BIOS Setup Utility Reference Manual" for each target server from the following website:

https://support.ts.fujitsu.com/

On the site above, select "Select a new Product" - [Browse For Product] and select product line: [Fujitsu Server PRIMERGY] - product group: [<Target server group>] - product family: [<Target server>].
Download from [Systemboard].

Reference procedures are subject to change without notice.

6.8.2.15 Set up BIOS

This section describes the BIOS setup procedure.

For Manual Discovery when registering nodes in ISM, set this item together with "6.8.2.14 Set the IP address of iRMC."

For Auto Discovery when registering nodes in ISM, you can set BIOS settings remotely with iRMC Video Redirection.

1. Refer to steps 1 and 2 in "6.8.2.16 Confirm networks" to display the iRMC screen of the target server. Log in and select Video Redirection.

   The Video Redirection screen (server screen) is displayed.

   Point

   When the Video Redirection screen (server screen) is not displayed:

   After logging in to iRMC, check the [Settings] tab - Advanced Video Redirection (AVR)] - [KVM Redirection Type], and confirm that "HTML5 Viewer" is set. If "JViewer (JAVA)" is set, select "HTML5 Viewer", and select the [Apply] button. And then select Video Redirection again.

2. From the video redirection menu, select [Power] - [Power On Server] or [Power Cycle].

   Select [Yes] for the confirmation dialog.
   Select [OK] for the normal execution dialog.

3. Press the [F2] key during boot to start the BIOS. And set the following on the "BIOS setup" screen.

Execute this for all target servers.

Table 6.21 BIOS settings (PRIMERGY CX M4, CX M5 series)

Item		Setting Value
Management - iRMC LAN Parameters Configuration	iRMC IPv6 LAN Stack	Disabled
Configuration - CPU Configuration [Note]	Power Technology	Custom
	Enhanced Speedstep	Disabled
	Turbomode	Disabled
	Override OS Energy Performance	Enabled
	CPU C1E Support	Disabled
	CPU C6 Report	Disabled
	Package C State limit	C0

Item		Setting Value
Configuration - UEFI Network Stack Configuration [Note]	Network Stack	Enabled
	IPv6 PXE Support	Disabled

[Note]: If this is specified in the ISM profile setting values (in the [Details] - [BIOS] tab), no settings are required.

Table 6.22 BIOS settings (PRIMERGY RX M4, RX M5 series)

Item		Setting Value
Server Mgmt - iRMC LAN Parameters Configuration	iRMC IPv6 LAN Stack	Disabled
Advanced - CPU Configuration [Note]	Override OS Energy Performance	Enabled
	Energy Performance	Performance
	Package C State Limit	C0
Advanced - Network Stack Configuration [Note]	Network Stack	Enabled
	IPv6 PXE Support	Disabled

[Note]: If this is specified in the ISM profile setting values (in the [Details] - [BIOS] tab), no settings are required.

Table 6.23 BIOS settings (PRIMERGY RX M6 series)

Item		Setting Value
Management - iRMC LAN Parameters Configuration	iRMC IPv6 LAN Stack	Disabled
Configuration - CPU Configuration [Note]	Enhanced Speedstep	Disabled
	Turbomode	Disabled
	Energy Performance	Performance
	Override OS Energy Performance	Enabled
	CPU C1E Support	Disabled
	CPU C6 Report	Disabled
	Package C State limit	C0
Configuration - UEFI Network Stack Configuration [Note]	Network Stack	Enabled
	IPv6 PXE Support	Disabled

[Note]: If this is specified in the ISM profile setting values (in the [Details] - [BIOS] tab), no settings are required.

Table 6.24 BIOS settings (PRIMERGY RX M7 series) (ISM 2.8.0.040 or later)

Item		Setting Value
Management - iRMC LAN Parameters Configuration	iRMC IPv6 LAN Stack	Disabled
Configuration - CPU Configuration [Note]	Enhanced Speedstep	Enabled
	Turbomode	Enabled
	Energy Performance	Performance
	Override OS Energy Performance	Enabled
	CPU C1E Support	Enabled
	CPU C6 Report	Enabled
	Package C State limit	C0
Configuration - UEFI Network Stack Configuration [Note]	Network Stack	Enabled
	IPv6 PXE Support	Disabled

[Note]: If this is specified in the ISM profile setting values (in the [Details] - [BIOS] tab), no settings are required.

After completing the BIOS settings, in the "BIOS setup" screen - the [Save & Exit] tab, execute "Save Changes and Exit" or "Commit setting and Exit," then power off after several minutes.

For Manual Discovery when registering nodes in ISM, continue to execute "Node registration using Manual Discovery" in "6.8.2.17 Register a node to ISM."

For Auto Discovery when registering nodes in ISM, continue to execute "6.8.3 Execute Cluster Creation or Cluster Expansion."

6.8.2.16 Confirm networks

For all target servers, check that "Network" is displayed with iRMC Web Server.

For iRMC S4

1. In a web browser, enter the IP address of iRMC for each server.
2. Enter the username and password, and then select [Login] to log in.

   The default username and password are "admin".
3. Select [System Information] - [Network Inventory] in the left tree.

   If the network list is displayed in the "Ethernet Ports" area, the system is working appropriately.
4. If you could not confirm the network in Step 3, turn on the server to verify that the BIOS process is complete.
   Then turn off the power.
5. Check to see if the network is displayed again.
6. Execute the above procedures for iRMC on all servers.

For iRMC S5

1. In a web browser, enter the IP address of iRMC for each server.
2. Enter the username and password, and then select [Login] to log in.

   The default username and password are "admin".
3. Select the [System] tab and select "Network."

   Open "Ethernet Ports (displayed as "Network Adapter" in iRMC 2.20P or later)," from the "Network" in the right pane. If the network list is displayed, the system is working appropriately.
4. If you could not confirm the network in Step 3, turn on the server to verify that the BIOS process is complete.
   Then turn off the power.
5. Check to see if the network is displayed again.
6. Execute the above procedures for iRMC on all servers.

For iRMC S6 (ISM 2.8.0.040 or later)

1. In a web browser, enter the IP address of iRMC for each server.
2. Enter the username and password, and then select [Login] to log in.

   The default username and password are "admin" and "<changed password [Note]>."

   [Note]: The password that you were prompted to change from the factory default password (noted on the tag attached to device) when you logged in to iRMC for the first time.

3. Select the [System] tab and select "Network."

   Open "Ethernet Ports," from the "Network" in the right pane. If the network list is displayed, the system is working appropriately.

4. If you could not confirm the network in Step 3, turn on the server to verify that the BIOS process is complete.
   Then turn off the power.

5. Check to see if the network is displayed again.

6. Execute the above procedures for iRMC on all servers.

6.8.2.17 Register a node to ISM

In order to use ISM to install an OS, register the target server in ISM.

To register a node to ISM, you can use both Manual Discovery and Auto Discovery.

Register all target servers.

Point

- When you execute node registration in ISM, you must enter the iRMC usernames and passwords for the target servers. The default username and password are both set to "admin." For iRMC S6 (ISM 2.8.0.040 or later), the default username and password are "admin" and "<changed password [Note]>."

  [Note]: The password that you were prompted to change from the factory default password (noted on the tag attached to device) when you logged in to iRMC for the first time.

- When registering a node, select the node group that the node belongs to. You can edit the node group later. If you do not set the node group, the node becomes node group unassigned. Only the user of Administrator group can manage the node whose node group is not assigned.

- Register new datacenters, floors, and racks, and then execute the alarm settings for the target servers as required. For the setting procedure, refer to "Chapter 2 Configure the Required Settings When Installing ISM."

Node registration using Manual Discovery

For the procedure for registering a node with Manual Discovery, refer to "3.1.2 Register a Node Directly."

Set the static IP address of the iRMC in the "Node Manual Registration" wizard.

Specify the IP address set in "6.8.2.14 Set the IP address of iRMC" when registering.

Continue to execute "6.8.3 Execute Cluster Creation or Cluster Expansion."

Node registration using Auto Discovery

For the procedure for registering a node with Auto Discovery, refer to "3.1.1 Discover Nodes in the Network and Register Nodes."

By specifying the range of the IP addresses, all target servers can be registered simultaneously.

Continue to execute "6.8.2.15 Set up BIOS."

6.8.3 Execute Cluster Creation or Cluster Expansion

You can execute Cluster Creation or Cluster Expansion to increase the resources for PRIMEFLEX HS/PRIMEFLEX for VMware vSAN.

Be sure to refer to "6.8.1 Operation Requirements" and check the operation requirements before executing Cluster Creation or Cluster Expansion.

- 6.8.3.1 Cluster Creation procedure
- 6.8.3.2 Cluster Expansion procedure

6.8.3.1 Cluster Creation procedure

This section describes the procedure for executing Cluster Creation of ISM for PRIMEFLEX.

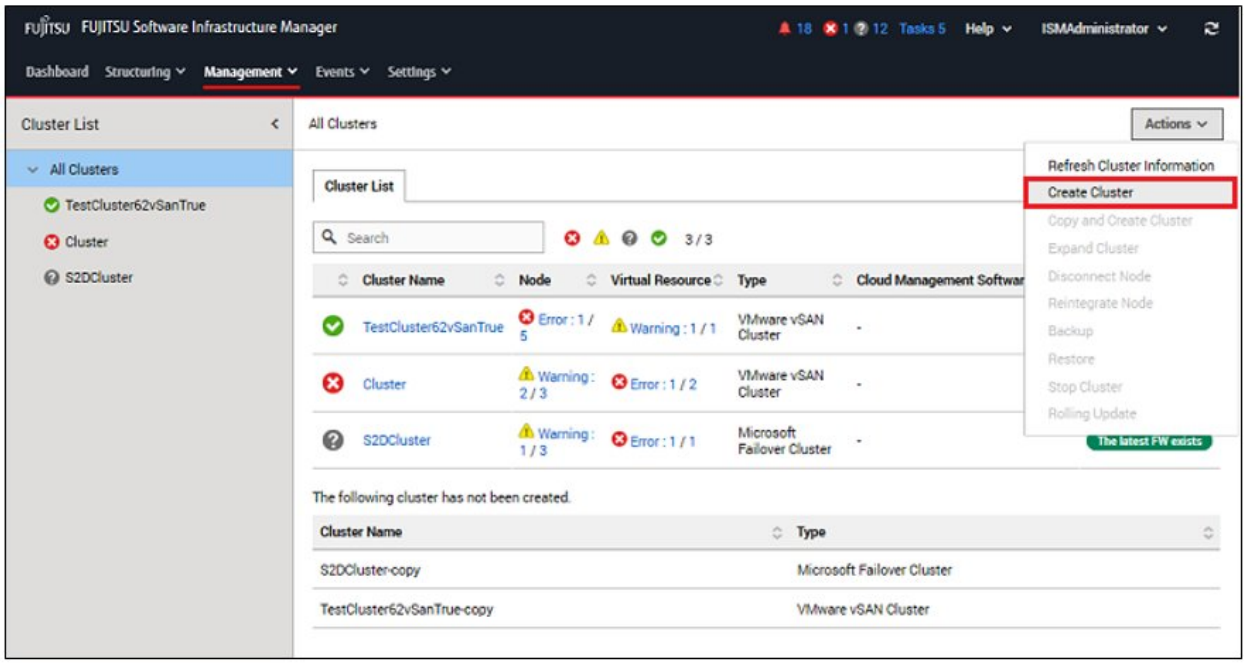
Note

Do not execute Cluster Creation while other ISM for PRIMEFLEX functions are being executed. Cluster Creation will fail. Check the ISM event log. Confirm the message by referring to "ISM for PRIMEFLEX Messages" and take action.

For ISM for PRIMEFLEX functions, refer to "2.12 Functions of ISM for PRIMEFLEX" in "User's Guide."

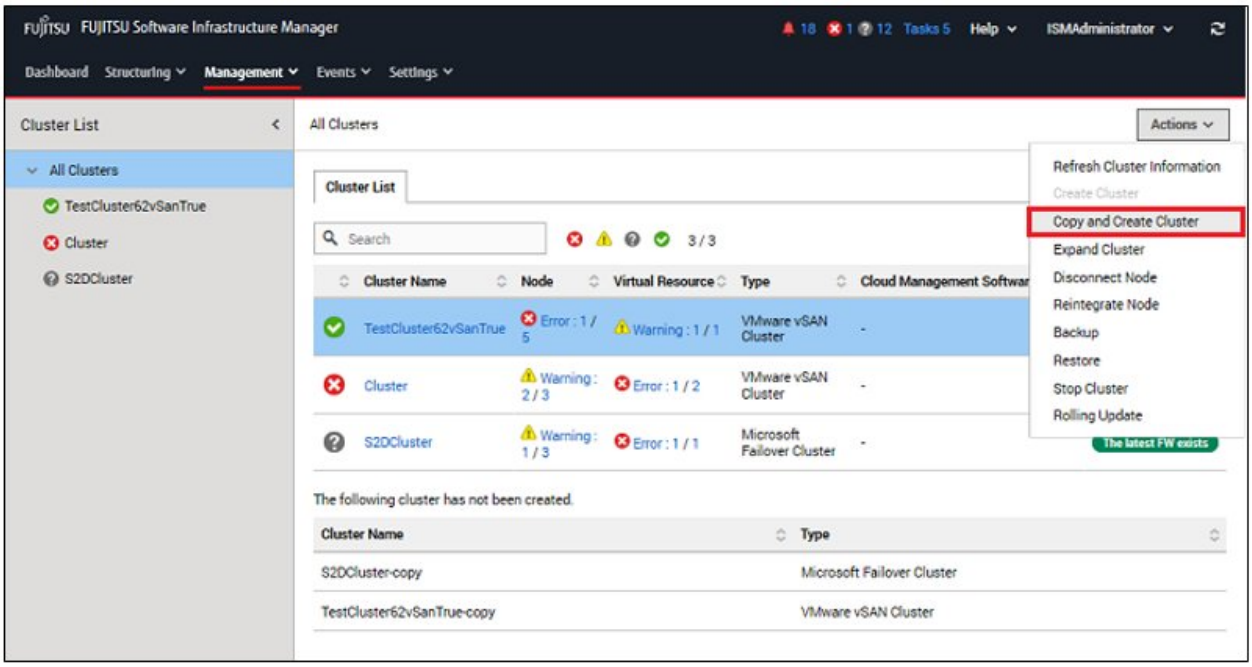
1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster].

   The "Cluster List" screen is displayed.
3. From the [Actions] button, select [Create Cluster].



The "Create Cluster" wizard is displayed.

If you create a cluster by referring the existing cluster, select the existing cluster, then from the [Actions] button, select [Copy and Create Cluster].

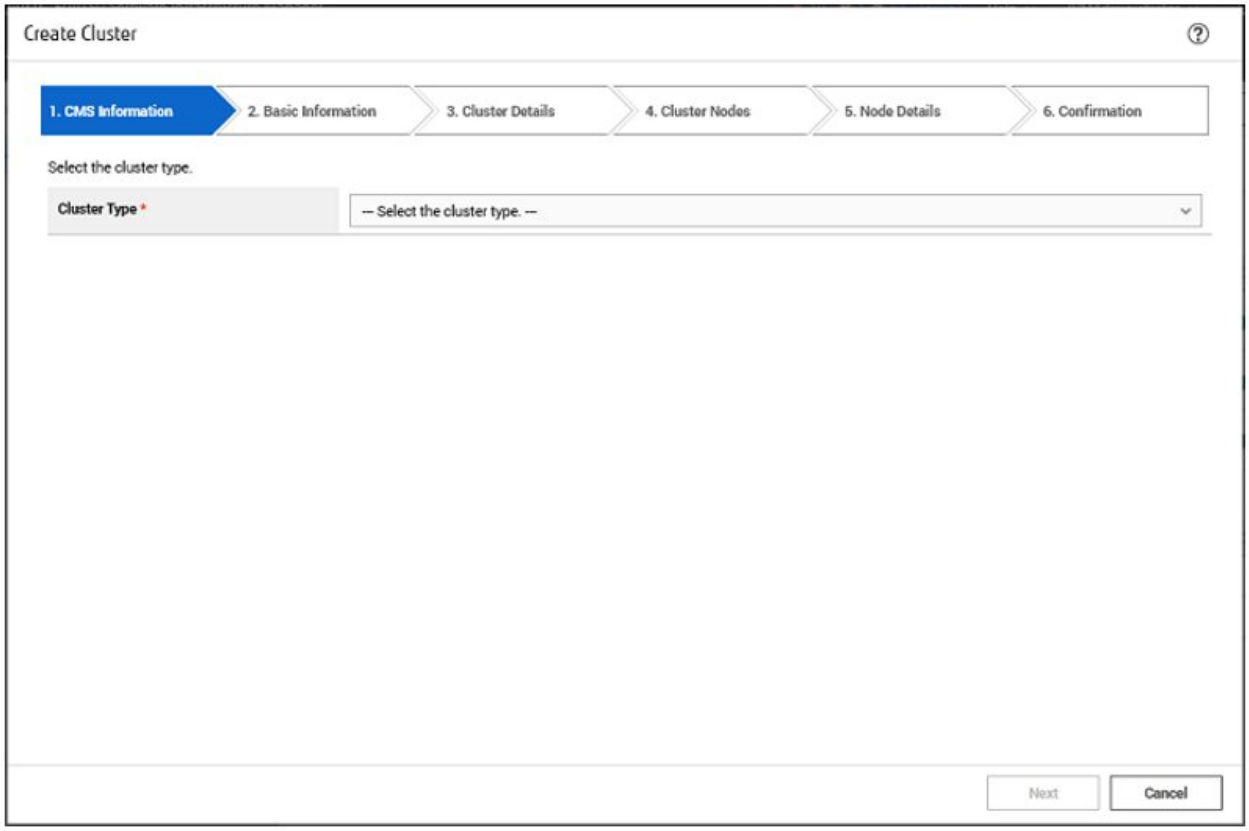


Note

For details on Cluster Definition Parameters, refer to "Chapter 3 Parameter List for Cluster Definition Parameters Settings" in "ISM for PRIMEFLEX Parameter List."

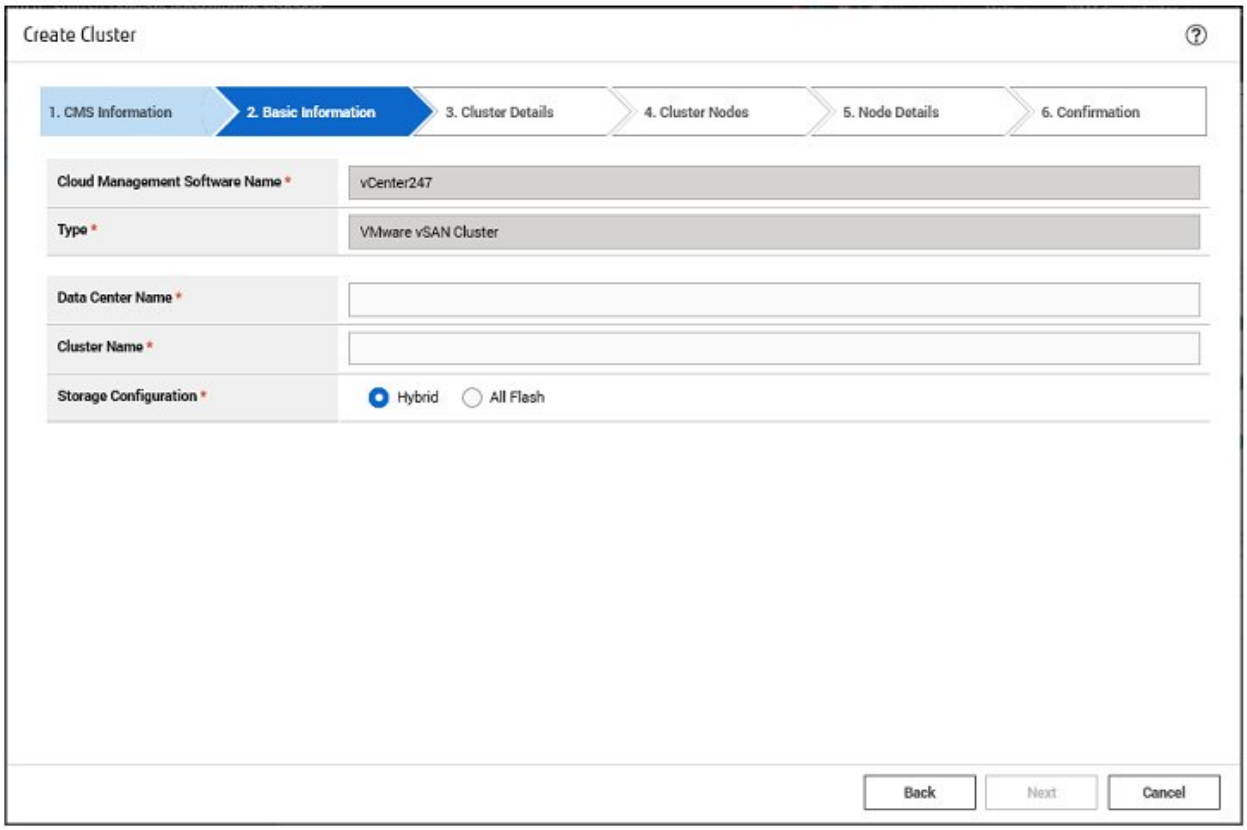
4. Enter each parameter on the "1. CMS Information" screen, and select the [Next] button.

   If executing Cluster Creation again because it was stopped due to an error, select the [Next] button if no parameters must be entered again, and proceed to Step 5.



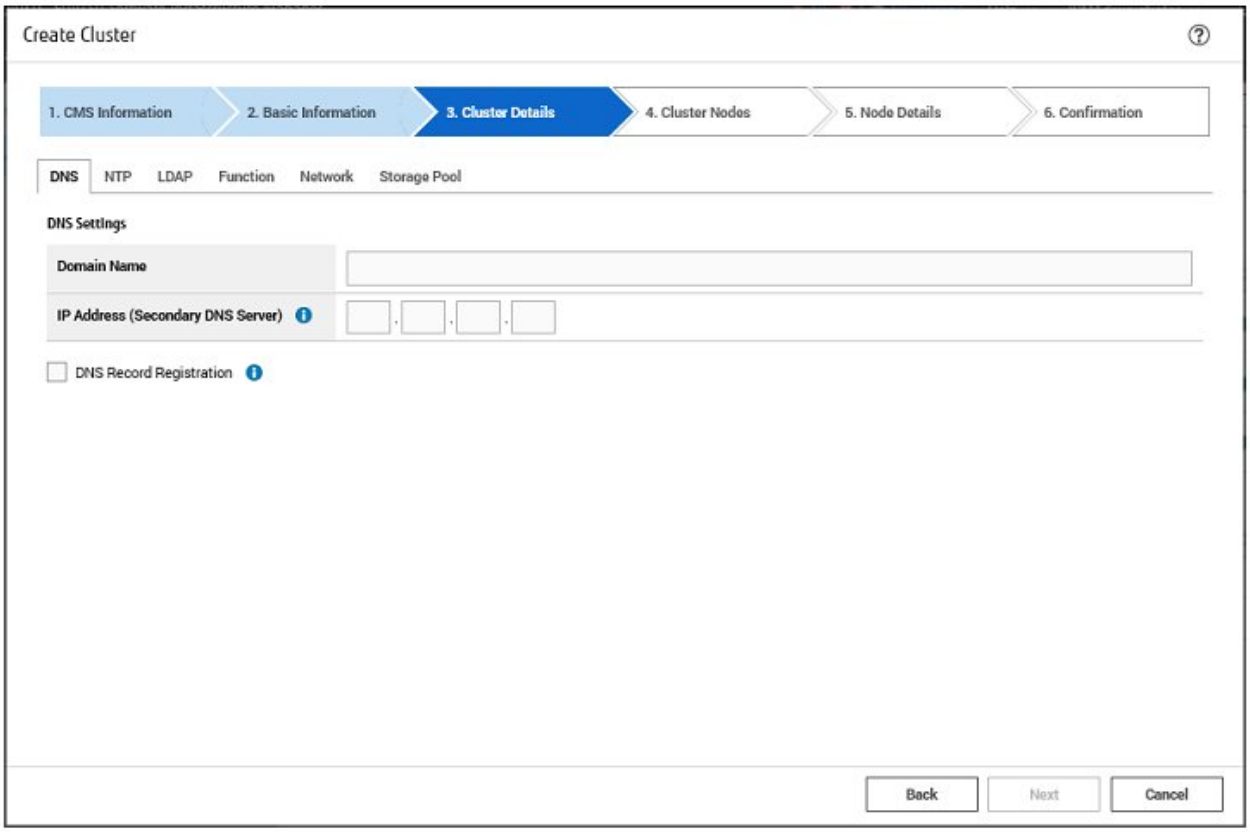
5. Enter each parameter on the "2. Basic Information" screen, and select the [Next] button.

   If executing Cluster Creation again because it was stopped due to an error, select the [Next] button if no parameters must be entered again, and proceed to Step 6.



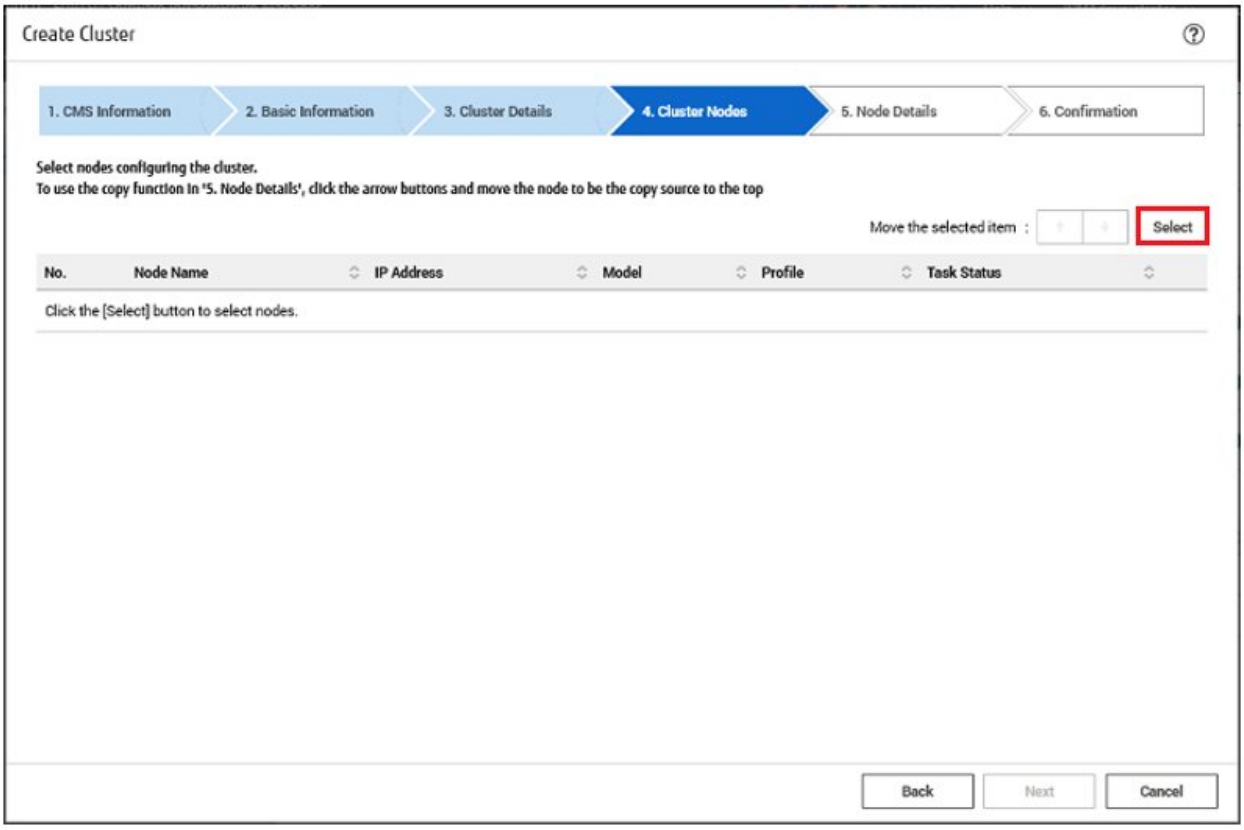
6. Enter each parameter on the "3. Cluster Details" screen, and select the [Next] button.

   If executing Cluster Creation again because it was stopped due to an error, select the [Next] button if no parameters must be entered again, and proceed to Step 7.



7. Select the [Select] button on the "4. Cluster Nodes Selection" screen, and then on the displayed "Target nodes selection" screen, select the target server.

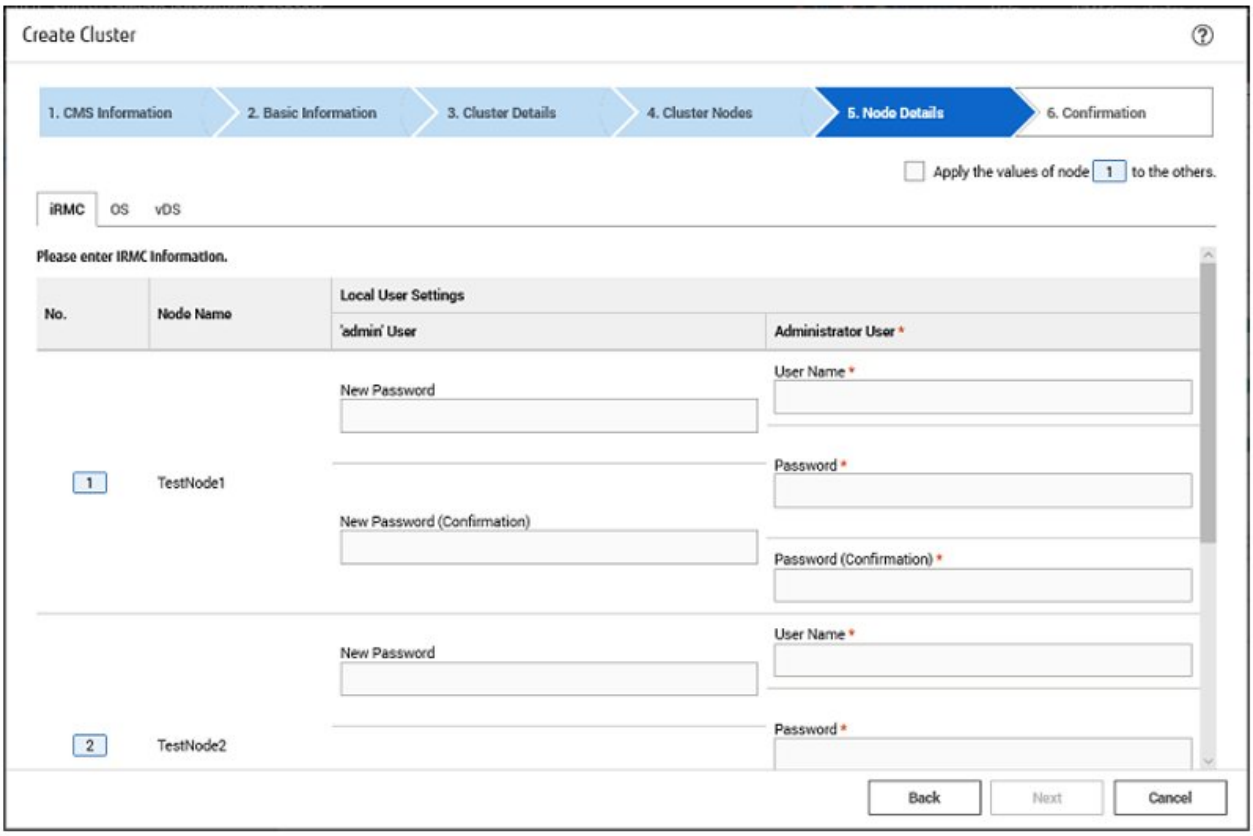
   If executing Cluster Creation again because it was stopped due to an error, this procedure is not required. Select the [Next] button and proceed to Step 9.



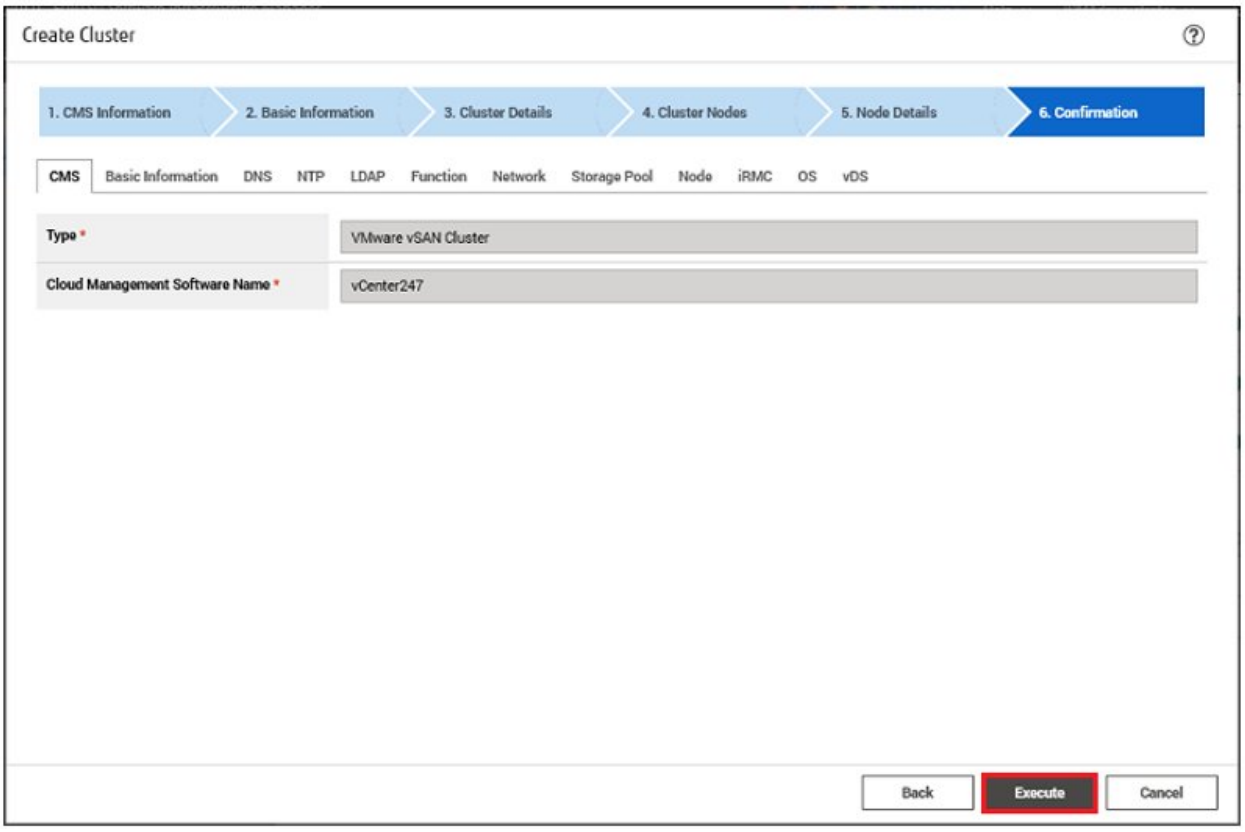
8. If a profile has not been assigned to the target server, select the [Select] button in the [Profile] item, select the profile to be assigned, and select the [Next] button.

9. Enter each parameter on the "5. Node Details" screen, and select the [Next] button.

   If executing Cluster Creation again because it was stopped due to an error, select the [Next] button if no parameters must be entered again, and proceed to Step 10.

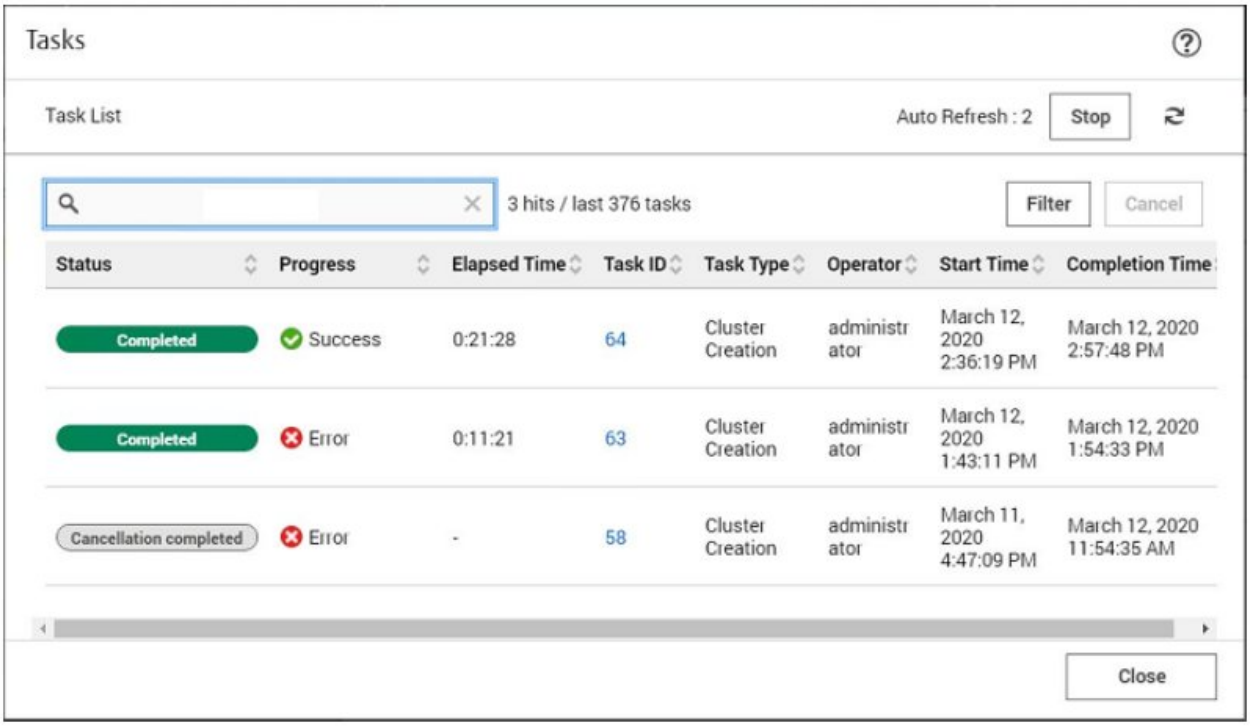


10. Check the parameters on the "6. Confirmation" screen, then select the [Execute] button.



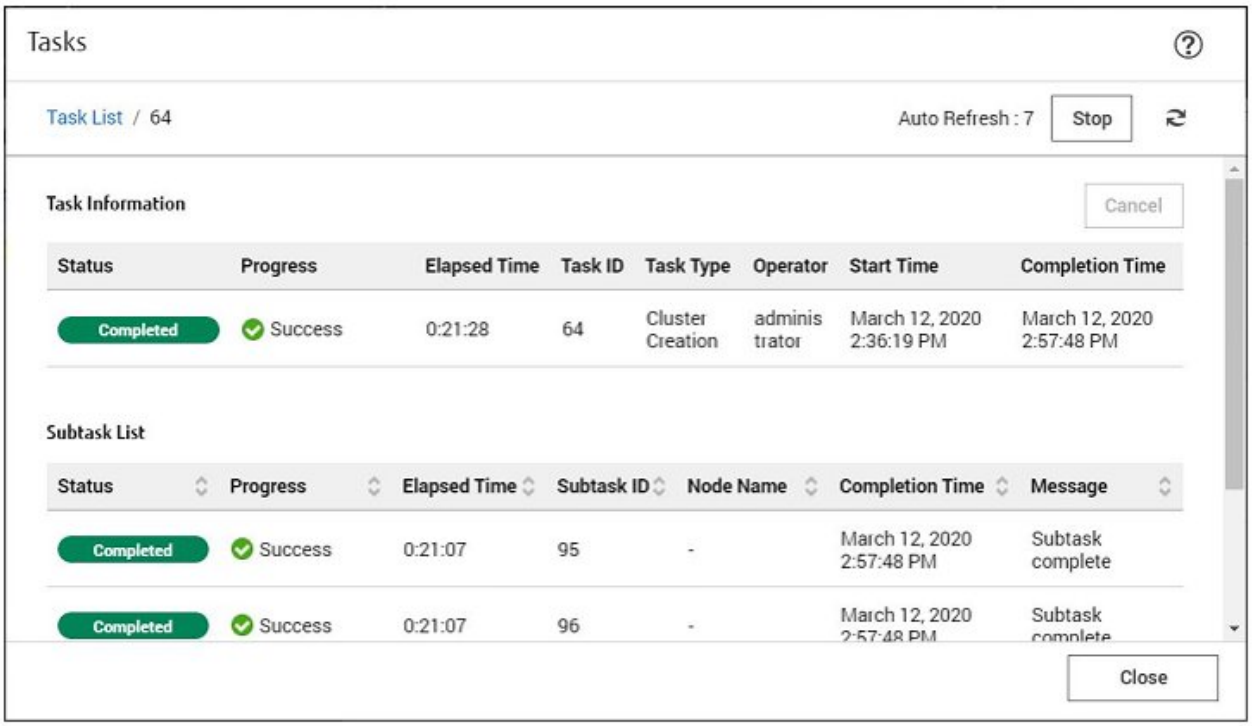
The execution of Cluster Creation is registered as an ISM task.

On the "Tasks" screen, which is displayed when you select [Tasks] on the top of the Global Navigation Menu, tasks whose Task Type is "Cluster Creation" are Cluster Creation tasks.



Point

If you select [Task ID] for "Cluster Creation" from the "Tasks" screen, the "Tasks" screen for "Cluster Creation" is displayed. On this screen, the subtask list is displayed and you can confirm the status of the task by checking the message.



11. Check that the status of "Cluster Creation" has become "Completed."
12. Check that the "Updating vSAN configuration" and "Configuring vSphere HA" processes are complete.

    Even when Cluster Creation is complete, the processing of "Updating vSAN configuration" and "Configuring vSphere HA" may be under execution. Proceed to "6.8.4 Follow-up Processing" after the processing of these tasks is completed.

    For vCSA 6.5 and earlier (Flash)

    Log in to vCSA with vSphere Web Client, and from the "Top" screen, confirm if the "Updating vSAN configuration" task and "Configuring vSphere HA" task displayed in the [Recent Tasks] are complete.

    For vCSA 6.7 or later (HTML5)

    Log in to vCSA with vSphere Client, and from the "Top" screen, confirm if the "Updating vSAN configuration" task and "Configuring vSphere HA" task displayed in the [Recent Tasks] are complete.

Note

- If an error is displayed on the ISM "Tasks" screen, check the ISM event log. Confirm the message by referring to "ISM for PRIMEFLEX Messages" and take action.

  After the error is resolved, execute Cluster Creation again.

  If the OS installation with Profile Management of ISM (Assigning profile tasks) ends normally, do not power off the target server when executing again.

- For the settings of the virtual network for workload on the target server, set them according to your environment.

- If an error is displayed on the ISM "Tasks" screen after you create the script to be executed before and after the application of VMware ESXi patches, refer to "6.8.4.2 Confirm the execution results of the scripts" to confirm the results of the script.

  Or refer to "ISM for PRIMEFLEX Messages" and take action.

6.8.3.2 Cluster Expansion procedure

This section describes the procedure for executing Cluster Expansion of ISM for PRIMEFLEX.

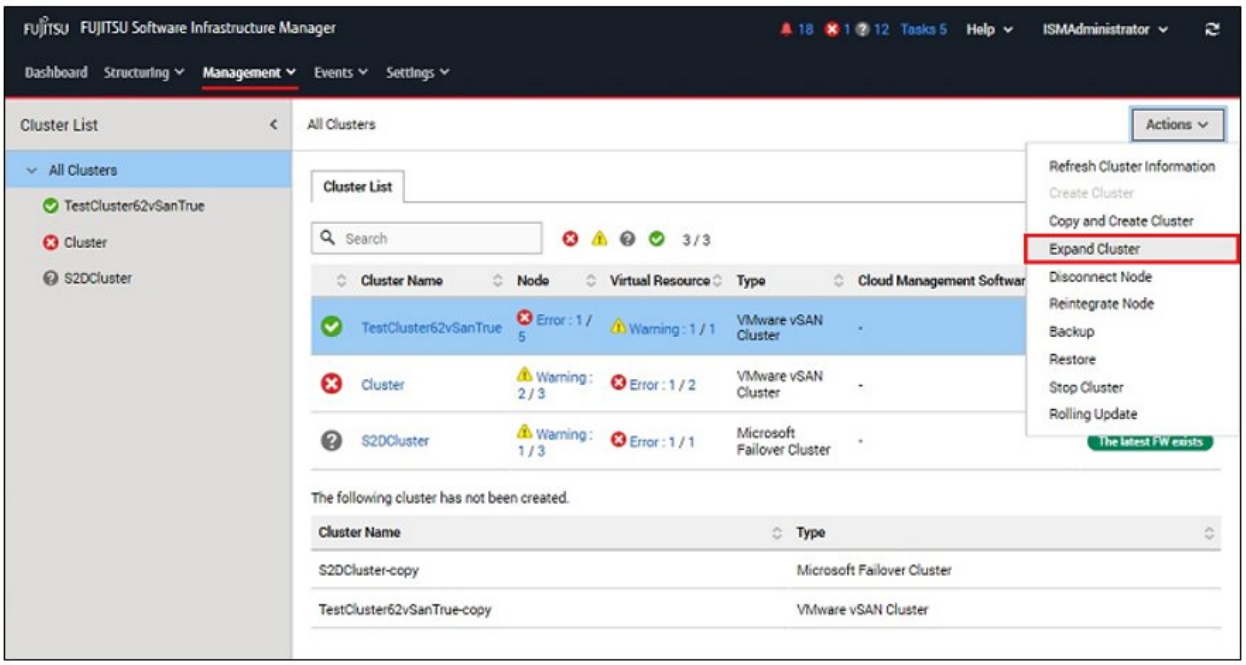
Note

Do not execute Cluster Expansion while other ISM for PRIMEFLEX functions are being executed. Cluster Expansion will fail. Check the ISM event log. Confirm the message by referring to "ISM for PRIMEFLEX Messages" and take action.

For ISM for PRIMEFLEX functions, refer to "2.12 Functions of ISM for PRIMEFLEX" in "User's Guide."

1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster].

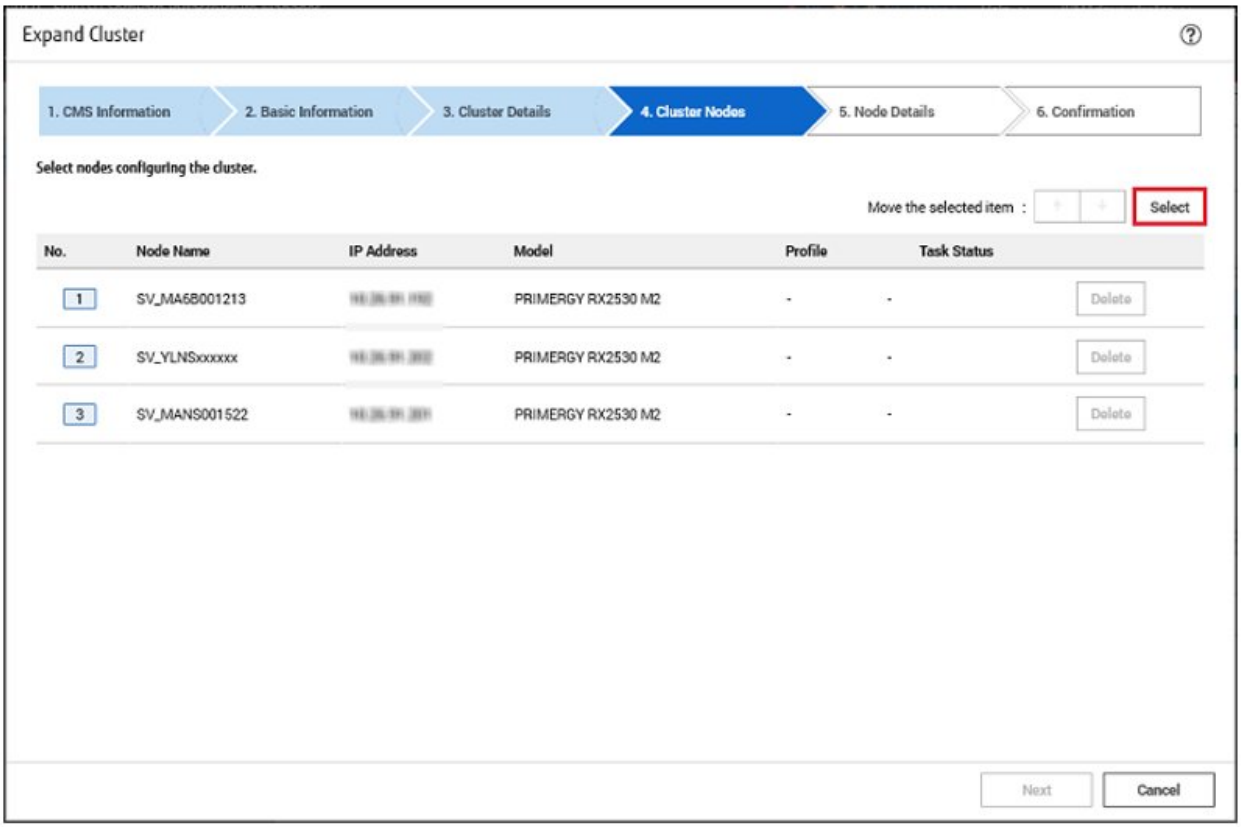
   The "Cluster List" screen is displayed.
3. Select [<Target cluster>], and then from the [Actions] button, select [Expand Cluster].



The "Expand Cluster" wizard is displayed.

4. Select the [Select] button on the "4. Cluster Nodes Selection" screen, and then on the displayed "Target nodes selection" screen, select the target server.

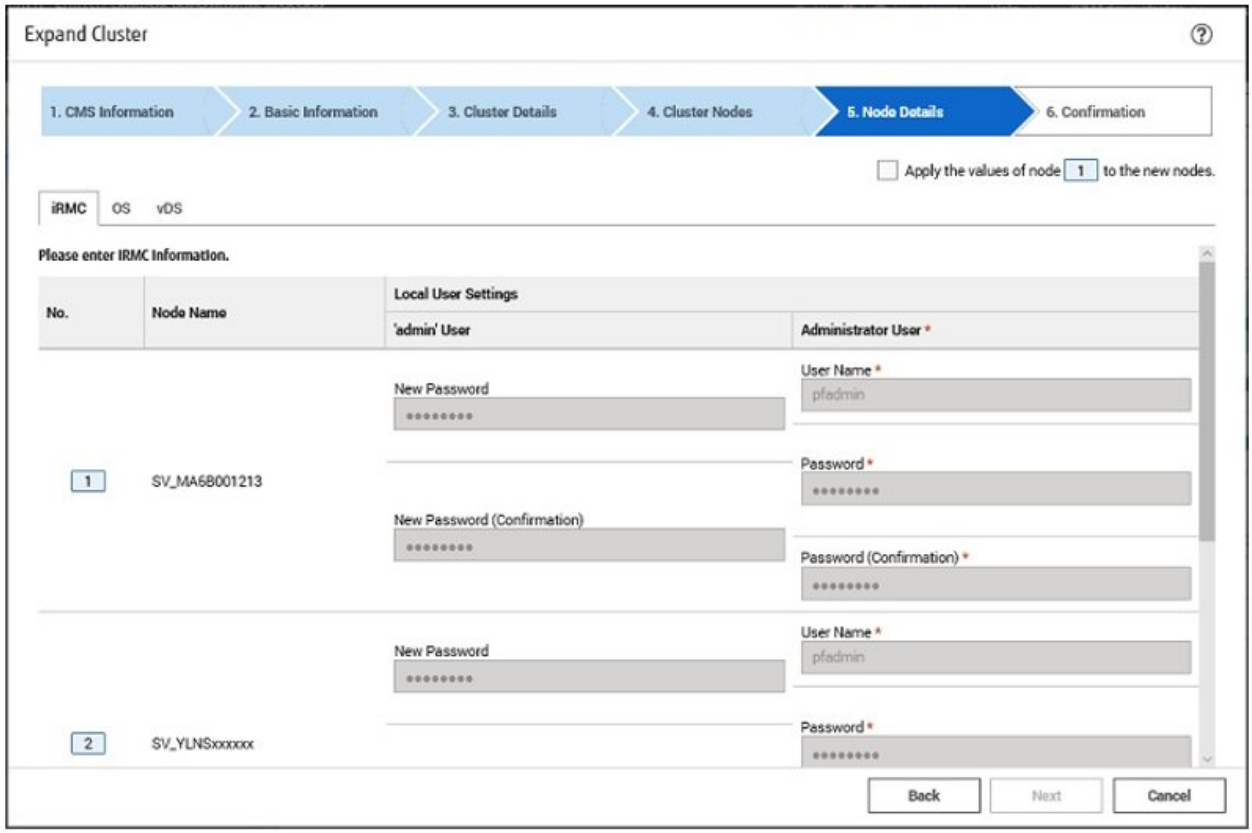
   If executing Cluster Expansion again because it was stopped due to an error, this procedure is not required. Select the [Next] button and proceed to Step 6.



5. If a profile has not been assigned to the target server, select the [Select] button in the [Profile] item, select the profile to be assigned, and select the [Next] button.

6. Enter each parameter for the target server on the "5. Node Details" screen, and select the [Next] button.

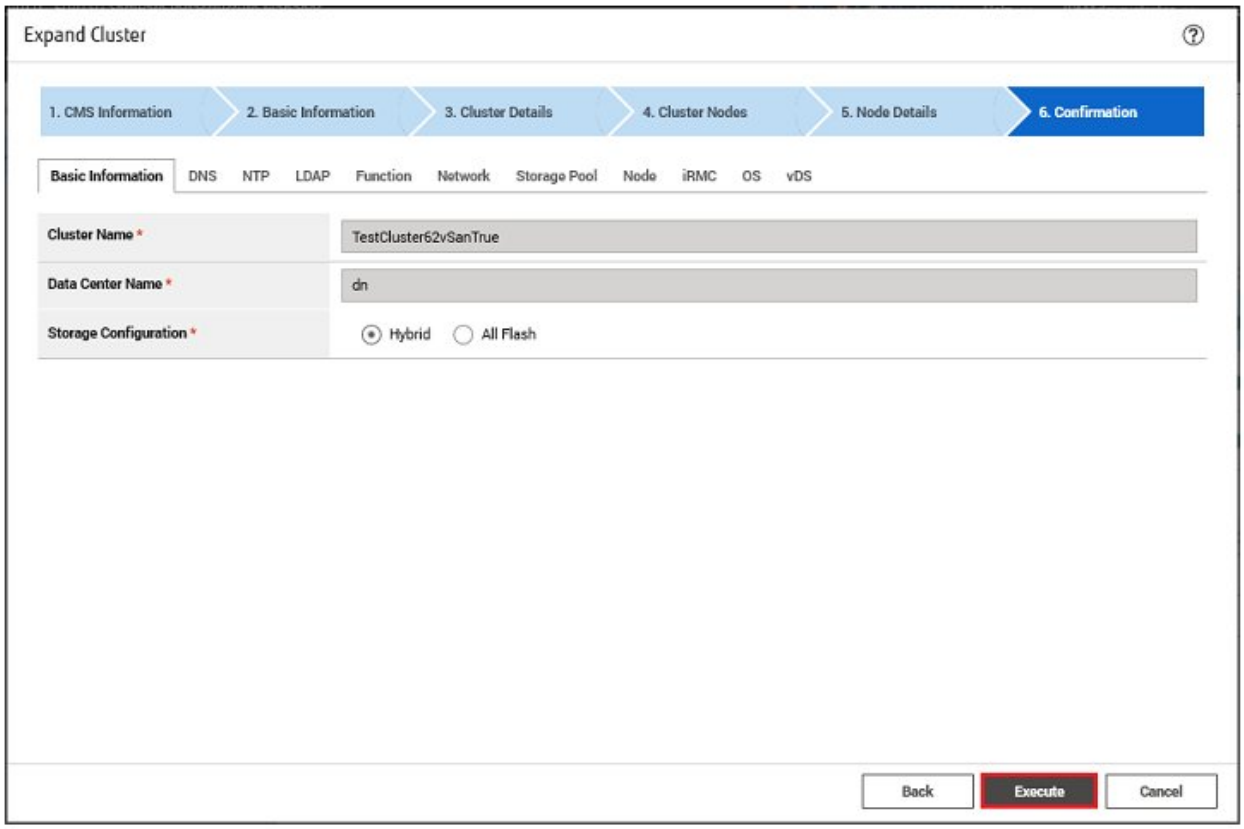
   If executing Cluster Expansion again because it was stopped due to an error, select the [Next] button if no parameters must be entered again, and proceed to Step 7.



Note

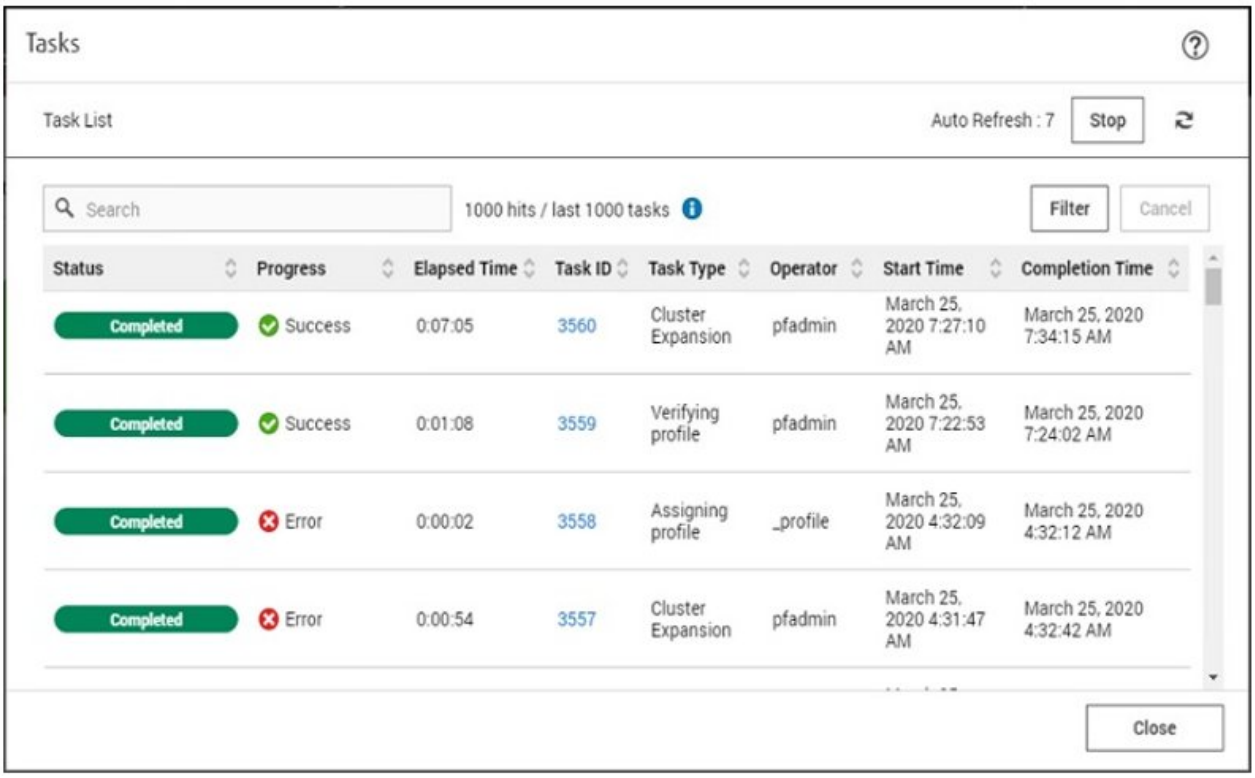
For details on Cluster Definition Parameters, refer to "Chapter 3 Parameter List for Cluster Definition Parameters Settings" in "ISM for PRIMEFLEX Parameter List."

7. Check the parameters on the "6. Confirmation" screen, then select the [Execute] button.



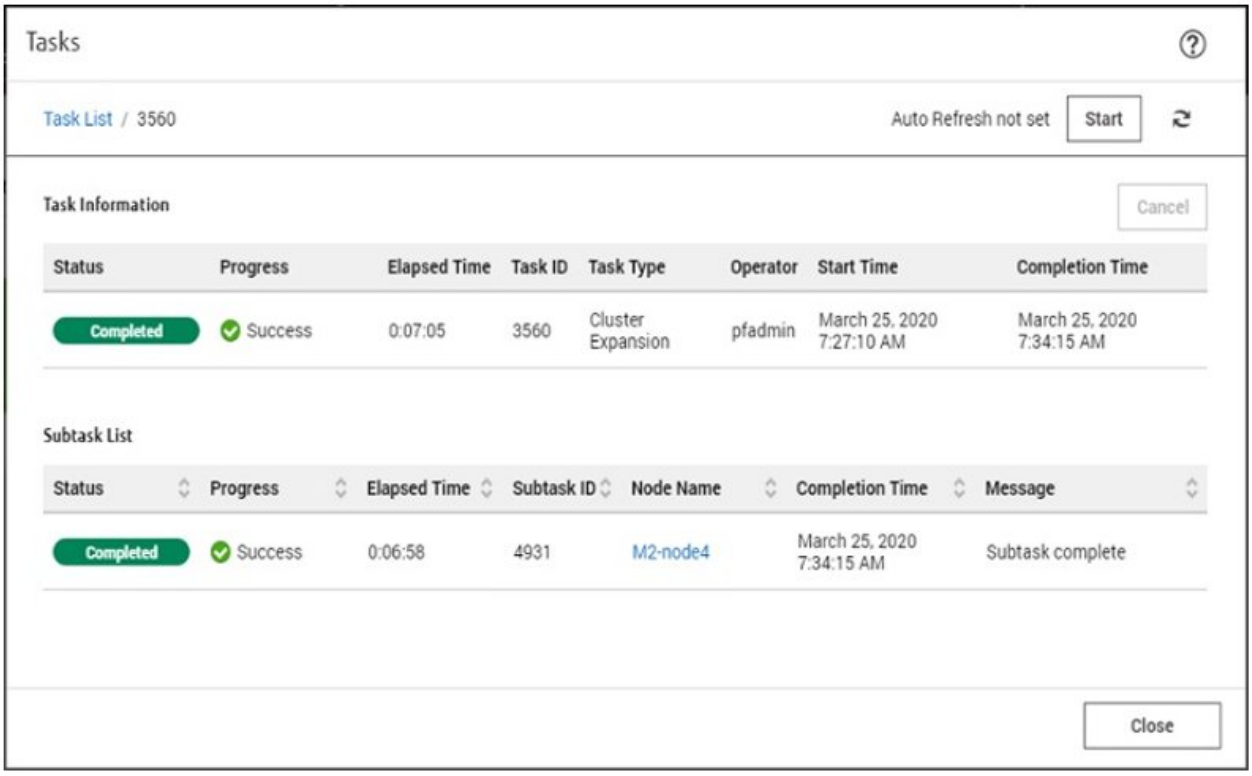
The execution of Cluster Expansion is registered as an ISM task.

On the "Tasks" screen, which is displayed when you select [Tasks] on the top of the Global Navigation Menu, tasks whose Task Type is "Cluster Expansion" are Cluster Expansion tasks.



Point

If you select [Task ID] for "Cluster Expansion" from the "Tasks" screen, the "Tasks" screen for "Cluster Expansion" is displayed. On this screen, the subtask list is displayed and you can confirm the status of the task by checking the message.



8. Check that the status of "Cluster Expansion" has become "Completed."

Note

- If an error is displayed on the ISM "Tasks" screen, check the ISM event log. Confirm the message by referring to "ISM for PRIMEFLEX Messages" and take action.

  After the error is resolved, execute Cluster Expansion again.

  If the OS installation with Profile Management of ISM (Assigning profile tasks) ends normally, do not power off the target server when executing again.

- For the settings of the virtual network for workload on the target server, set them according to your environment.

- If an error is displayed on the ISM "Tasks" screen after you create the script to be executed before and after the application of VMware ESXi patches, refer to "6.8.4.2 Confirm the execution results of the scripts" to confirm the results of the script.

  Or refer to "ISM for PRIMEFLEX Messages" and take action.

6.8.4 Follow-up Processing

This section describes the follow-up processing required after the cluster creation or cluster expansion.

6.8.4.1 Confirm resources

Confirm the vSAN cluster with the following procedure.

1. Confirm the following.

   For vCSA 6.5 and earlier (Flash)

   Log in to vCSA with vSphere Web Client to confirm the following:

   - The created cluster is displayed from the "Top" screen - [Home] tab - [Inventories] - [Hosts and Clusters]
   - The disks of the target server are displayed from the "Top" screen - [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Monitor] - [vSAN] - [Physical Disk]
   - From the "Top" screen, select [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Monitor] - [vSAN] - [Health], execute the test again and check that there are no errors

   For vCSA 6.7 or later (HTML5)

   Log in to vCSA with vSphere Client to confirm the following:

   - The created cluster is displayed from the "Top" screen - [Shortcuts] - [Inventories] - [Hosts and Clusters]
   - The disks of the target server are displayed from the "Top" screen - [Shortcuts] - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Monitor] - [vSAN] - [Physical Disk]

     For vCSA 7.0U3 or later, confirm the following.

     From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Configure] - [vSAN] - [Disk Management], target server, and then select [VIEW DISKS].

   - There are no errors when executing the following test again; From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Monitor] - [vSAN] - [Skyline Health]

   Sometimes a warning may be displayed to the Statistics DB object of the Performance service, but ignore this.

Point

If there are health errors, check the details of the error in question, and then solve it.

If you are using a vSAN6.7U3 environment (VMware ESXi 6.7 Update 3), health errors and the countermeasures are described below:

- Virtual SAN Disk Balance

  Execute proactive balancing for the disks.

  For vCSA 7.0 or later, execute automatic rebalance configuration.

- Controller driver is VMware certified

  Apply the recommended driver for the SAS controller to the target host.

- Controller firmware is VMware certified

  No countermeasures required. A warning is displayed since the VIB (VMware Infrastructure Bundle) that retrieves the firmware version of the sas3flash controller is not installed. Since this VIB is not included in the custom image this is expected.

- vSAN Build Recommendation Engine Health

  Recover the network connection.

Note

For vCSA 6.5 and earlier (Flash)

To check the fault domain host of the target server, move from "Top" screen - [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Settings] - [vSAN] - [Fault Domains & Stretched Cluster] - [Fault Domains].

For vCSA 6.7 or later (HTML5)

To check the fault domain host of the target server, move from "Top" screen - [Shortcuts] - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Configure] - [vSAN] - [Fault Domains] - [Fault Domains].

If multiple hosts are set for one fault domain, check that [OS (for each node)] - [Network] - [DHCP] - [Get Computer Name from DNS Server] - [Computer Name] of the profile does not overlap with the computer names of the current cluster or target servers. If the result of checking is that they overlap, refer to the following and take action:

- For Cluster Creation

  "3.2 Action Examples for when a Cluster Creation Error Occurs" - "Action example 23" in "ISM for PRIMEFLEX Messages"

- For Cluster Expansion

  "3.1 Action Examples for when a Cluster Expansion Error Occurs" - "Action example 19" in "ISM for PRIMEFLEX Messages"

2. From the Global Navigation Menu on the ISM GUI, select [Management] - [Virtual Resource].

   The "All Storage Pool" screen is displayed.

3. From the [Actions] button, select [Refresh Virtual Resource Information].

   The information is refreshed.

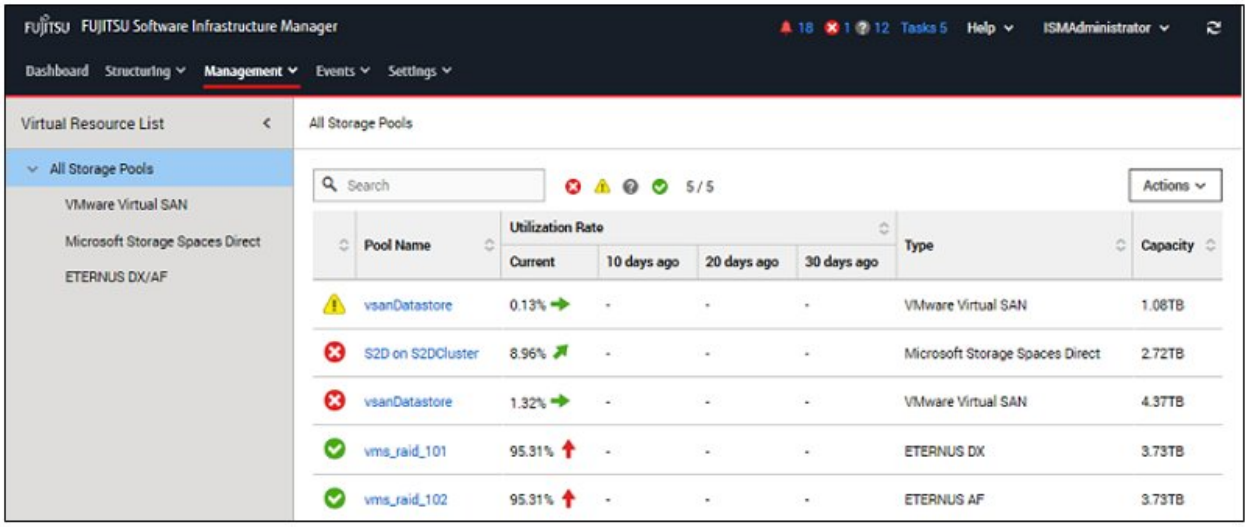
4. After the information is refreshed, check the following:

   - For Cluster Creation

     Confirm that the target vSAN datastore is displayed.

   - For Cluster Expansion

     Confirm that the [Capacity] of the target vSAN datastore has increased.



Note

Even when Cluster Creation or Cluster Expansion completes successfully, the following situations may occur:

- The vSAN storage is not displayed
- The vSAN storage capacity is less than expected
- The previously checked vSAN storage has not been expanded

In the above situations, it can be assumed that the cause is a communication failure for the vSAN network.

Check the settings and the wiring of the switch.

6.8.4.2 Confirm the execution results of the scripts

Confirm the execution results of the scripts that were created in "6.8.2.8 Creating scripts to execute before and after a VMware ESXi patch application" with the output log.

The following messages are output in the log file when the scripts have been executed successfully.

The following message is output for the script that is executed before VMware ESXi patch application in (Example: /scratch/log/pre_script.log).

```
pre_script End
```

The following message is output for the script that is executed at VMware ESXi patch application in (Example: /scratch/log/post01_script.log).

```
post01_script End
```

The following message is output for the script that is executed after VMware ESXi patch application in (Example: /scratch/log/post02_script.log).

```
post02_script End
```

If the script execution failed, check the script logs and take action. After resolving the error, execute the content of the script manually. For details, contact your local Fujitsu customer service partner.

6.8.4.3 Restrictions/precautions for VMware vSphere

Carefully read "Readme [Fujitsu VMware ESXi Customized Image]" in the file downloaded and take actions for the system restrictions that apply to your system.

Execute for all target servers.

http://support.ts.fujitsu.com/Index.asp?lng=COM

6.8.4.4 Confirm and migrate the vCLS virtual machine datastore

This operation is required after you have created cluster with vCSA 7.0 U1 or later.

Creating a cluster with vCSA to 7.0 U1 or later enables the vSphere Cluster Service (vCLS) and creates a vCLS virtual machine on the cluster. A maximum of three vCLS virtual machines are created in a cluster.

If this vCLS virtual machine was created in the local datastore, it must be migrated to the vSAN datastore.

Perform this on target clusters.

Point

Depending on the user type that logs in to vCSA, vSphere Cluster Service (vCLS) may not be displayed.
Use the administrator for the vCenter Single Sign-On domain to perform vSphere Cluster Service (vCLS) -related operations.

Procedure to confirm the datastore in which the vCLS virtual machine is placed

Confirm the datastore in which the vCLS virtual machine is placed.

1. Log in to vCSA with vSphere Client.
2. From the "Top" screen, select [Shortcuts] - [Hosts and Clusters] - [<Cluster name>] - [VMs] - [Virtual Machines] - [<vCLS name>].
   - For vCSA 7.0U2 and earlier:

     <vCLS name> is displayed as "vCLS (n)" (n is a number).
   - For vCSA 7.0U3 or later:

     <vCLS name> is displayed as "vCLS-XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX" (X is a 16 digit number).

3. Check that [Data Store] - [Name] is the vSAN datastore name.

   To confirm the vSAN datastore name, use the ISM GUI to check Cluster Definition Parameters for the target cluster in the [Cluster Details] - [Storage Pool] tab under [Storage Pool Name].

   If it is not the vSAN datastore name, perform "Procedure for migrating to the vSAN datastore."

4. Repeat Step 2 to 3 for all vCLS virtual machine.

Procedure for migrating to the vSAN datastore

Migrate the vCLS virtual machine to the vSAN datastore.

For vCSA 7.0U2 and earlier

1. Log in to vCSA with vSphere Client.
2. From the "Top" screen, select [Shortcuts] - [Hosts and Clusters] - [<Cluster name>] - [VMs] - [Virtual Machines] - [<vCLS name>].
3. Select [ACTIONS] - [Migrate].

   A confirmation screen is displayed.

4. Select [YES] on the confirmation screen.

   The "Migrate" screen is displayed.

5. Select "Change storage only" in [1 Select migration type], then select the [NEXT] button.
6. Select the vSAN data store in [2 Select storage] and select the [NEXT] button.

   You can view the vSAN datastore in "vSAN" in [Type].

7. Use [3 Ready to complete] to check the settings and select the [FINISH] button.

For vCSA 7.0U3 or later

1. Log in to vCSA with vSphere Client.
2. From the "Top" screen, select [Shortcuts] - [Hosts and Clusters] - [<Cluster name>].
3. Select [Configure] - [vSphere Cluster Service] - [Datastores] - [ADD].

   The "Add datastores" screen is displayed.

4. On the "Add datastores" screen, select a vSAN datastore and select [ADD].

6.8.4.5 Register a target server to ServerView RAID Manager

To execute Monitoring of SSD lifetime, you must register the target server in ServerView RAID Manager.

In this procedure, execute the following according to the configuration.

Configuration	Location for implementation
When using a configuration with an ADVM of the PRIMEFLEX configuration	ADVM#1
When not using a configuration with an ADVM of the PRIMEFLEX configuration	The server in your environment where the ServerView RAID Manager is installed

This step is required if the target server uses a SAS controller card other than CP2100-8i (CP400i, CP403i, CP503i).

1. Open command prompt with administrator privilege and execute the following command.

```
>cd "C:\Program Files\Fujitsu\ServerView Suite\RAID Manager\bin"
```

2. Execute the following command on all target servers.

```
>amCLI -e 21/0 add_server name=<IP address of ESXi of the target server> port=5989 username=root
password=<root password>
```

3. Execute the following command to check that all target servers have been registered.

```
>amCLI -e 21/0 show_server_list
```

4. From Server Manager, select [Tool] - [Service].
5. Right-click [ServerView RAID Manager], and then select [Restart].
6. Log in to ServerView RAID Manager and select [Host] in the left tree to display all servers.

   Check that the status of all servers is normal.

6.8.4.6 Delete unnecessary files

Delete unnecessary files with the following procedure after completing Cluster Creation or Cluster Expansion.

(1) Deleting certificates

The certificate created in "6.8.2.2 Create ADVM certificates" is not required after once registered.

Note

The certificates uploaded to ADVM#1 and ADVM#2 in "6.8.2.2 Create ADVM certificates" have security risks. If you cannot accept this risk, delete the certificate.

(2) Deleting unnecessary files in ISM-VA

Execute for ISM-VA.

1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. Delete any files that are no longer needed by checking the following items and referring to "1.4.2 Delete Files Uploaded to ISM-VA."

Item	Value
Root Directory	Administrator/ftp
Directory Name	Administrator/ftp/kickstart
File Name	- VMware ESXi patch files in "6.8.2.7 Upload the VMware ESXi patch file." - Offline bundle of the VMware SMIS Provider in "6.8.2.9 Upload VMware SMIS provider."

(3) Delete scripts that are executed before and after the application of VMware ESXi patches

Execute for ISM-VA.

1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. Delete any files that are no longer needed by checking the following items and referring to "1.4.2 Delete Files Uploaded to ISM-VA."

Item	Value
Root Directory	Administrator/ftp
Directory Name	Administrator/ftp/ClusterOperation/ESXi/script
File Name	Script that is executed before and after the application of VMware ESXi patches "6.8.2.8 Creating scripts to execute before and after a VMware ESXi patch application."

6.8.4.7 Confirm the settings for VMware EVC mode

Perform this task when you use Cluster Extension. This is not required when you use Cluster Creation.

Confirm that VMware EVC mode is set up.

For these procedures, refer to "6.8.2.1 Set up VMware EVC for vCenter Server."

If it is not set up, migrate vCSA out of the vSAN cluster, stop all virtual machines on the vSAN cluster, and then set up VMware EVC mode as described in "6.8.2.1 Set up VMware EVC for vCenter Server."

6.9 Increase the Resources for PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI

You can execute Cluster Creation or Cluster Expansion to increase the resources for PRIMEFLEX for Microsoft Storage Spaces Direct/ PRIMEFLEX for Microsoft Azure Stack HCI.

This function can be used only when the ISM Operation Mode is "Advanced for PRIMEFLEX."

Servers for creating a new cluster or servers for expanding a cluster will hereafter be referred to as "target servers."

Cluster Creation or Cluster Expansion is executed according to the following work flow.

Table 6.25 Cluster Creation or Cluster Expansion work flow

Cluster Creation or Cluster Expansion procedure		Tasks
1	Preparations	- Creating target server certificates - DHCP settings - Importing ServerView Installation Manager that is provided with the ServerView Suite DVD, and the ISO image of the OS installation media to ISM-VA - Creating profiles - Creating and editing Cluster Definition Parameters - Installation and Wiring - Setting the IP address of iRMC - BIOS settings - Creating system disk (RAID1) - Confirming networks - Registering nodes in ISM - Confirming the firmware version of the LAN card and downloading the driver
2	Execute Cluster Creation or Cluster Expansion	
3	Follow-up Processing	- Refreshing cluster information - Confirming resources - Deleting unnecessary files - Disabling TLS1.0/TLS1.1 of iRMC - Deleting "Possible Owners" of ISM-VA - Setting the processor compatibility of virtual machines - Setting the network adapter

6.9.1 Operation Requirements

To use Cluster Creation or Cluster Expansion, the following requirements must be met.

- Common operation requirements for Cluster Creation and Cluster Expansion
- Operation requirements for Cluster Creation

- Operation requirements for Cluster Expansion

Common operation requirements for Cluster Creation and Cluster Expansion

Operation requirements for existing clusters

- That the AD, DNS, and NTP are all running normally and can be used
- That the time settings synchronize with the NTP server.
- That the information of the DNS server is registered in ISM-VA
- That you register the target server in AD in advance when configuring an AD that already exists in your environment, since registering a computer in AD is restricted by policies etc.
- For PRIMEFLEX for Microsoft Storage Spaces Direct V2 (PRIMEFLEX for Microsoft Azure Stack HCI V1), the CAS settings for ISM must be executed

  For details, refer to "3.7.2 Set CAS Settings."
- The network configuration is the same as the environment that has been structured with PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI installation service
- NetBIOS domain name is not used for the Active Directory domain name

Operation requirements for target servers

- One of the following ethernet adapters must be installed in the target server

Target server	Ethernet adapter
PRIMERGY M4 series	Intel or Mellanox
PRIMERGY M5 series	Marvell (Cavium/QLogic) or Mellanox
PRIMERGY M6 series (ISM 2.8.0.010 or later)	Intel or Mellanox

- The Ethernet adapter can handle over 10 GB traffic
- That there is only one logical disk (Configure 2 HDD or 2 SSD as RAID 1) created in "6.9.2.9 Create system disk (RAID1)"
- That for each target server in PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI storage configurations there is the following

Storage configuration	Storage type	Number of devices
Hybrid	Cache device	At least 2
	Capacity device	At least 4
All-Flash	Capacity device	At least 4

- The power of the target server is off

  The following is an operation requirement when executing Cluster Creation or Cluster Expansion again with the OS installation completed using profile assignment.

  - The power of the target server is on

  To check if the OS installation has been completed, use the following procedure.

  1. At the top of the Global Navigation Menu on the ISM GUI, select [Tasks].
  2. From the cluster list on the "Tasks" screen, select the task ID whose task type is "Assigning profile."
  3. Check that all the results of the tasks in the subtask list have become "Success."
- BIOS settings for the target server are specified as described in "6.9.2.8 Set up BIOS"

- The OS information has not been registered for the target server

  The target server is excluded from the selection of target nodes if the OS information has been registered.

- A profile has been created for the target server with Profile Management of ISM
- The computer name of the target servers which you specify in the profile must be unique among all nodes managed by ISM.

  Check if the computer name is unique by comparing with the following conditions:

  - Upper case characters and lower case characters are not distinguished
  - Domain name is excluded

- The IP address of the OS of the target servers which you specify in the profile must be unique among all IP addresses of the OS of the nodes managed by ISM
- The profile has not been applied to the target server

  The target server is excluded from the selection of target nodes if the profile has been applied.

- IPv4 address for the management network port group is the same as the profile setting ([Details] - [OS (for each node)] tab - [Network] - [DHCP] - [IP address]).
- The network information is displayed on iRMC

  For details, refer to "6.9.2.10 Confirm networks."

Operation requirements for Cluster Creation

Operation requirements for existing clusters

- There is one or more existing clusters
- When configuring an ADVM dedicated to PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI, that the following files for PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI installation service exist on ADVM#1 and ADVM#2:
  - c:\FISCRB\PowerShellScript\fis_advm_ftp_put.ps1
  - c:\FISCRB\PowerShellScript\FIS_JOB_ADVM_RECEIVE_FILES.ps1

Operation requirements for target servers

- The type of the target servers must be the same
- There are two or more target servers

  When creating a cluster with two nodes, a quorum is required.

- The devices for PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI are configured as follows

Device	Default	Utilization
PCI card 1 (Port1), PCI card 2 (Port1)	Virtual switch for workload	Production LAN
PCI card 1 (Port0), PCI card 2 (Port0)	Virtual switch for management	Management LAN Storage_1 LAN, Storage_2 LAN (for Heart Beat and Live Migration of the failover cluster)

The configuration of the device for PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI can be checked using the following procedure.

1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes] to display the "Node List" screen.

3. On the [<Target node>] - [Component] tab, confirm that [PCI Devices] and [Port Information] are in the device configuration.

You must set the device configuration for Cluster Definition Parameters.

For details, refer to "6.9.2.5 Create and edit Cluster Definition Parameters."

- On the "2. Basic Information" screen in the "Create Cluster" wizard, the name in [Cluster Name] must be 15 characters or less

Operation requirements for Cluster Expansion

Operation requirements for existing clusters

- That the existing cluster is operating normally
- That the virtual networks for PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI are configured as follows

Setting items	Setting Value
Switch Embedded Teaming	Virtual switch for workload
	Virtual switch for management
Virtual Network Adapter	- vEthernet (Management) - vEthernet (Storage_1) - vEthernet (Storage_2)

The configuration of the virtual network for PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI can be checked using the following procedure.

1. Use remote desktop to connect to the cluster representative IP (cluster access point).
2. Open PowerShell from the command prompt using administrator privilege and execute the following two commands.

```
>Get-VMSwitchTeam
```

```
>Get-NetAdapter
```

3. Check that the setting value is output in "Name."

- The devices for PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI are configured as below

Device	Default	Utilization
PCI card 1 (Port1), PCI card 2 (Port1)	Virtual switch for workload	Production LAN
PCI card 1 (Port0), PCI card 2 (Port0)	Virtual switch for management	Management LAN Storage_1 LAN, Storage_2 LAN (for Heart Beat and Live Migration of the failover cluster)

The configuration of the device for PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI can be checked using the following procedure.

1. Use remote desktop to connect to the cluster representative IP (cluster access point).
2. Open PowerShell from the command prompt with administrator privilege and execute the following commands.

```
>Get-VMSwitchTeam
```

3. Check that "Name" and "NetAdapterInterfaceDescription" has become the device configuration.

- The "Health Status" of the virtual disk becomes normal

The "Health Status" of the virtual disk can be checked with the following procedure.

1. Use remote desktop to connect to the cluster representative IP (cluster access point).
2. Open PowerShell from the command prompt with administrator privilege and execute the following commands.

```
>Get-Virtualdisk
```

3. Check that "HealthStatus" is "Healthy."

- Cluster Management pre-settings have been executed for the cluster to be expanded

  For settings of Cluster Management, refer to "3.8 Pre-Settings for Managing Virtual Resources/Clusters" in "User's Guide."

- Embedded teaming must be enabled for the workload and management virtual switches on the server configuring the cluster

Operation requirements for target servers

- The target servers must be the same or a successor to a server that is configured in an existing cluster

  For the detailed information, refer to "Support Matrix" ([Details of ISM for PRIMEFLEX] sheet).
  https://support.ts.fujitsu.com/index.asp

  Select [Select a new Product] on the above site and enter "Infrastructure Manager" in [Product Search:].
  Select [DOWNLOADS] and select the target operating system.
  The reference procedures are subject to change without notice.

- The type of the Ethernet adapters must be the same
- Cluster Definition Parameters have been set

  For details, refer to "6.9.2.5 Create and edit Cluster Definition Parameters."

- The version of the Windows update program is the same as that of the existing cluster

  Apply the latest version of the Windows update program.

Point

You must confirm that the resources have increased after executing Cluster Expansion. Confirm the current PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI storage capacity before executing Cluster Expansion in advance. For the procedure to confirm, refer to "6.9.4.2 Confirm resources."

6.9.2 Preparations

This section describes the preparations required before cluster creation or cluster expansion.

6.9.2.1 Create certificates for target servers

You must create and register certificates for target servers because Cluster Creation or Cluster Expansion executes settings from ISM with SSL encrypted communication.

(1) Creating certificates

Use the tool to create certificates (makecert.exe) and the tool to create files to replace personal information (pvk2pfx.exe) to create the following three files from the management terminal. Create certificates for all target servers.

- CER file (certificate)
- PVK file (private key file)
- PFX file (service certificate)

(1-1) Preparations for required tools

There are two tools required for creating certificates:

- .NET Framework 4.5 (Download site)

  https://www.microsoft.com/en-us/download/details.aspx?id=30653

- Windows Software Development Kit (Download site)

  https://developer.microsoft.com/en-us/windows/downloads/windows-10-sdk

Note

- Install the above tool to the management terminal.
- Download the .NET Framework 4.5 in the URL above in the same language that is set for the management terminal used to create certificates.
- The Windows Software Development Kit works for Windows 8.1, Windows Server 2012 and later OS versions. Install the appropriate Windows Software Development Kit if installing other OSes.
- When using Windows 10 SDK on a platform other than Windows 10, Universal CRT must be installed (Refer to KB2999226 "https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows"). To avoid errors occurring during the setup, make sure to install the latest recommended update programs and patches from Microsoft Update before installing Windows SDK.

(1-2) Creating certificate and private key file

Open the command prompt (administrator) on the management terminal and execute the following command.

```
>makecert.exe -r -pe -n "CN=<IP address of the target server OS>" -e <expiration date for the certificate (mm/dd/yyyy)> -eku 1.3.6.1.5.5.7.3.1 -ss My -sr localMachine -sky exchange <computer name that is set for the ISM profile>.cer -sv <file name of the private key>.pvk
```

The following is a command example where the IP address of the target server OS is "192.168.10.10," the certificate expiration date is March 30, 2018, the computer name that is set for the ISM profile, and the file name of the private key are "hv-host4."

Execution example:

```
>makecert.exe -r -pe -n "CN=192.168.10.10" -e 03/30/2018 -eku 1.3.6.1.5.5.7.3.1 -ss My -sr localMachine -sky exchange hv-host4.cer -sv hv-host4.pvk
```

As you will be required to enter the password to be set to the certificate twice in the process, enter it correctly. If an error occurs, perform the same process to execute the command above again.

Execute the following command to check the creation of <computer name that is set for the ISM profile>.cer and <file name of the private key>.pvk.

```
>dir
```

(1-3) Creating service certificates

Open the command prompt (administrator) on the management terminal and execute the following command.

```
>pvk2pfx.exe -pvk <file name of the private key>.pvk -spc <computer name that is set for the ISM profile>.cer -pfx <computer name that is set for the ISM profile>.pfx
```

The following is a command example when you set the file name of the private key and the computer name that is set for the ISM profile to "hv-host4."

Execution example:

```
>pvk2pfx.exe -pvk hv-host4.pvk -spc hv-host4.cer -pfx hv-host4.pfx
```

You will be required to enter the password set in (1-2) during the process, then enter it accordingly.

Execute the following command to check the creation of <computer name that is set for the ISM profile>.pfx.

```
>dir
```

(2) Registering certificates

A certificate is registered when the OS setup script is executed during OS installation.

Upload the certificates created in (1), checking the following items and referring to "1.4.1 Upload Files to ISM-VA."

Item	Value
Root Directory	Administrator/ftp
File Type	Certificate for cluster management
Upload Target Path	Administrator/ftp/postscript_ClusterOperation
File	The certificate created in (1)

6.9.2.2 Set up DHCP

For Cluster Creation or Cluster Expansion, execute OS installation by using profile assignment. To execute OS installation with profile assignment, a DHCP server is required.

Although ISM-VA has a DHCP server function internally, you can also prepare an external DHCP server for ISM-VA. If you are going to use an internal DHCP server, set it up with reference to "4.15 ISM-VA Internal DHCP Server" in "User's Guide."

Set it so that multiple leases are possible for all target servers.

Note

- Confirm that any DHCP services to be used are started.
- If you have multiple DHCP servers running within the same network, they may not always function properly. Stop any DHCP services that are not in use.
- Set lease periods so that they do not expire while any work is in progress.
- Since the management network is made redundant in the configuration of this product, IP addresses are leased to two ports. Make the settings so that there are always two IP addresses that can be leased for a node.
- Check whether the settings are for internal or external DHCP of ISM, and modify them according to the same DHCP that you are using. For information on the procedure to modify the settings, refer to "4.15.4 Switch of DHCP Servers" in "User's Guide."

6.9.2.3 Import ServerView Installation Manager provided with the ServerView Suite DVD, and the ISO image of the OS installation media to ISM-VA

Import ServerView Installation Manager (hereafter referred to as "SVIM") that is provided with the ServerView Suite DVD, and the OS installation media into ISM.

You must import the applicable ServerView Installation Manager for the target server.

For information on import operations, refer to "2.13.2 Repository Management" in "User's Guide."

For the support version, refer to "3.1 Profiles for Windows Server" in "Items for Profile Settings (for Profile Management)."

Add ISM-VA virtual disks if necessary. For information on the procedure to add virtual disks, refer to "3.7 Allocation of Virtual Disks" in "User's Guide."

6.9.2.4 Create a profile

Use ISM Profile Management to create the profiles for target servers.

To create a profile, refer to "3.3 Execute Settings on a Server/Install Server OS."

For the detailed profile setting values, refer to "Chapter 4 Parameter List for Profile Settings" in "ISM for PRIMEFLEX Parameter List."

- When using Cluster Creation

  If the target server is the same as the server in the existing cluster environment, copy and create from the existing profile.
  If the target server is different from the server in the existing cluster environment, create a new profile.

- When using Cluster Expansion

  - If the target server is the same as the server in the existing cluster environment, create and copy from the existing profile.
    If you add a successor server, create a new profile.

  - If the target server is the same as the server in the existing cluster environment, create and copy from the existing profile or policy, and assign a profile again. For this operation refer to "Procedures to change [Verify Status] back to [Match] if it is [Mismatch] (For items in which the node setting changes were intended)" in "3.3.5 Compare Assigned Profiles and Hardware Settings."

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
2. To create a new profile, from the [Actions] button, select [Add Profile].
   To copy and create a profile, select the duplication source from existing profile, and select [Duplicate Profile] from the [Actions] button.
3. Set each item.

Point

Refer to "2.4.3 OS Installation Settings" in "User's Guide" to perform the preparation tasks required when installing an OS.

Note

- Do not check the following item.
  - In the [OS (for each node)] tab, [DHCP]

    This item is not required to be set because the fixed IP address is used for the management LAN.
- There is no problem if the following items are selected.

  This is because it is automatically set by Cluster Creation and Cluster Expansion.
  - In the [OS] tab, [Execute Script after Installation]

    If this item is set in the OS policy, make sure that the following settings are configured. If the values are different, Cluster Creation and Cluster Expansion will end in an error.

    - In the [OS] tab, [Execute Script after Installation]: Enabled
    - In the [OS] tab, [Directory Forwarded to the OS]: postscript_ClusterOperation
    - In the [OS] tab, [Script to Execute]: WinSvr_Setting.bat
- Set the following items so that they do not overlap:
  - In the [OS (for each node)] tab, [Computer Name]
  - In the [OS (for each node)] tab, [Network] - [DHCP] - [IP Address]

6.9.2.5 Create and edit Cluster Definition Parameters

This operation is required to use Cluster Expansion. This is not required to use Cluster Creation.

Use the ISM GUI to create and edit Cluster Definition Parameters as required.

Create Cluster Definition Parameters for the cluster to be expanded. If there are multiple clusters to expand, create the parameters for all the clusters. You do not need to create Cluster Definition Parameters for the servers for expanding a cluster. Set these when executing Cluster Expansion.

If Cluster Definition Parameters are already created, check the contents. If the contents require modifications, edit them.

From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster] - [<Target Cluster>] - [Cluster Definition Parameters] tab.

- If creating a new parameter

  From the [Parameter Actions] button, select [Create].

- If editing a current parameter

  From the [Parameter Actions] button, select [Edit].

Point

- For the operation of creating and editing Cluster Definition Parameters, refer to the online help.
- For details on Cluster Definition Parameters, refer to "Chapter 3 Parameter List for Cluster Definition Parameters Settings" in "ISM for PRIMEFLEX Parameter List."
- Edit the Cluster Definition Parameters if there are setting items for which Cluster Definition Parameters are not set after the ISM upgrade. In addition, some items in ISM GUI are input automatically. Check if the setting values are correct.

Note

If Rolling Update is being executed or has ended with an error, do not create or edit Cluster Definition Parameters. Creating and editing Cluster Definition Parameters will fail.

6.9.2.6 Execute installation and wiring

Install a target server at its physical location and connect the cables. For details, refer to the "Operating Manual" of the target server. Execute the settings for your network switches as appropriate, referring to the manual for the switches.

Point

Only one ISM network interface can be defined. If creating a new cluster in a network other than the current one, set the router and set it so that communication is possible between each network. For the network configuration, refer to "1.2 Configuration" in "User's Guide."

Execute for all target servers.

The order of the operations differs depending on the node discovery method at the node registration in the ISM.

- For Manual Discovery of nodes

  Execute the operations in the following procedures.

  1. "6.9.2.7 Set the IP address of iRMC"
  2. "6.9.2.8 Set up BIOS"
  3. "6.9.2.9 Create system disk (RAID1)"
  4. "Node registration using Manual Discovery" in "6.9.2.11 Register a node to ISM"
  5. "6.9.2.12 Confirm the firmware version of the LAN card and download the driver"
  6. "6.9.3 Execute Cluster Creation or Cluster Expansion"

- For Auto Discovery of nodes

  Execute the operations in the following procedures.

  1. "Node registration using Auto Discovery" in "6.9.2.11 Register a node to ISM."
  2. "6.9.2.8 Set up BIOS"

3. "6.9.2.9 Create system disk (RAID1)"
4. "6.9.2.12 Confirm the firmware version of the LAN card and download the driver"
5. "6.9.3 Execute Cluster Creation or Cluster Expansion"

6.9.2.7 Set the IP address of iRMC

When you register a target server by using Manual Discovery, set a static IP address for the iRMC.

Boot the BIOS of the target server, and on the "BIOS setup" screen, set a static IP address. To execute this operation, you must execute "6.9.2.6 Execute installation and wiring." Moreover, to display and operate the "BIOS setup" screen, connect a display and keyboard to the target server.

For information on booting the BIOS and setting the IP address for the iRMC, refer to the "BIOS Setup Utility Reference Manual" for the target server.

Set for all target servers.

Also, execute "6.9.2.8 Set up BIOS" as well as setting of the IP address.

You can obtain the "BIOS Setup Utility Reference Manual" for each target server from the following website:

https://support.ts.fujitsu.com/

On the site above, select "Select a new Product" - [Browse For Product] and select product line: [Fujitsu Server PRIMERGY] - product group: [<Target server group>] - product family: [<Target server>].
Download from [Systemboard].

Reference procedures are subject to change without notice.

6.9.2.8 Set up BIOS

This section describes the BIOS setup procedure.

For Manual Discovery when registering nodes in ISM, set this item together with "6.9.2.7 Set the IP address of iRMC."

For Auto Discovery when registering nodes in ISM, you can set BIOS settings remotely with iRMC Video Redirection.

1. Refer to steps 1 and 2 in "6.9.2.10 Confirm networks" to display the iRMC screen of the target server. Log in and select Video Redirection.

   The Video Redirection screen (server screen) is displayed.

   Point

   When the Video Redirection screen (server screen) is not displayed:

   After logging in to iRMC, check the [Settings] tab - [Advanced Video Redirection (AVR)] - [KVM Redirection Type], and confirm that "HTML5 Viewer" is set. If "JViewer (JAVA)" is set, select "HTML5 Viewer", and select the [Apply] button. And then select Video Redirection again.

2. From the video redirection menu, select [Power] - [Power On Server] or [Power Cycle].

   Select [Yes] for the confirmation dialog.
   Select [OK] for the normal execution dialog.

3. Press the [F2] key during boot to start the BIOS. And set the following on the "BIOS setup" screen.

Execute this for all target servers.

Table 6.26 BIOS settings (PRIMERGY M4, M5 series)

Item		Setting Value
Main	System Date	Local date
	System Time	Local date
Advanced - CPU Configuration [Note]	Override OS Energy Performance	Enabled

Item		Setting Value
	Energy Performance	Performance
	Package C State Limit	C0
Advanced - Network Stack Configuration	Network Stack	Enabled
	IPv4 PXE Support	Enabled
	IPv6 PXE Support	Disabled
Security - Security Boot Configuration	Secure Boot Control	Enabled
Server Mgmt - iRMC LAN Parameters Configuration	iRMC IPv6 LAN Stack	Disabled

[Note]: If this is specified in the ISM profile setting values (in the [Details] - [BIOS] tab), no settings are required.

Table 6.27 BIOS settings (PRIMERGY M6 series (ISM 2.8.0.010 or later))

Item		Setting Value
Information	System Date	Local date
	System Time	Local date
Configuration - CPU Configuration [Note 1]	Override OS Energy Performance	Enabled
	Energy Performance	Performance
	Package C State Limit	C0
Configuration - UEFI Network Stack Configuration	Network Stack	Enabled
	IPv4 PXE Support	Enabled
	IPv6 PXE Support	Disabled
Security - Security Boot Configuration [Note 2]	Current Secure Boot State	Enabled
	Secure Boot Control	Enabled ("X" is displayed on the screen)
Management - iRMC LAN Parameters Configuration	iRMC IPv6 LAN Stack	Disabled

[Note 1]: If this is specified in the ISM profile setting values (in the [Details] - [BIOS] tab), no settings are required.

[Note 2]: "Security Boot Configuration" should be set as follows:

1. In the [Security] tab, select [Secure Boot Configuration] and select the [Enter] key.
2. If [Secure Boot Control] - [(blank)] is available to select, proceed to Step 7. If not, select [Secure Boot Mode] - <Standard Mode>, and then select the [Enter] key.
3. Select [Custom Mode] and select the [Enter] key.
4. Select [Custom Secure Boot Options], and select the [Enter] key.
5. Select [Load Default Key], and then select the [Enter] key. [Are you sure you want to Load Default Key?] is displayed, and then enter [Y].
6. Select the [Esc] key to return to the previous screen, and confirm that [Enabled] is displayed in [Current Secure Boot State].
7. If [Secure Boot Control] - [X] is displayed, proceed to Step 9.

   If not displayed, select [Secure Boot Control] - [(blank)], and then select the [Enter] key. [Configuration changed, please reset the platform to take effect!] is displayed, and then select the [Enter] key again.
8. Confirm that [Secure Boot Control] - [X] is displayed.
9. Select the [Esc] key to return to the previous screen, and then select the [Exit] tab.
10. In the [Exit] tab, select [Commit settings and Exit], and then select the [Enter] key.

11. [Commit settings and exit?] is displayed, then enter [Y].

Note

After completing the BIOS settings, in the "BIOS setup" screen - the [Save & Exit] tab, execute "Save Changes and Exit," or "Commit setting and Exit" then power off after several minutes.

Continue to execute "6.9.2.9 Create system disk (RAID1)."

6.9.2.9 Create system disk (RAID1)

The logical disk to be used as a system disk (Configure 2 HDD or 2 SSD as RAID 1) is created in the "UEFI" screen in PRIMERGY. Execute for all target servers.

1. Start the "BIOS setup" screen.
2. Select the [Advanced] tab or the [Configuration] tab, then confirm the selected items.

   If "LSI SAS3 MPT Controller SAS3008" is displayed, use the following procedure to create the system disk.

   a. Select "LSI SAS3 MPT Controller SAS3008" and select the [Enter] key.
   b. Select "LSI SAS3 MPT Controller Version X.XX.XX.XX" and select the [Enter] key.
   c. Select "Controller Management" and select the [Enter] key.
   d. Select "Create Configuration" and select the [Enter] key.
   e. In "Select RAID level" select "RAID 1," select "Select Physical Disks" and then select the [Enter] key.
   f. Select the type of the system disk prepared in "Select Interface Type."
   g. In "Select Media Type" select the media of the system disk (HDD). If "No changes have been detected from the current configuration and the settings will be retained." Is displayed, execute the procedure from Step j.
   h. Select two system disks for your OS booting from the disk list displayed in "Select Media Type."
   i. Change the two disks to be used as system disk to "Enabled," select "Apply Changes" and select the [Enter] key.
   j. A confirmation screen is displayed and after changing "Confirm" to "Enabled," select "Yes" and select s the [Enter] key.
   k. In "Operation completed successfully," select "OK" and select the [Enter] key.
   l. Select the [Esc] key several times, in "Exit Without Saving," select "Yes" and select the [Enter] key.

   If "MSCC SmartHBA 2100-8i" or "Adaptec SmartHBA 2100-8i" is displayed, use the following procedure to create the system disk.

   a. Select [MSCC SmartHBA 2100-8i] or [Adaptec SmartHBA 2100-8i] and select the [Enter] key.
   b. Select [Configure Controller Settings] and select the [Enter] key.
   c. Select [Modify Controller Settings] and select the [Enter] key.
   d. If [Port CN0 Mode] and [Port CN1 Mode] are displayed, proceed to Step e.
      If not displayed, press the [ESC] key twice, and proceed to Step l.
   e. Select [Port CN0 Mode] and select [Mixed].
   f. Select [Port CN1 Mode] and select [Mixed].
   g. Confirm that [Mixed] is selected for [Port CN0 Mode] and [Port CN1 Mode], and select [Submit Changes].
   h. Confirm that [Controller Settings Applied Successfully. To reflect Connector Settings Restart System] is displayed, and select [Back to Main Menu].
      If "No changes have been detected from the current configuration and the settings will be retained." is displayed, execute the procedure from Step j.

i. Restart the system.

   1. Select the [ESC] key to go back to the [Setup Utility] top screen.
   2. From the [Save & Exit] tab, select [Save Changes and Reset] and [Yes]. The reboot begins.
      Or from the [Exit] tab, select [Commit settings and Exit], and then reboot the server.

j. On the startup screen, select the [F2] key to display [Setup Utility].

k. Select the [Advanced] tab or [Configuration] tab, and select [MSCC SmartHBA 2100-8i] or [Adaptec SmartHBA 2100-8i].

l. Select [Array Configuration].

m. Select [Create Array].

   The disk connected to the SAS controller is displayed.

n. Select both of the disks to be used as the boot device and select [Enabled] or [X].

o. Confirm that [Enabled] or [X] is displayed for both of the disks and select [Proceed to next Form].

p. Select [RAID Level] and select [RAID1].

q. Select [Proceed to next Form].

r. On the parameter settings screen for [Logical Drive Label], keep the default settings and select [Submit Changes].

s. Confirm that [Logical Drive Creation Successful] is displayed, and select [Back to Main Menu].

t. Select the [ESC] key to go back to the [Setup Utility] top screen.

u. From the [Save & Exit] tab, select [Save Changes and Reset], or from the [Exit] tab, select [Commit settings and Exit]

3. The power of the server is turned off.

For Manual Discovery when registering nodes in ISM, continue to execute "Node registration using Manual Discovery" in "6.9.2.11 Register a node to ISM."

For Auto Discovery when registering nodes in ISM, continue to execute "6.9.3 Execute Cluster Creation or Cluster Expansion."

6.9.2.10 Confirm networks

For all target servers, check that "Network" is displayed with iRMC Web Server.

For iRMC S4

1. In a web browser, enter the IP address of iRMC for each server.
2. Enter the username and password, and then select [Login] to log in.

   The default username and password are "admin".

3. Select [System Information] - [Network Inventory] in the left tree.

   If the network list is displayed in the "Ethernet Ports" area, the system is working appropriately.

4. If you could not confirm the network in Step 3, turn on the server to verify that the BIOS process is complete.
   Then turn off the power.
5. Check to see if the network is displayed again.
6. Execute the above procedures for iRMC on all servers.

For iRMC S5

1. In a web browser, enter the IP address of iRMC for each server.
2. Enter the username and password, and then select [Login] to log in.

   The default username and password are "admin".

3. Select the [System] tab and select "Network."

   Open "Ethernet Ports (displayed as "Network Adapter" in iRMC 2.20P or later)," from the "Network" in the right pane. If the network list is displayed, the system is working appropriately.

4. If you could not confirm the network in Step 3, turn on the server to verify that the BIOS process is complete.
   Then turn off the power.

5. Check to see if the network is displayed again.

6. Execute the above procedures for iRMC on all servers.

6.9.2.11 Register a node to ISM

In order to use ISM to install an OS, register the target server in ISM.

To register a node to ISM, you can use both Manual Discovery and Auto Discovery.

Register all target servers.

Point

- When you execute node registration in ISM, you must enter the iRMC user names and passwords for the target servers. The user name and password are both set to "admin" by default.
- When registering a node, select the node group that the node belongs to. You can edit the node group later. If you do not set the node group, the node becomes node group unassigned. Only the user of Administrator group can manage the node whose node group is not assigned.
- Register new datacenters, floors, and racks, and then execute the alarm settings for the target servers as required. For the setting procedure, refer to "Chapter 2 Configure the Required Settings When Installing ISM."

Node registration using Manual Discovery

For the procedure for registering a node with Manual Discovery, refer to "3.1.2 Register a Node Directly."

Set the static IP address of the iRMC in the "Node Manual Registration" wizard.

Specify the IP address set in "6.9.2.7 Set the IP address of iRMC" when registering.

Continue to execute "6.9.3 Execute Cluster Creation or Cluster Expansion."

Node registration using Auto Discovery

For the procedure for registering a node with Auto Discovery, refer to "3.1.1 Discover Nodes in the Network and Register Nodes."

By specifying the range of the IP addresses, all target servers can be registered simultaneously.

Continue to execute "6.9.2.8 Set up BIOS."

6.9.2.12 Confirm the firmware version of the LAN card and download the driver

The following LAN cards have a dependency on the supported firmware and driver versions. Check the firmware version of the affected LAN card and the corresponding driver version and download it.

- Marvell (Cavium/QLogic) LAN card

  S26361-F4068-E202 PLAN EP QL41112 2X 10GBASE-T, LP

  S26361-F4056-E202 PLAN EP QL41212 25Gb 2p SFP28 LP

- Mellanox LAN card

  S26361-F4054-E202 PLAN EP MCX4-LX 25Gb 2p SFP28 LP

For hardware firmware, drivers, server attachments (ServerView, etc.) dependencies, and availability contact your local Fujitsu customer service partner.

Check the driver version and update in "6.9.3.1 Cluster Creation procedure" or "6.9.3.2 Cluster Expansion procedure."

6.9.3 Execute Cluster Creation or Cluster Expansion

You can execute Cluster Creation or Cluster Expansion to increase the resources for PRIMEFLEX for Microsoft Storage Spaces Direct/ PRIMEFLEX for Microsoft Azure Stack HCI.

Be sure to refer to "6.9.1 Operation Requirements" and check the operation requirements before executing Cluster Creation or Cluster Expansion.

- 6.9.3.1 Cluster Creation procedure
- 6.9.3.2 Cluster Expansion procedure

6.9.3.1 Cluster Creation procedure

This section describes the procedure for executing Cluster Creation of ISM for PRIMEFLEX.

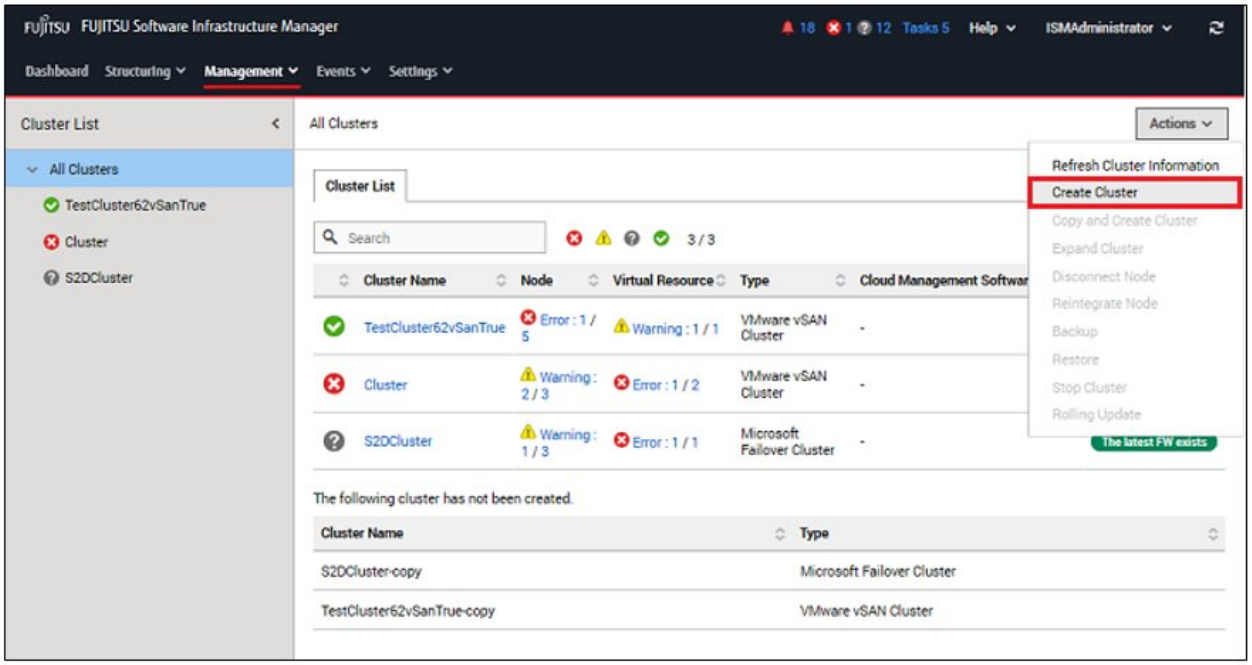
Note

Do not execute Cluster Creation while other ISM for PRIMEFLEX functions are being executed. Cluster Creation will fail. Check the ISM event log. Confirm the message by referring to "ISM for PRIMEFLEX Messages" and take action.

For ISM for PRIMEFLEX functions, refer to "2.12 Functions of ISM for PRIMEFLEX" in "User's Guide."

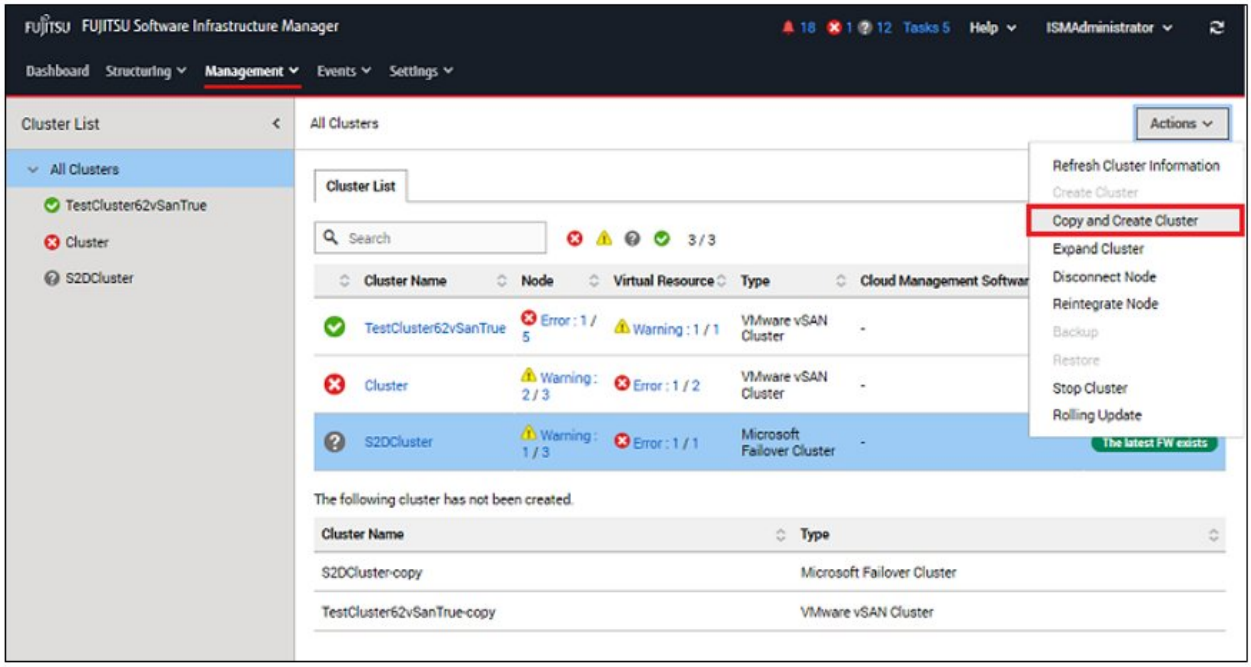
1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster].

   The "Cluster List" screen is displayed.
3. From the [Actions] button, select [Create Cluster].



The "Create Cluster" wizard is displayed.

If you create a cluster by referring the existing cluster, select the existing cluster, then from the [Actions] button, select [Copy and Create Cluster].

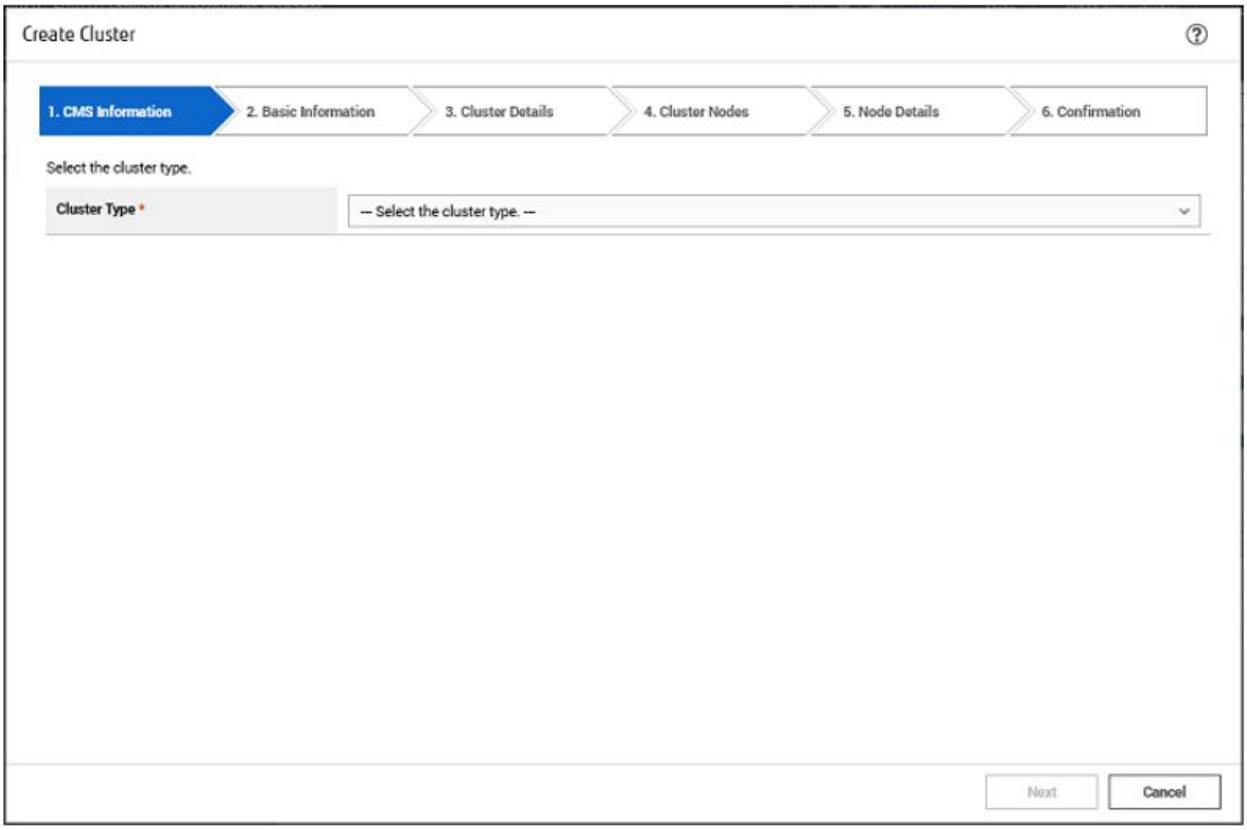


Note

For details on Cluster Definition Parameters, refer to "Chapter 3 Parameter List for Cluster Definition Parameters Settings" in "ISM for PRIMEFLEX Parameter List."

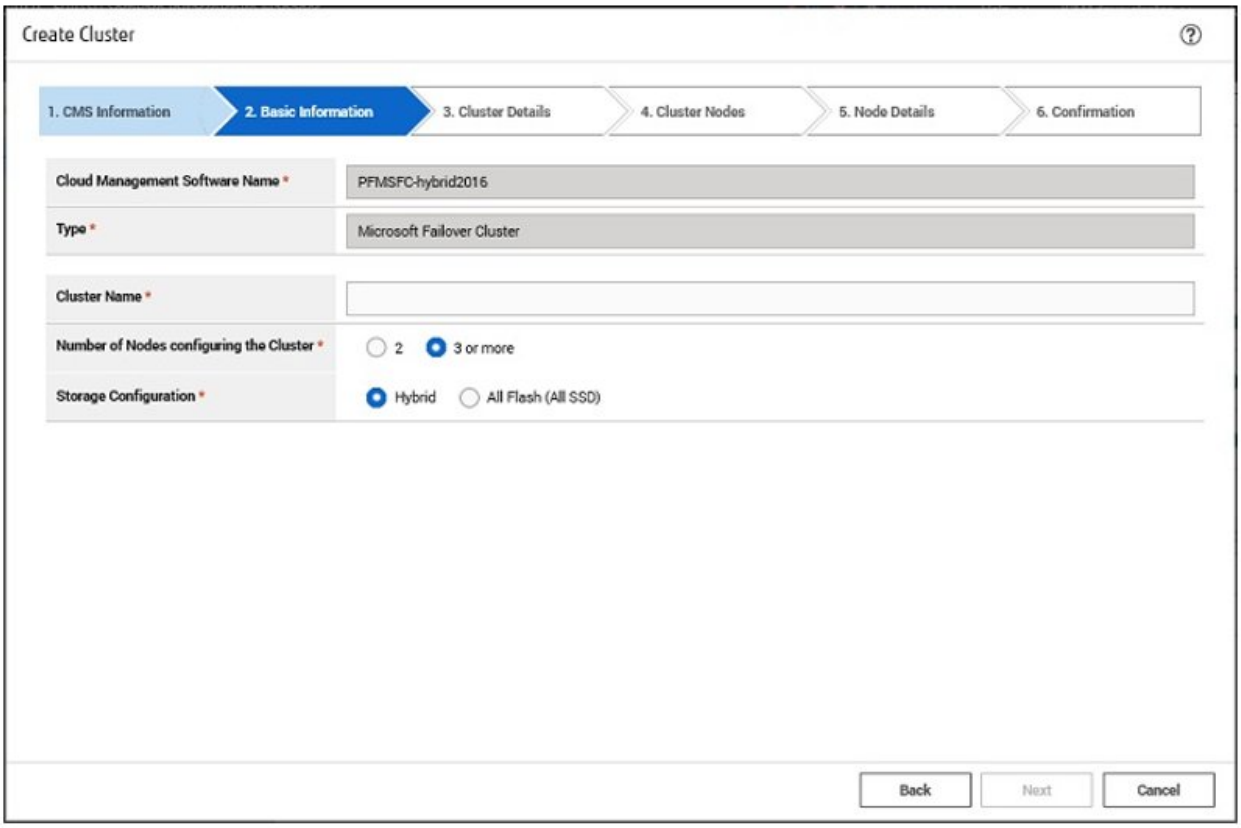
4. Enter each parameter on the "1. CMS Information" screen, and select the [Next] button.

   If executing Cluster Creation again because it was stopped due to an error, select the [Next] button if no parameters must be entered again, and proceed to Step 5.



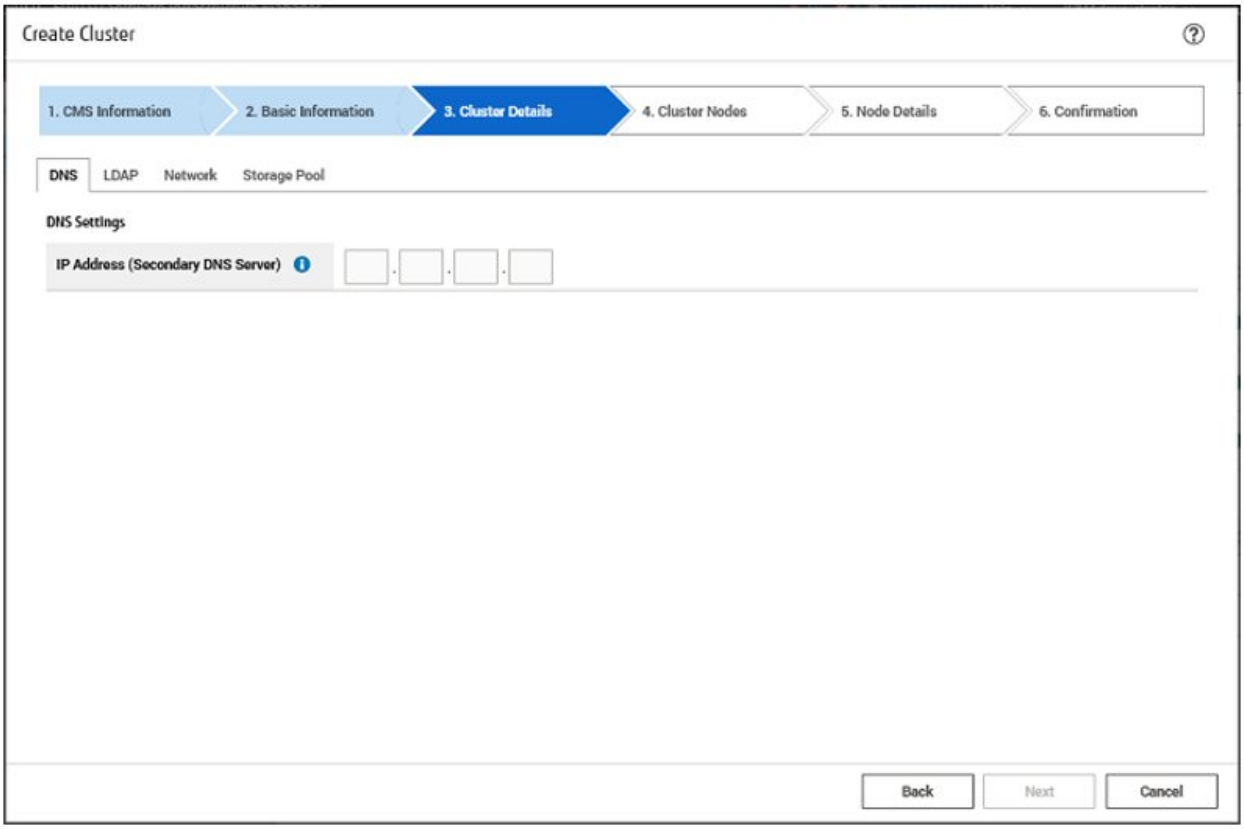
5. Enter each parameter on the "2. Basic Information" screen, and select the [Next] button.

   If executing Cluster Creation again because it was stopped due to an error, select the [Next] button if no parameters must be entered again, and proceed to Step 6.



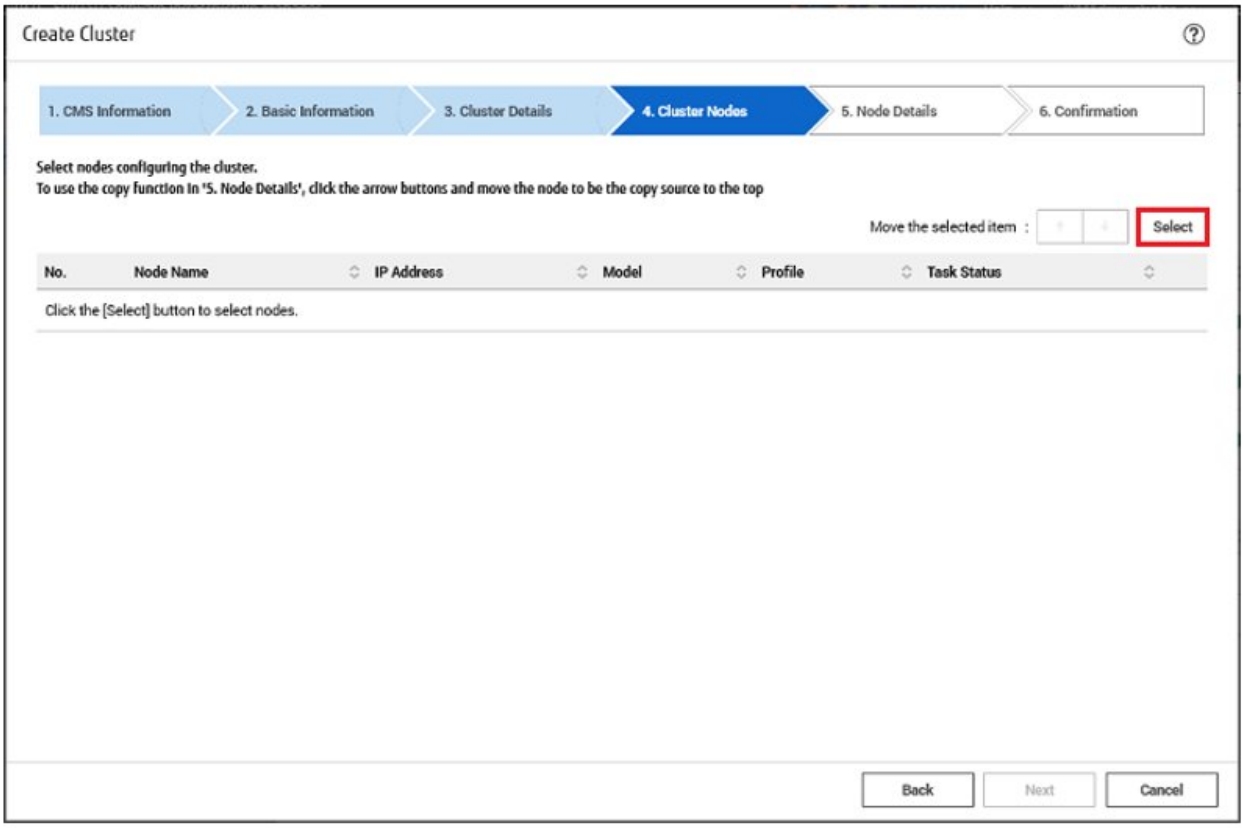
6. Enter each parameter on the "3. Cluster Details" screen, and select the [Next] button.

   If executing Cluster Creation again because it was stopped due to an error, select the [Next] button if no parameters must be entered again, and proceed to Step 7.



7. Select the [Select] button on the "4. Cluster Nodes Selection" screen, and then on the displayed "Target nodes selection" screen, select the target server.

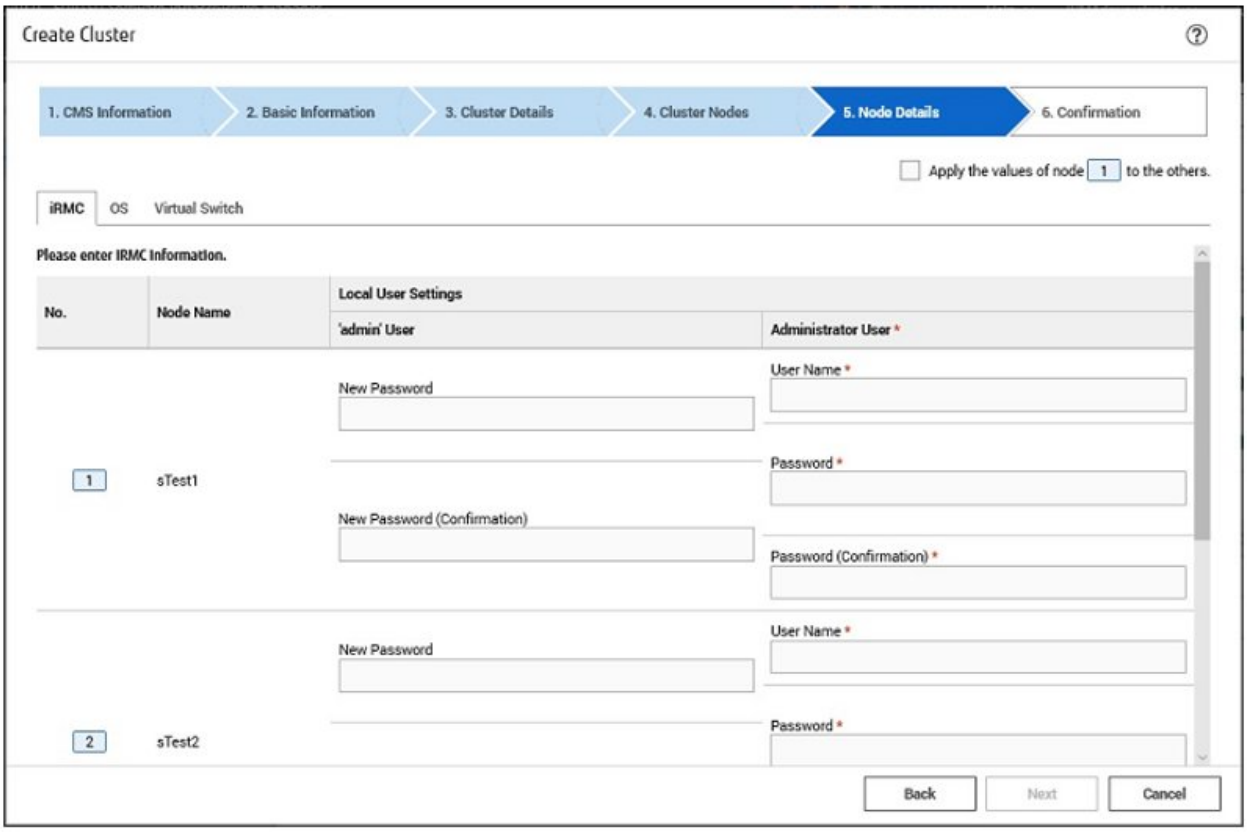
   If executing Cluster Creation again because it was stopped due to an error, this procedure is not required. Select the [Next] button and proceed to Step 9.



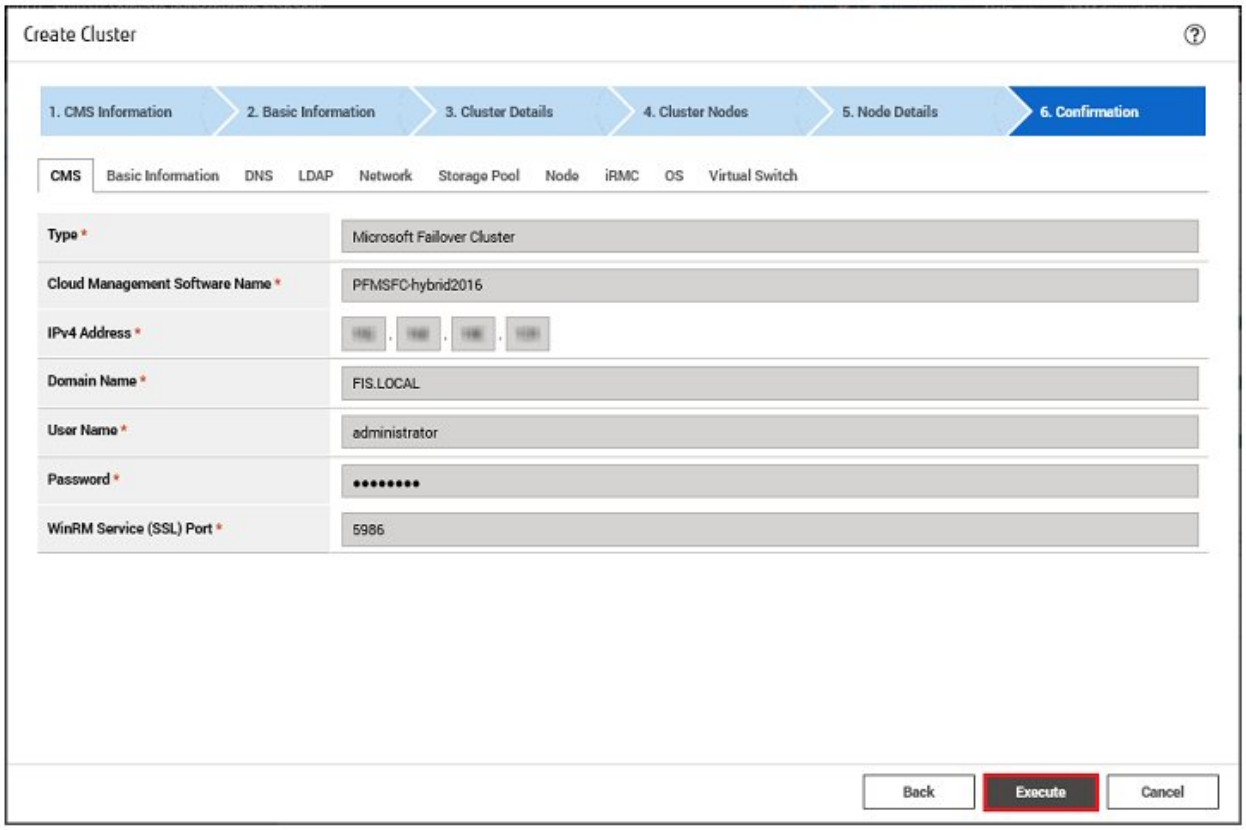
8. If a profile has not been assigned to the target server, select the [Select] button in the [Profile] item, select the profile to be assigned, and then select the [Next] button.

9. Enter each parameter on the "5. Node Details" screen, and select the [Next] button.

   If executing Cluster Creation again because it was stopped due to an error, select the [Next] button if no parameters must be entered again, and proceed to Step 10.

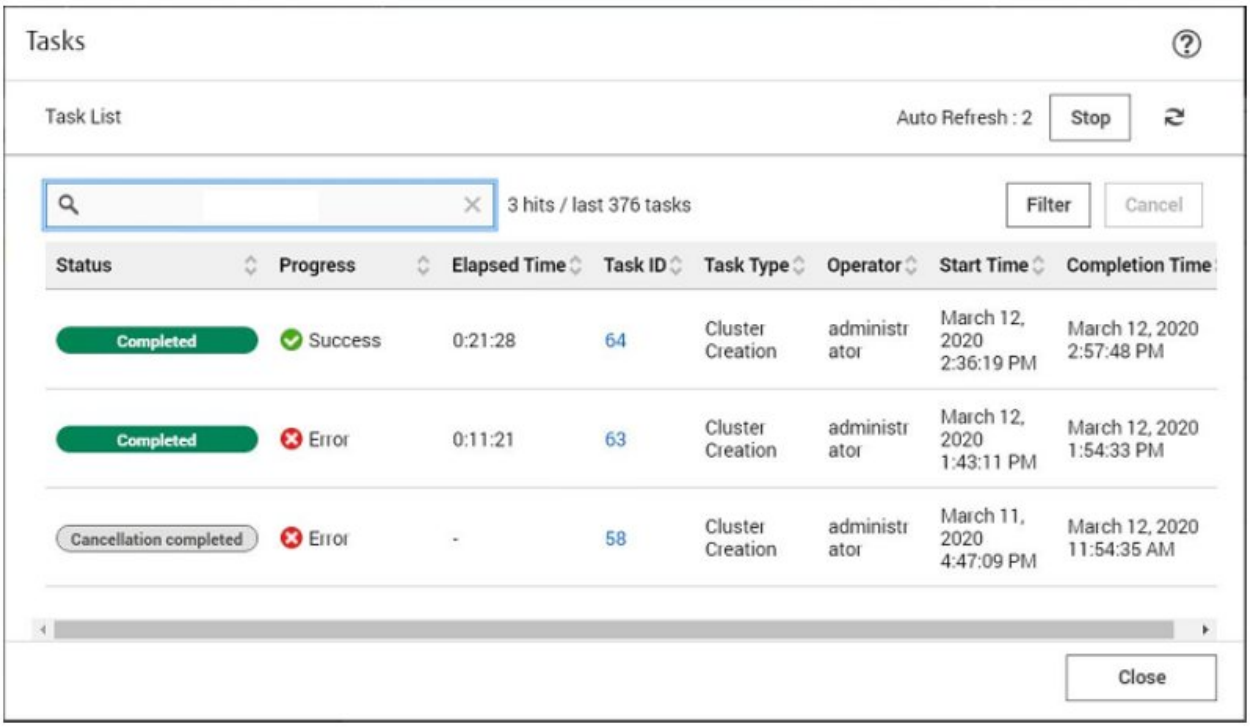


10. Check the parameters on the "6. Confirmation" screen, then select the [Execute] button.



The execution of Cluster Creation is registered as an ISM task.

On the "Tasks" screen, which is displayed when you select [Tasks] on the top of the Global Navigation Menu, tasks whose Task Type is "Cluster Creation" are Cluster Creation tasks.



11. Select [Task ID] whose Task type is "Assigning profile" from the task list displayed in the "Tasks" screen.

Note

- During task execution of Cluster Creation for the PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI, you must accept the conditions of the license.

  Also, in order to ensure stable operation, apply the latest Windows update programs.

  Execute the following Step 12 to 27 within 180 minutes after completing profile assignment. Note that the following message is output in the ISM Event Logs and Cluster Creation will time out and finish with an error if the time is exceeded.

  ```
  50215309: Failed to create cluster. An error occurred during the setting process of the
  Cluster Creation task. (The task type setting process retried out; task type = Cluster
  Creation; id = xxxx; task item set name = OS Installation; task item name = Wait Hyperv OS
  Boot; detail code = E010205)
  ```

  If Cluster Creation times out and finishes with an error, execute up to Step 27, and then execute Step 1 to 11 to execute Cluster Creation again.

  Even if Cluster Creation times out and ends with an error during the execution of Step 12 to 27, continue and execute to Step 27.

  You can execute Step 12 to 27 at the same time for all target servers.

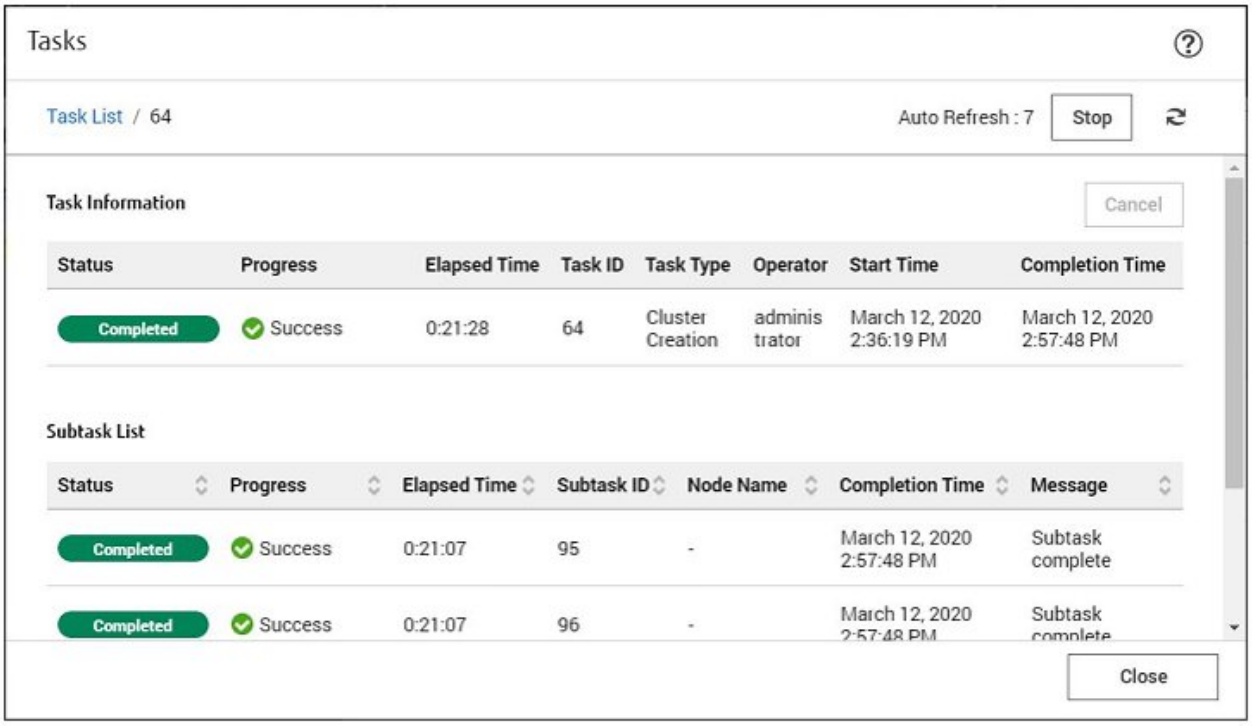
- If the following update programs provided between July 12, 2022 to September 13, 2022 are applied to Hyper-V on the management and workload server that ISM-VA is installed, OS installation on the target server results in an error, and on the "Tasks" screen, the status of the " Assigning profile" task displays as "Assigning profile (OSInstallation) failed".

  In this case, skip the following steps and follow the "6.9.3.3 Manual OS Installation procedure" procedure.

Window Type	Update Program
Windows Server 2016	KB5017305, KB5016622, KB5015808
Windows Server 2019	KB5017315, KB5016690, KB5016623, KB5015880, KB5015811

Point

If you select [Task ID] for "Cluster Creation" from the "Tasks" screen, the "Tasks" screen for "Cluster Creation" is displayed. On this screen, the subtask list is displayed and you can confirm the status of the task by checking the message.



12. After the status of [Assigning profile] task has turned to [Completed], refer to steps 1 and 2 in "6.9.2.10 Confirm networks" to display the iRMC screen of the target server. Log in, and then select [Video Redirection].

    When the security warning is displayed, select the [I accept the risk and want to run this application] checkbox, and then select the [Run] button.

    The video redirection screen of the server is displayed.

Point

When the Video Redirection screen (server screen) is not displayed:

After logging in to iRMC, check the [Settings] tab - [Advanced Video Redirection (AVR)] - [KVM Redirection Type], and confirm that "HTML5 Viewer" is set. If "JViewer (JAVA)" is set, select "HTML5 Viewer", and select the [Apply] button. And then select Video Redirection again.

13. When the "Enter the Product Key" screen is displayed, enter the product key of the installation media, and then select [Next].

Note

Depending on the OS installation media, it may not be displayed.

14. Select the [Accept] button in the License Terms screen.

15. In the [Keyboard] tab, select [Ctrl+Alt+Del] and log in with a user that has Administrator privilege.

    The ServerView Installation Manager script is executed.

Note

On the video redirection screen, do not select the [Restart system] button on the "ServerView Installation Manager" screen and do not restart Windows.

It will not be possible to apply the Windows update program and LAN driver.

16. Use a user with Administrator privileges on the remote desktop to access the Windows OS of the target server.

    Note

    If an error message is displayed and you cannot connect while using remote desktop connection, the cause may be one of the errors described at the following link. From the video redirection screen, use a shared folder to transfer and apply the latest update program on the destination of remote desktop connection.

    https://support.microsoft.com/en-us/help/4093492/credssp-updates-for-cve-2018-0886-march-13-2018

17. Transfer the latest Windows update program to the target server.
18. Apply the Windows update program transferred to the target servers.
19. Check the driver version of your LAN card.

    You can check the LAN driver version at [Control Panel] - [Program] - [Programs and Functions] - [Uninstall or Change programs]. For more information, refer to the documentation included with the downloaded file.

20. Transfer the LAN driver that matches the firmware of your LAN card to the target server.

    Use the LAN driver downloaded in "6.9.2.12 Confirm the firmware version of the LAN card and download the driver."

    If you already applied the LAN driver, this step is not required. Proceed to Step 22.

    Note

    If the target LAN driver is not applied, install the target LAN card driver in Step 21.

21. Apply the LAN driver transferred to the target servers.

    For instructions on how to apply the LAN driver, refer to the documentation included with the file obtained in "6.9.2.12 Confirm the firmware version of the LAN card and download the driver."

22. After the application of the Windows update program has been completed, the screen to confirm the restart is displayed. Select the [Close] button and then, close the remote desktop to return to the Video Redirection screen.

    If the screen is locked, re-log in as a user with Administrator privileges.

23. If Server Manager is displayed at the front, minimize it to display the "SVIM Messenger: System Restart Required" screen.
24. Select the [Restart system] button when the "SVIM Messenger: System Restart Required" screen is displayed.

    The "Sign out" screen is displayed and the server is restarted.

25. After restarting, log in with a user that has Administrator privilege.
26. Delete the Windows update program transferred in Step 17.
27. Delete the LAN driver transferred in Step 20.
28. Repeat Step 12 to 27 for all target servers.
29. Check that the status of "Cluster Creation" has become "Completed."

Note

- If an error is displayed on the ISM "Tasks" screen, check the ISM event log. Confirm the message by referring to "ISM for PRIMEFLEX Messages" and take action.

  After the error is resolved, execute Cluster Creation again.

  If the OS installation with Profile Management of ISM (Assigning profile tasks) ends normally, do not power off the target server when executing again.

- For the settings of the virtual network for workload on the target server, set them according to your environment.

6.9.3.2 Cluster Expansion procedure

This section describes the procedure for executing Cluster Expansion of ISM for PRIMEFLEX.

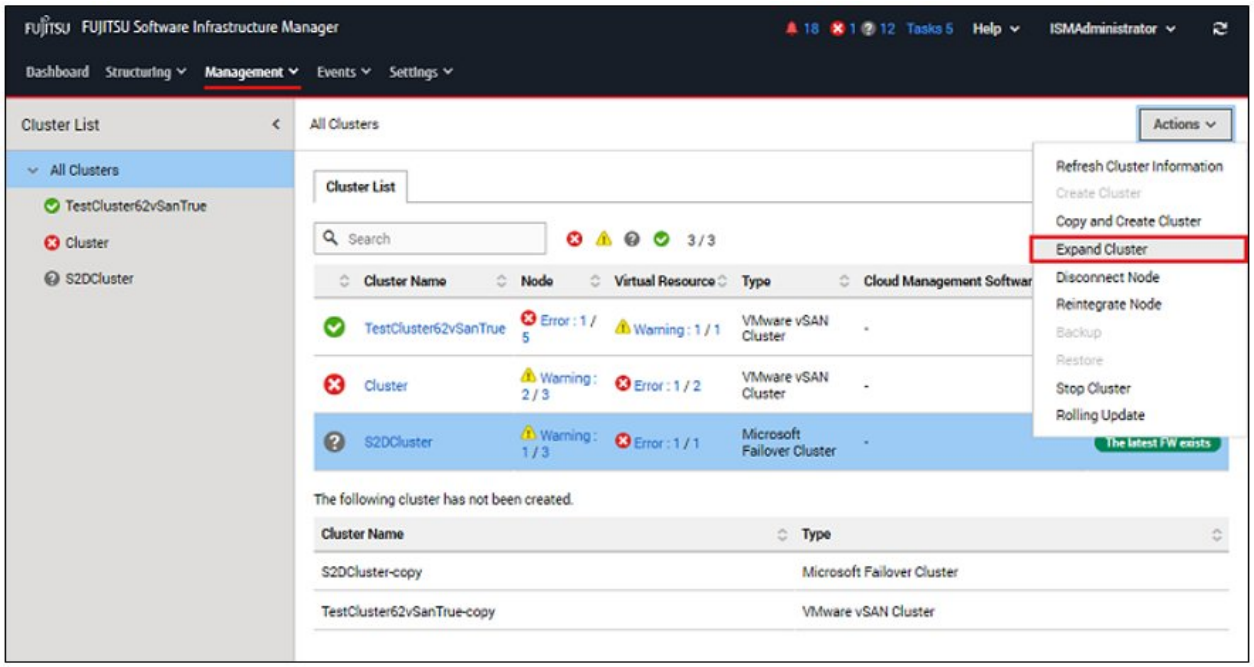
Note

Do not execute Cluster Expansion while other ISM for PRIMEFLEX functions are being executed. Cluster Expansion will fail. Check the ISM event log. Confirm the message by referring to "ISM for PRIMEFLEX Messages" and take action.

For ISM for PRIMEFLEX functions, refer to "2.12 Functions of ISM for PRIMEFLEX" in "User's Guide."

1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster].

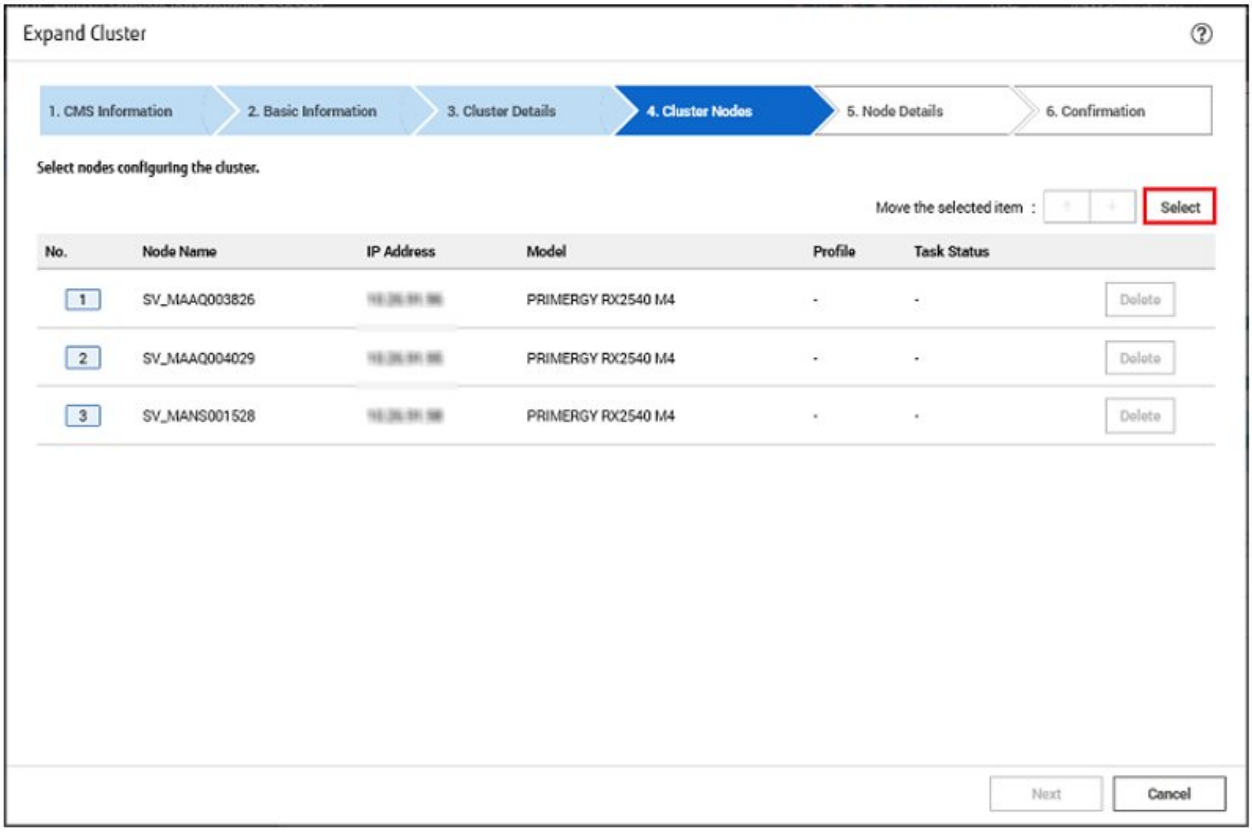
   The "Cluster List" screen is displayed.
3. Select [<Target cluster>], and then from the [Actions] button, select [Expand Cluster].



The "Expand Cluster" wizard is displayed.

4. Select the [Select] button on the "4. Cluster Nodes" screen, and then on the displayed "Target nodes selection" screen, select the target server.

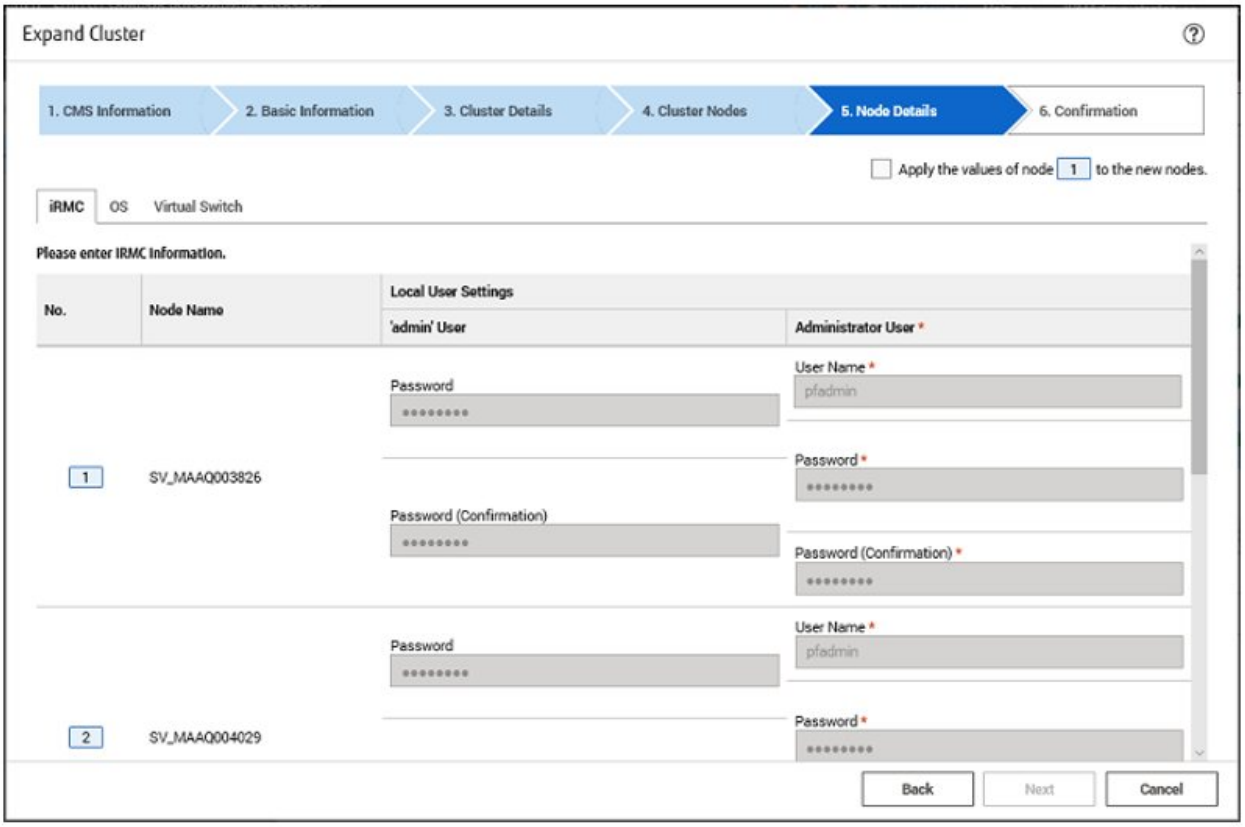
   If executing Cluster Expansion again because it was stopped due to an error, this procedure is not required. Select the [Next] button and proceed to Step 6.



5. If a profile has not been assigned to the target server, select the [Select] button in the [Profile] item, select the profile to be assigned, and then select the [Next] button.

6. Enter each parameter for the target server on the "5. Node Details" screen, and select the [Next] button.

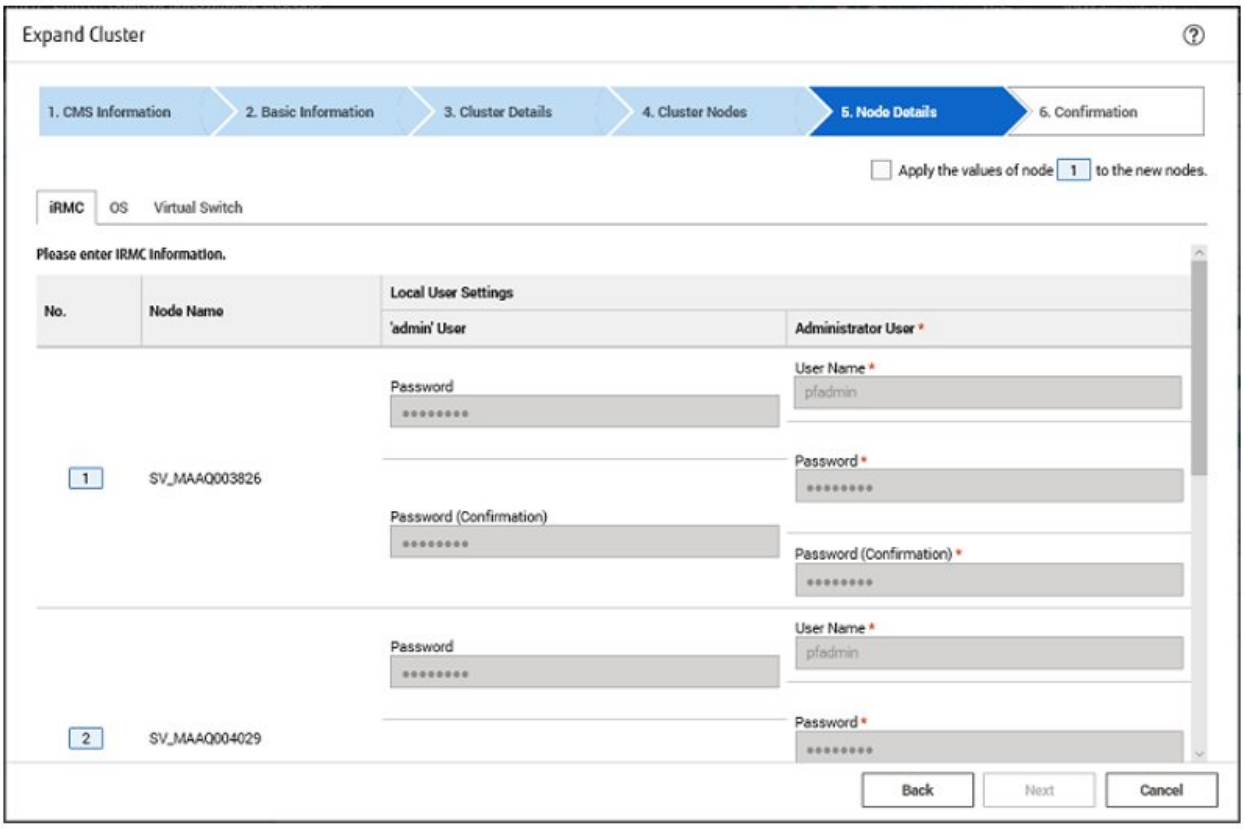
   If executing Cluster Expansion again because it was stopped due to an error, select the [Next] button if no parameters must be entered again, and proceed to Step 7.



Note

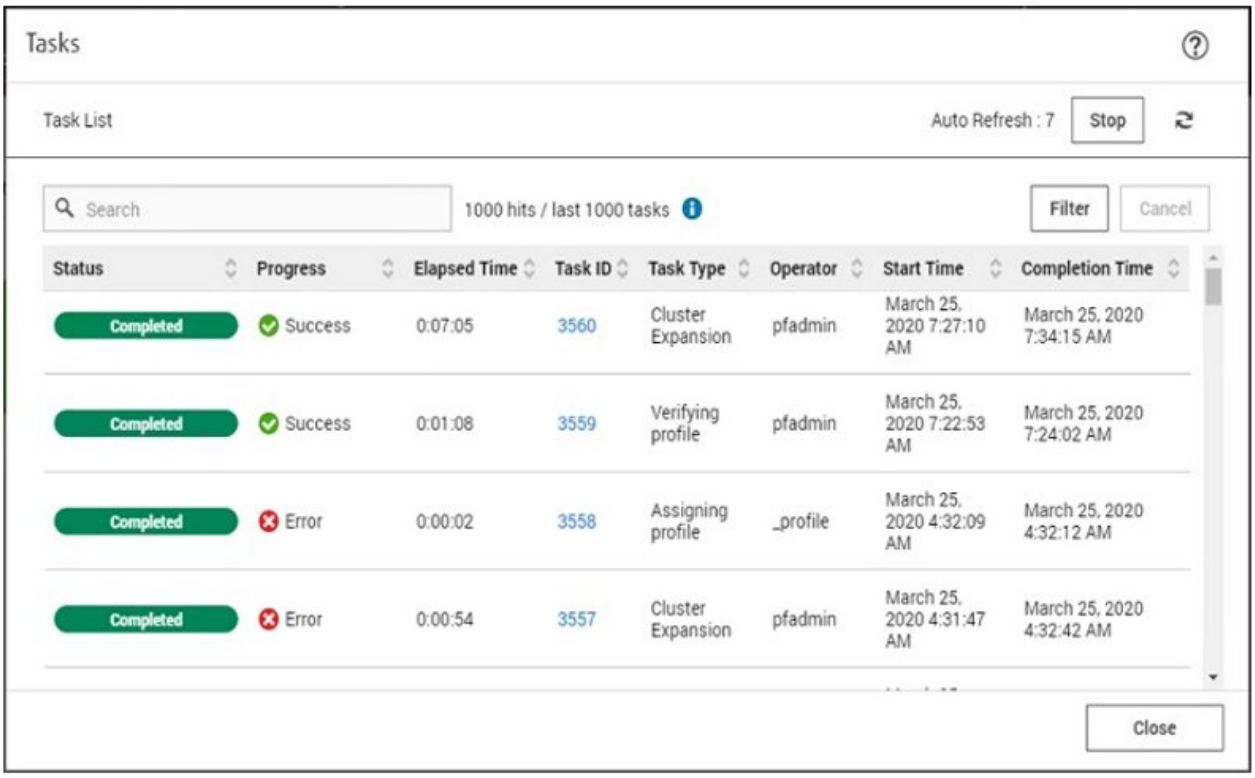
For details on Cluster Definition Parameters, refer to "Chapter 3 Parameter List for Cluster Definition Parameters Settings" in "ISM for PRIMEFLEX Parameter List."

7. Check the parameters on the "6. Confirmation" screen, then select the [Execute] button.



The execution of Cluster Expansion is registered as an ISM task.

On the "Tasks" screen, which is displayed when you select [Tasks] on the top of the Global Navigation Menu, tasks whose Task Type is "Cluster Expansion" are Cluster Expansion tasks.



8. Select [Task ID] whose Task type is "Assigning profile" from the task list displayed in the "Tasks" screen.

Note

- During task execution of Cluster Expansion for the PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI, you must accept the conditions of the license.

  Also, in order to ensure stable operation, apply the latest Windows update programs.

  Execute the following Step 9 to 24 within 180 minutes after completing profile assignment. Note that the following message is output in the ISM Event Logs and Cluster Expansion will time out and finish with an error if the time is exceeded.

  ```
  50215109: Failed to execute Cluster Expansion. An error occurred during the setting process of the Cluster Expansion task. (The task type setting process retried out; task type = Cluster Expansion; id = xxxx; task item set name = OS Installation; task item name = Wait Hyperv OS Boot; detail code = E010205)
  ```

  If Cluster Expansion times out and finishes with an error, execute up to Step 24, and then execute Step 1 to 8 to Cluster Expansion again.

  Even if Cluster Expansion times out and ends with an error during the execution of Step 9 to 24, continue and execute to Step 24.

  You can execute Step 9 to 24 at the same time for all target servers.

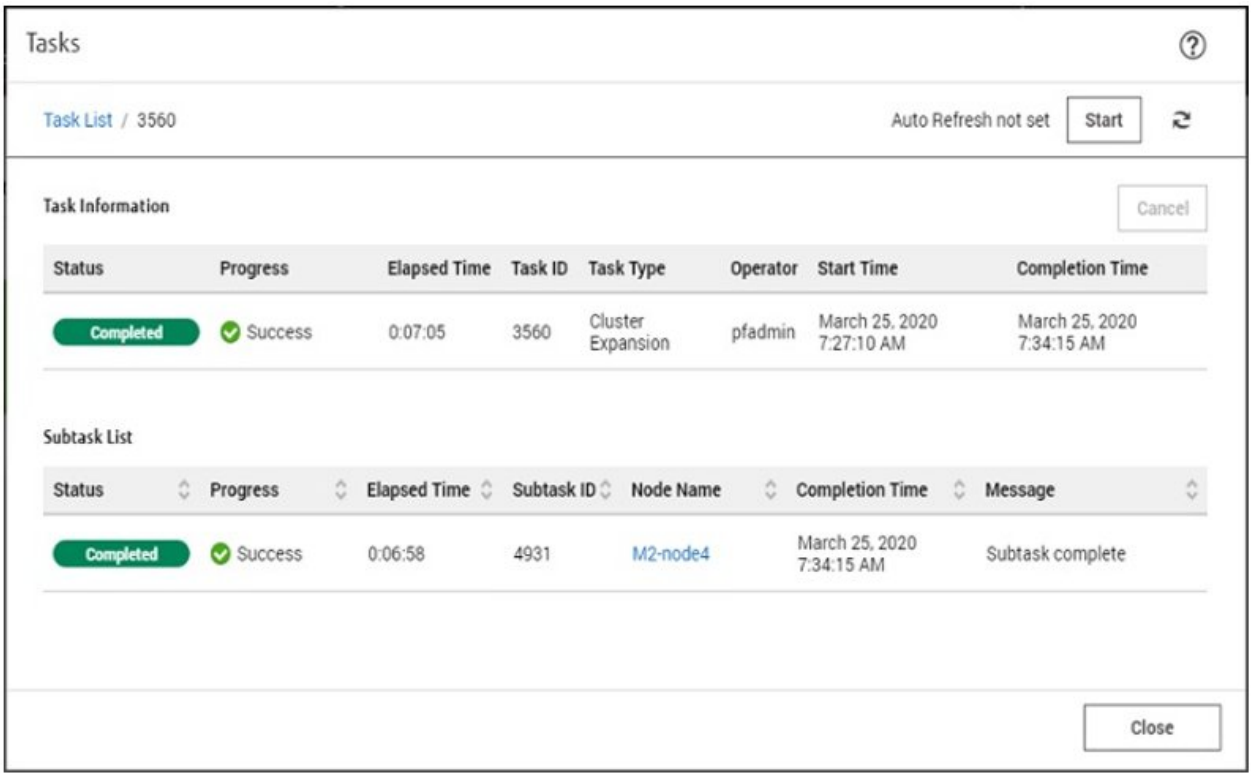
- If the following update programs provided between July 12, 2022 to September 13, 2022 are applied to Hyper-V on the management and workload server that ISM-VA is installed, OS installation on the target server results in an error, and on the "Tasks" screen, the status of the " Assigning profile" task displays as "Assigning profile (OSInstallation) failed".

  In this case, skip the following steps and follow the "6.9.3.3 Manual OS Installation procedure" procedure.

Window Type	Update Program
Windows Server 2016	KB5017305, KB5016622, KB5015808
Windows Server 2019	KB5017315, KB5016690, KB5016623, KB5015880, KB5015811

Point

If you select [Task ID] for "Cluster Expansion" from the "Tasks" screen, the "Tasks" screen for "Cluster Expansion" is displayed. On this screen, the subtask list is displayed and you can confirm the status of the task by checking the message.



9. After the status of [Assigning profile] task has turned to [Completed], display the iRMC screen of the target server, log in, and then select [Video Redirection].

   When the security warning is displayed, select the [I accept the risk and want to run this application] checkbox, and then select the [Run] button.

   The video redirection screen of the server is displayed.

10. Select the [Accept] button in the License Terms screen.

11. When the "Enter the Product Key" screen is displayed, enter the product key of the installation media, and then select [Next].

    Note

    Depending on the OS installation media, it may not be displayed.

12. In the [Keyboard] tab, select [Ctrl+Alt+Del] and log in with a user that has Administrator privilege.

    The ServerView Installation Manager script is executed.

    Note

    On the video redirection screen, do not select the [Restart system] button on the "ServerView Installation Manager" screen and do not restart Windows.

    It will not be possible to apply the Windows update program and LAN driver.

13. Use a user with Administrator privileges on the remote desktop to access the Windows OS of the target server.

Note

If an error message is displayed and you cannot connect while using remote desktop connection, the cause may be one of the errors described at the following link. From the video redirection screen, use a shared folder to transfer and apply the latest update program on the destination of remote desktop connection.

https://support.microsoft.com/en-us/help/4093492/credssp-updates-for-cve-2018-0886-march-13-2018

14. Transfer the same Windows update program as that of the current cluster to the target server.
15. Apply the Windows update program transferred to the target servers.
16. Check the driver version of your LAN card.

    You can check the LAN driver version at [Control Panel] - [Program] - [Programs and Functions] - [Uninstall or Change programs]. For more information, refer to the documentation included with the downloaded file.
17. Transfer the LAN driver that matches the firmware of your LAN card to the target server.

    Use the LAN driver downloaded in "6.9.2.12 Confirm the firmware version of the LAN card and download the driver."

    If you already applied the LAN driver, this step is not required. Proceed to Step 19.

Note

If the target LAN driver is not applied, install the target LAN card driver in Step 18.

18. Apply the LAN driver transferred to the target servers.

    For instructions on how to apply the LAN driver, refer to the documentation included with the file obtained in "6.9.2.12 Confirm the firmware version of the LAN card and download the driver."
19. After the application of the Windows update program has been completed, the screen to confirm the restart is displayed. Select the [Close] button and then, close the remote desktop to return to the Video Redirection screen.

    If the screen is locked, re-log in as a user with Administrator privileges.
20. If Server Manager is displayed at the front, minimize it to display the "SVIM Messenger: System Restart Required" screen.
21. Select the [Restart system] button when the "SVIM Messenger: System Restart Required" screen is displayed.

    The sign out screen is displayed, and the server is restarted.
22. After restarting, log in with a user that has Administrator privilege.
23. Delete the Windows update program transferred in Step 14.
24. Delete the LAN driver transferred in Step 17.
25. Repeat Step 9 to 24 for all target servers.
26. Check that the status of "Cluster Expansion" has become "Completed."

Note

- If an error is displayed on the ISM "Tasks" screen, check the ISM event log. Confirm the message by referring to "ISM for PRIMEFLEX Messages" and take action.

  After the error is resolved, execute Cluster Expansion again.

  If the OS installation with Profile Management of ISM (Assigning profile tasks) ends normally, do not power off the target server when executing again.
- For the settings of the virtual network for workload on the target server, set them according to your environment.

6.9.3.3 Manual OS Installation procedure

This section describes the procedure for executing Manual OS Installation of ISM for PRIMEFLEX.

Step 1 to 52 can be executed in parallel for all target servers.

1. On the "Tasks" screen, when the status of the "Assigning profile" task is displayed as "Assigning profile (OSInstallation) failed," refer to steps 1 and 2 in "6.9.2.10 Confirm networks" to display the iRMC screen of the target server. log in, and then select [Video Redirection].

   The video redirection screen (server screen) is displayed.

   Point

   When the Video Redirection screen (server screen) is not displayed:

   After logging in to iRMC, check the [Settings] tab - [Advanced Video Redirection (AVR)] - [KVM Redirection Type], and confirm that "HTML5 Viewer" is set. If "JViewer (JAVA)" is set, select "HTML5 Viewer", and select the [Apply] button. And then select Video Redirection again.

2. From the video redirection menu on the upper-right of the screen, select [Select...] of CD image, select the media of ServerView Installation Manager, and select [Open].
3. From the video redirection menu on the upper-right of the screen, select [Start Media]. (For iRMC S6, do not select the checkbox next to Media Boost.)
4. From the video redirection menu, select [Power] - [Power On Server or Power Cycle].
   Select [Yes] for the execution confirmation dialog.
   Select [OK] for the successfully completed dialog.
5. Press the [F12] key on the BIOS screen to display the Boot Menu screen. On the Boot Menu screen, select [Fujitsu Virtual CDROM0 X.XX], and press the [Enter] key.
6. On the language selection screen, select [en - KeyboardLayout US].
7. On the displayed "Parameter dialog" screen, set "Keyboard layout:" to [US - International], and then select [OK].

   From Step 8, procedures are for the case that you selected "US - International."
8. In "Welcome to ServerView Installation Manager," select [Deployment].
9. In "Installation Manager Deployment Process Selection," select "Customized" and select [Next].
10. In "Configure your Unattended Operating System Installation," select the following in "Select the operating system" and then select [Next].

Item	Setting Value
Select the operating system	Windows
	MS Windows Server 2016 or MS Windows Server 2019
	Windows Server 2016 Datacenter or Windows Server 2019 Datacenter
	(first release)

11. In "Configuration for Disks and RAID Controllers," select [Remove Partition] for all the disks. Select [OK] for all Warnings.
12. In the already created RAID disk (lsi logical volume, mscc logical volume, or adaptec logical volume), select [Add Partition]. Expand the tree of the added partition, set "Partition Size" to "Maximum" and then select [Apply]. Then select [Next].
13. In "Select the Installation Image," set the following and select [Next].
    - For MS Windows Server 2016
      - In "Type of the Installation Source Medium," select the purchased media.
      - For PRIMERGY Media, select "Fujitsu OEM."

- Microsoft official media/PRIMERGY Media (downgrade), select " Microsoft."
- In "Type of Installation," select "Full."
- In "Setup Language," select the language to use (for some media, unselectable).

- For MS Windows Server 2019
  - In "Type of the Installation Source Medium," select the purchased media.
  - For PRIMERGY Media, select "Fujitsu OEM."
  - For Microsoft official media, select "Microsoft."
  - In "Type of Installation," select "Full."
  - In "Setup Language," select the language to use (for some media, unselectable).

14. Enter the following in "Basic Settings" and then select [Next].

Item	Setting Value
Name	PRIMEFLEX
Organization name	FUJITSU
Computer name	(Arbitrary)
Administrator password	PasZw0rd
Time zone	For MS Windows Server 2016: (Arbitrary)
	For MS Windows Server 2019: Tokyo Standard Time
Format, Language	(Language to be set)
Keyboard	(Keyboard to be set)

15. In "System Settings," select [Next] with the default settings.
16. In "TCP/IP System," select [Next] with the default settings.
17. In "Roles and Features," select [Show Details] with "SNMP Service" checked.

    Implement the following in the expanded box.

    - Select "public: Read_only" of "Accept Community Name:", and select [remove]
    - Check "Send Authentication Trap"

18. Select [Next].
19. In "Additional Parameters," select "enable Remote Desktop" in "Remote Desktop", and then select [Next].
20. In the "Application Wizard," expand the tree and check only the following items, and then select [Next].

    Clear the checkboxes for all but the following:

    - For MS Windows Server 2016
      - ServerView RAID Manager
      - Software Support Guide (only when the language settings in the Windows OS is Japanese. This is not selectable if the setting is one other than Japanese.)
    - For MS Windows Server 2019
      - ServerView Agents
      - ServerView RAID Manager
      - Software Support Guide (only when the language settings in the Windows OS is Japanese. This is not selectable if the setting is one other than Japanese.)

21. Confirm that the setting values in "Summary" are correct. (More specifically, confirm that PartitionSize is set to AUTOMATIC.) Select "Start Installation."

    The installation is started.

22. If the screen of "Please Insert w2k19x64 media" is displayed, from the video redirection menu on the upper-right of the screen, select [Stop Media] to clear the connect the ServerView Installation Manager media. Select [Select...] of CD image, select the Windows OS media, and select [Open].

23. From the video redirection menu on the upper-right of the screen, select [Start Media].

24. If the message "Please remove SVIM/OS media" is displayed is displayed, from the video redirection menu on the upper-right of the screen, select [Stop Media] to clear the connection of OS media, and select [OK].

    The OS is restarted.

25. If the "Windows boot manager" screen is displayed after restarting the OS, select "Windows Server 2019 or Windows Server 2016."

26. When the "Enter product key" screen is displayed, enter the product key of the installation media and select [Next].

    Note

    Depending on the OS media, this may not be displayed

27. When "License terms" is displayed, check the contents and then select [Accept].

28. Select [Ctrl + Alt + Del] from [Keyboard] tab, and log in as a user with Administrator privileges.

    The ServerView Installation Manager script is executed.

    Note

    On the video redirection screen, do not select the [Restart system] button on the "ServerView Installation Manager" screen, or do not restart Windows.

    It will not be possible to apply the Windows update program and LAN driver.

29. Select [Server Manager] - [Local Server] - [Slot 02 Port 1].
    (This is the example of when setting "02" for the slot ID.)

30. On the Network Connections screen, right-click on the network name for [Slot 02 Port 1], and then select [Property].

31. On the Property screen, select [Internet Protocol Version 4 (TCP/IPv4)], and then select [Property].

32. On the "Internet Protocol Version 4 (TCP/IPv4)" on the property screen, check [Use the following IP address], enter the following information, and select [OK].

Item	Setting Value
IP address	Enter the IP address in the IPv4 format
Subnet mask	Enter the subnet mask in the IPv4 format
Default gateway	Enter the gateway IP address in the IPv4 format

33. On the Property screen, select [Close].

34. Use a user with Administrator privileges on the remote desktop to access the Windows OS of the target server.

    Note

    If an error message is displayed and you cannot connect while using remote desktop connection, the cause may be one of the errors described at the following link. Use a shared folder from the video redirection screen to forward and apply the latest update programs to the destination of remote desktop connection.

https://support.microsoft.com/en-us/help/4093492/credssp-updates-for-cve-2018-0886-march-13-2018

35. Transfer the latest Windows update program to the target server.

36. Apply the Windows update program transferred to the target servers.

37. Open Explorer and transfer the postscript_ClusterOperation in the following folder:

    - C:\PostInstall\UserApplication\postscript_ClusterOperation
      (Create the UserApplication folder under C:\PostInstall\ in advance.)
    - For postscript_ClusterOperation, access "ftp://<ISM-VA IP address>/Administrator/ftp" via FTP and download the ISM postscript_ClusterOperation.

38. Open the command prompt with administrator privilege and execute the following command.

```
cd C:\PostInstall\UserApplication\postscript_ClusterOperation\
WinSvr_Setting.bat
```

39. Open Explorer and confirm that the following two holders are created under C:\FISCRB\.

    - Log folder
    - Powershell folder

    If the above two folders were created, the bat file was successfully executed.

    If the above two folders were not created, empty the folder under C:\FISCRB\, and reconfirm the path name in Step 37, and then repeat Step 38.

40. Check the driver version of your LAN card.

    You can check the LAN driver version at [Control Panel] - [Program] - [Programs and Functions] - [Uninstall or Change programs]. For more information, refer to the documentation included with the download file.

41. Transfer the LAN driver that matches the firmware of your LAN card to the target server.

    Use the LAN driver downloaded in "6.9.2.12 Confirm the firmware version of the LAN card and download the driver."

    If you already applied the target LAN driver, this step is not required. Proceed to Step 44.

Note

If the target LAN driver is not applied, install the target LAN card driver in Step 42.

42. Apply the LAN driver transferred to the target servers.

    For instructions on how to apply the LAN driver, refer to the manual included in the file downloaded in "6.9.2.12 Confirm the firmware version of the LAN card and download the driver."

43. Register a record in DNS.

    - Add the Hyper-V host record to <domain name> of the forward lookup zone.

Item	Setting Value
Host IP address	<IP address>
Host name	<System name>

    - Add the Hyper-V host to the reverse lookup zone.

Item	Setting Value
Host IP address	<IP address>
Host name	<System name>

44. Join the domain.

    a. Right-click the Windows button, and select [System] - [System Properties].

    b. Select [Computer Name] tab - [Change].

    c. Enter the followings:

Item	Setting Value
Belonging group	Check domain (D)
Domain name	<domain name>

    d. Select the [OK] button, and enter the user name and password for Active Directory.

45. After the application of the Windows update program has been completed, the screen to confirm the restart is displayed. Select the [Close] button and then, close the remote desktop to return to the video redirection screen.

    If the screen is locked, re-log in as a user with Administrator privileges.

46. If Server Manager is displayed at the front, minimize it to display the "SVIM Messenger: System Restart Required" screen.

47. On the "SVIM Messenger: System Restart Required" screen, select the [Restart system] button.

    The "Sign out" screen is displayed, and the server is restarted.

48. After restarting, log in as a user with Administrator privileges.

49. Delete the Windows update program transferred in Step 35.

50. Delete the LAN driver transferred in Step 41.

51. Execute the assign of advanced profiles.

    a. Log in to ISM as an ISM administrator (who belongs to an Administrator group and has an Administrator role.)

    b. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles], and then select the profile of the target host.

    c. From the [Actions] button, select [Assign/Reassign Profile], and select the [Enable Advanced Settings] checkbox on the upper-right of the screen. And then select [Handle profile as assigned in ISM without actually assigning it to the node.], and select [Confirm]. (Select [Yes] on the "Caution" screen.)

    d. Select the [Above contents are correct.] checkbox, and then select [Assign].

    e. Confirm that the status of the target host is [Assigned].

52. Edit the OS information of nodes.

    a. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].

    b. On the "Node List" screen, select the target node.

    c. Select the [OS] tab.

    d. Select [OS Actions] - [Edit OS Information] and enter the following settings, and then select the [Apply] button.

Item	Setting Value
OS Type	WindowServer
OS Version	Applicable version
OS IP Address	OS IP address
Domain Name	<blank>
Account	Administrator
Password	PasZw0rd
Password (for confirmation)	PasZw0rd

Item	Setting Value
OS Connection Port Number	5986

53. Execute Step 1 to 52 on all target servers.
54. Re-execute Cluster Creation/Cluster Expansion.
55. Check that the status of execution of "Cluster Execution/Cluster Expansion" has become "Completed."

6.9.4 Follow-up Processing

This section describes the follow-up processing required after the cluster creation or cluster expansion.

6.9.4.1 Refresh cluster information

Execute the settings to monitor new clusters and target servers with Cluster Management. After that, refresh the cluster information.

This operation is required for setting a new cluster when Cluster Creation is used. This operation is not required when Cluster Expansion is used.

(1) Add the Service Principal Name for Active Directory

This operation is required when Cluster Creation is used. This operation is not required when Cluster Expansion is used.

Register a Service Principal Name (SPN) for a new cluster in Active Directory.

1. Execute the following command to register the Service Principal Name (SPN) of a new cluster in Active Directory.

```
>setspn -A HOST/<IP address of monitoring target cluster> <Name of monitoring target cluster>
```

2. Execute the following command and check that the service principal name of the monitored cluster is registered in Active Directory.

```
>setspn -L <Name of monitoring target cluster>
```

If HOST/<IP address of monitoring target cluster> is displayed as in the following, the SPN of the WinRM service is registered.

```
>setspn -L <Name of monitoring target cluster>
HOST/<IP address of monitoring target cluster>
```

(2) Configure Kerberos delegation for Active Directory

The Kerberos delegation of all target servers and new clusters is configured in Active Directory.

This operation is required for configuring Kerberos delegation of a new cluster when Cluster Creation is used. This operation is not required when Cluster Expansion is used.

1. Log in to the Active Directory server.
2. Open Server Manager.
3. From the [Tools] button, select [Active Directory Users and Computers].
4. Open the domain, then open the [Computers] folder.
5. On the right side of the screen, right-click on <Cluster node name> or <Cluster name>, then select [Properties].
6. In the [Delegation] tab, select the [Trust this computer for delegation to any service (Kerberos only)] checkbox if it is cleared.
7. Select the [OK] button, then repeat Step 5 to 6 for all nodes configuring the cluster and clusters.

(3) Refresh cluster information

Retrieve the information of the virtualized platform on the ISM GUI and update the displayed information.

For details, refer to "2.12.1.3 Refreshing cluster information" in "User's Guide."

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster].

   The "Cluster List" screen is displayed.

2. From the [Actions] button, select [Refresh Cluster Information].

3. Select [Yes] on the "Refresh Cluster Information" screen.

4. Check that the update of the cluster information has become "Complete," then after waiting a while, refresh the ISM GUI screen (select the [Refresh] button on the upper-right of the screen).

The following procedure must be performed when Cluster Creation is used. This operation is not required when Cluster Expansion is used.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster].

2. Check that Cluster Definition Parameters are displayed in the [<Target Cluster>] - [Cluster Definition Parameters] tab.

   If Cluster Definition Parameters are not displayed, wait for a while and then refresh the screen (select the [Refresh] button on the upper-right of the screen) and repeat until it is displayed.

6.9.4.2 Confirm resources

Use the following procedure to check the status of a PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI cluster.

1. Access the Failover Cluster Manager to confirm the following:

   - That [<Cluster name>] is displayed
   - That the node of the target server is displayed in [<Cluster name>] - [Node]
   - That there are no warnings or errors in the cluster events of the [<Cluster name>]
   - That the status of [<Cluster name>] - [Node] - [<Node name>] is "Running"
   - That the health status of all the disks in [<Cluster name>] - [Storage] - [Pool] - [<Pool name>] - [Physical disks] is "Normal"
   - That the health status of [<Cluster name>] - [Storage] - [Pool] - [<Pool name>] - [Virtual disk] is "Normal" when using Cluster Expansion

   Note

   If you cannot confirm the points above, collect maintenance data and contact your local Fujitsu customer service partner.

2. From the Global Navigation Menu on the ISM GUI, select [Management] - [Virtual Resource].

   The "All Storage Pool" screen is displayed.

3. From the [Actions] button, select [Refresh Virtual Resource Information].

   The information is refreshed.

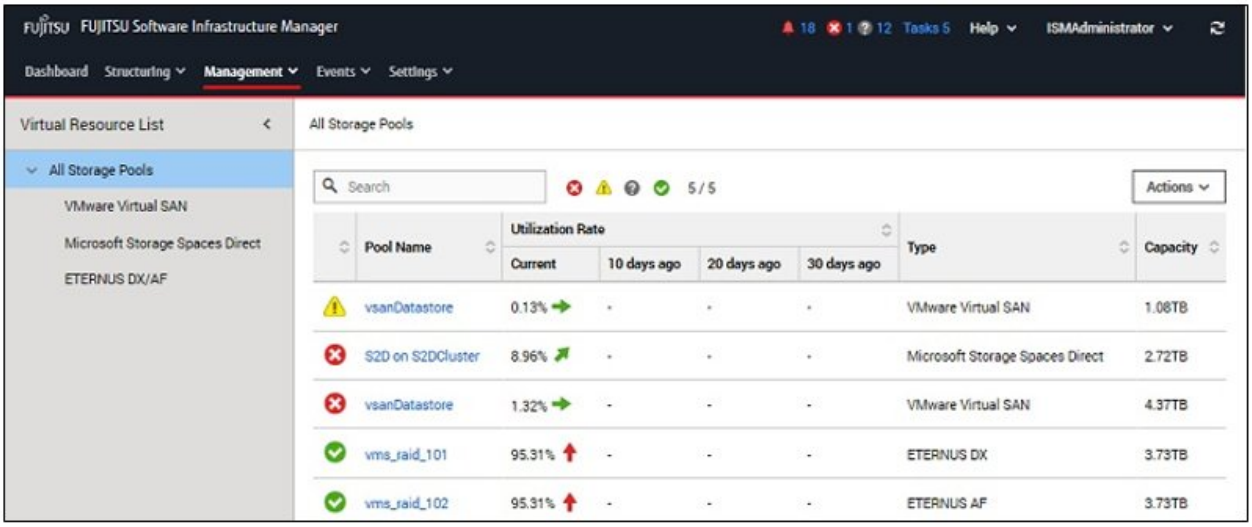
4. After the information is refreshed, check the following content:

   - For Cluster Creation

     Confirm that the target storage pool is displayed.

- For Cluster Expansion

  Confirm that the [Capacity] of the target storage pool has increased.



Note

- Even when Cluster Creation has completed successfully, if the storage pool is not displayed, communication for the PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI network could fail. Check the settings and the wiring of the switch.
- Even when Cluster Expansion has completed successfully, if the previously checked storage pool has not been expanded, communication for the PRIMEFLEX for Microsoft Storage Spaces Direct/PRIMEFLEX for Microsoft Azure Stack HCI network could fail. Check the settings and the wiring of the switch.

  In order to confirm that the expansion is actually executed, first check the current storage pool capacity in advance.
- After completion of the task, if the warning is displayed in the cluster event of the [<Cluster name>] in the Failover Cluster Manager, confirm the event ID and the details of the event. If the following content is included, it is only a temporary warning and is not an error. Execute [Resetting of the latest event] in the right pane.

Event ID	Details of Event
5120	Cluster Shared Volume 'Volume1'('Cluster virtual disk (Vdisk)') is no longer available on this node because of 'STATUS_DEVICE_NOT_CONNECTED (c000009d)'. All I/O will temporarily be queued until a path to the volume is reestablished.

Point

To execute Monitoring of SSD lifetime in ServerView RAID Manager, refer to "FUJITSU Software ServerView Suite ServerView RAID Manager" to perform the required settings.

6.9.4.3 Delete unnecessary files

Delete unnecessary files with the following procedure after completing Cluster Creation or Cluster Expansion.

(1) Deleting certificates

The certificates created in "6.9.2.1 Create certificates for target servers" are transferred and registered to the target server when installing an OS. Use the following procedure to delete the certificate.

Execute for all target servers.

1. Use remote desktop to access the Windows OS of the target server.
2. Open Explorer and delete the following files:
   - C:\PostInstall\UserApplication\postscript_ClusterOperation\<computer name that is set for the ISM profile>.cer
   - C:\PostInstall\UserApplication\postscript_ClusterOperation\<computer name that is set for the ISM profile >.pfx
   - C:\DeploymentRepository\Add-on\UserApplication\postscript_ClusterOperation\<computer name that is set for the ISM profile>.cer
   - C:\DeploymentRepository\Add-on\UserApplication\postscript_ClusterOperation\<computer name that is set for the ISM profile>.pfx

Note

The certificates uploaded to ISM-VA in "6.9.2.1 Create certificates for target servers" have security risks. If you cannot accept this risk, delete the certificate.

If the deletion target file does not exist, you do not need to delete it.

(2) Deleting unnecessary files of the target server

Execute for all target servers.

1. Use remote desktop to access the Windows OS of the target server.
2. Open Explorer and delete all files and directories under the following directories:
   - C:\PostInstall\UserApplication\postscript_ClusterOperation
   - C:\FISCRB\PowershellScript

(3) Deleting unnecessary files in ISM-VA

Execute for ISM-VA.

1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. Delete any files that are no longer needed by checking the following items and referring to "1.4.2 Delete Files Uploaded to ISM-VA."

Item	Value
Root Directory	Administrator/ftp
Directory Name	postscript_ClusterOperation
File Name	The certificate created in (1) in "6.9.2.1 Create certificates for target servers"

6.9.4.4 Disable TLS 1.0/TLS 1.1 of iRMC

This operation is required to use PRIMEFLEX for Microsoft Storage Spaces Direct V2 (PRIMEFLEX for Microsoft Azure Stack HCI V1). Execute settings for all target servers.

Use the following procedure to set TLS 1.0/TLS 1.1 on your iRMC to "Disabled."

1. Connect to the iRMC Web Server on the target server. Start a web browser (IE, etc.) and enter the IP address of the iRMC of the target server in the address bar.
2. Enter your username/password and select [Login]. If the iRMC firmware version is 1.60P or later, the "Fujitsu End User Software License Agreement" screen is displayed. Confirm the contents and select the [Agree] button.
3. Select [Settings] - [Services] and clear "Enable TLS 1.0" and "Enable TLS 1.1" from [Web Access] - [Security Protocols].
4. Select the [Apply] button.

   The settings are saved.

Note

Depending on the firmware version of iRMC, "Enable TLS 1.0" may not be displayed.

6.9.4.5 Delete the possible owner of ISM-VA

This operation is required when Cluster Expansion is used. This operation is not required when Cluster Creation is used.

Delete the possible owner to disable ISM-VA on the target servers.

Execute for all target servers.

Use the following procedure to set the possible owner.

1. Use remote desktop to connect to the cluster representative IP (cluster access point).
2. From Failover Cluster Manager, select [<Cluster name>] - [Roles] in the left pane.

   The "Roles" screen is displayed in the center pane.
3. Select ISM-VA from the list.
4. On the screen that is displayed at the bottom of the center pane, select the [Resources] tab.
5. Select ISM-VA that is displayed on the [Resources] tab, right-click on it to select [Properties].
6. Select the [Advanced Policies] tab on the "Properties" screen, clear the checkbox for the target server in [Possible Owners], and then select [OK].

6.9.4.6 Set the processor compatibility of virtual machines

This operation is required when Cluster Expansion is used. This operation is not required when Cluster Creation is used.

This setting is required for adding successor servers to PRIMEFLEX.

By using the processor compatible mode, you can migrate the running virtual machines in the entire host in the cluster.

Execute for all target servers.

Use the following procedure to set the processor compatibility of virtual machines.

1. Use remote desktop to connect to the cluster representative IP (cluster access point).
2. From Hyper-V manager, select the virtual machine that you want to set the processor compatibility from the list.
   If [Status] of the virtual machine is not [Off], right-click on the virtual machine and select [Shut Down].
3. Select [Settings] in the right pane. The "Settings for <Virtual machine name>" screen is displayed.
4. Select [Processor] - [Compatibility].
5. Select the [Migrate to a physical computer with a different processor version] checkbox in [Compatibility], and select [OK].
6. Restart the virtual machine as required.

6.9.4.7 Set the network adapter

This operation is required when Cluster Expansion is used in the following environments. This action is required only for ISM 2.8.0.010.

- Adding the PRIMERGY M6 series server to the PRIMERGY M4 series cluster
- Adding the PRIMERGY M6 series server to the PRIMERGY M5 series cluster

Use the following procedure to set the network adapter with the expanded target server.

The following is an example of when Intel E810 (S26361-F5822-E202 Dual port LAN card (25GBASE)) is mounted.

1. Access the Windows OS of the target server using remote desktop.
2. Right-click on the Windows button and select [Device Manager].
3. Right-click on [Network adapters] of the target, and select [Properties].

4. Select the [Advanced] tab - [SR-IOV], and disable the values, and then select [OK] button.

   If [SR-IOV] is not displayed, in the [Advanced] tab, as [Virtualization] has been selected, select [Properties]. And on the displayed window, clear the [Enable SR-IOV] checkbox, and select the [OK] button.

   Then in the [Advanced] tab, select the [OK] button.

5. Repeat Step 3 and 4 for all target network adapters.

The following procedure is required only when adding the PRIMERGY M6 series server to the PRIMERGY M5 series cluster.

1. From Server Manager, select [Tool] - [Hyper-V Manager].
2. From the <Target server>, select [Hyper-V Settings] - [Live Migrations] - [Advanced Features] - [Performance options] - [SMB], and then select the [OK] button.

6.10 Export/Import/Delete Cluster Definition Parameters

This section describes the procedures to export/import/delete Cluster Definition Parameters.

This function can be used only when the ISM Operation Mode is "Advanced for PRIMEFLEX."

6.10.1 Export Cluster Definition Parameters

This section describes the procedure to export Cluster Definition Parameters.

Cluster Definition Parameters are exported in the format of a text file written in JSON format.

1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster].

   The "Cluster List" screen is displayed.

3. Select the [<Target Cluster>] - [Cluster Definition Parameters] tab of the export target.
4. From the [Parameter Actions] button, select [Export].
5. Select the [Export] button.

   When the export has been completed, the Result screen is displayed.

6. Select the link displayed in [Download URL] to download the file.

   If the file download is complete, the export of the Cluster Definition Parameters is complete.

6.10.2 Import Cluster Definition Parameters

This section describes the procedure to import Cluster Definition Parameters.

Cluster Definition Parameters are imported in the format of a text file written in JSON format.

Note

- If Cluster Definition Parameters are already created in the import target cluster, they cannot be imported. Delete Cluster Definition Parameters in advance.
- The following are the requirements for an ISM-VA that can be used as an import destination. Imports to an ISM-VA that do not meet the following requirements are not available.
  - Cluster Definition Parameters have been exported
  - Node information or profiles for the node configuring the cluster have not been deleted or re-registered

1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster].

   The "Cluster List" screen is displayed.
3. Select the [<Target Cluster>] - [Cluster Definition Parameters] tab of the import target.
4. From the [Parameter Actions] button, select [Import].
5. Select the file selection method in [File selection method], then set the file of the import target in [File Path].
6. Select the [Import] button.
7. From the "Cluster List" screen, select the [<Target Cluster>] - [Cluster Definition Parameters] tab of the import target. If Cluster Definition Parameters are displayed, import of the Cluster Definition Parameters is complete.

Note

You must edit Cluster Definition Parameters after import.

Edit Cluster Definition Parameters according to the following procedure.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster].
2. Select the [<Target Cluster>] - [Cluster Definition Parameters] tab.
3. From the [Parameter Actions] button, select [Edit].

   Passwords are not exported. Enter the values.

For details on Cluster Definition Parameters, refer to "Chapter 3 Parameter List for Cluster Definition Parameters Settings" in "ISM for PRIMEFLEX Parameter List."

6.10.3 Delete Cluster Definition Parameters

This section describes the procedures to delete Cluster Definition Parameters.

1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster].

   The "Cluster List" screen is displayed.
3. Select the [<Target Cluster>] - [Cluster Definition Parameters] tab of the one to be deleted.
4. From the [Parameter Actions] button, select [Delete].
5. Select the [Delete] button.
6. From the "Cluster List" screen, select the [<Target Cluster>] - [Cluster Definition Parameters] tab of the deletion target. If the message "No Cluster Definition Parameters have been created." is displayed, deletion of Cluster Definition Parameters is complete.

Point

If Cluster Definition Parameters of the cluster to be imported already are created, they cannot be imported. If you delete the Cluster Definition Parameters with the operation above, it becomes possible to import.

6.11 Execute Maintenance on Nodes Configuring a Cluster

Execute Node Disconnection or Node Reintegration to perform maintenance operations that involve restarting servers for PRIMEFLEX for VMware vSAN.

This function can be used only when the ISM Operation Mode is "Advanced for PRIMEFLEX."

Node Disconnection/Reintegration is executed according to the following work flow.

Table 6.28 Maintenance work flow for nodes configuring a cluster

Procedure for the maintenance of nodes configuring a cluster		Tasks
1	Preparations	- Migrating virtual machines to a non-maintenance target server
2	Execute Node Disconnection	
3	Maintenance	- Executing maintenance such as replacing expansion boards
4	Execute Node Reintegration	
5	Follow-up Processing	- Migrating virtual machines to maintenance target servers

6.11.1 Operation Requirements

To use Node Disconnection and Node Reintegration, the following requirements must be met.

Common operation requirements for Node Disconnection and Node Reintegration

Operation requirements for target clusters

- The cluster must be the PRIMEFLEX for VMware vSAN cluster
- A cluster of maintenance target servers is registered in the cloud management software
- Cluster Definition Parameters are specified

  For details, refer to "6.8.2.11 Create and edit Cluster Definition Parameters."
- Cluster Management for the target cluster for Node Disconnection/Reintegration has been preset

  For Cluster Management settings, refer to "3.8 Pre-Settings for Managing Virtual Resources/Clusters" in "User's Guide."
- The latest cluster information is displayed

  For details, refer to "2.12.1.3 Refreshing cluster information" in "User's Guide."
- Use the administrator of the vCenter Single Sign-On domain for your cloud management software registration account information
- A configuration of four or more normal nodes

  You cannot use Node Disconnection and Node Reintegration in a configuration of three nodes or less.

Operation requirements for target servers

- Maintenance target servers are registered in ISM

Operation requirements for Node Disconnection

Operation requirements for target clusters

- Not more than one server is powered off in the cluster

Operation requirements for target servers

- All virtual machines on the maintenance target server have been migrated to other servers

  (For vSphere 7.0 Update 1 or later, migrated including the vCLS virtual machine.)

6.11.2 Preparations

This section describes the preparations required before performing maintenance operations for nodes configuring a cluster.

6.11.2.1 Migrate virtual machines to the non-maintenance target server

The operations performed are different depending on the DRS settings.

6.11.2.1.1 When DRS is on

You do not need to migrate virtual machines if DRS is enabled, because virtual machines that are running on maintenance target servers are migrated to other working nodes automatically.

However, the automation level of vSphere DRS must be set to "Automatic."

Confirm the automation level of vSphere DRS with the following procedure.

For vCSA 6.5 and earlier (Flash)

1. Log in to vCSA with vSphere Web Client.
2. From the "Top" screen, select the [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Configure] to confirm that the automation level of vSphere DRS is "Automatic."

For vCSA 6.7 or later (HTML5)

1. Log in to vCSA with vSphere Client.
2. From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Configure] to confirm that the automation level of vSphere DRS is "Automatic."
3. For vSphere 7.0 Update 1 and later, check the health of the vSphere Cluster Service, which is required for vSphere DRS to operate.

   Select [<Cluster Name>] - [Summary] on the "Hosts and Clusters" screen, and check that the [Cluster Service health] value for [Cluster Services] is "Healthy."

6.11.2.1.2 When DRS is off

Use the following procedure to migrate virtual machines if DRS is disabled.

Perform this procedure for all virtual machines running on the maintenance target servers.

For vSphere 7.0 Update 1 or later, migrate the vCLS virtual machine with the following procedures.

For vCSA 6.5 and earlier (Flash)

1. Log in to vCSA with vSphere Web Client.
2. From the "Top" screen, select the [Home] tab - [Inventories] - [Hosts and Clusters].
3. On the screen that is displayed, check if there are any virtual machines running on the maintenance target server.
4. If there are any virtual machines running on the maintenance target server, record the name of the maintenance target server and all of the names of the virtual machines running on that server.
5. Select the virtual machine that is running on the maintenance target server, and then select [<Virtual machine name>] - [Migration].
6. On the "Select the migration type" screen, select [Change compute resource only] and then select the [Next] button.
7. On the "Select a compute resource" screen, select [Hosts], select the destination server for the virtual machine running on the maintenance target server, and then select the [Next] button.
8. On the "Select networks" screen, select the destination network, and then select the [Next] button.
9. On the "Select vMotion priority" screen, select the vMotion schedule, and then select the [Next] button.
10. On the "Ready to complete" screen, check the content displayed, and then select the [Finish] button.
11. Confirm that "Completed" is displayed for the status of [Relocate virtual machine] displayed in [Recent Tasks] .
12. Repeat Step 4 to 10 until there are no virtual machines running on the maintenance target server.

For vCSA 6.7 or later (HTML5)

1. Log in to vCSA with the vSphere Client.
2. From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters].
3. On the screen that is displayed, check if there are any virtual machines running on the maintenance target server.
4. If there are any virtual machines running on the maintenance target server, record the name of the maintenance target server and all of the names of the virtual machines running on that server.
5. Select the virtual machine that is running on the maintenance target server, and then select [<Virtual machine name>] - [Migration].
6. On the "Select the migration type" screen, select [Change compute resource only] and then select the [NEXT] button.
7. On the "Select a compute resource" screen, select [Hosts], select the destination server for the virtual machine running on the maintenance target server, and then select the [NEXT] button.
8. On the "Select networks" screen, select the destination network, and then select the [NEXT] button.
9. On the "Select vMotion priority" screen, select the vMotion schedule, and then select the [NEXT] button.
10. On the "Ready to complete" screen, check the content displayed, and then select the [FINISH] button.
11. Confirm that "Completed" is displayed for the status of [Relocate virtual machine] displayed in [Recent Tasks].
12. Repeat Step 4 to 10 until there are no virtual machines running on the maintenance target server.

6.11.3 Execute Node Disconnection/Reintegration

Use Node Disconnection/Reintegration to disconnect or reintegrate nodes in PRIMEFLEX for VMware vSAN.

Be sure to refer to "6.11.1 Operation Requirements" and check the operation requirements before executing Node Disconnection/Reintegration.

- 6.11.3.1 Node Disconnection procedure
- 6.11.3.2 Node Reintegration procedure

6.11.3.1 Node Disconnection procedure

This section describes the procedure for executing Node Disconnection of ISM for PRIMEFLEX.

Note

Do not execute Node Disconnection while other ISM for PRIMEFLEX functions are being executed. Node Disconnection will fail. Check the ISM event log. Confirm the message by referring to "ISM for PRIMEFLEX Messages" and take action.

For ISM for PRIMEFLEX functions, refer to "2.12 Functions of ISM for PRIMEFLEX" in "User's Guide."

1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster].

   The "Cluster List" screen is displayed.
3. Select [<Target cluster>] and from the [Actions] button, select [Disconnect Node].
4. On the "Disconnect Node" screen, confirm the target cluster.
5. Select the server that you want to disconnect, and then select the [Run] button.

Point

If "Full Data Migration" is selected for the Data Evacuation Mode, all data of the node is migrated to another node. Therefore, it may take certain time for operation depending on the amount of data on the node.

The execution of Node Disconnection is registered as an ISM task.

On the "Tasks" screen, which is displayed when you select [Tasks] on the top of the Global Navigation Menu, tasks whose Task Type is "Node Disconnection" are Node Disconnection tasks.

Point

If you select [Task ID] for "Node Disconnection" from the "Tasks" screen, the "Tasks" screen for "Node Disconnection" is displayed. On this screen, the subtask list is displayed and you can confirm the status of the task by checking the message.

6. Check that the status of "Node Disconnection" has become "Completed."

Note

- If an error is displayed on the ISM "Tasks" screen, check the ISM event log. Confirm the message by referring to "ISM for PRIMEFLEX Messages" and take action.

  After the error is resolved, execute Node Disconnection again.

- In a vCSA 6.7u2 environment, the following Health errors may occur after executing Node Disconnection. You do not need to take any action for these health errors. Errors will be resolved automatically after executing Node Reintegration for the maintenance target servers.

  - Virtual SAN Health alarm, "Hosts disconnected from VC"

  - Connection status and power status of the host

6.11.3.2 Node Reintegration procedure

This section describes the procedure for executing Node Reintegration of ISM for PRIMEFLEX.

Note

Do not execute Node Reintegration while other ISM for PRIMEFLEX functions are being executed. Node Reintegration will fail. Check the ISM event log. Confirm the message by referring to "ISM for PRIMEFLEX Messages" and take action.

For ISM for PRIMEFLEX functions, refer to "2.12 Functions of ISM for PRIMEFLEX" in "User's Guide."

1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster].

   The "Cluster List" screen is displayed.
3. Select [<Target cluster>] and from the [Actions] button, select [Reintegrate Node].
4. On the "Reintegrate Node" screen, confirm the target cluster.
5. Select the server that you want to reintegrate, and then select the [Run] button.

   The execution of Node Reintegration is registered as an ISM task.

   On the "Tasks" screen, which is displayed when you select [Tasks] on the top of the Global Navigation Menu, tasks whose Task Type is "Node Reintegration" are Node Reintegration tasks.

Point

If you select [Task ID] for "Node Reintegration" from the "Tasks" screen, the "Tasks" screen for "Node Reintegration" is displayed. On this screen, the subtask list is displayed and you can confirm the status of the task by checking the message.

6. Check that the status of "Node Reintegration" has become "Completed."

Point

If you cancel a task from ISM or an error is displayed on the ISM "Task" screen, you may need to set maintenance mode for VMware to change the status back to the way it was before Node Reintegration was executed. In this case, the Data Evacuation Mode specified is "Ensure Accessibility."

Note

If an error is displayed on the ISM "Tasks" screen, check the ISM event log. Confirm the message by referring to "ISM for PRIMEFLEX Messages" and take action.

After the error is resolved, execute Node Reintegration again.

6.11.4 Follow-up Processing

This section describes the follow-up process required after executing the maintenance for nodes configuring a cluster of ISM for PRIMEFLEX.

6.11.4.1 Migrate virtual machines to the maintenance target server

After performing maintenance, return the virtual machines that were migrated to another server back to the server that was maintained.

Perform this procedure for all virtual machines that have been migrated to a non-maintenance target server.

For vCSA 6.5 and earlier (Flash)

1. Log in to vCSA with vSphere Web Client.
2. From the "Top" screen, select the [Home] tab - [Inventories] - [Hosts and Clusters].
3. On the screen that is displayed, select the virtual machine that you recorded in "6.11.2.1 Migrate virtual machines to the non-maintenance target server" and then select [<Virtual machine name>] - [Migrate].
4. On the "Select the migration type" screen, select [Change compute resource only], and then select the [Next] button.
5. On the "Select a compute resource" screen, open the cluster and select the maintenance target servers that you recorded in "6.11.2.1 Migrate virtual machines to the non-maintenance target server" and then select the [Next] button.
6. On the "Select networks" screen, select the destination network, and then select the [Next] button.
7. On the "Select vMotion priority" screen, select the vMotion schedule, and then select the [Next] button.
8. On the "Ready to complete" screen, check the content displayed, and then select the [Finish] button.
9. Confirm that "Completed" is displayed for the status of [Relocate virtual machine] displayed in [Recent Tasks].
10. Repeat Step 2 to 8 until all the virtual machines recorded in "6.11.2.1 Migrate virtual machines to the non-maintenance target server" are back on the maintenance target server.

For vCSA 6.7 or later (HTML5)

1. Log in to vCSA with the vSphere Client.

2. From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters].
3. On the screen that is displayed, select the virtual machine that you recorded in "6.11.2.1 Migrate virtual machines to the non-maintenance target server" and then select [<Virtual machine name>] - [Migrate].
4. On the "Select the migration type" screen, select [Change compute resource only], and then select the [Next] button.
5. On the "Select a compute resource" screen, select [Hosts], select the maintenance target servers that you recorded in "6.11.2.1 Migrate virtual machines to the non-maintenance target server" and then select the [Next] button.
6. On the "Select networks" screen, select the destination network for the virtual machine, and then select the [Next] button.
7. On the "Select vMotion priority" screen, select the vMotion schedule, and then select the [Next] button.
8. On the "Ready to complete" screen, check the content displayed, and then select the [Finish] button.
9. Confirm that "Completed" is displayed for the status of [Relocate virtual machine] displayed in [Recent Tasks].
10. Repeat Step 2 to 8 until all the virtual machines recorded in "6.11.2.1 Migrate virtual machines to the non-maintenance target server" are back on the maintenance target server.

6.12 Back up Nodes or vCSA Structuring a Cluster

You can execute Backup to prepare for system recovery from failures in PRIMEFLEX for VMware vSAN.

This function can be used only when the ISM Operation Mode is "Advanced for PRIMEFLEX."

The following is the work flow for executing Backup.

Table 6.29 Work flow for backup of nodes or vCSA structuring a cluster

Backup procedures for nodes or vCSA structuring a cluster		Tasks
1	Preparations	Preparation for a server to store backups
2	Execute Backup	
3	Follow-up Processing	Starting the TSM-SSH service

6.12.1 Operation Requirements

To use Backup, the following requirements must be met.

- Sufficient space on the disk of the backup destination server is available

  The approximate amount of disk space required for backups is as follows:

  - For VMware ESXi backup

    0.05 MB or more per VMware ESXi

  - For vCenter Server Appliance backup

    1 GB + 1 MB or more for each virtual distributed switch

Operation requirements for target clusters

- The cluster must be the PRIMEFLEX for VMware vSAN cluster
- A cluster of backup target servers is registered in the cloud management software
- Cluster Definition Parameters are specified

  For details, refer to "6.8.2.11 Create and edit Cluster Definition Parameters."
- Cluster Management for the cluster of the target server for Backup has been preset

  For Cluster Management settings, refer to "3.8 Pre-Settings for Managing Virtual Resources/Clusters" in "User's Guide."

- The latest cluster information is displayed

  For details, refer to "2.12.1.3 Refreshing cluster information" in "User's Guide."

- PRIMEFLEX for VMware vSAN version must be the following:
  - VMware ESXi v6.7 Update 1 or later
  - VMware vCenter Server Appliance v6.7 Update 1 or later
- Use the administrator of the vCenter Single Sign-On domain for your cloud management software registration account information
- The cluster for the backup target servers is operating normally
- Backup target vCenter Server is started
- vCSA virtual machines are managed on vCenter that is registered on the ISM "Cloud Management Software List" screen when backing up vCSA.

Operation requirements for target servers

- Backup target servers are registered in ISM
- Backup target servers are started and operating normally

6.12.2 Preparations

This section describes preparations required before executing Backup for nodes or vCSA structuring a cluster.

6.12.2.1 Prepare a server to store backups

1. Prepare a backup destination server and create a SMB/CIFS shared folder on the server.

   The following is an example of when setting the shared folder on the backup destination server (Windows Server 2019).

   a. Create a folder to store the backups on the backup destination server.

   b. Right-click the folder and select [Properties].

   c. From the [Sharing] tab, select [Share].

   d. From the users on the backup destination server, select the users you want to share and select [Share].

   e. If the "Network discovery and file sharing" window is displayed, select either "Yes" or "No" for public network discovery and file sharing settings, depending on your environment.

   f. Select [Close].

2. Connect the destination server to the management LAN network of PRIMEFLEX for VMware vSAN.

6.12.3 Execute Backup

Perform Backup to back up PRIMEFLEX for VMware vSAN nodes or vCSA.

Be sure to refer to "6.12.1 Operation Requirements" and check the operation requirements before executing Backup.

Note

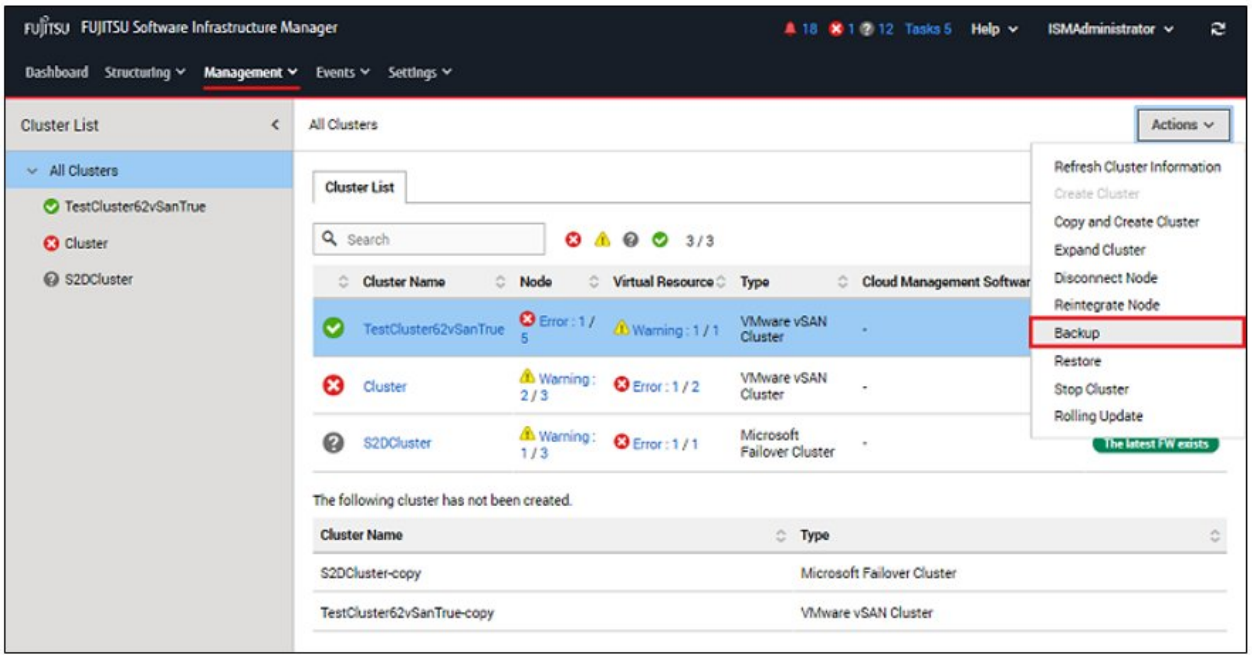
- Do not execute Backup while other ISM for PRIMEFLEX functions are being executed. Backup will fail. Check the ISM event log. Confirm the message by referring to "ISM for PRIMEFLEX Messages" and take action.

  For ISM for PRIMEFLEX functions, refer to "2.12 Functions of ISM for PRIMEFLEX" in "User's Guide."

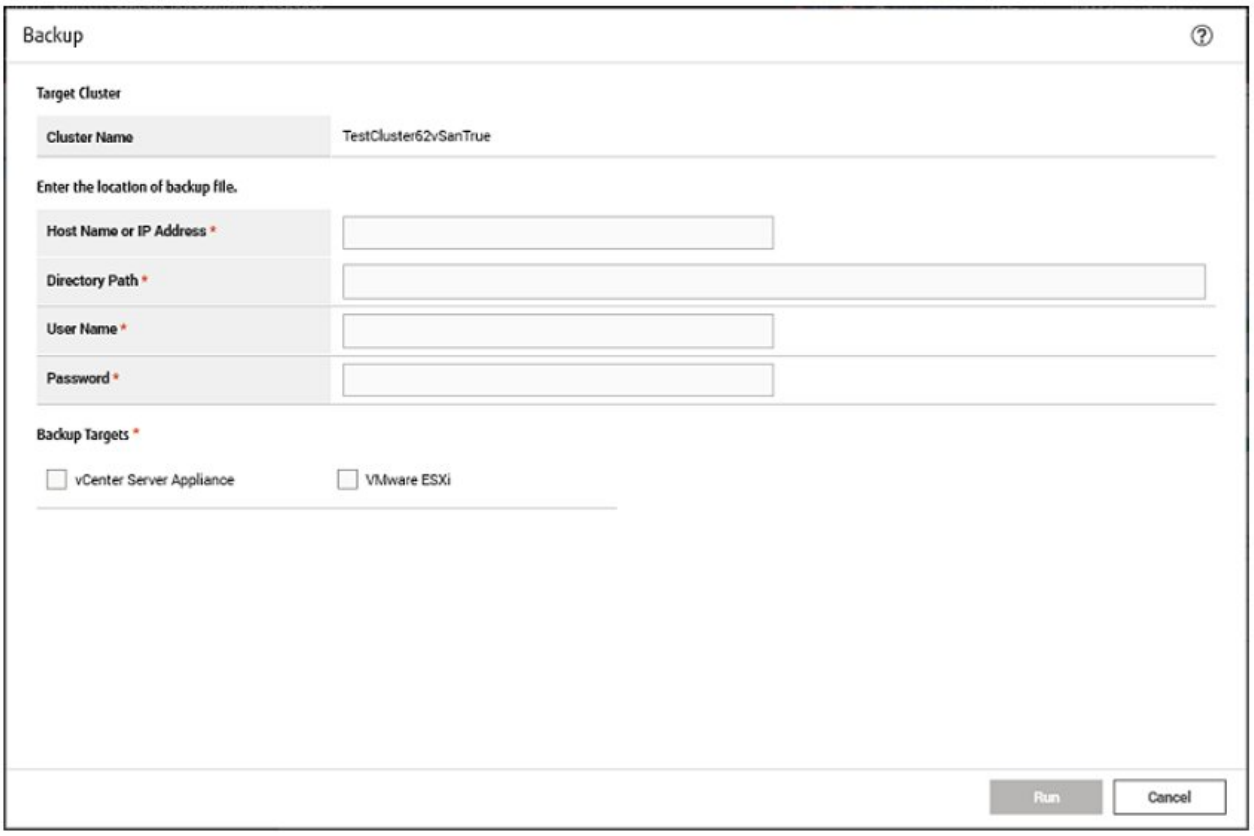
- During the execution of Backup, ISM for PRIMEFLEX stops the TSM-SSH service on the target node. Check the startup status of the service before executing the Backup. If the service is running, restart it manually after Backup is executed.

1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster].

   The "Cluster List" screen is displayed.
3. Select [<Target cluster>] and from the [Actions] button, select [Backup].



4. On the "Backup" screen, confirm the target cluster.

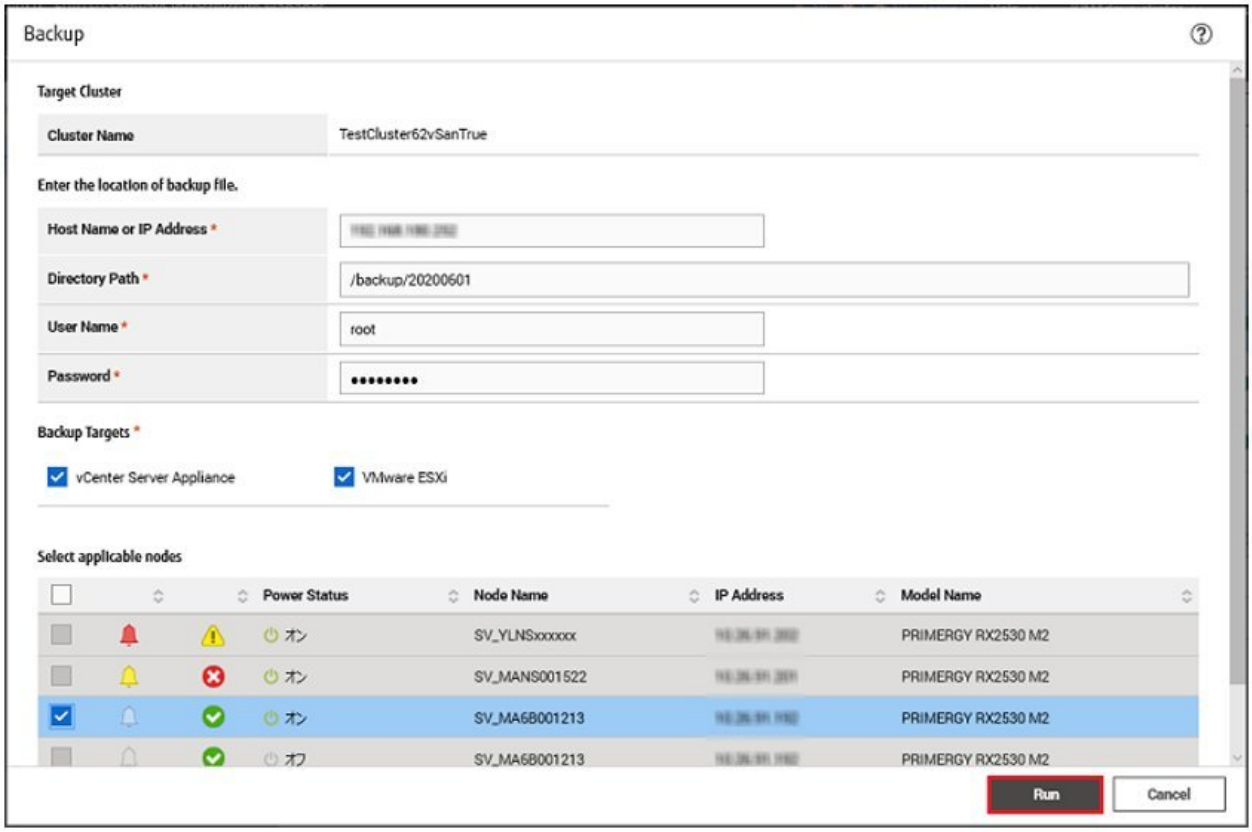


5. Select the backup targets and applicable nodes, and enter each parameter, and then select the [Run] button.

Point

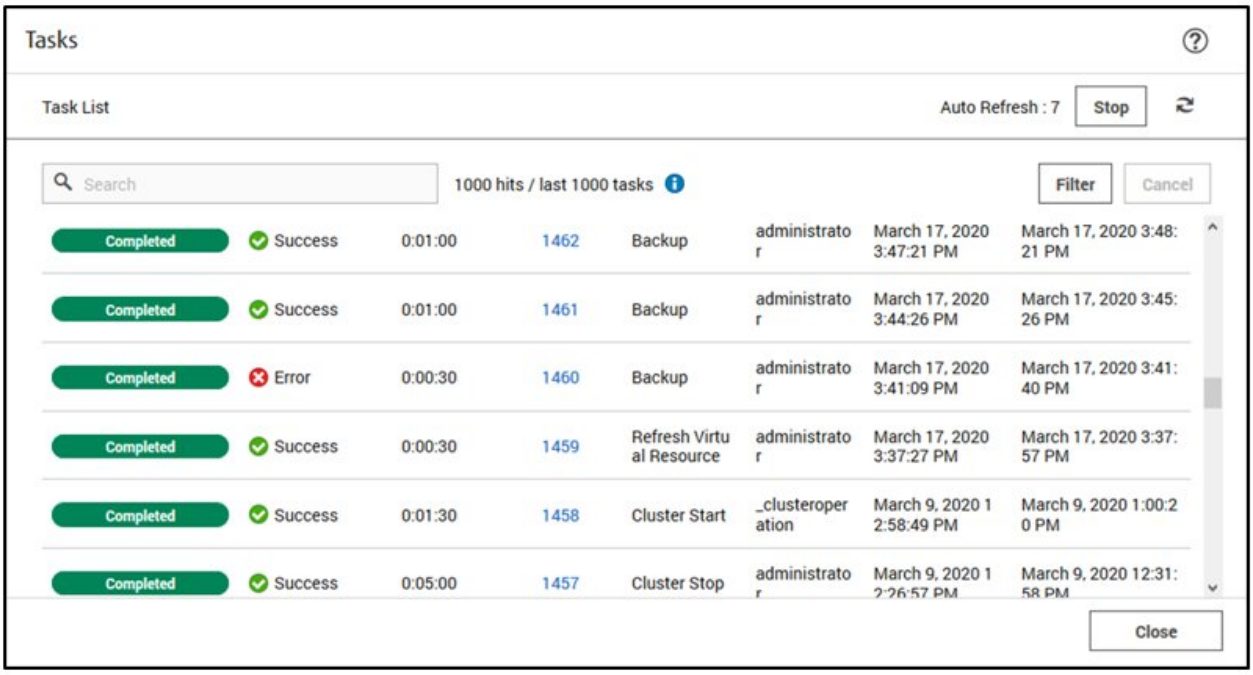
Enter the user name in the following format when specifying the domain user.

<Domain name>\<User name> or <User name>@<Domain name>



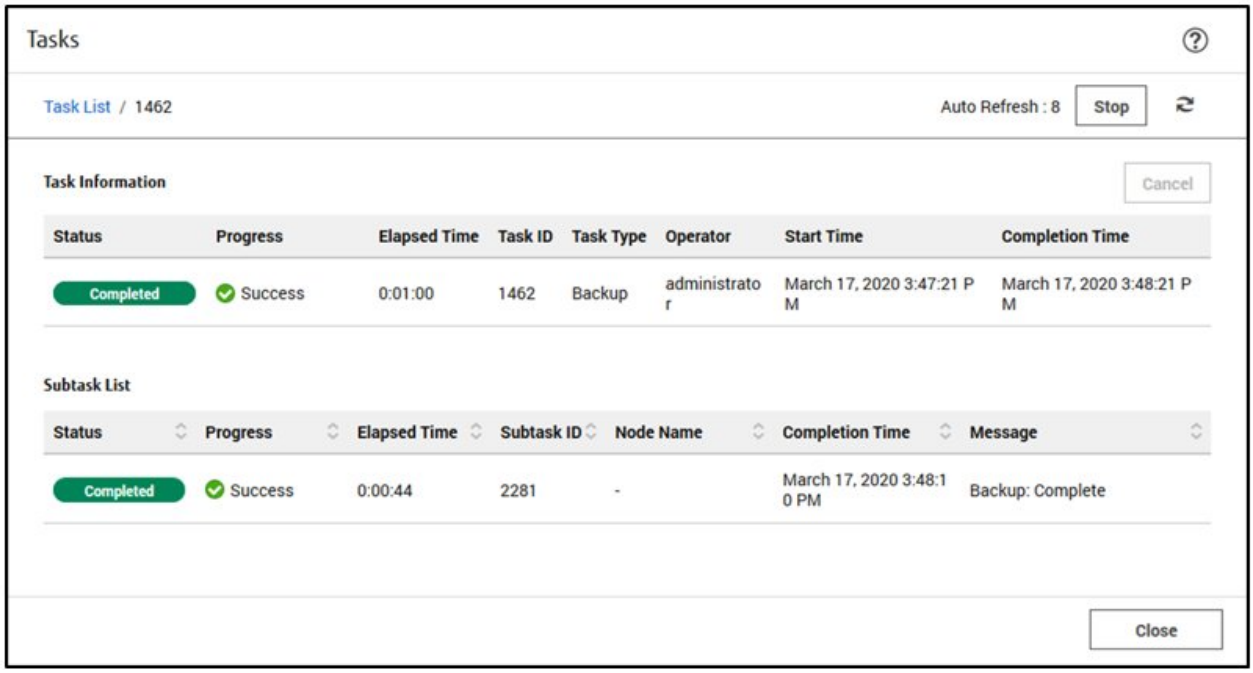
The execution of Backup is registered as an ISM task.

On the "Tasks" screen, which is displayed when you select [Tasks] on the top of the Global Navigation Menu, tasks whose Task Type is "Backup" are Backup tasks.



Point

If you select [Task ID] for "Backup" from the "Tasks" screen, the "Tasks" screen for "Backup" is displayed. On this screen, the subtask list is displayed and you can confirm the status of the task by checking the message.



6. Check that the status of "Backup" has become "Completed."
7. Confirm that the backup files are created in the Backup folder. The folder format is as follows.

Folder	Description
<Date>_<ISM task ID>	Root folder Specify <Date> in the form "YYYYMMDD_hhmmss."
vcsa_<vCSA IP address>	Parent folder for vCSA backup
va	Backup folder for vCSA [Note]
vds	Backup folder for vDS
esxi_<ESXi IP address>	Backup folder for ESXi

[Note]: A unique ISM backup file that creates the following file in the "va" folder.

The following file is only used for vCSA restoration which is used by ISM.

File:

pfx_vcsa_disk.json

Note

- If an error is displayed on the ISM "Tasks" screen, check the ISM event log. Confirm the message by referring to "ISM for PRIMEFLEX Messages" and take action.

  After the error is resolved, execute Backup again.

- If you changed the following settings, you must execute Backup again. When executing Restore, if the following settings have been changed, it ends with an error.
  - Virtual distributed switch and distributed port group settings
  - User name and password for vCSA
  - User name and password for ESXi

6.12.4 Follow-up Processing

This section describes the follow-up process for Backup of nodes or vCSA structuring a cluster.

6.12.4.1 Start the TSM-SSH service

After executing Backup, the TSM-SSH service on the node being backed up is stopped. If the service was started before Backup was executed, restart the service if necessary. For the procedure to start the service, refer to "Enable the ESXi Shell (TSM) and the SSH (TSM-SSH) services on the server" in "PRIMEFLEX for VMware vSAN Operations and Maintenance Guide."

If you need the manual, contact your local Fujitsu customer service partner.

6.13 Restore vCSA Structuring a Cluster

You can execute Restore to prepare for system recovery from failures in PRIMEFLEX for VMware vSAN.

This function can be used only when the ISM Operation Mode is "Advanced for PRIMEFLEX."

The following is the work flow for executing Restore.

Table 6.30 Work flow for restoring vCSA structuring a cluster

Procedures for restoring vCSA structuring a cluster		Tasks
1	Preparations	- Preparation for a server in which backups are stored - Upload of the vCSA installer file to ISM-VA
2	Execute Restore	

Procedures for restoring vCSA structuring a cluster		Tasks
3	Follow-up Processing	- Modification of vCSA port groups - Deletion of the existing vCSA - Starting the TSM-SSH service

6.13.1 Operation Requirements

To use Restore, the following requirements must be met.

To restore a backup that was collected on ISM 2.5.0.030 or earlier, the following requirements must also be met.

- If the vCenter Server has been upgraded, the storage size is specified with the default value
- If the vCenter Server has been restored manually, the storage size was specified with the default value at that time
- The disk capacity of the vCenter Server has not been expanded

If a backup was collected on ISM 2.5.0.030 or earlier, the following file is not in the backup folder.

File:

<Backup folder>\vcsa_<IP address of vCSA>\va\pfx_vcsa_disk.json

Example:

20200203_004120_1353\vcsa_192.168.120.1\va\pfx_vcsa_disk.json

If the storage size is not the default value or the capacity has been expanded, refer to "PRIMEFLEX Operation & Maintenance Guide" for PRIMEFLEX for VMware vSAN and execute a manual restoration.

For manual restoration, loading a backup file with the SMB/CIFS protocol is not supported. Load a backup file by using another protocol.

If you need this manual, contact your local Fujitsu customer service partner.

Operation requirements for target clusters

- The cluster must be the PRIMEFLEX for VMware vSAN cluster
- A cluster of restoration target servers is registered in the cloud management software
- Cluster Definition Parameters are specified

  For details, refer to "6.8.2.11 Create and edit Cluster Definition Parameters."
- Cluster Management for the cluster of the target server for restoration has been preset

  For Cluster Management settings, refer to "3.8 Pre-Settings for Managing Virtual Resources/Clusters" in "User's Guide."
- The latest cluster information is displayed

  For details, refer to "2.12.1.3 Refreshing cluster information" in "User's Guide."
- Version of PRIMEFLEX for VMware vSAN must be the following
  - VMware ESXi v6.7 Update 1 or later
  - VMware vCenter Server Appliance v6.7 Update 1 or later
- Use the administrator of the vCenter Single Sign-On domain for your cloud management software registration account information
- vCenter Server has been deleted or stopped and a server with vCenter Server IP address does not exist
- Name resolution by DNS server is possible for vCenter Server FQDN

- NIC (vmnic) of vDS for management has redundant configuration

Operation requirements for target servers

- Restoration target servers are registered in ISM

6.13.2 Preparations

This section describes preparations required before executing Restore for vCSA structuring a cluster.

6.13.2.1 Prepare a server in which backups are stored

1. Prepare a server in which backups are stored and create a SMB/CIFS shared folder on the server.
2. Connect the server in which backups are stored to the management LAN network of PRIMEFLEX for VMware vSAN.

6.13.2.2 Upload vCSA installer file to ISM-VA

Download the vCSA installer file from the VMware web site.

Upload the vCSA installer file by checking the following items and referring to "1.4.1 Upload Files to ISM-VA."

Add ISM-VA virtual disks if necessary. For information on the procedure to add virtual disks, refer to "3.7 Allocation of Virtual Disks" in "User's Guide."

Item	Value
Root Directory	Administrator/ftp
File Type	Other
Upload Target Path	Administrator/ftp/ClusterOperation/vCSA
File	vCSA installer file [Note] Example: VMware-VCSA-all-6.7.0-10244745.iso

[Note]: Upload the vCSA installer file of the same version of the vCSA at the time of backup.

6.13.3 Execute Restore

Execute Restore to restore vCSA in PRIMEFLEX for VMware vSAN.

Be sure to refer to "6.13.1 Operation Requirements" and check the operation requirements before executing Restore.

Note

- Do not execute Restore while other ISM for PRIMEFLEX functions are being executed. Restore will fail. Check the ISM event log. Confirm the message by referring to "ISM for PRIMEFLEX Messages" and take action.

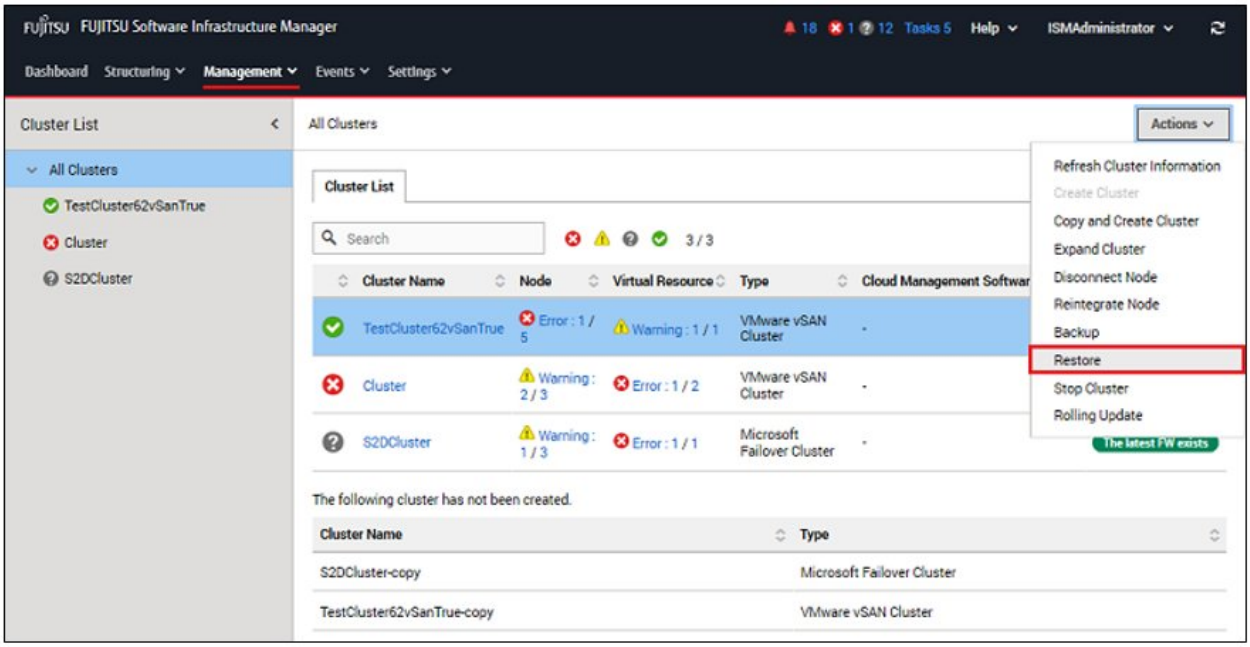
  For ISM for PRIMEFLEX functions, refer to "2.12 Functions of ISM for PRIMEFLEX" in "User's Guide."

- During the execution of Restore, ISM for PRIMEFLEX stops the TSM-SSH service on the target node. Check the startup status of the service before executing Restore. If the service is running, restart it manually after Restore is executed.

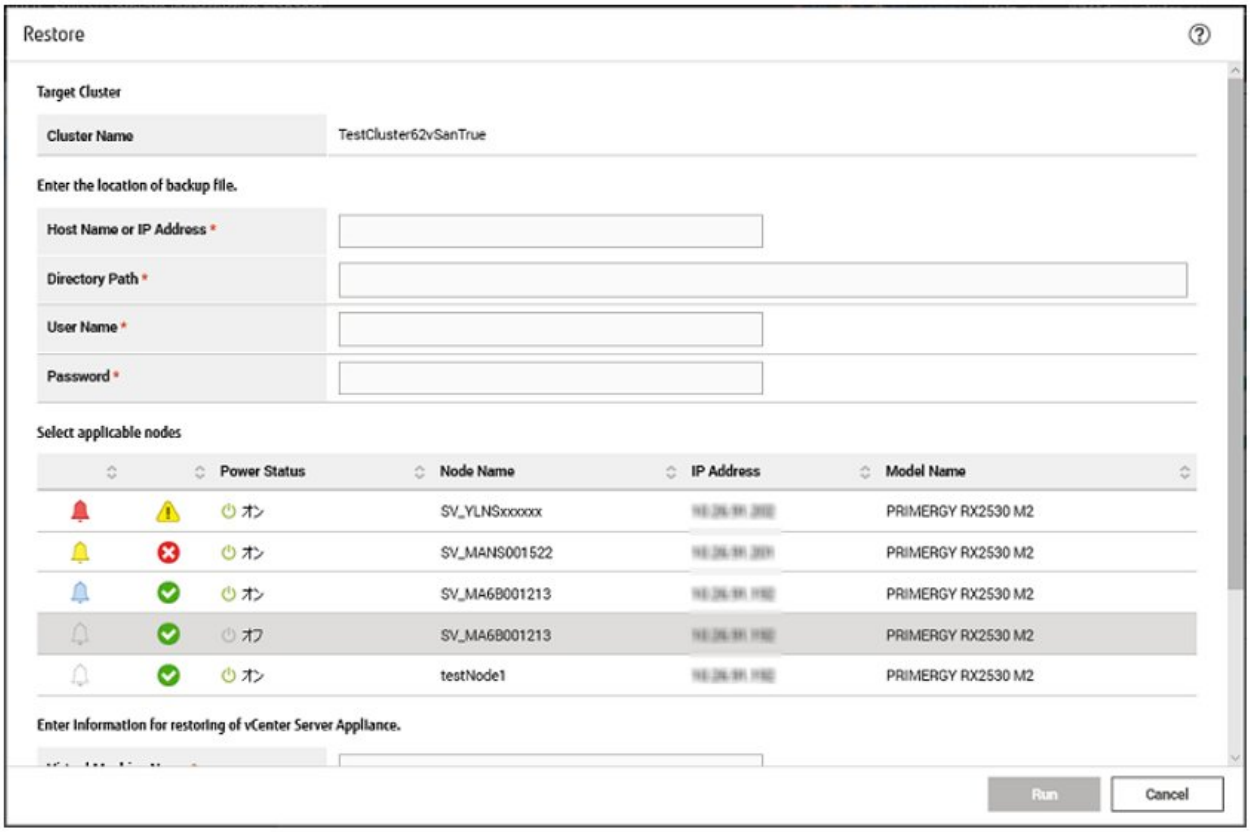
1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster].

   The "Cluster List" screen is displayed.

3. Select [<Target cluster>] and from the [Actions] button, select [Restore].



4. On the "Restore" screen, confirm the target cluster.



5. Select the applicable nodes, and enter each parameter, and then select the [Run] button.

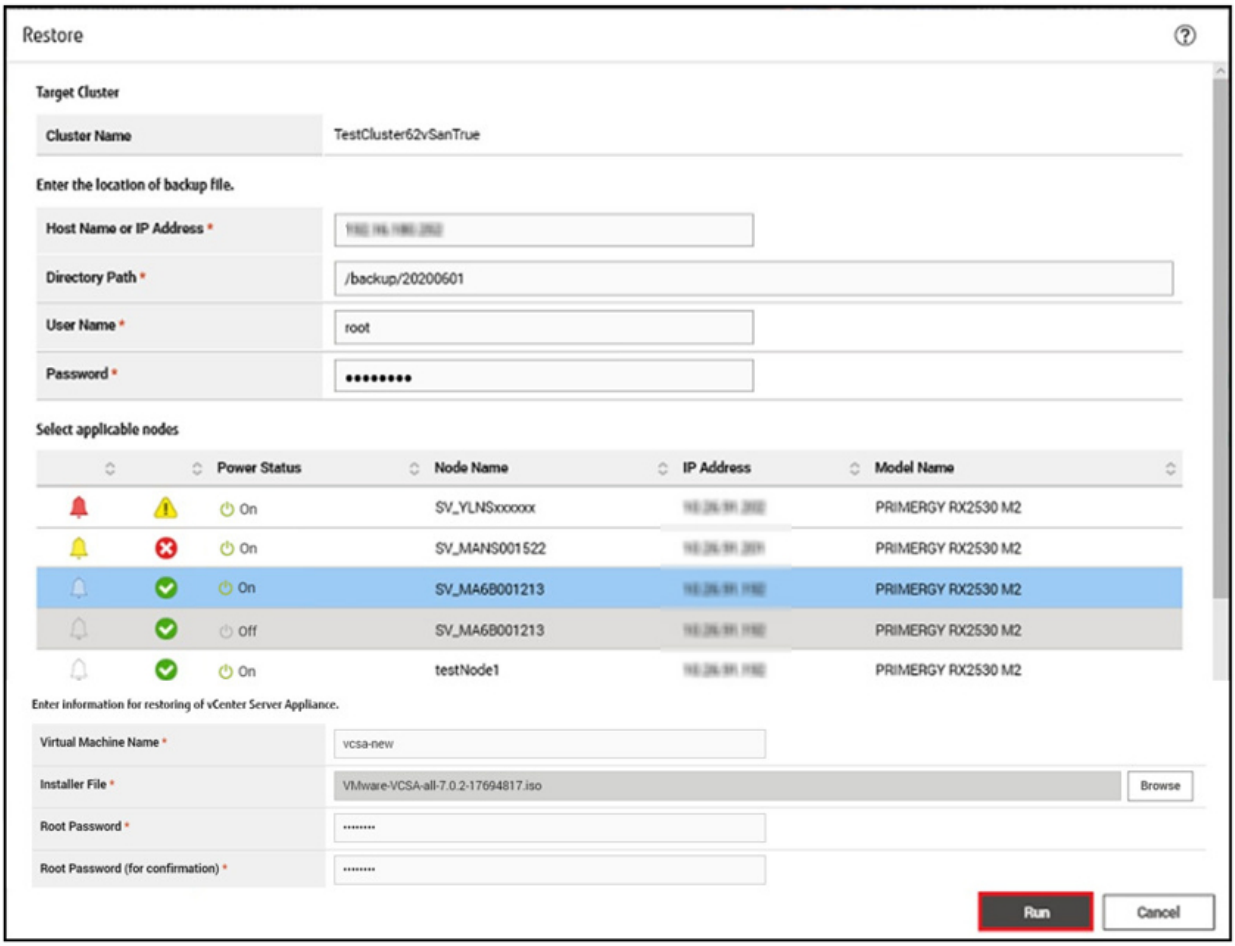
Point

- For the [Directory Path] for the backup file, enter the root folder of the following backup folder that was created by Backup of ISM for PRIMEFLEX.

  Backup folder/<Date>_<ISM task ID>

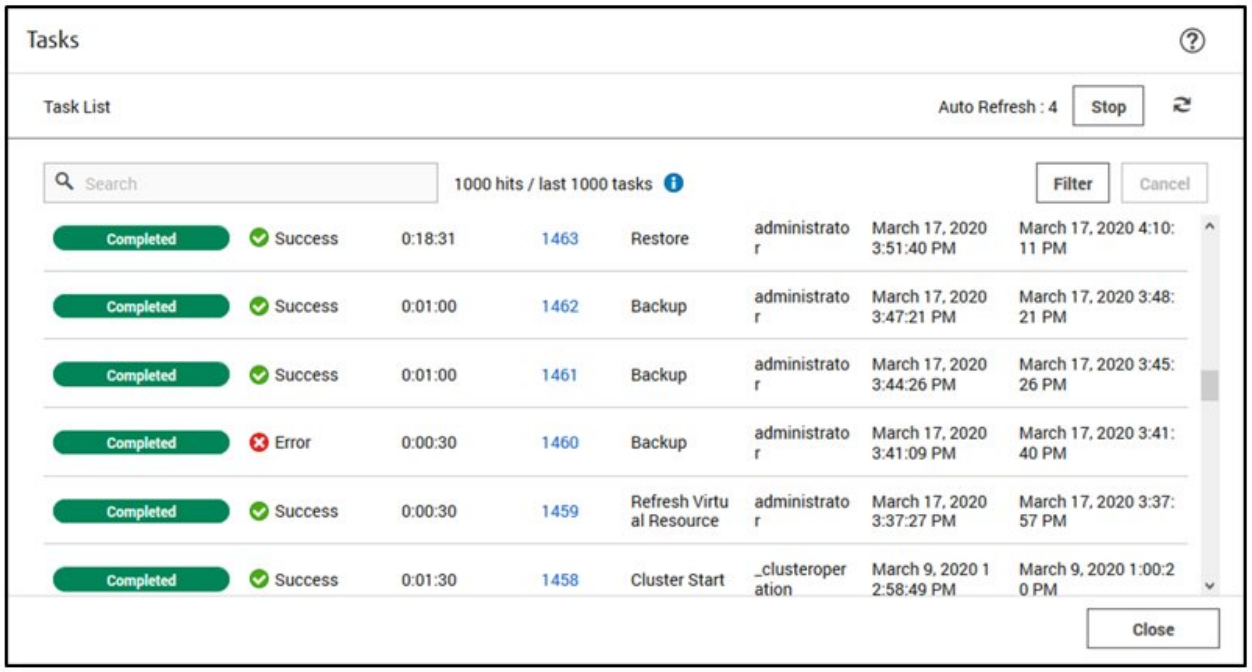
- Enter the [User Name] in the following format when specifying the domain user.
  <Domain name>\<User name> or <User name>@<Domain name>

- For the [Virtual Machine Name], specify a unique virtual machine name.



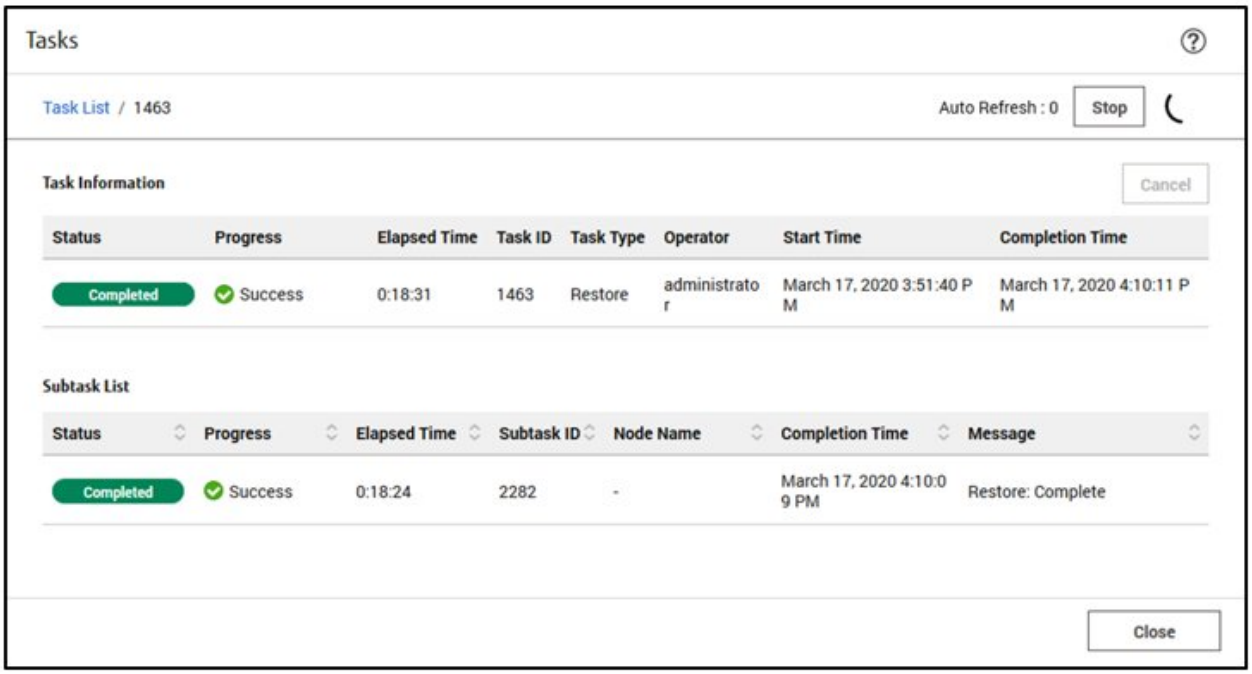
The execution of Restore is registered as an ISM task.

On the "Tasks" screen, which is displayed when you select [Tasks] on the top of the Global Navigation Menu, tasks whose Task Type is "Restore" are Restore tasks.



Point

If you select [Task ID] for "Restore" from the "Tasks" screen, the "Tasks" screen for "Restore" is displayed. On this screen, the subtask list is displayed and you can confirm the status of the task by checking the message.



6. Check that the status of "Restore" has become "Completed."

Point

If "Info: Please change the port group of the vCSA" is in the message of the subtask, execute "6.13.4.1 Modify the vCSA port group" after this procedure.

Note

If the subtask message contains the following, the vCSA is in the vSAN default storage policy after the restoration. You must apply the storage policy again.

```
[Warning]: The storage policy for management VMs is not applied. Log in to vCSA with vSphere
Client and apply the storage policy for management VMs.
```

Perform the following procedures. Note that "PRIMEFLEX Design Guide" for PRIMEFLEX for VMware vSAN is required to perform the procedures.

Contact your local Fujitsu customer service partner.

For vCSA 6.5 and earlier (Flash)

1. Log in to vCSA with vSphere Web Client.
2. From the "Top" screen, select the [Home] tab - [Operations and policies] - [VM Storage Policies].
3. Select [Create New VM Storage Policy].
4. Refer to the following to enter the setting values for the storage policy of the management VM.

   "PRIMEFLEX Design Guide" for PRIMEFLEX for VMware vSAN - "Storage policy"

   In the settings for policy structure, set [Use rules-sets in the storage policy] - [vSAN].
5. Select the [Finish] button to create the virtual machine storage policy.
6. From the "Top" screen, select the [Home] tab - [Inventories] - [Hosts and Clusters] [<vCSA name>] - [Configure] - [Policies] - [Edit VM Storage Policies].
7. From the virtual machine storage policy pulldown menu, select the storage policy you created in Step 5.
8. Select the [OK] button to apply the modifications.

For vCSA 6.7 or later (HTML5)

1. Log in to vCSA with vSphere Client.
2. From the "Top" screen, select the [Shortcuts] - [Monitor] - [VM Storage Policies].
3. Select "VM Storage Policies" - [Create].
4. Refer to the following to enter the setting values for the storage policy of the management VM.

   "PRIMEFLEX Design Guide" for PRIMEFLEX for VMware vSAN - "Storage policy"

   In the settings for policy structure, set [Datastore specific rules] - [Enable rules in "vSAN" storage].
5. Select the [FINISH] button to create the virtual machine storage policy.
6. From the "Top" screen, select the [Shortcuts] - [Inventories] - [Hosts and Clusters] - [<vCSA name>] - [Configure] - [Policies] - [EDIT VM STORAGE POLICIES].
7. From the virtual machine storage policy pulldown menu, select the storage policy you created in Step 5.
8. Select the [OK] button to apply the modifications.

Note

If an error is displayed on the ISM "Tasks" screen, check the ISM event log. Confirm the message by referring to "ISM for PRIMEFLEX Messages" and take action.

After the error is resolved, execute Restore again.

6.13.4 Follow-up Processing

This section describes the follow-up processing required after executing Restore of vCSA.

6.13.4.1 Modify the vCSA port group

Connect vCSA to the management VM port group if necessary.

If "Info: Please change the port group of the vCSA" is in the message of the subtask after vCSA is restored, it is connected to the port group for the ESXi VMkernel.
Therefore, execute the following procedure to connect it to the port group for the vCSA management VM.
The default port group name for management VMs is "Management Port Group."

For vCSA 6.5 and earlier (Flash)

1. Log in to vCSA with vSphere Web Client.
2. From the "Top" screen, select the [Home] tab - [Inventories] - [Hosts and Clusters].
3. On the screen that is displayed, select the virtual machine for vCSA, and then select [<Virtual machine name>] - [Edit Settings].
4. Modify the value for [Virtual Hardware] tab - [Network adapter 1] to the port group for management VMs.
5. Select the [OK] button to apply the modifications.

For vCSA 6.7 or later (HTML5)

1. Log in to vCSA with vSphere Client.
2. From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters].
3. On the screen that is displayed, select the virtual machine for vCSA, and then select [<Virtual machine name>] - [Edit Settings].
4. Modify the value for [Virtual Hardware] tab - [Network adapter 1] to the port group for management VMs.
5. Select the [OK] button to apply the modifications.

6.13.4.2 Delete the existing vCSA

After executing Restore, delete the existing vCSA if necessary.

For vCSA 6.5 and earlier (Flash)

1. Log in to vCSA with vSphere Web Client.
2. From the "Top" screen, select the [Home] tab - [Inventories] - [Hosts and Clusters].
3. On the screen that is displayed, select the virtual machine for vCSA, and then select [<Virtual machine name>] - [Delete from Disk].
4. On the "Confirm Delete" screen, select the [Yes] button.
5. Confirm that "Completed" is displayed for the status of [Delete virtual machine] displayed in [Recent Tasks].

For vCSA 6.7 or later (HTML5)

1. Log in to vCSA with the vSphere Client.
2. From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters].

3. On the screen that is displayed, select the virtual machine for vCSA, and then select [<Virtual machine name>] - [Delete from Disk].
4. On the "Confirm Delete" screen, select the [Yes] button.
5. Confirm that "Completed" is displayed for the status of [Delete virtual machine] displayed in [Recent Tasks].

6.13.4.3 Start the TSM-SSH service

After executing Restore, the TSM-SSH service on the node being backed up is stopped. If the service was started before Restore was executed, restart the service if necessary. For the procedure to start the service, refer to "Enable the ESXi Shell (TSM) and the SSH (TSM-SSH) services on the server" in "PRIMEFLEX for VMware vSAN Operations and Maintenance Guide."

If you need the manual, contact your local Fujitsu customer service partner.

6.14 Stop a Cluster

To stop a PRIMEFLEX for VMware vSAN cluster, execute Cluster Stop.

This function can be used only when the ISM Operation Mode is "Advanced for PRIMEFLEX."

To start a cluster that has been stopped by this function, use the Cluster Start command.
For the procedure to obtain the Cluster Start command, refer to "2.12.8 Cluster Stop in "User's Guide."

Before executing Cluster Stop, refer to "6.14.1 Operation Requirements," and be sure to confirm the operation requirements.

The following is the work flow for executing Cluster Stop.

Table 6.31 Work flow for executing Cluster Stop

Stopping a cluster procedure		Tasks
1	Preparations	- Executing cluster pre-settings - Executing vSAN health check test - Refreshing the ISM cluster information - Stopping workload VMs
2	Cluster Stop procedure	
3	Follow-up Processing	- Checking the power status

6.14.1 Operation Requirements

To use Cluster Stop, the following requirements must be met.

- The cluster must be the PRIMEFLEX for VMware vSAN cluster
- ISM for PRIMEFLEX operation environment
  - All servers in the target cluster are registered in ISM
  - The target cluster is registered in the cloud management software
- Cluster configuration and operating status
  - The status of the target cluster is normal
  - When there are running clusters other than the target cluster, ISM-VA and vCSA must not exist in the target cluster
    ISM-VA and vCSA can exist within the target cluster only when the target cluster is running.
  - All servers in the target cluster are running and the servers are not in ISM Maintenance Mode and ESXi Maintenance Mode
  - Cluster Definition Parameters have been set.
  - Virtual Resource Management pre-settings have been execute

    For details, refer to "3.8 Pre-Settings for Managing Virtual Resources/Clusters" in "User's Guide."

- Cloud management software registration status
  - Use the administrator of the vCenter Single Sign-On domain for your cloud management software registration account information

6.14.2 Preparations

This section describes the preparations required before executing Cluster Stop for a cluster.

6.14.2.1 Execute cluster pre-settings

Execute the Cluster Management pre-settings.

For details, refer to "3.8 Pre-Settings for Managing Virtual Resources/Clusters" in "User's Guide."

6.14.2.2 Execute the vSAN Health test for a cluster

Perform the vSAN Health test for a cluster.

For vCSA 6.5 and earlier (Flash)

1. Log in to vCSA with vSphere Web Client.
2. From the "Top" screen, select the [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Monitor] - [vSAN] - [Health].
3. Take action for "Failed" in [Test result] displayed in [vSAN Health].

For vCSA 6.7 or later (HTML 5)

1. Log in to vCSA with vSphere Client.
2. From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Monitor] - [vSAN] - [Health [Note]].
3. Take action for the item displayed in red in [Health [Note]].

[Note]: In vCSA 7.0 or later, it is displayed as [Skyline Health].

6.14.2.3 Refresh the ISM cluster information

Refresh the cluster information.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster].

   The "Cluster List" screen is displayed.
2. From the [Actions] button, select [Refresh Cluster Information].
3. Check that the update of the cluster information has become "Complete."

6.14.2.4 Stop workload VMs

Stop all workload VMs running on the Cluster Stop target cluster.

For vSphere 7.0 Update 1 or later, the vCLS virtual machine is stopped automatically by ISM. It does not need to be stopped in this step.

For vCSA 6.5 and earlier (Flash)

1. Log in to vCSA with vSphere Web Client.
2. From the "Top" screen, select the [Home] tab - [Inventories] - [Hosts and Clusters].
3. On the screen that is displayed, check if there are any virtual machines running on the target cluster.
4. Select the virtual machine that is running, and then select [<Virtual machine name>] - [Power] - [Shut Down Guest OS].
5. On the displayed "Confirm Guest Shut Down" screen, select the [Yes] button.

6. Confirm that "Completed" is displayed for the status of [Initiate guest OS shutdown] displayed in [Recent Tasks].
7. Repeat Step 4 to 6 until there are no running virtual machines.

For vCSA 6.7 or later (HTML5)

1. Log in to vCSA with the vSphere Client.
2. From the "Top" screen, select [Shortcuts] - [Inventories] - [Hosts and Clusters].
3. On the screen that is displayed, check if there are any virtual machines running on the target cluster.
4. Select the virtual machine that is running, and then select [<Virtual machine name>] - [Power] - [Shut Down Guest OS].
5. On the displayed "Confirm Guest Shut Down" screen, select the [Yes] button.
6. Confirm that "Completed" is displayed for the status of [Initiate guest OS shutdown] displayed in [Recent Tasks].
7. Repeat Step 4 to 6 until there are no running virtual machines.

6.14.3 Execute Cluster Stop

Execute Cluster Stop to stop a cluster in PRIMEFLEX for VMware vSAN.

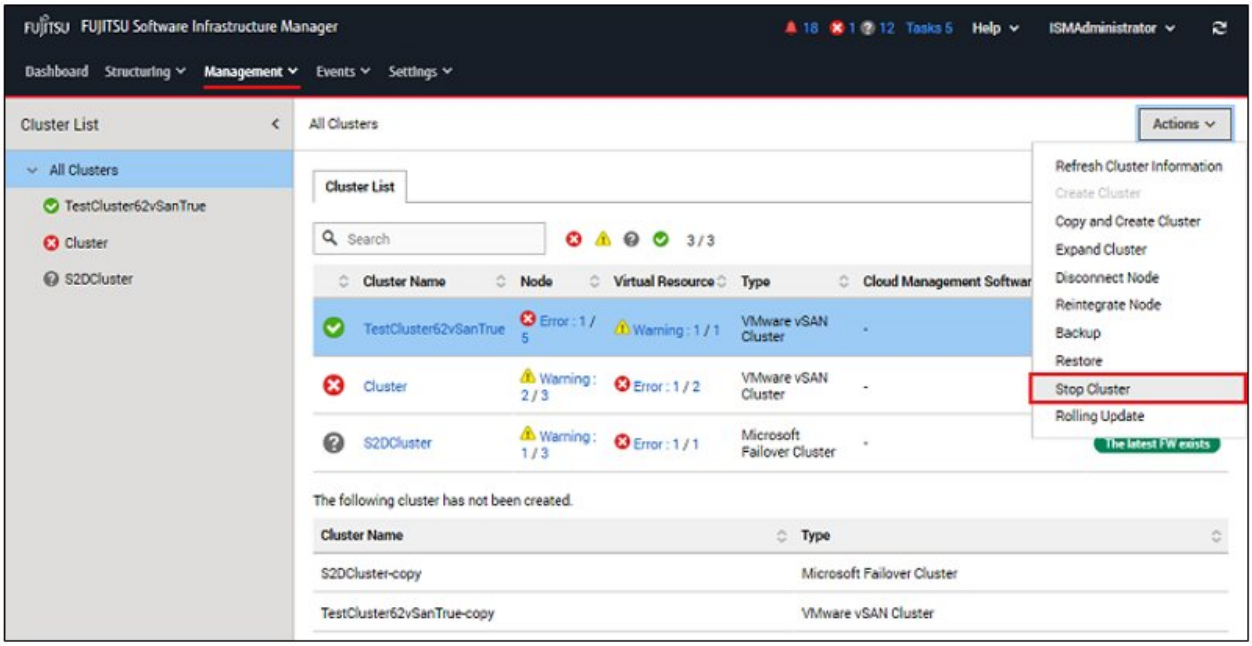
Refer to "6.14.1 Operation Requirements" and "6.14.2 Preparations," and check the operation requirements and perform preparations.

Note

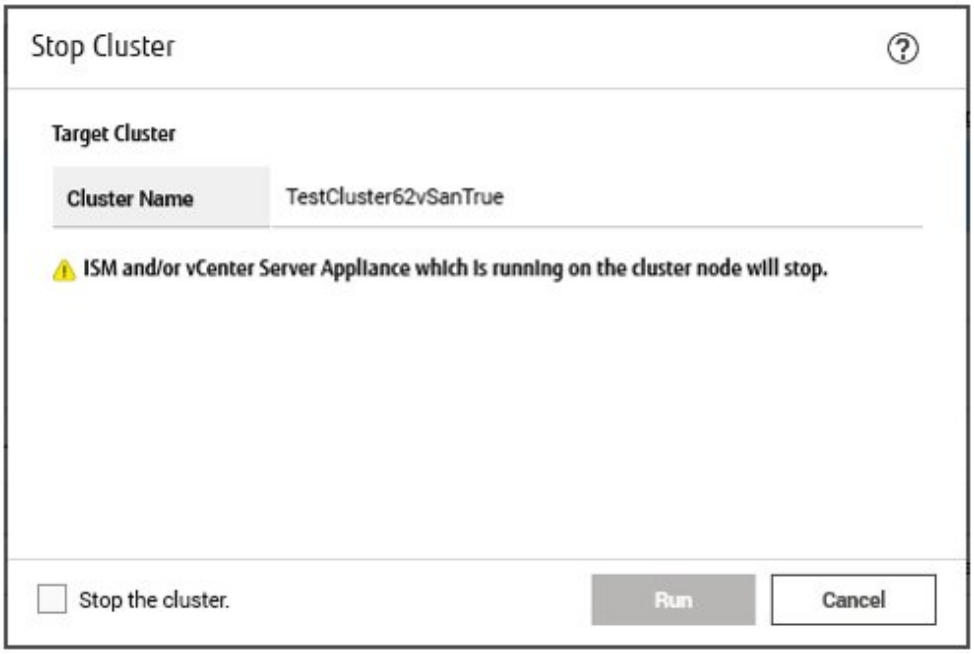
Do not execute Cluster Stop while other ISM for PRIMEFLEX functions are being executed. Cluster Stop will fail.

1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster].

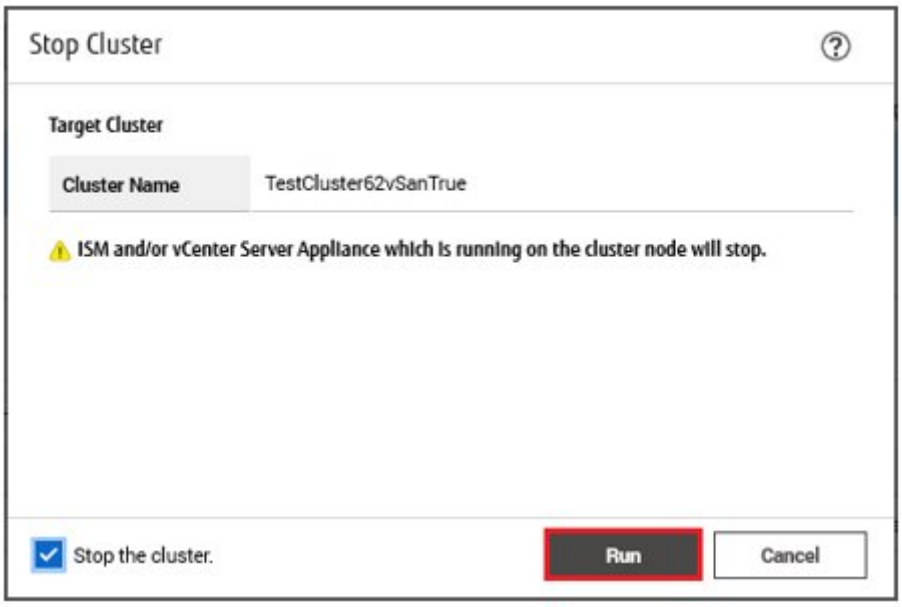
   The "Cluster List" screen is displayed.
3. Select [<Target cluster>], and then from the [Actions] button, select [Stop Cluster].



4. On the "Stop Cluster" screen, confirm the target cluster.

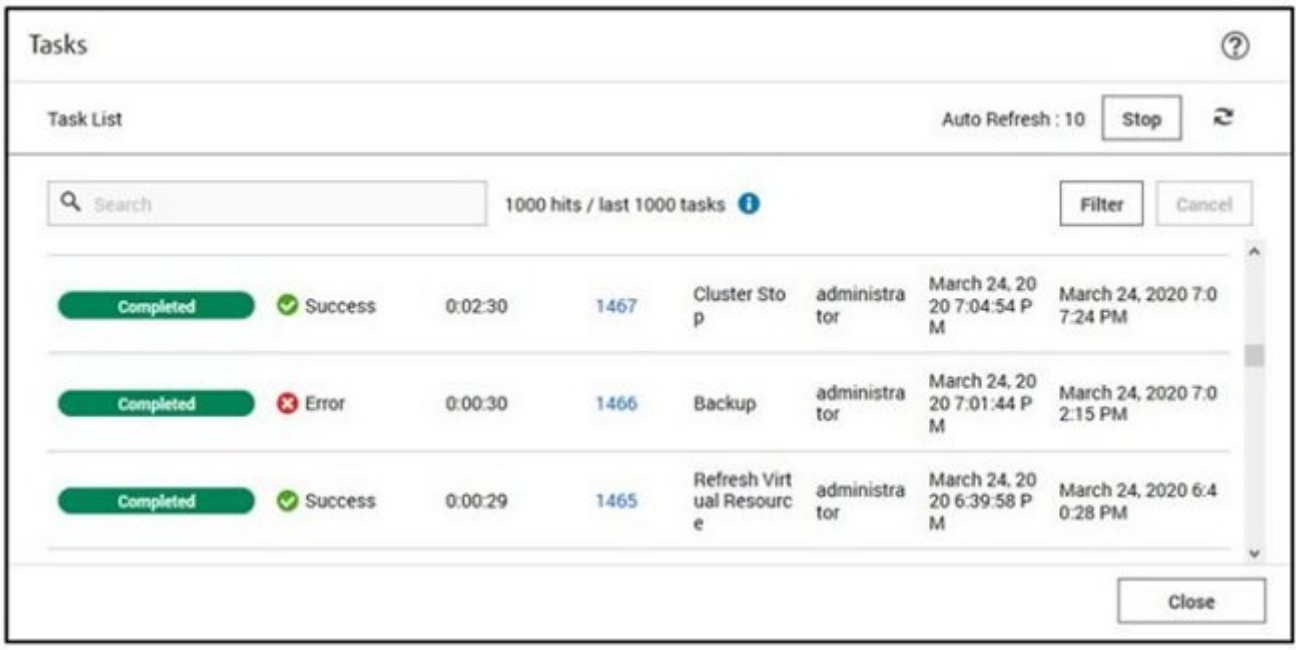


5. Select the [Stop the cluster.] checkbox and then select the [Run] button.



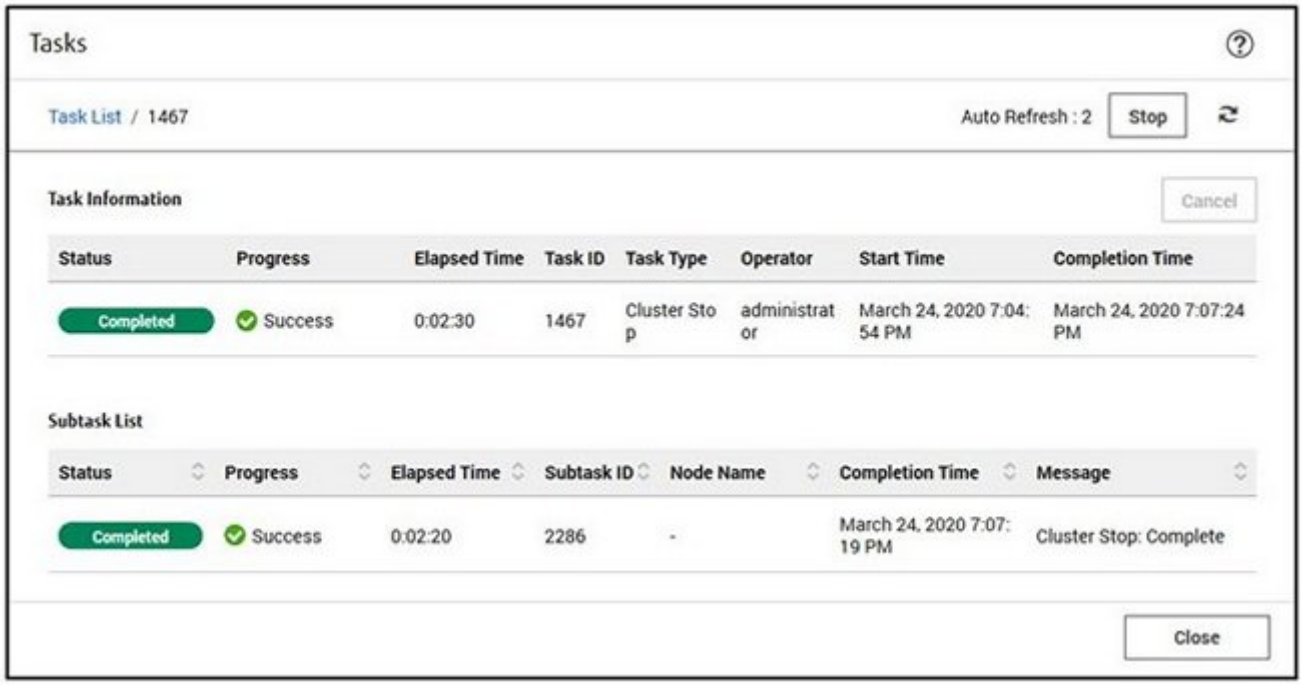
The execution of Cluster Stop is registered as an ISM task.

On the "Tasks" screen, which is displayed when you select [Tasks] on the top of the Global Navigation Menu, tasks whose Task Type is "Cluster Stop" are Cluster Stop tasks.



Point

If you select [Task ID] for "Cluster Stop" from the "Tasks" screen, the "Tasks" screen for "Cluster Stop" is displayed. On this screen, the subtask list is displayed and you can confirm the status of the task by checking the message.



6. Check that the status of "Cluster Stop" has become "Completed."

Note

- If the ISM-VA exists in the Cluster Stop target cluster, the ISM-VA will also stop as the Cluster Stop process progresses. As a result, the GUI screen update stops and the network connection to ISM-VA is lost. However, this is normal. If no ISM-VA exists, the task will continue to "Complete" without losing network connectivity.

- If an error is displayed on the "Tasks" screen of ISM, check the ISM event log. After the error is resolved, execute Cluster Stop again.

6.14.4 Follow-up Processing

This section describes the follow-up processing required after executing Cluster Stop.

6.14.4.1 Confirm the power status

After completing the task, physically check that the power lights are in the down status for all servers in the cluster. It may take approximately 10 minutes to power down all servers from the completion of the task.

6.15 View/Switch Generations of PRIMEFLEX (ISM 2.8.0.060 or later)

This section describes the procedure to view/switch generations of PRIMEFLEX.

This function can be used only when the ISM Operation Mode is "Advanced for PRIMEFLEX."

The PRIMEFLEX generation refers to the PRIMEFLEX model name (examples: PRIMEFLEX HS, PRIMEFLEX for VMware vSAN V1, PRIMEFLEX for VMware vSAN V2).

Switching the generation of PRIMEFLEX means installation of additional servers of successor models and removing servers of all older models, and then migrate the generation of PRIMEFLEX to the successor models.

If multiple generations of servers are mixed, the generation corresponds to the oldest generation of servers (example: for a system with mixed M4/M5 servers without execution of switch generations, the generation is PRIMEFLEX for VMware vSAN V1).

Note that to switch the generations, SupportDesk contract for PRIMEFLEX is required.

For details, refer to "Server Expansion/Generation Switching Guide."

If you need the manual, contact your local Fujitsu customer service partner.

6.15.1 Operation Requirements

To use Switch Generations, the following requirements must be met.

- The cluster must be the PRIMEFLEX for VMware vSAN cluster
- To be implemented after the installation of additional servers of successor models and the removing servers of all older models

  If you have multiple clusters of PRIMEFLEX for VMware vSAN, execute this by adding servers of successor models and reducing all older generation servers in all clusters.

6.15.2 Display Generation of PRIMEFLEX

This section describes the procedure to display the generations of PRIMEFLEX configured with Cluster Creation or Virtualized Platform Structure of PRIMEFLEX.

On a per-node basis, along with the registered generation, you can also view the function (such as Cluster Creation) of the node when it was registered in the cluster (Registration Trigger).

If the user has switched PRIMEFLEX generations for the target cluster, the switched generation (Switch Generation) can also be viewed.

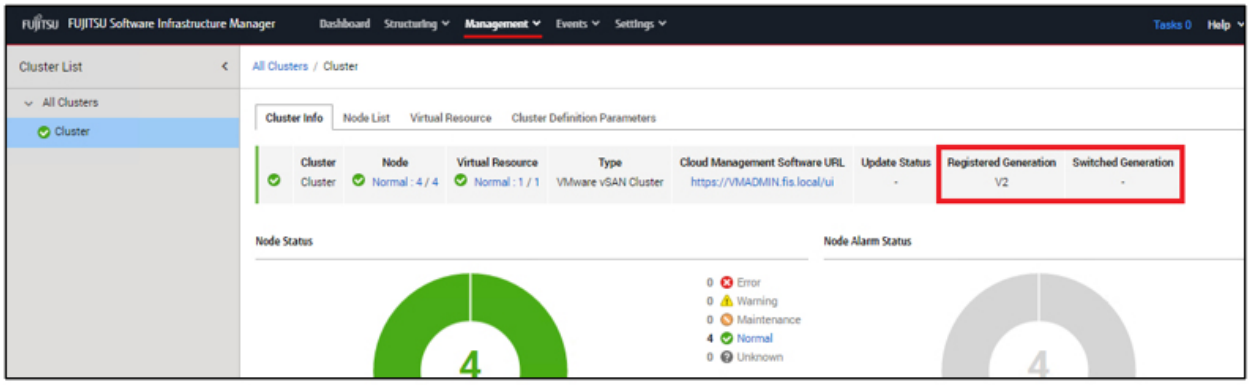
1. Log in to ISM.
2. From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster].

   The "Cluster List" screen is displayed.
3. Select [<Target cluster>].

   In [Registered Generation] and [Switched Generation] the generation of PRIMEFLEX is displayed in the format of Vx (x is lower-case letters).

   If Switch Generation is not executed, "-" is displayed in [Switched Generation].

For Switch Generation, refer to "6.15.3 Switch Generation of PRIMEFLEX."

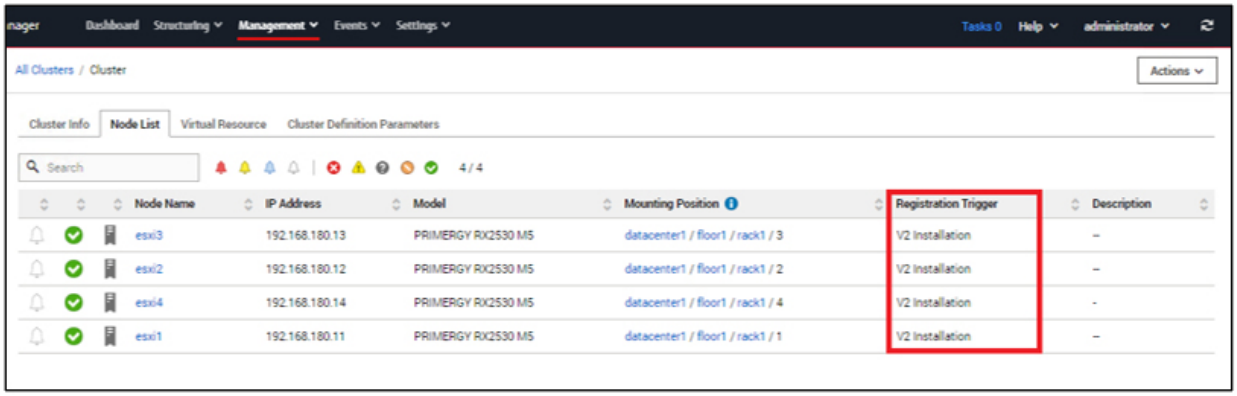


4. Select the [Node List] tab.

   In [Registration Trigger] the generation of PRIMEFLEX is displayed in the format of Vx (x is lower-case letters)

   Along with Vx, the following text is displayed when a node is registered:

   - Installation: node registration with Virtualized Platform Structure
   - Cluster Creation: node registration with Cluster Creation
   - Cluster Expansion: node registration with Cluster Expansion



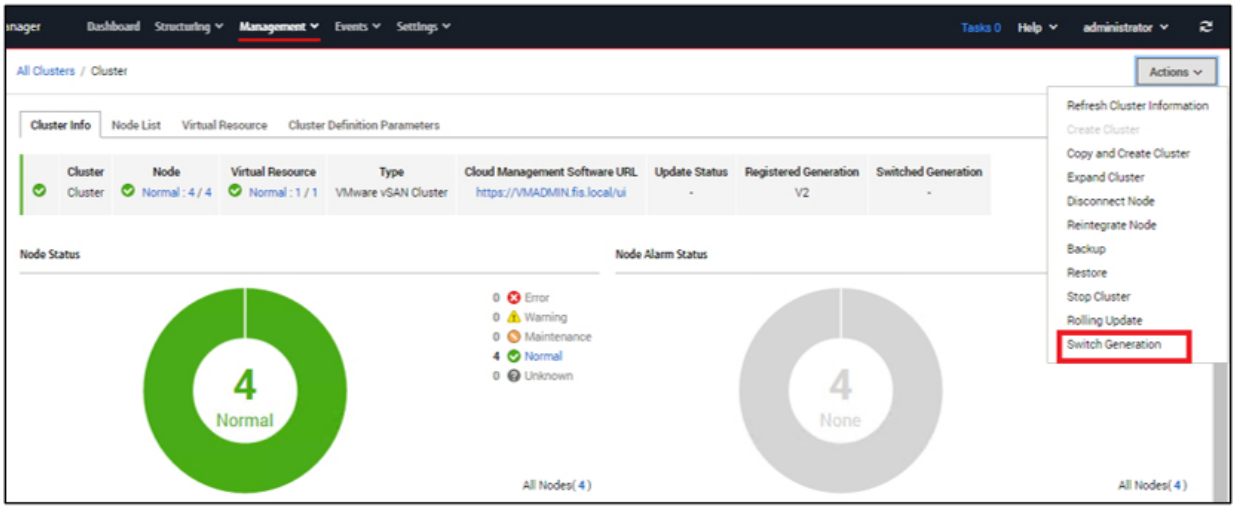
6.15.3 Switch Generation of PRIMEFLEX

This section describes the procedure to switch the generations of PRIMEFLEX.

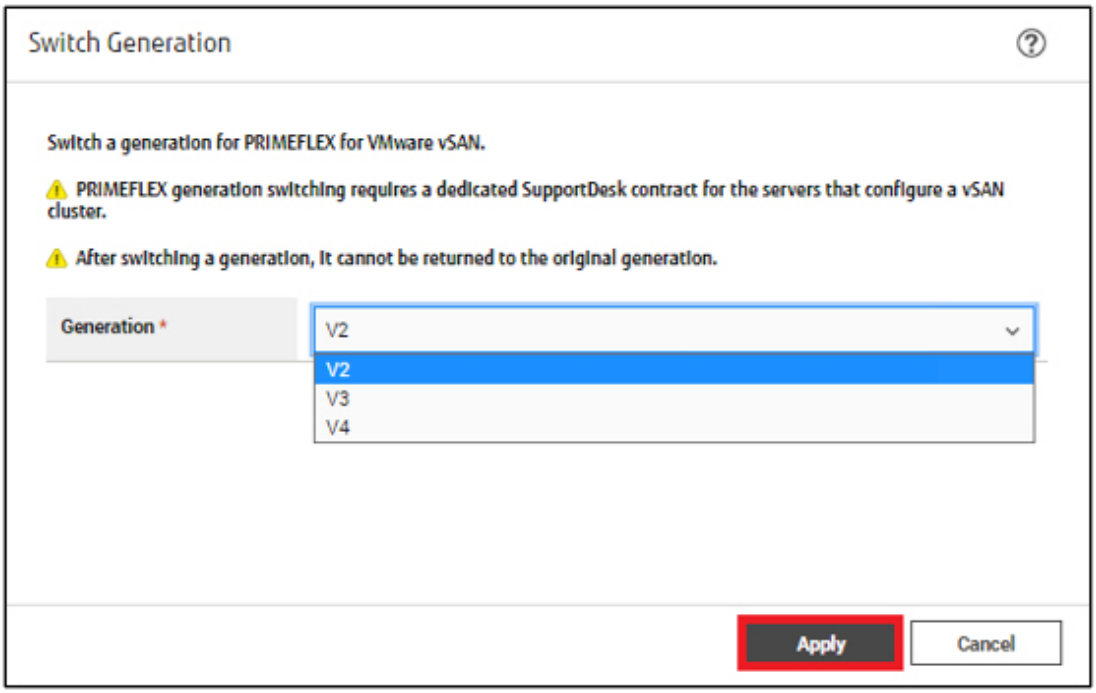
1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.
2. From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster].

   The "Cluster List" screen is displayed.

3. Select [<Target cluster>], and then from the [Actions] button, select [Switch Generation].



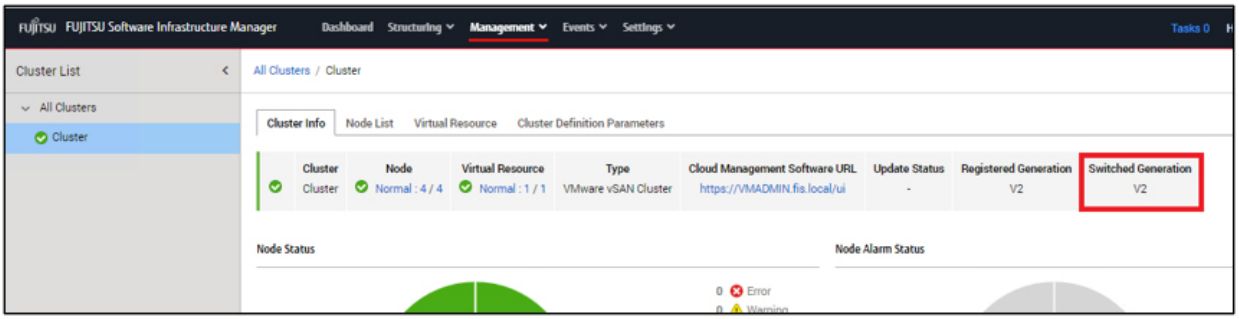
4. Select [Generation] and select the [Apply] button.



Point

If "There is no generation that can be switched. It's the latest generation." Is displayed, select the [Close] button.

5. Switched generation is updated.



Note

- If the result of Switch Generation shows an error display, select the [Close] button to confirm that the operation requirements are met. Then repeat step 4 or select the [Cancel] button to exit.

- If you have multiple clusters of PRIMEFLEX for VMware vSAN, select one of the clusters and select [Switch Generation] from the [Actions] button. The switched generation will be updated on all clusters.

6.16 Display iRMC AVR Screen Directly from ISM (ISM 2.8.0.060 or later)

To display the Advanced Video Redirection (AVR) (hereafter referred to as "AVR screen") of iRMC from ISM, the existing procedure is to register the IP address of iRMC in [Web I/F URL] on the Details of Node screen, open the web interface, and then operate the web interface to display the AVR screen. However, this procedure requires a login operation.

This section describes how to display the AVR screen directly without logging in to iRMC.

Note

- Pop-up Blocker must be turned off. Allow pop-ups to the ISM URL in your web browser.
- This function is not available for PRIMERGY that does not support iRMC login.

  For the status of iRMC login support, refer to "Support Matrix."

https://support.ts.fujitsu.com/index.asp

Select [Select a new Product] on the above site and enter "Infrastructure Manager" in [Product Search:].

Select [DOWNLOADS] and select the target operating system.

The reference procedures are subject to change without notice.

- Display of AVR screen via relay route is not supported.

Point

To use AVR, requires the purchase of an iRMC license (product name "Remote Management Controller upgrade").

6.16.1 Display AVR Screen Directly from ISM

The procedure for displaying the AVR screen directly from ISM is described below.

The [Start] button described below displays only for nodes that can display the AVR screen.

Enable Display of AVR screen

Enable AVR screen display for the user groups.

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [Users].
2. From the menu on the left side of the screen, select [User Groups].
3. Select the target user group, and then from the [Actions] button, select [Edit].
4. Select [Enable] in [iRMC Login/AVR].

Display AVR screen from Node List

Select the [Start] button on the node list to display the AVR screen.

1. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].

   The "Node List" screen is displayed.

2. On the Node List in the [AVR] column for the target node, select the [Start] button.

   The AVR screen is displayed in a separate web browser window.

Display AVR screen from Details of Node screen

Select the [Start] button on the Details of Node screen to display the AVR screen.

1. In the [AVR] on the Details of Node screen, select the [Start] button.

   The AVR screen is displayed in a separate web browser window.

Chapter 7 Prepare for errors of Managed Nodes

This chapter describes preparations for errors which may occur on the managed nodes and countermeasures for them.

7.1 Backup/Restore Server Settings

By saving the hardware settings of a server registered in ISM to a file, you can restore hardware settings, add a profile, or export or import hardware settings to another ISM.

7.1.1 Backup Server Settings

Collect the hardware settings (BIOS/iRMC) for the server registered in ISM and store them as files. Moreover, you can export the stored files.

Backup procedures

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
2. From the menu on the left side of the screen, select [Backup / Restore Hardware Settings].
3. Select a node, from the [Actions] button, select [Backup Hardware Settings].

   The "Backup Hardware Settings" screen will be displayed.
4. When backing up the BIOS hardware settings, switch off the power of the server in advance, select the [Get power status] button, and check that the power status has turned to "Off."
5. Select the checkboxes for the [Server (BIOS)] or [Server (iRMC)] which you want to back up settings, and then select [Execute].

Export Procedures

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
2. From the menu on the left side of the screen, select [Backup / Restore Hardware Settings].
3. Select a node, from the [Actions] button, select [Export (Backup file)].

   The "Export Backup File" screen will be displayed.
4. Select a file, and then select the [Execute] button according to the instructions on the screen.

Point

You can select multiple nodes and hardware settings for backing up and exporting.

Note

Backing up of hardware settings may fail in some iRMC firmware versions if LDAP is enabled in the iRMC settings, and HTTP is specified as the protocol in [Web I/F URL] on the Details of Node screen. In this case, edit the node information to set HTTPS in [Web I/F URL] as the protocol. For information on editing nodes, refer to "2.2.3 Editing of Datacenters/Floors/Racks/Nodes" in "User's Guide."

7.1.2 Create Profile from Backup Files

Create profiles from the hardware setting file saved in "7.1.1 Backup Server Settings."

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
2. From the menu on the left side of the screen, select [Backup / Restore Hardware Settings].
3. Select a node, from the [Actions] button, select [Add Profile From Backup].

4. Follow the instructions on the "Add Profile From Backup" wizard and enter the setting items.

   Refer to the help screen for entering the setting items.

Point

You can select multiple hardware settings for creating profiles.

Note

Profile for each model cannot be added from Backup (ISM 2.8.0.020 or later).

7.1.3 Create Policy from Backup Files

Create policies from the hardware settings saved in "7.1.1 Backup Server Settings."

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
2. From the menu on the left side of the screen, select [Backup / Restore Hardware Settings].
3. Select a node, from the [Actions] button, select [Add Policy From Backup].
4. Follow the instructions on the "Add Policy From Backup" wizard and enter the setting items.

   Refer to the help screen for entering the setting items.

Point

You can select multiple hardware settings for creating policies.

Note

Policy for each model cannot be added from Backup (ISM 2.8.0.020 or later).

7.1.4 Import Server Settings

Import the hardware setting files of the node exported in "7.1.1 Backup Server Settings" or the hardware setting files collected from iRMC.

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
2. From the menu on the left side of the screen, select [Backup / Restore Hardware Settings].
3. Select a node, from the [Actions] button, select [Import].

   The "Import Backup File" screen is displayed.
4. Select the file location in [File selection method].

   - Local

     Import a backup file kept locally.

   - FTP

     Import a backup file from the FTP server of ISM-VA.
     You must transfer the backup file to the directory under the "/<user group name>/ftp" of ISM-VA in advance.

     For details on FTP connection and transferring procedures, refer to "2.1.2 FTP Access" in "User's Guide."
5. Specify the import target backup file in [File], and then select the [Execute] button.

   Import will be executed.

Point

You can select multiple nodes for importing.

7.1.5 Restore Server Settings

Restore the hardware setting files saved in "7.1.1 Backup Server Settings" or the files imported in "7.1.4 Import Server Settings" to the server registered in ISM.

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
2. From the menu on the left side of the screen, select [Backup / Restore Hardware Settings].
3. In the [Column Display] field on the "Node List" screen, select [Restore].
4. Select a node, from the [Actions] button, select [Restore Hardware Settings].

   The "Restore hardware settings" screen will be displayed.
5. When restoring the BIOS hardware settings, switch off the power of the server in advance, select the [Get power status] button, and then check that the power status has turned to "Off."
6. Select a file, then select the [Confirm] button according to the instructions on the screen.
7. Confirm the settings, select the [Above contents are correct.] checkbox and then select the [Execute] button.

Point

You can select multiple nodes for restoring.

Note

Restoration of hardware settings may fail in some iRMC firmware versions if LDAP is enabled in the iRMC settings, and HTTP is specified as the protocol in [Web I/F URL] on the Details of Node screen. In this case, edit the node information to set HTTPS in [Web I/F URL] as the protocol. For information on editing nodes, refer to "2.2.3 Editing of Datacenters/Floors/Racks/Nodes" in "User's Guide."

7.2 Backup/Restore Settings of Switches and Storages

By saving switch or storage settings registered in ISM to a file, you can restore hardware settings or export or import hardware settings to another ISM.

7.2.1 Backup Settings of Switches and Storages

Collect the settings for the switches and storages registered in ISM and store them as files. Moreover, you can export the stored files.

1. Before backing up, power on the hardware.
2. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
3. From the menu on the left side of the screen, select [Backup / Restore Hardware Settings].
4. Select a node, from the [Actions] button, select [Backup Hardware Settings].

   The "Backup Hardware Settings" screen will be displayed.
5. Select the checkboxes for [Switch] and [Storage] that you want to back up settings, and then select the [Execute] button.

Point

You can select multiple nodes and hardware settings, and back them up collectively.

7.2.2 Export Settings of Switch and Storage

You can export the files stored in "7.2.1 Backup Settings of Switches and Storages."

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
2. From the menu on the left side of the screen, select [Backup / Restore Hardware Settings].
3. Select a node, from the [Actions] button, select [Export (Backup file)].

   The "Export Backup File" screen will be displayed.
4. Select a file, and then select the [Execute] button according to the instructions on the screen.

Point

You can select multiple nodes and hardware settings to export them collectively.

7.2.3 Import Settings of Switches

Import the hardware setting file of the switch exported in "7.2.2 Export Settings of Switch and Storage."

1. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
2. From the menu on the left side of the screen, select [Backup / Restore Hardware Settings].
3. Select a node, from the [Actions] button, select [Import].

   The "Import Backup File" screen is displayed.
4. Select the file location in [File selection method].

   - Local

     Import a backup file kept in local.

   - FTP

     Import a backup file from the FTP server of ISM-VA.
     You must transfer the backup file to the directory under the "/<user group name>/ftp" of ISM-VA in advance.

     For details on FTP connection and transferring procedures, refer to "2.1.2 FTP Access" in "User's Guide."
5. Specify the import target backup file in [File], and then select the [Execute] button.

   Import will be executed.

Point

You can select multiple nodes for importing.

7.2.4 Restore Settings of Switches

Restore the hardware setting files of the switches that are registered in ISM. The following files can be restored:

- The hardware setting file of the switch saved in "7.2.1 Backup Settings of Switches and Storages."
- The file imported in "7.2.3 Import Settings of Switches."

1. Before restoring, power on the hardware.
2. From the Global Navigation Menu on the ISM GUI, select [Structuring] - [Profiles].
3. From the menu on the left side of the screen, select [Backup / Restore Hardware Settings].
4. In the [Column Display] field on the "Node List" screen, select [Restore].
5. Select a node, from the [Actions] button, select [Restore Hardware Settings].

   The "Restore hardware settings" screen will be displayed.
6. Select a file, then select the [Confirm] button according to the instructions on the screen.
7. Confirm the settings, select the [Above contents are correct.] checkbox and then select the [Execute] button.

Point

You can select multiple nodes for restoring.

Note

When you restore the ExtremeSwitching VDX, execute restoration after initializing setting items. If the setting items are not initialized before restoration, contents of the backup may not be reflected.

For VDX, some setting items cannot be restored. The following are the setting items that cannot be restored:

- License information
- Switch mode
- Chassis/host name
- Password
- Management port
- NTP server setting
- Date and time settings (clock set command)

Confirm the settings after restoration and execute settings if required.

Chapter 8 Prepare/handle ISM errors

This chapter describes preparations for errors which may occur in ISM and countermeasures for them.

8.1 Backup/Restore ISM

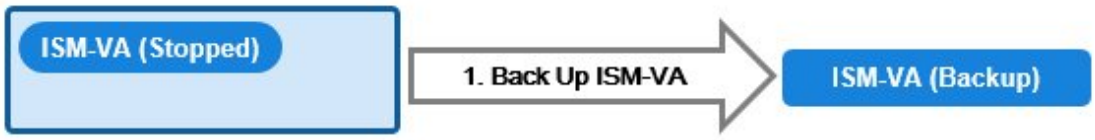
This section describes the procedure to Backup/Restore ISM.

With use of this procedure, you can back up the running ISM-VA without switching off its power, being different from the backups using the hypervisor. Also, you can back up in a short time since the backup targets are limited.

The following is the procedure to backup/restore ISM.

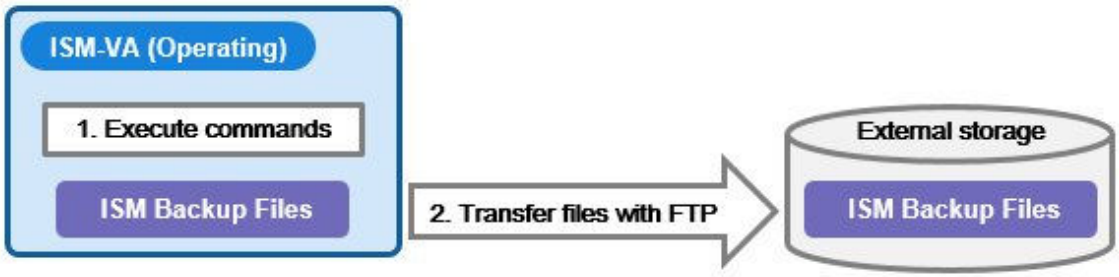
1. As a preparation, back up the ISM-VA on which you are going to restore ISM.

   Refer to "8.1.1 Back up ISM-VA."



2. Back up the ISM.

   Refer to "8.1.2 Back up ISM."



3. Restore the ISM.

   Refer to "8.1.3 Restore ISM."

Figure 8.1 When restoring to ISM-VA that was backed up in "8.1.1 Back up ISM-VA"

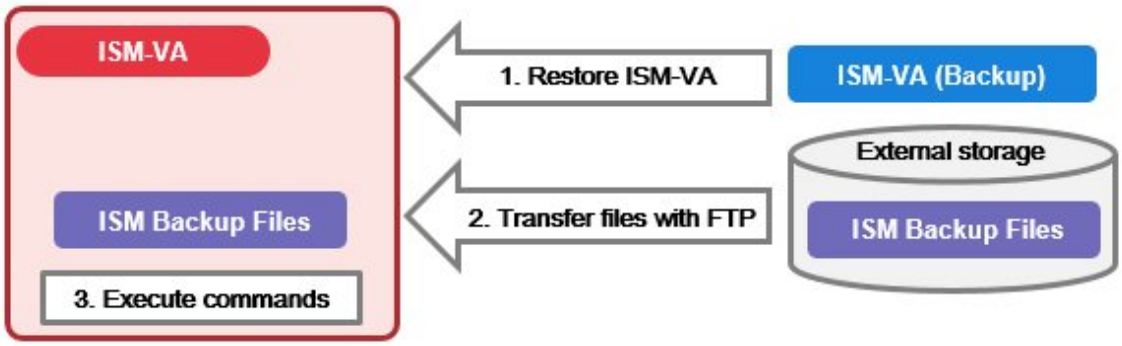
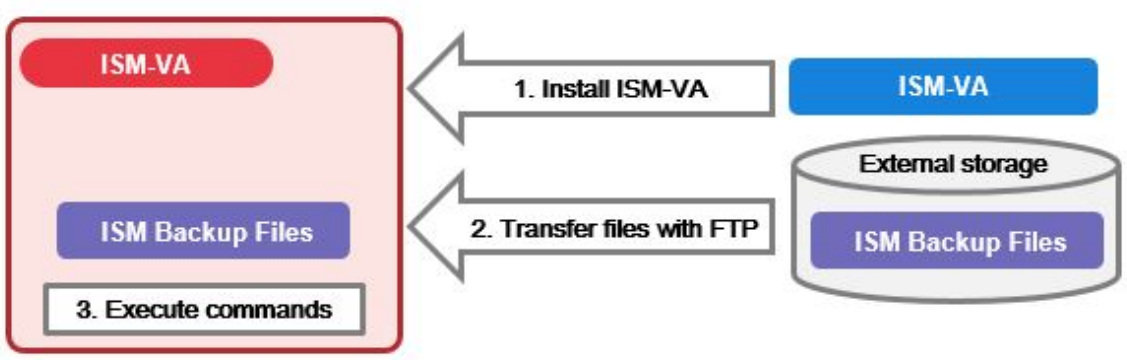


Figure 8.2 ISM-VA right after installation (Including ISM upgrade and ISM patches)



8.1.1 Back up ISM-VA

Back up the ISM-VA on which you are going to restore backup files of the ISM.

ISM-VA is backed up using the export function of the hypervisor or backup software. Back up the ISM-VA of the version that you intend to use.

The following procedures describe the procedure to backup ISM-VA from Microsoft Windows Server Hyper-V, VMware vSphere Hypervisor, and KVM.

If you are using backup software to back up the ISM-VA, refer to the backup software documentation to back up the ISM-VA virtual machine.

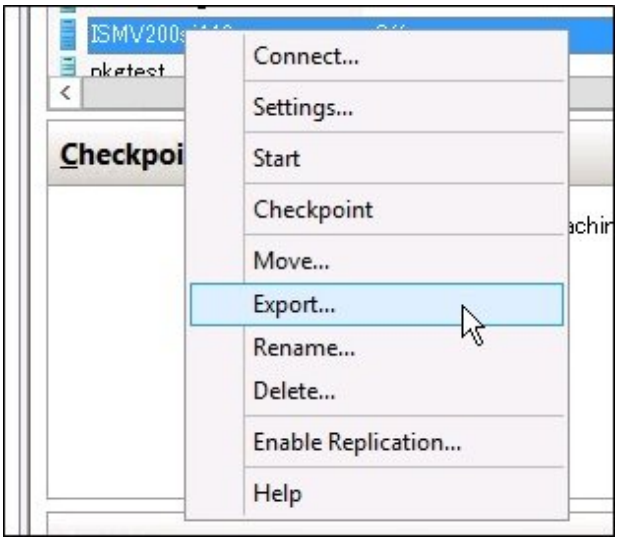
Note

- Be sure to back up ISM-VA after the following operations:
  - ISM implementation
  - ISM upgrade
  - Patch application for ISM
- Before backing up ISM-VA, stop ISM-VA. For the procedure to stop ISM-VA, refer to "4.1.2 Stop of ISM-VA" in "User's Guide."
- The virtual machine acting as the ISM-VA contains swap space required for the operational foundation of the ISM-VA. When using backup software to back up the ISM-VA, back up the entire virtual machine (virtual disk), including the swap space.

  If you do not back up the swap space, the restored ISM-VA may run out of memory and become inoperable.
- You can use Nutanix AHV as a hypervisor for the KVM version of ISM-VA. However, when using Nutanix AHV, you cannot back up ISM-VA using the hypervisor export function. Use the replication function for Nutanix remote. For details, refer to the Nutanix documentation.

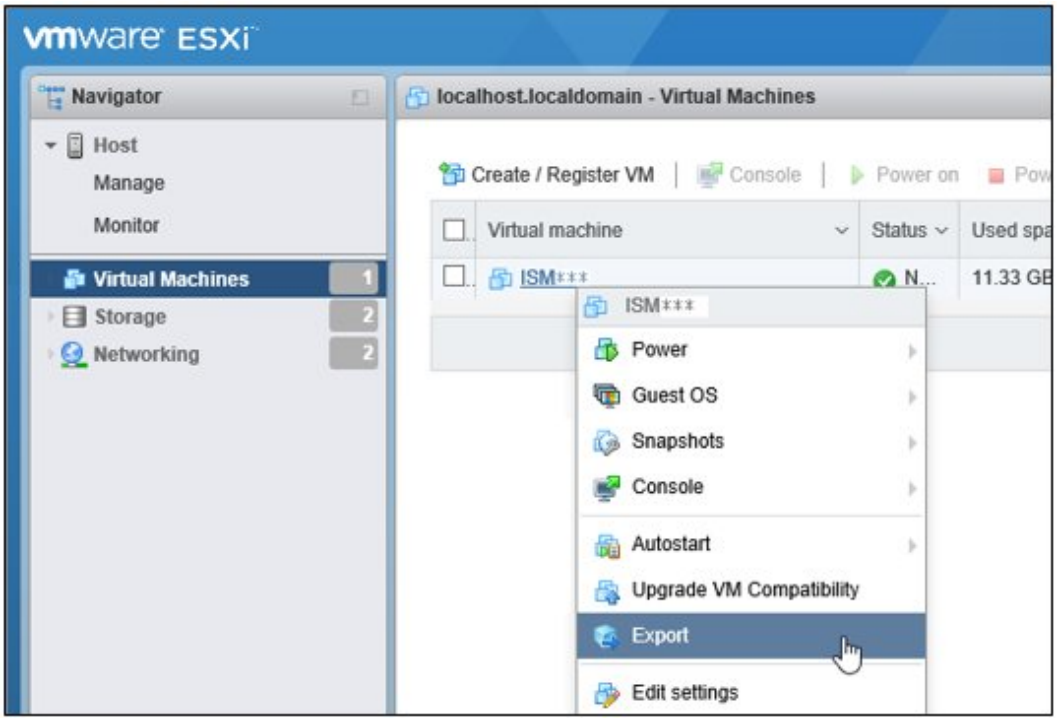
8.1.1.1 Back up ISM-VA running on Microsoft Windows Server Hyper-V

In Hyper-V Manager, right-click on the installed ISM-VA, and then select [Export].



8.1.1.2 Back up ISM-VA running on VMware vSphere Hypervisor 6.5 or later

In vSphere Client (HTML5), right-click on the installed ISM-VA, and then select [Export].



8.1.1.3 Back up ISM-VA running on KVM

Back up the KVM files that are stored in the following locations to other locations as necessary:

- /etc/libvirt/qemu
- /var/lib/libvirt/images

8.1.2 Back up ISM

Collect backup target files such as ISM-VA configuration information and node management data, and then create an ISM backup file.

Note

- In the following cases, you cannot create backups:
  - When you do not have enough disk space on ISM-VA required for backing up ISM
    Delete repositories, Archived Logs or Node Logs, or assign a virtual disk on the system.
  - When ISM services are stopped
    Start ISM services.
  - When the tasks such as profile assignment or firmware updates are working
    Wait to complete the tasks or cancel the tasks.
- During backing up of the ISM, all ISM services (Node Management, Monitoring, etc.) are stopped. After backups are complete, all ISM services will restart automatically.
- Backup execution by using GUI, REST API or the workflow service is not provided.

1. From the Console as an administrator, log in to ISM-VA.
2. Execute a command for backing up the ISM.

   ```
   # ismadm system backup
   ```

   Example of ISM backup command execution:

   ```
   # ismadm system backup
   [System Information]
     Version : 2.8.0.x (S2022xxxx-xx)

   [Disk Space Available]
     System          : 30000MB

   [Disk Space Required]
     System          : 2400MB

   Start backup process? [y/n]:
   ```

   After executing the command, the backup confirmation screen is displayed.
3. Enter "y" to start backup.

   After completing backup, backup file names of the ISM will be displayed.

   Example of ISM backup file name display:

   ```
   ism backup end.
   Output file: ism2.8.0.x-backup-20220601120000.tar.gz
   ```

   ISM backup file name: ism<version>-backup-<backup date/time>.tar.gz
4. Download the backup file of the ISM created.

   Access "ftp://<ISM-VA IP address>/Administrator/ftp" with FTP to download the backup file of the ISM.

   Note

   When you transfer backup files with FTP, transfer them in binary mode.

8.1.3 Restore ISM

Restore the backup file of ISM created in "8.1.2 Back up ISM" to the ISM-VA.

Note

- In the following cases, you cannot execute ISM restoring:
  - When the version of the backup file of ISM is different from the version of ISM-VA in the restore destination
    You must restore the files to the same version of the ISM-VA as that of the ISM.
  - When the disk of the ISM-VA does not have enough space for restoring ISM
    Delete repositories Archived Logs or Node Logs, or allocate a virtual disk on ISM-VA.
  - When the configuration of the virtual disk of the ISM backup file is different from the configuration of the virtual disk in the restore destination of ISM-VA (ISM 2.8.0.030 or later)
    You must restore the file to the same virtual disk configuration of the ISM-VA as that of ISM.
- Restore execution by using GUI, REST API or the workflow service is not provided.

1. Prepare one of the following ISM-VA as a restore destination.
   - ISM-VA that was backed up in "8.1.1 Back up ISM-VA."

     For information on restoring procedures, refer to "3.3 Installation of ISM-VA" in "User's Guide."
   - ISM-VA right after installation (Including ISM upgrade and ISM patches)

     For information on installation procedures, refer to "3.3 Installation of ISM-VA" in "User's Guide."

     For information on patch application procedures, refer to "9.1 Apply Patches and Upgrade Programs to ISM."
2. Prepare the ISM backup file created in "8.1.2 Back up ISM."
3. Transfer the file to the ISM-VA which is the restore destination with FTP. Access "ftp://<ISM-VA IP address of the restore destination>/Administrator/ftp" with FTP to store the backup file of the ISM prepared in Step 2.
4. From the console as an administrator, log in to the ISM-VA of the restore destination.
5. Execute a command for restoring the ISM.

   ```
   # ismadm system restore -file <backup file name>
   ```

   Example of ISM restore command execution:

   ```
   # ismadm system restore -file ism2.8.0.x-backup-20220601120000.tar.gz
   [System Information]
     Version : 2.8.0.x (S2022xxxx-xx)

   [Backup File Information]
     Version : 2.8.0.x (S2022xxxx-xx)

   [Disk Space Available]
     System         : 30000MB

   [Disk Space Required]
     System         : 2400MB

   Start restore process? [y/n]:
   ```

   After executing the command, the restoration confirmation screen is displayed.
6. Enter "y" to start restoring.

   After completing restoring, the following message is displayed.

   ```
   You need to reboot the system to use.
   It will take several minutes to complete.
   Immediately reboots the system.  [y/n]:
   ```
7. Enter "y" to restart ISM-VA.

8. Allocate virtual disks.

   Point

   After restoring ISM, the allocation of virtual disk for all user groups is released. Also, the status of the virtual disk in ISM-VA is back the status of ISM-VA that had backed up.

   For ISM 2.8.0.030 or later, after restoring ISM, the virtual disk allocation of the user group and the system virtual disk allocation are as they were when the ISM-VA was backed up.

   Confirm the status of allocation of the virtual disk and allocate the virtual disk of the user groups as according to the procedure to allocate new virtual disks. For information on virtual disk allocation, refer to "3.7 Allocation of Virtual Disks" in "User's Guide."

   For ISM 2.8.0.030 or later, allocation of virtual disk is not required.

9. After allocating the virtual disks, restart ISM-VA.
10. Execute the Power Capping settings.

    Point

    After restoring the ISM, the Power Capping on each rack is disabled.

    If you are using the Power Capping for the racks, enable the Power Capping policy.

    For information on enabling the power capping policy, refer to "6.5.3 Enable the Power Capping Policy of the Racks."

11. When restoring ISM, repositories, Archived Logs and Node Logs are deleted. Execute import of repositories and collection of logs as required.

8.2 Collect Maintenance Data

There are two ways to collect the maintenance data of ISM, one is using the GUI and the other is using a command.

Point

Refer to "4.5.1 Required Maintenance Data" in "User's Guide" for maintenance data on the following functions.

- Virtual Resources Management
- Cluster Management
- Cluster Creation
- Cluster Expansion

8.2.1 Collect Maintenance Data with GUI

Log in to the ISM GUI to collect and download the maintenance data with the following procedure.

Point

This operation can be executed only by ISM Administrators (who belong to an Administrator group and have an Administrator role).

Collect New Maintenance Data

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [General].

2. From the menu on the left side of the screen, select [Maintenance Data].

   The "Maintenance Data" screen is displayed.

3. From the [Actions] button, select [Collect].
4. On the screen displayed, select the following, and then select the [Run] button.
   - Collection Target
     - Full: Collection of ISM RAS Logs, ISM-VA Operation System Logs, and database information together
     - Limited: Collection of ISM RAS Logs only
   - Collection Period
     - Entire period
     - Specify by Date: Specify Start Date and End Date for collection

   Note

   Batch collection of maintenance data takes several hours to complete and requires large amounts of free disk space. For details, refer to "3.2.1.5 Estimation of required disk space for maintenance data" in "User's Guide."

   Collection starts and the progress of the collection is displayed in the [Status] column. Refresh the screen to update the displayed progress.

   The progress can also be checked from the "Task" screen. The displayed task type is "Collecting Maintenance Data."

   When the collection is complete, the Status icon becomes "Complete" and you can download the data.

Download Maintenance Data

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [General].
2. From the menu on the left side of the screen, select [Maintenance Data].

   The "Maintenance Data" screen is displayed.

3. Select the [Download] button of the maintenance data that you want to collect.
4. Download the maintenance data according to the download confirmation of the browser.

Delete Maintenance Data

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [General].
2. From the menu on the left side of the screen, select [Maintenance Data].

   The "Maintenance Data" screen is displayed.

3. Select the checkbox for the Maintenance Data you want to delete, from the [Actions] button, select [Delete].

   The file name of the data to be deleted is displayed.

4. Confirm the file name, then select the [Run] button.

Cancel collecting Maintenance Data

1. From the Global Navigation Menu on the ISM GUI, select [Settings] - [General].
2. From the menu on the left side of the screen, select [Maintenance Data].

   The "Maintenance Data" screen is displayed.

3. Select the checkbox for the Maintenance Data being collected, from the [Actions] button, select [Cancel].

   For the Maintenance Data being collected, the progress status is displayed in the [Status] column.

4. On the displayed confirmation screen, select the [Yes] button.

   Canceled maintenance data will be deleted.

Note

- The maintenance data collected from the "Maintenance Data" screen in ISM GUI are retained in the following directory and only the maintenance data under this directory will be displayed:

  Maintenance Data storage directory: /Administrator/transfer

  The maintenance data retained in the FTP communication directory of ISM-VA/Administrator/ftp are not displayed on the "Maintenance Data" screen.

- The maintenance data will be retained for five generations. If it exceeds five generations, it will be deleted automatically from the oldest creation date and time.

- The maintenance data will be deleted automatically five weeks after collected.

8.2.2 Collect Maintenance Data to Execute the Command

Use the ISM-VA commands to collect ISM maintenance data.

1. After starting up ISM-VA, log in to ISM-VA from the console as an administrator.
2. Collect the ISM maintenance data.

   Sample investigation of malfunctions in ISM and/or ISM-VA

   - For the collection of ISM RAS Logs only (no time period specified)

```
# ismadm system snap -dir /Administrator/ftp
snap start
Your snap has been generated and saved in:
  /Administrator/ftp/ismsnap-20220110175323.zip
```

   - For the batch collection of ISM RAS Logs, ISM-VA Operating System Logs, and database information (no time period specified)

```
# ismadm system snap -dir /Administrator/ftp -full
snap start
Your snap has been generated and saved in:
 /Administrator/ftp/ismsnap-20220110175808-full.zip
```

   - For the batch collection of ISM RAS Logs, ISM-VA Operating System Logs, database information, collected statistics information by Anomaly Detection and Packet Analysis of Virtual Network (collection period required)

     A collection period (2022/05/18 to 2022/05/19) is specified.

```
# ismadm system snap -dir /Administrator/ftp -full -extstats -from 20220518 -to 20220519
snap start
Your snap has been generated and saved in:
 /Administrator/ftp/ismsnap-20220519072513-20220518-20220519-full-extstats.zip
```

   - For the collection of ISM RAS Logs only with a collection period (2021/12/10 to 2022/1/10) specified

```
# ismadm system snap -dir /Administrator/ftp -from 20211210 -to 20220110
snap start
Your snap has been generated and saved in:
  /Administrator/ftp/ismsnap-20220110175323-20211210-20220110.zip
```

   - For the batch collection of ISM RAS Logs, ISM-VA Operating System Logs, and database information with a collection period (2021/12/10 to 2022/1/10) specified

```
# ismadm system snap -dir /Administrator/ftp -full -from 20211210 -to 20220110
snap start
```

```
Your snap has been generated and saved in:
 /Administrator/ftp/ismsnap-20220110175808-20211210-20220110-full.zip
```

Point

- "-dir" specifies the output destination path. By specifying a file transfer area as described in "2.1.2 FTP Access" in "User's Guide," you can obtain the maintenance data collected with FTP access.
- To specify the period of maintenance data to be collected, specify the collection start date and collection end date by adding the "-from" and "-to" options. Specify the date in "YYYYMMDD" format. If you specify the period of maintenance data to be collected, the collection start date and collection end date are added to the file name. The collection start date and collection end date are set based on the time zone set in ISM-VA.

  If no period is specified, maintenance data is collected for the entire period.

Note

- Batch collection of maintenance data takes several hours to complete and requires large amounts of free disk space. For details, refer to "3.2.1.5 Estimation of required disk space for maintenance data" in "User's Guide."
- When you execute a command, the following message may be displayed on the hypervisor console, but this does not mean there is a problem.

```
blk_update_request:I/O error, dev fd0, sector 0
```

3. Download the collected maintenance data.

   When you execute the command for collection, the output destination path and file names are displayed; access and download these with FTP as an administrator from the management terminal.

Note

The five latest files are stored in the maintenance data created in the directory where the maintenance data is stored. Use the FTP client software and manually delete maintenance data that are no longer required since saved maintenance data is not deleted automatically.

Chapter 9 Update ISM

This chapter describes procedures to update ISM such as application of patches and upgrade of ISM-VA.

9.1 Apply Patches and Upgrade Programs to ISM

Apply patches and upgrade programs to ISM.

Point

For ISM patches and upgrades contact your local Fujitsu customer service partner.

Note

- Before applying patches and upgrade programs, back up ISM-VA.

  For information on the procedure to back up ISM-VA, refer to "8.1.1 Back up ISM-VA."

- If you have upgraded to ISM 2.8.0 from ISM 2.7.0.030 and earlier, you cannot use Log Management after the upgrade.
  If you have upgraded from ISM 2.7.0.030 and earlier and you have not used the system update command, you cannot use Log Management after applying the patch.

  You must execute the command after restarting ISM-VA (Step 11) to be able to use Log Management.

- ISM-VA disk space is used for system updates. For disk space requirements, refer to "System updates after applying a patch or upgrade" in "1.3.1 Requirements for Hypervisor to Run ISM-VA (Virtual Machines)" in "User's Guide."

1. Confirm the amount of disk space required for when the patch or upgrade is applied.

   For patches

   a. Log in to ISM-VA from the console as an administrator and execute the following command.

   ```
   # apply-update
   ```

   One of the following messages is displayed.

   If (Message 3) is displayed, Steps b to d are not needed.

   (Message 1)

   ```
   Ready to start System update.

   Number of total node logs: 75416
   Disk size required for system updates: 31.1MB
   Size of available space: 20.8MB
   Not Enough hard disk space for system update without deleting Node Log.
   If system update without deleting Node Log, after selection “0: Cancel System Update” please
   free at least an additional 31.1MB of disk space on ‘/’ .
   If you do not need the node logs, please select "1: System Update (Delete Node Log)" from the
   menu below.

   1: System Update (Delete Node Log)
   0: Cancel System Update
   Please select one of the mode:
   ```

Point

If "Disk size required for system updates" appears in the message, the node logs must be deleted during the system update due to lack of disk space.
If you want to keep past node logs, execute one of the following.

- Confirm the amount of space in "Size of available space" (Current available disk space) and free up memory until you have the amount of space mentioned in "Disk size required for system updates."
- Refer to "2.5.6 Downloading Node Logs" in "User's Guide" to download node logs beforehand.

(Message 2)

```
Ready to start System update

Number of total node logs: 27364
Time of System update depends on the number of Node log.
If you do not need the node logs, please select "1: System Update (Delete Node Log)" from the
menu below.
"Delete Node Log" contributes to shortening of System upgrade.

1: System Update (Delete Node Log)
2: System Update (Node Log Undeleted)
0: Cancel System Update
Please select one of the mode:
```

(Message 3)

```
Your system is up to date.
```

b. Confirm the number (Number of node logs for all nodes registered in ISM) in the "Number of total node logs" row.

c. Select "0: Cancel System Update" to close the message.

d. Calculate the required disk space using the following formula.

```
<Number confirmed in Step b> x 500 Bytes
```

For upgrades

a. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].

b. Select the node name on the "Node List" screen.

c. On the Details of Node screen, select the [Properties] tab, and check the number of logs displayed in "Node Logs."

d. Add up the number of Node Logs for all nodes registered with ISM and use the following formula to calculate the required disk space.

```
<Number of Node Logs for all nodes> x 500 bytes
```

2. Log in to ISM-VA from the console as an administrator, check the system space (entire ISM-VA), and free disk space for the Administrator user group.

```
# ismadm volume show -disk
```

To determine the amount of free disk space in the system (entire ISM-VA), see "Avail" in the "/" mount location.

If you have allocated virtual disks to the Administrator user group, also check the free disk space in the Administrator user group.

Refer to "Avail" in the "'RepositoryRoot'/Administrator" mount location for free disk space for the Administrator user group.

3. Add the disks required for when the patch or upgrade is applied.

Determine how much disk space is required to apply it based on the disk space calculated in Step 1 and the size of the patch or upgrade file.

- If no virtual disk is allocated to the Administrator user group

  Free space required for the system (entire ISM-VA):

  The total of the "capacity calculated in Step 1" and the "capacity approximately six times the patch or upgrade file size"

- If virtual disks are allocated to the Administrator user group

  - Free space required for the system (entire ISM-VA):

    "About three times the patch or upgrade file size"

  - Administrator user group requires:

    The total of the "capacity calculated in Step 1" and the "capacity around three times the patch or upgrade file size"

If you run out of space, add virtual disks for both the system (entire ISM-VA) and the Administrator user group. Refer to "3.7 Allocation of Virtual Disks" and "4.6 Management of Virtual Disks" in "User's Guide" to add virtual disks.

4. From the Global Navigation Menu on the ISM GUI, select [Settings] - [General].
5. From the menu on the left side of the screen, select [ISM patch / upgrade program].

   The current version of ISM is displayed.
6. Select the [Update ISM] button.
7. Follow the instructions on the "ISM Patch / Upgrade Program" screen and input the setting items. Select the [Confirm] button.
8. Confirm the contents, and then select the [Yes] button.
9. Wait for the patch or upgrade to be applied.

   After application of the patch or upgrade is completed, clear the cache and go to the login screen.
10. After logging into ISM, confirm that the patch or upgrade is applied.

    From the Global Navigation Menu on the ISM GUI, select [Help] - [About ISM].
    Confirm that selected version is displayed.
11. Log in to ISM-VA from the console as an administrator and execute the following system update command.

```
# apply-update
```

If the following message is displayed, the system is already up to date. The procedures below are not required.

```
Your system is up to date.
```

If the following message is displayed, you must update the system.

- If there is enough disk space required to save node logs

```
# apply-update
Ready to start System update.

Number of total node logs: 27364
Time of System update depends on the number of Node log.
If you do not need the node logs, please select "1: System Update (Delete Node Log)" from the
menu below.
"Delete Node Log" contributes to shortening of System upgrade.

1: System Update (Delete Node Log)
2: System Update (Node Log Undeleted)
0: Cancel System Update
Please select one of the mode:
```

- If there is not enough disk space required to save node logs

```
Ready to start System update.

Number of total node logs: 75416
```

```
Disk size required for system updates: 31.1MB
Size of available space: 20.8MB
Not Enough hard disk space for system update without deleting Node Log.
If system update without deleting Node Log, after selection “0: Cancel System Update” please
free at least an additional 31.1MB of disk space on ‘/’ .
If you do not need the node logs, please select "1: System Update (Delete Node Log)" from the
menu below.

1: System Update (Delete Node Log)
0: Cancel System Update
Please select one of the mode:
```

Choose whether to delete the Node Logs stored on ISM-VA during system updates (1 or 2).

For more details, refer to "4.17 Application of Patches" or "4.18 Upgrade of ISM-VA" in "User's Guide."

The system update process continues in the background.

Note

- Do not turn off ISM-VA during a system update. In the unlikely event that ISM-VA is rebooted, restore to a version of ISM-VA that was backed up before the patch was applied.
- During a system update, if you perform an operation that uses a lot of system space, such as a DVD import, the system update may fail. In this case, perform the system update again.

12. Confirm the status of system update.

    Log in to ISM-VA from the console as an administrator and execute the following system update command.

    After the update is completed, all ISM functions will be available.

```
# apply-update
```

    - During the system update

      The following message is displayed.

```
System update - progress (XX/yy)
```

      Displays the progress of the system update as a section. Where XX is the current section number and yy is the total number of sections. When the current section number is equal to the total number of sections, the system update is complete.

    - When the system update is complete

      The following message is displayed.

```
Your system is up to date.
```

Point

The system update failed if the "50140050" log is output.

Collect maintenance data for ISM and contact your local Fujitsu customer service partner.