FUJITSU Software
Infrastructure Manager V2.4
Infrastructure Manager for PRIMEFLEX V2.4

Operating Procedures

CA92344-2708-04
October 2019

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

Note

"Infrastructure Manager for PRIMEFLEX" is available only in Japan, APAC, and North America.

Product Manuals

Manual Name	Description
FUJITSU Software Infrastructure Manager V2.4 Infrastructure Manager for PRIMEFLEX V2.4 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 V2.4 Infrastructure Manager for PRIMEFLEX V2.4 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 V2.4 Infrastructure Manager for PRIMEFLEX V2.4 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 V2.4 Infrastructure Manager for PRIMEFLEX V2.4 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 V2.4 Infrastructure Manager for PRIMEFLEX V2.4 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 V2.4 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 V2.4 Infrastructure Manager for PRIMEFLEX V2.4 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 V2.4 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.

Manual Name	Description
	In this manual, it is referred to as "ISM for PRIMEFLEX Parameter List."
FUJITSU Software Infrastructure Manager V2.4 Infrastructure Manager for PRIMEFLEX V2.4 Glossary	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."
FUJITSU Software Infrastructure Manager V2.4 Infrastructure Manager for PRIMEFLEX V2.4 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 - Infrastructure Manager Plug-in for VMware vRealize Orchestrator 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.

http://manuals.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 following abbreviations.

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	
Microsoft(R) Windows Server(R) 2016 Datacenter	Windows Server 2016 Datacenter	Windows Server 2016
Microsoft(R) Windows Server(R) 2016 Standard	Windows Server 2016 Standard	
Microsoft(R) Windows Server(R) 2016 Essentials	Windows Server 2016 Essentials	
Microsoft(R) Windows Server(R) 2012 R2 Datacenter	Windows Server 2012 R2 Datacenter	Windows Server 2012 R2
Microsoft(R) Windows Server(R) 2012 R2 Standard	Windows Server 2012 R2 Standard	
Microsoft(R) Windows Server(R) 2012 R2 Essentials	Windows Server 2012 R2 Essentials	
Microsoft(R) Windows Server(R) 2012 Datacenter	Windows Server 2012 Datacenter	Windows Server 2012
Microsoft(R) Windows Server(R) 2012 Standard	Windows Server 2012 Standard	
Microsoft(R) Windows Server(R) 2012 Essentials	Windows Server 2012 Essentials	
Microsoft(R) Windows Server(R) 2008 R2 Datacenter	Windows Server 2008 R2 Datacenter	Windows Server 2008 R2
Microsoft(R) Windows Server(R) 2008 R2 Enterprise	Windows Server 2008 R2 Enterprise	
Microsoft(R) Windows Server(R) 2008 R2 Standard	Windows Server 2008 R2 Standard	
Red Hat Enterprise Linux 8.0 (for Intel64)	RHEL 8.0	Red Hat Enterprise Linux Or Linux
Red Hat Enterprise Linux 7.7 (for Intel64)	RHEL 7.7	
Red Hat Enterprise Linux 7.6 (for Intel64)	RHEL 7.6	
Red Hat Enterprise Linux 7.5 (for Intel64)	RHEL 7.5	
Red Hat Enterprise Linux 7.4 (for Intel64)	RHEL 7.4	

Official name	Abbreviation	
Red Hat Enterprise Linux 7.3 (for Intel64)	RHEL 7.3	
Red Hat Enterprise Linux 7.2 (for Intel64)	RHEL 7.2	
Red Hat Enterprise Linux 7.1 (for Intel64)	RHEL 7.1	
Red Hat Enterprise Linux 6.10 (for Intel64)	RHEL 6.10(Intel64)	
Red Hat Enterprise Linux 6.10 (for x86)	RHEL 6.10(x86)	
Red Hat Enterprise Linux 6.9 (for Intel64)	RHEL 6.9(Intel64)	
Red Hat Enterprise Linux 6.9 (for x86)	RHEL 6.9(x86)	
Red Hat Enterprise Linux 6.8 (for Intel64)	RHEL 6.8(Intel64)	
Red Hat Enterprise Linux 6.8 (for x86)	RHEL 6.8(x86)	
Red Hat Enterprise Linux 6.7 (for Intel64)	RHEL 6.7(Intel64)	
Red Hat Enterprise Linux 6.7 (for x86)	RHEL 6.7(x86)	
Red Hat Enterprise Linux 6.6 (for Intel64)	RHEL 6.6(Intel64)	
Red Hat Enterprise Linux 6.6 (for x86)	RHEL 6.6(x86)	
SUSE Linux Enterprise Server 15 SP1 (for AMD64 & Intel64)	SUSE 15 SP1 (AMD64) SUSE 15 SP1 (Intel64) or SLES 15 SP1 (AMD64) SLES 15 SP1 (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)	
SUSE Linux Enterprise Server 12 SP4 (for AMD64 & Intel64)	SUSE 12 SP4(AMD64) SUSE 12 SP4(Intel64) or SLES 12 SP4(AMD64) SLES 12 SP4(Intel64)	
SUSE Linux Enterprise Server 12 SP3 (for AMD64 & Intel64)	SUSE 12 SP3(AMD64) SUSE 12 SP3(Intel64) or SLES 12 SP3(AMD64) SLES 12 SP3(Intel64)	
SUSE Linux Enterprise Server 12 SP2 (for AMD64 & Intel64)	SUSE 12 SP2(AMD64) SUSE 12 SP2(Intel64) or SLES 12 SP2(AMD64) SLES 12 SP2(Intel64)	
SUSE Linux Enterprise Server 12 SP1 (for AMD64 & Intel64)	SUSE 12 SP1(AMD64) SUSE 12 SP1(Intel64) or SLES 12 SP1(AMD64) SLES 12 SP1(Intel64)	
SUSE Linux Enterprise Server 12 (for AMD64 & Intel64)	SUSE 12(AMD64) SUSE 12(Intel64) or SLES 12(AMD64) SLES 12(Intel64)	

Official name	Abbreviation	
SUSE Linux Enterprise Server 11 SP4 (for AMD64 & Intel64)	SUSE 11 SP4(AMD64) SUSE 11 SP4(Intel64) or SLES 11 SP4(AMD64) SLES 11 SP4(Intel64)	
SUSE Linux Enterprise Server 11 SP4 (for x86)	SUSE 11 SP4(x86) or SLES 11 SP4(x86)	
VMware(R) vSphere(TM) ESXi 6.7	VMware ESXi 6.7	VMware ESXi
VMware(R) vSphere(TM) ESXi 6.5	VMware ESXi 6.5	
VMware(R) vSphere(TM) ESXi 6.0	VMware ESXi 6.0	
VMware(R) vSphere(TM) ESXi 5.5	VMware ESXi 5.5	
VMware Virtual SAN	vSAN	

Terms

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

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.

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

Copyright 2019 FUJITSU LIMITED

This manual shall not be reproduced or copied without the permission of Fujitsu Limited.

Modification History

Edition	Publication Date	Modification Overview	Section	
01	February 2019	First edition	-	-
02	April 2019 Modification for ISM 2.4.0.b patch application	Added Operation Mode to the description on the output of results command	2.1.4 Register Licenses	Table "Description on output for "license show" command results"
		Added an article on linking with Microsoft Active Directory groups and user roles	2.7.2.1 Add user groups	-
		Added user roles to information that can be edited	2.7.2.2 Edit user groups	-
		Added an article on linking with a user on a directory server	2.7.3 Link with Microsoft Active Directory or LDAP	-
		Added a new article on the procedure for managing users and passwords on a directory server	2.7.3.2 Manage users and passwords on directory servers (ISM 2.4.0.b or Later)	Title and article
		Added an article on including the FQDN name in the range for searches	3.1.1 Discover Nodes in the Network and Register Nodes	Discovery (When you select "Normal" for [Discovery method])
		Added an article on the procedure for setting an OS policy	3.3.3 Create a Policy to Simplify Profile Creation	-
		Added a new article on the procedure for creating batch profiles and allocating profiles to nodes	3.5 Create a Batch of Multiple Profiles and Allocate Them to Nodes	-
		Added an article on packet analysis results	6.5.8 Check Packet Analysis Result	-

Edition	Publication Date	Modification Overview	Section	
		Added an article for the types of firmware data and the update procedure for firmware data supported by Firmware Rolling Update	6.6.2.1 Operation requirements for Firmware Rolling Update	-
		Added an article on the preparation for setting up vCenter Server VMware EVC	6.9.1.1 Set up vCenter Server VMware EVC	-
03	May 2019 Modification for ISM 2.4.0.c patch application	Added an article on discovery and registration of PRIMERGY GX2580 M5	3.1.1 Discover Nodes in the Network and Register Nodes	-
		Added an article on registration of PRIMERGY GX2580 M5	3.1.2 Register a Node Directly	-
		Added an article on the PRIMERGY M5 series	6.7 Create a Cluster for PRIMEFLEX HS/PRIMEFLEX for VMware vSAN	-
			6.7.1.10 Set up BIOS	-
			6.9 Expand a Cluster for PRIMEFLEX HS/PRIMEFLEX for VMware vSAN	-
			6.9.1.8 Create a profile	-
			6.9.1.12 Set up BIOS	-
	May 2019 Major re-organization of the manual construction	Added an article on operation requirements for Cluster Creation	6.7.2.1 Operation requirements for Cluster Creation	-
			6.8.2.1 Operation requirements for Cluster Creation	-
04	October 2019 Major re-organization of the manual construction	Modified an article on adding a successor server to PRIMEFLEX	6.9.1.1 Set up vCenter Server VMware EVC	"Note"

Contents

Chapter 1 Common Operations

This chapter describes the common operations for each screen.

1.1 Display the Help Screen

A help screen has been prepared to describe detailed descriptions for each screen in ISM. Refer to the help screen for descriptions of the content displayed.

There are two ways to display the help screen. Select an appropriate procedure to display the operating screen.

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

1.2 Refresh the Screen

Except for some screens, ISM retrieves information when screens are displayed. The information in 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 (⟳Refresh), the information will be retrieved again and the screen will be refreshed.

Chapter 2 Install ISM

This chapter describes operations required for ISM installation.

2.1 Install ISM-VA

This chapter describes the following hypervisor operations which are required to operate ISM.

- 2.1.1 Import ISM-VA
- 2.1.2 Export ISM-VA
- 2.1.3 Connect Virtual Disks

After executing the operations above, register the license with ISM-VA Management.

- 2.1.4 Register Licenses

2.1.1 Import ISM-VA

The ISM software is supplied with the FUJITSU Software Infrastructure Manager Media Pack for each product.

Install ISM-VA with the procedure depending on the hypervisor on which the ISM-VA is to be installed.

ISM-VA is installed by using the importing function of the hypervisor.

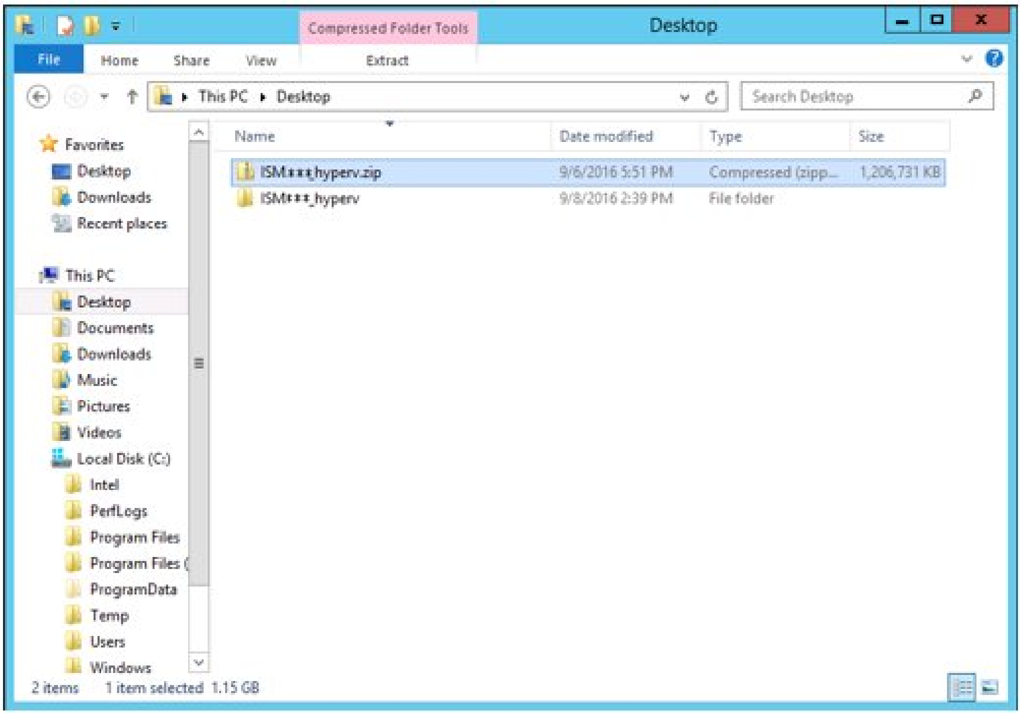
The following procedures describe the procedure to install ISM-VA on Microsoft Windows Server Hyper-V, VMware vSphere Hypervisor, and KVM.

- 2.1.1.1 Install ISM-VA on the Microsoft Windows Server Hyper-V
- 2.1.1.2 Install ISM -VA on VMware vSphere Hypervisor
- 2.1.1.3 Install ISM-VA on KVM

2.1.1.1 Install ISM-VA on the Microsoft Windows Server Hyper-V

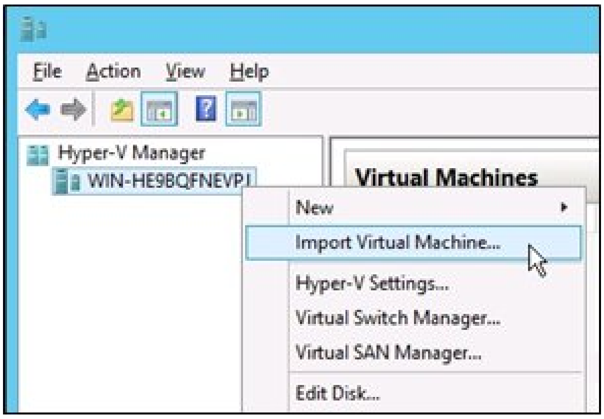
For installation, use the zip file that is included in the DVD media. For details on selecting installation destinations and network adapters that are to be specified midway during installation, refer to the Hyper-V manuals.

1. Deploy the zip file that is included in the DVD media in a temporary deployment location on the Windows server to be used as the Hyper-V host.



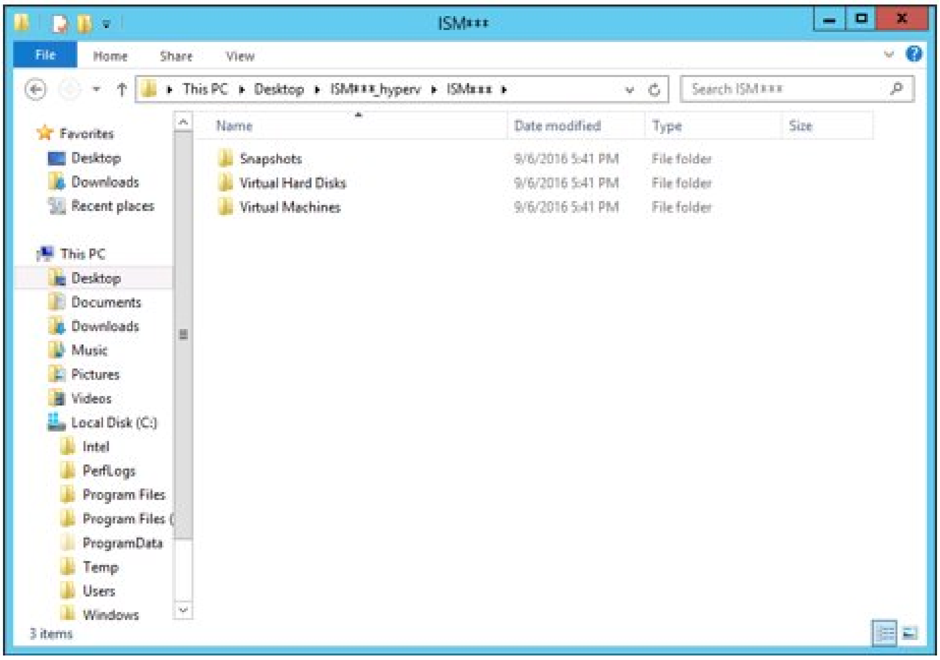
Name	Date modified	Type	Size
ISM***_hyperv.zip	9/6/2016 5:51 PM	Compressed (zipp...	1,206,731 KB
ISM***_hyperv	9/8/2016 2:39 PM	File folder	

2. Start Hyper-V Manager, right-click on the Windows server to be used as the Hyper-V host, and then select [Import Virtual Machine].



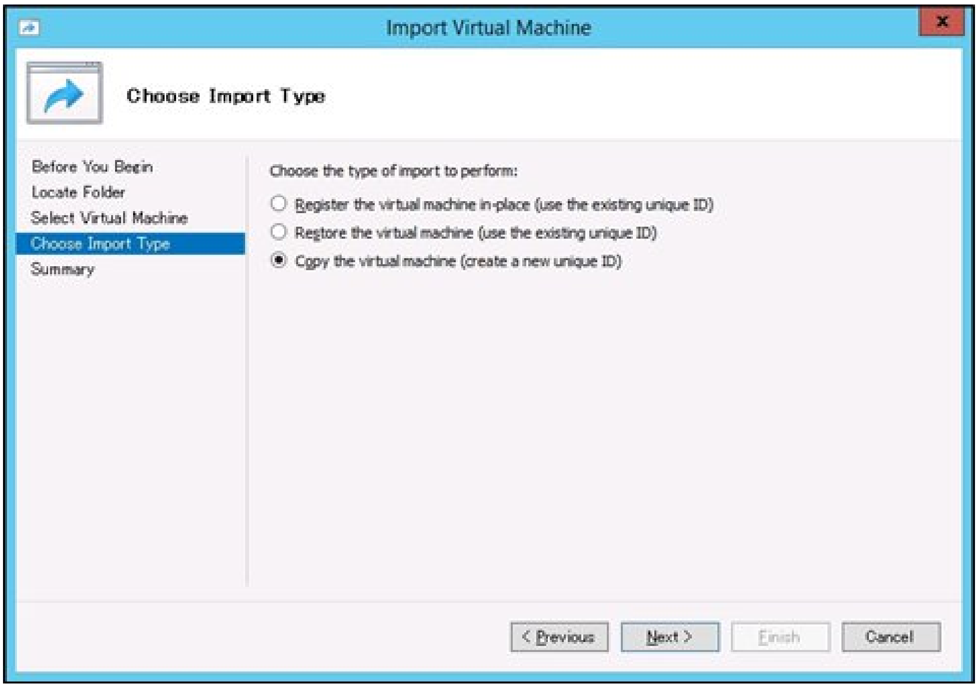
3. On the "Select Folder" screen, select the directory in which you deployed the file in Step 1.

   The directory to be selected is the parent directory of the directories "Snapshots," "Virtual Hard Disks," and "Virtual Machines."



Name	Date modified	Type	Size
Snapshots	9/6/2016 5:41 PM	File folder	
Virtual Hard Disks	9/6/2016 5:41 PM	File folder	
Virtual Machines	9/6/2016 5:41 PM	File folder	

4. On the "Choose Import Type" screen, select [Copy the virtual machine (create a new unique ID)], and then select [Next].



Choose Import Type

Choose the type of import to perform:

○ Register the virtual machine in-place (use the existing unique ID)

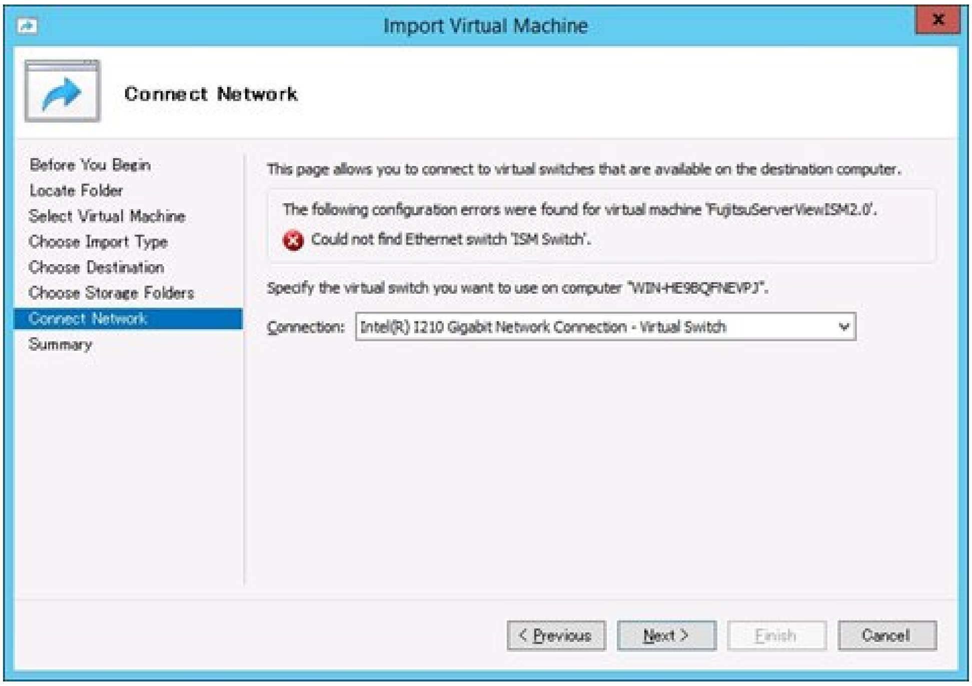
○ Restore the virtual machine (use the existing unique ID)

● Copy the virtual machine (create a new unique ID)

5. On the "Choose Destination" and "Choose Storage Folders" screens, select the import destination for ISM-VA.

   A default location is displayed, but you can change it to another one as required.

6. On the "Connect Network" screen, select the virtual switch to be used by ISM-VA, and then select [Next].



This page allows you to connect to virtual switches that are available on the destination computer.

The following configuration errors were found for virtual machine 'FujitsuServerViewISM2.0'.

Could not find Ethernet switch 'ISM Switch'.

Specify the virtual switch you want to use on computer "WIN-HE9BQFNEVPJ".

Connection: Intel(R) I210 Gigabit Network Connection - Virtual Switch

7. Select [Finish] to finish the import wizard.

8. When the import of ISM-VA is complete, convert the virtual hard disk to a fixed capacity.

   For details on the procedure to convert, refer to the Hyper-V manual.

2.1.1.2 Install ISM -VA on VMware vSphere Hypervisor

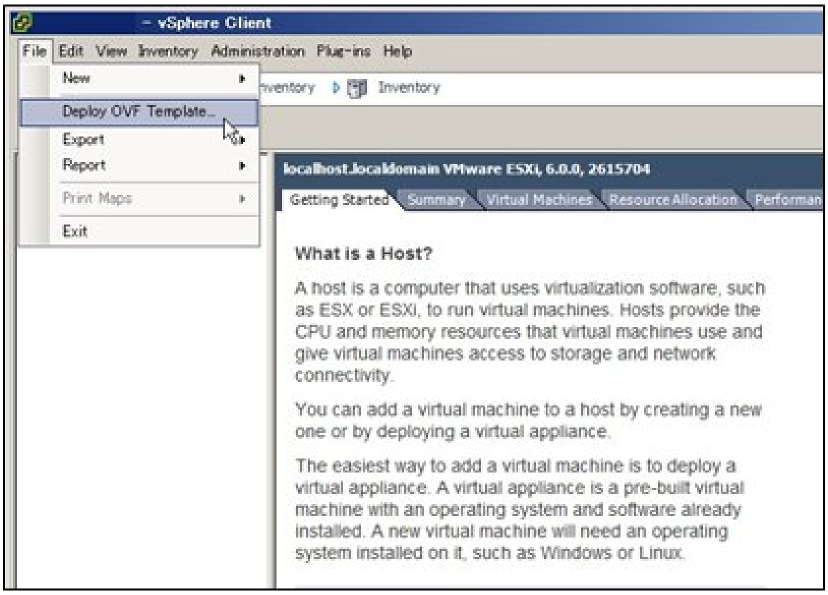
For installation, use the ova file that is included in the DVD media.

Procedures differ depending on the version of VMware ESXi. Refer to the specific reference for your version.

- Install on VMware ESXi 5.5 or VMware ESXi 6.0
- Install on VMware ESXi 6.5 or later

Install on VMware ESXi 5.5 or VMware ESXi 6.0

1. Start vSphere Client and from the [File] menu, select [Deploy OVF Template].



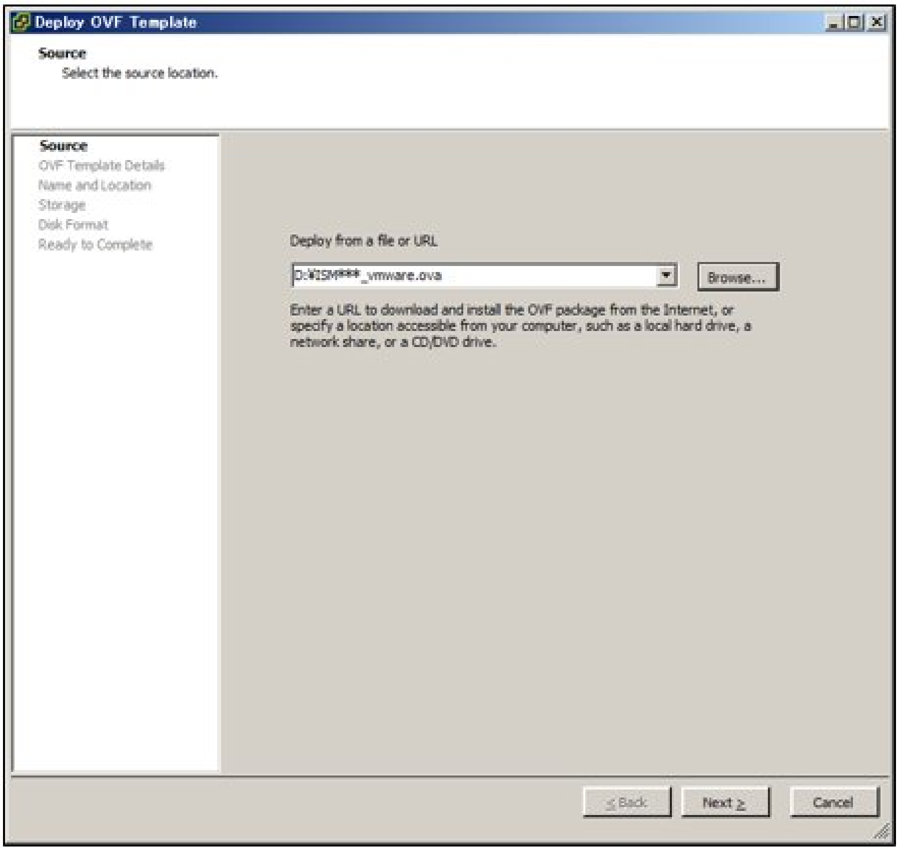
What is a Host?

A host is a computer that uses virtualization software, such as ESX or ESXi, to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use and give virtual machines access to storage and network connectivity.

You can add a virtual machine to a host by creating a new one or by deploying a virtual appliance.

The easiest way to add a virtual machine is to deploy a virtual appliance. A virtual appliance is a pre-built virtual machine with an operating system and software already installed. A new virtual machine will need an operating system installed on it, such as Windows or Linux.

2. On the source selection screen, select the ova file that is included in the DVD media, and then select [Next].

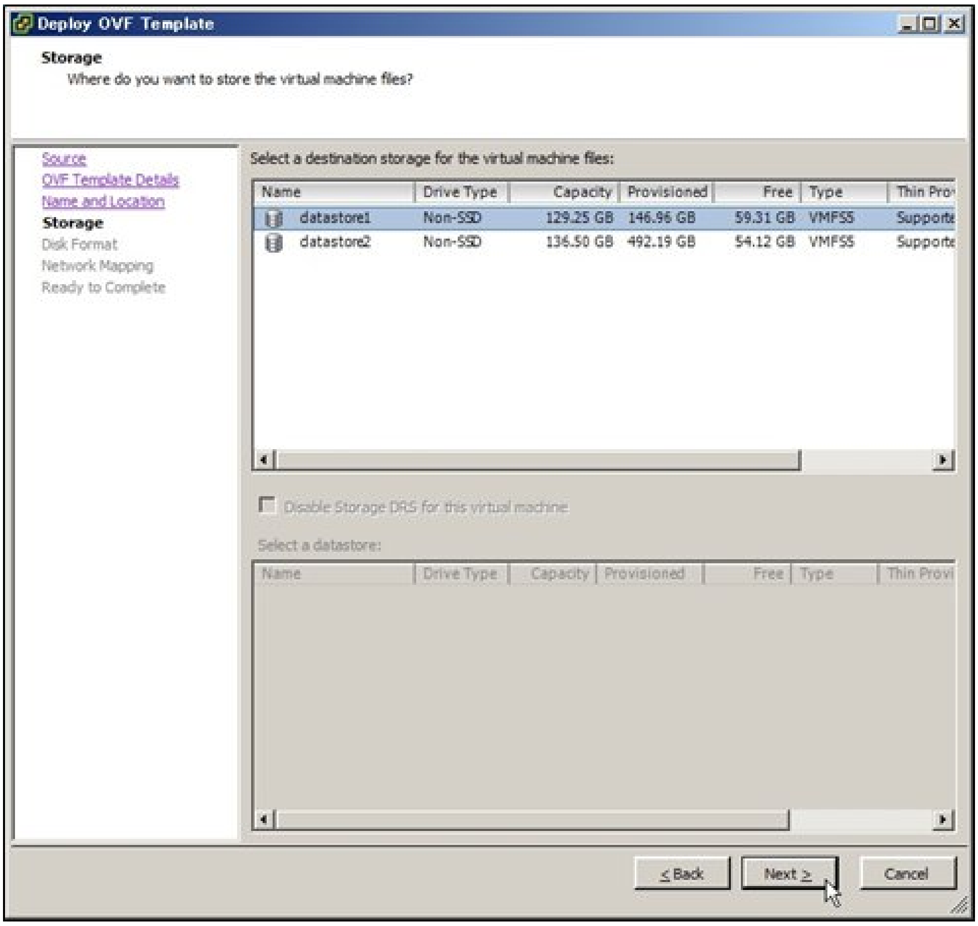


Deploy from a file or URL

D:¥ISM***_vmware.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

3. On the "Storage" screen, specify the location where the virtual machine is saved, and then select [Next].



Storage

Where do you want to store the virtual machine files?

Select a destination storage for the virtual machine files:

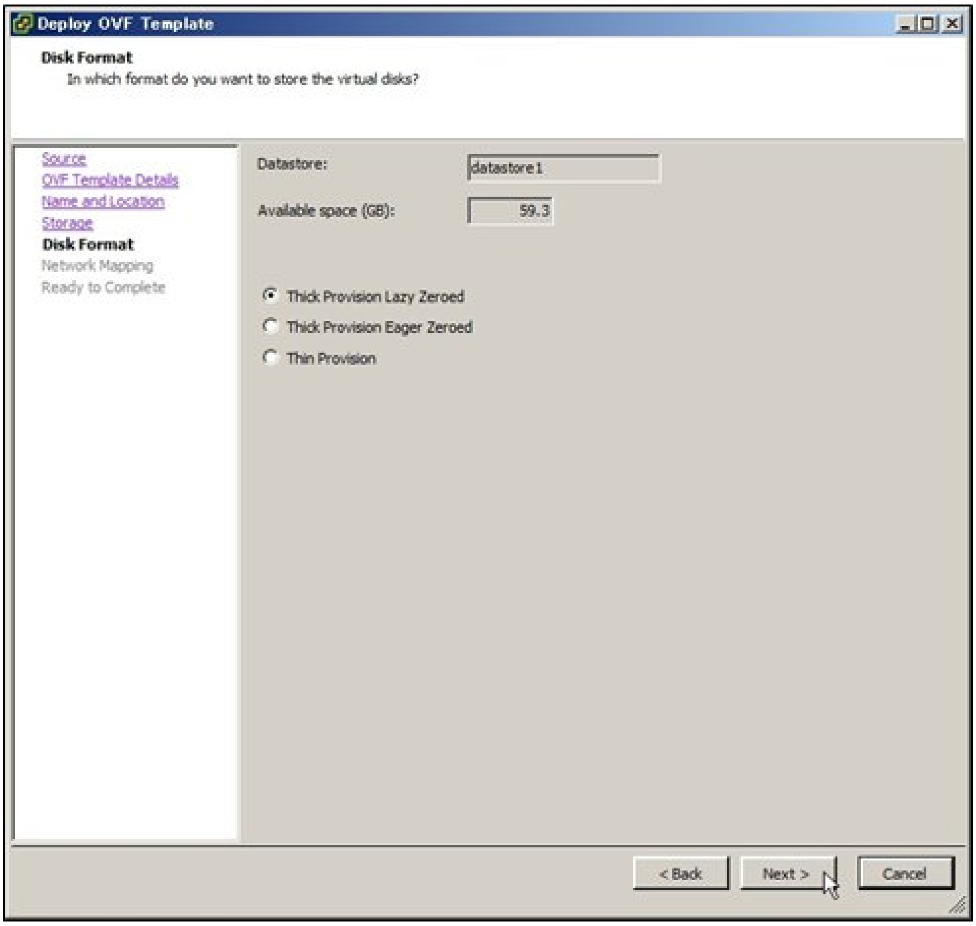
Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Pro
datastore1	Non-SSD	129.25 GB	146.96 GB	59.31 GB	VMFS5	Supporte
datastore2	Non-SSD	136.50 GB	492.19 GB	54.12 GB	VMFS5	Supporte

□ Disable Storage DRS for this virtual machine

Select a datastore:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Provi

4. On the "Disk Format" screen, select [Thick Provision Lazy Zeroed] or [Thick Provision Eager Zeroed], and then select [Next].



Deploy OVF Template

Disk Format

In which format do you want to store the virtual disks?

Datastore: datastore1

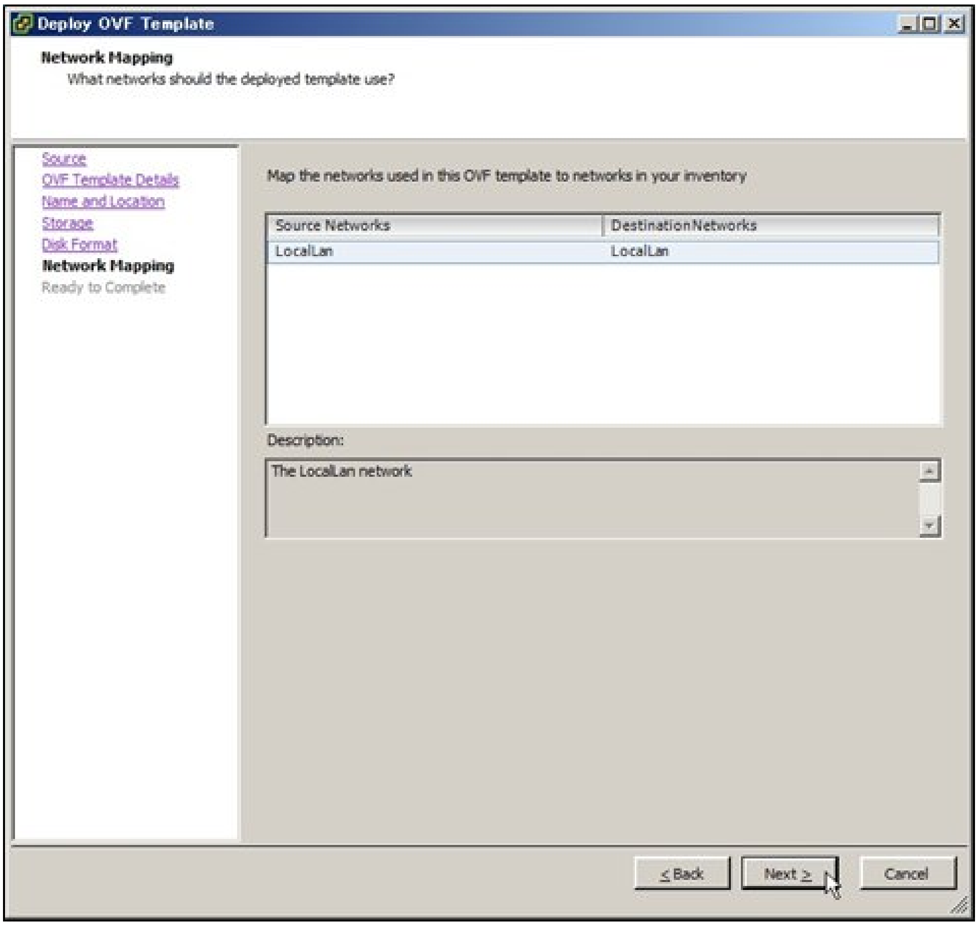
Available space (GB): 59.3

● Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

○ Thin Provision

5. On the "Network Mapping" screen, select the network to be used by ISM, and then select [Next].



Deploy OVF Template

Network Mapping
What networks should the deployed template use?

Map the networks used in this OVF template to networks in your inventory

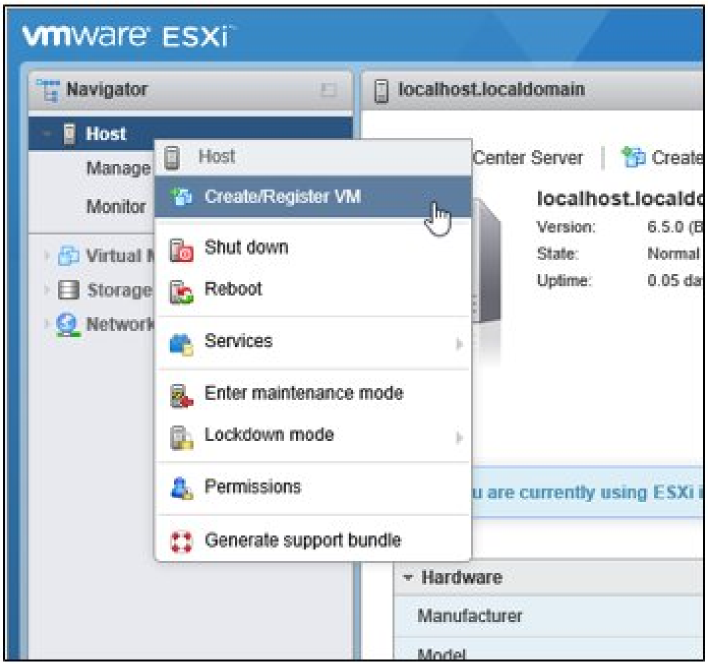
Source Networks	DestinationNetworks
LocalLan	LocalLan

Description:
The LocalLan network

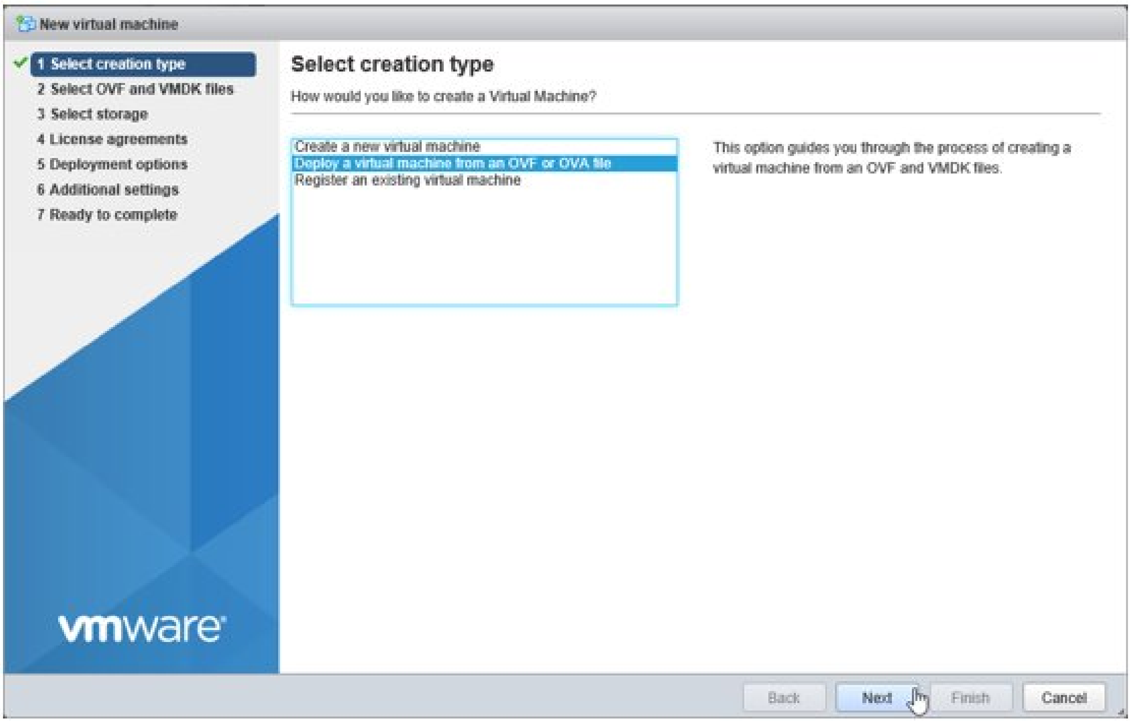
6. Select [Finish] to finish deployment of OVF templates.

Install on VMware ESXi 6.5 or later

1. Start the vSphere Client (HTML5), right-click on the [Host] of the navigator, and then select [Create/Register VM].



2. On the "Select creation type" screen, select [Deploy a virtual machine from an OVF or OVA file] and then select [Next].



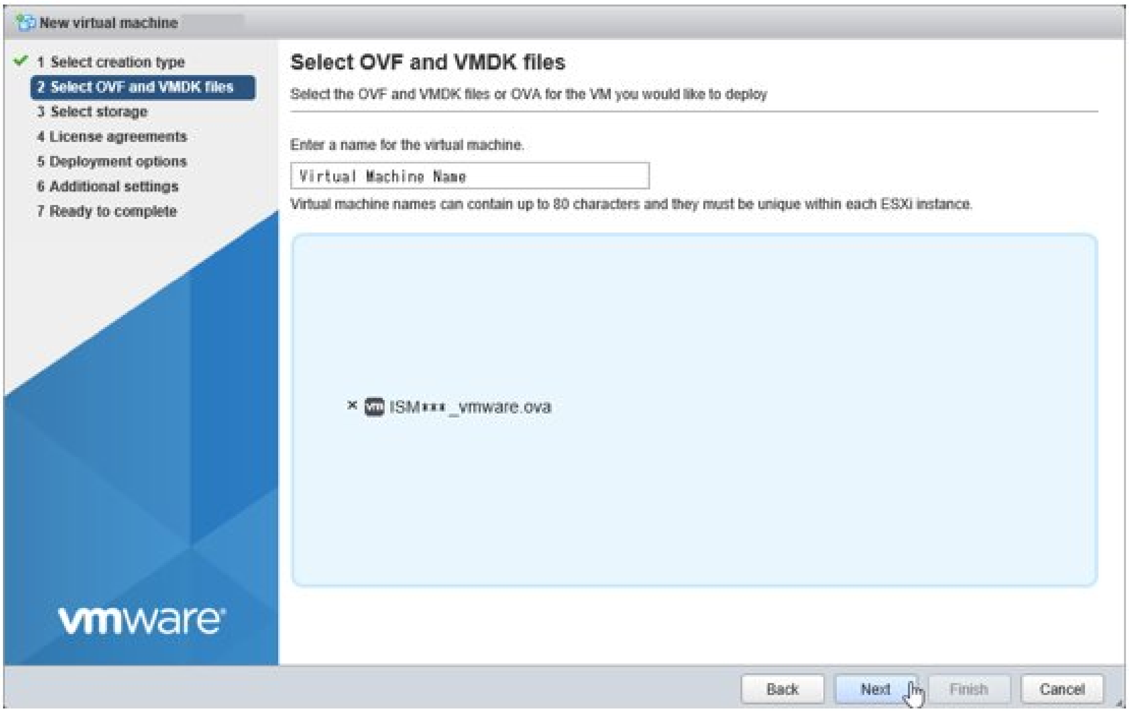
Select creation type

How would you like to create a Virtual Machine?

Create a new virtual machine
Deploy a virtual machine from an OVF or OVA file
Register an existing virtual machine

This option guides you through the process of creating a virtual machine from an OVF and VMDK files.

3. On the "Select OVF and VMDK files" screen, specify an arbitrary name for the virtual machine, then set deployment for the ova file included on the DVD, and then select [Next].



Select OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM you would like to deploy

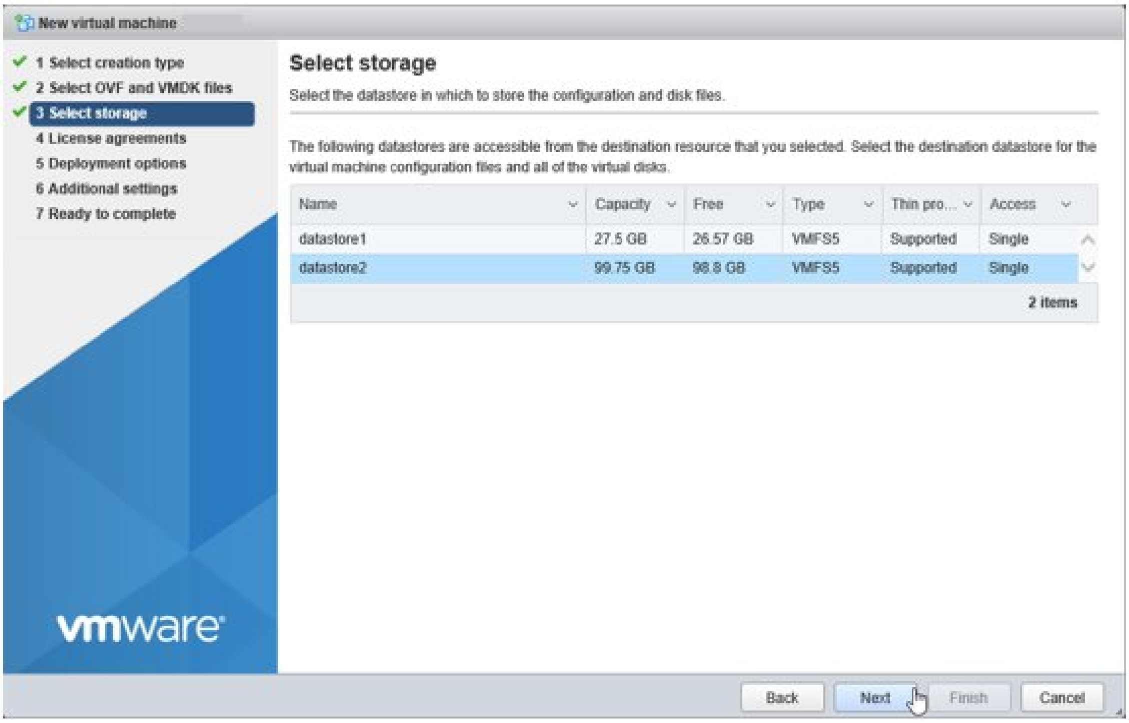
Enter a name for the virtual machine.

Virtual Machine Name

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

× ISM***_vmware.ova

4. On the "Select storage" screen, select the datastore to deploy to, and then select [Next].



Select storage

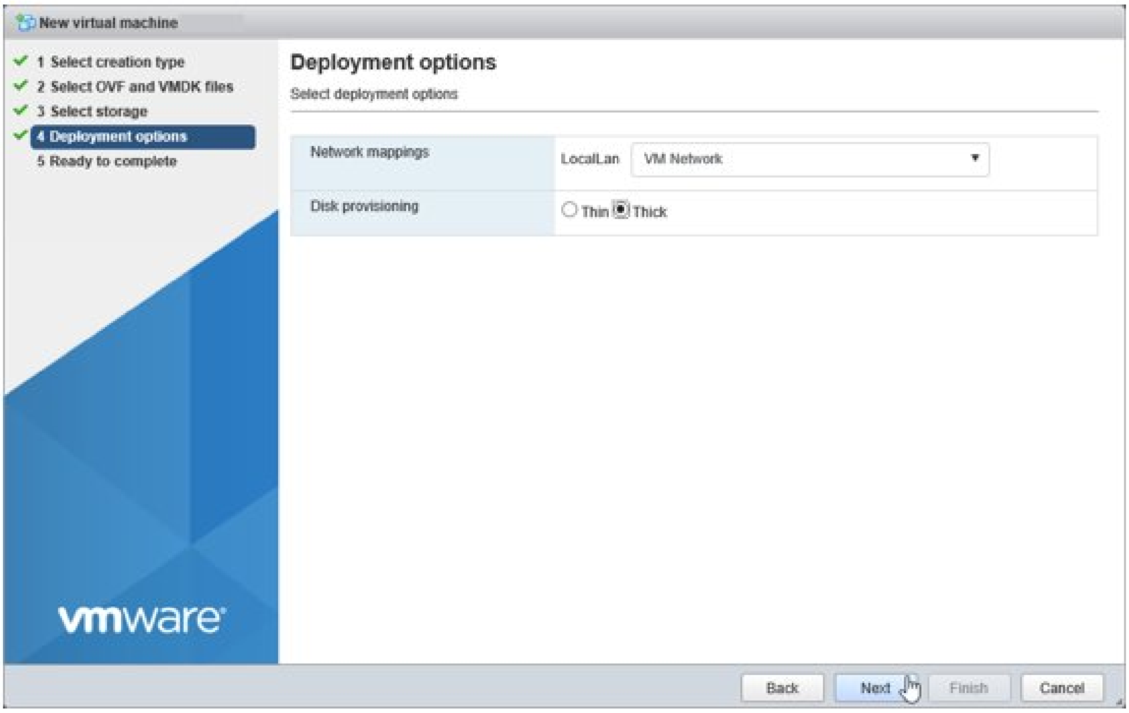
Select the datastore in which to store the configuration and disk files.

The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
datastore1	27.5 GB	26.57 GB	VMFS5	Supported	Single
datastore2	99.75 GB	98.8 GB	VMFS5	Supported	Single

2 items

5. On the "Deployment options" screen, select the network being used. For Disk provisioning, select "Thick," and then select [Next].



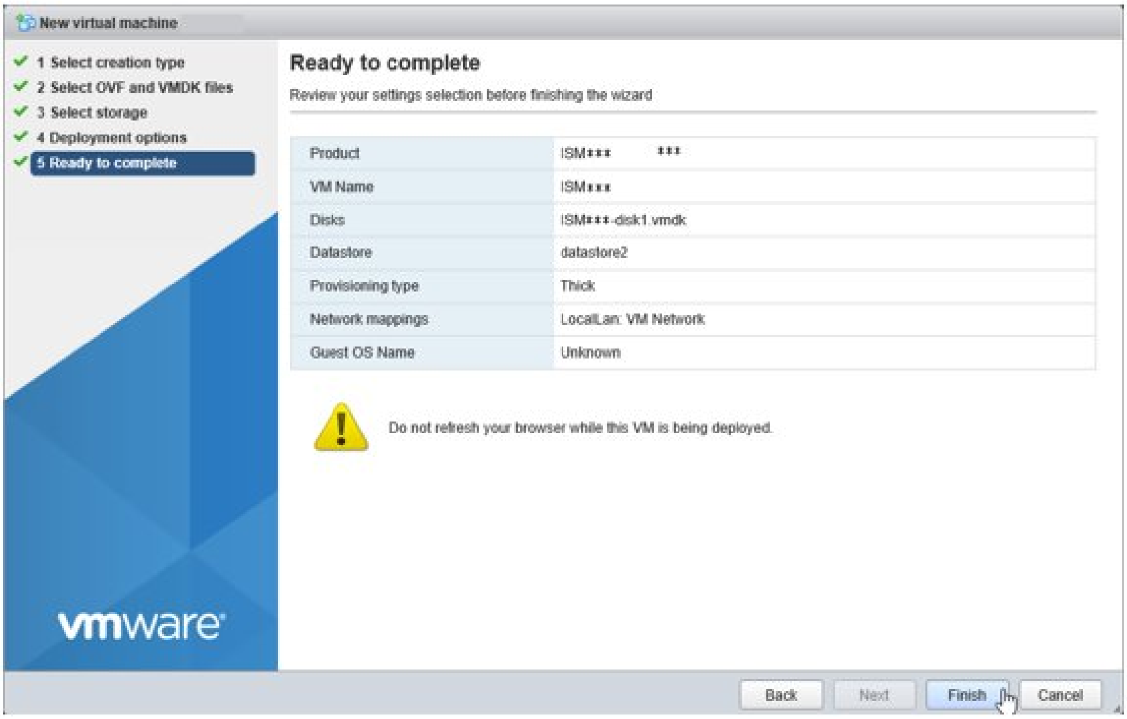
Deployment options

Select deployment options

Network mappings: LocalLan VM Network ▾

Disk provisioning: ○ Thin ● Thick

6. On the "Ready to complete" screen, confirm the settings, and then select [Finish] to complete deployment.



Ready to complete

Review your settings selection before finishing the wizard

Product	ISM*** ***
VM Name	ISM***
Disks	ISM***-disk1.vmdk
Datastore	datastore2
Provisioning type	Thick
Network mappings	LocalLan: VM Network
Guest OS Name	Unknown

Do not refresh your browser while this VM is being deployed.

2.1.1.3 Install ISM-VA on KVM

For installation, use the tar.gz file that is included in the DVD media.

1. Transfer the tar.gz file to any suitable directory on the KVM host and decompress it there.

```
# tar xzvf ISM<Version>_kvm.tar.gz
ISM<Version>_kvm/
ISM<Version>_kvm/ISM<Version>_kvm.qcow2
ISM<Version>_kvm/ISM<Version>.xml
```

   The <Version> part shows the number according to ISM-VA version.

2. Copy the files in the decompressed directory to their respective designated locations.

   a. Copy the qcow2 file to /var/lib/libvirt/images.

```
# cp ISM<Version>_kvm.qcow2 /var/lib/libvirt/images
```

   b. Copy the xml file to /etc/libvirt/qemu.

```
# cp ISM<Version>.xml /etc/libvirt/qemu
```

Point

When installing SUSE Linux Enterprise Server, edit the xml file with vi directly before or after copying to change the <emulator> portion.

Before change

```
<emulator>/usr/libexec/qemu-kvm</emulator>
```

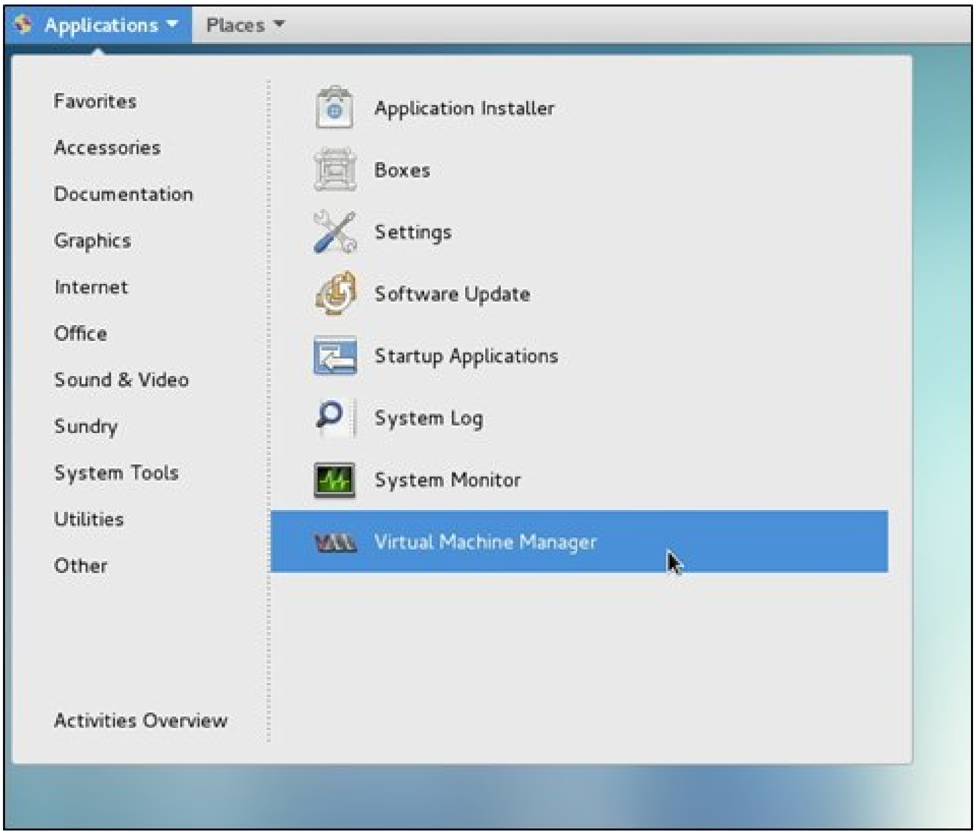
After change

```
<emulator>/usr/bin/qemu-system-x86_64</emulator>
```

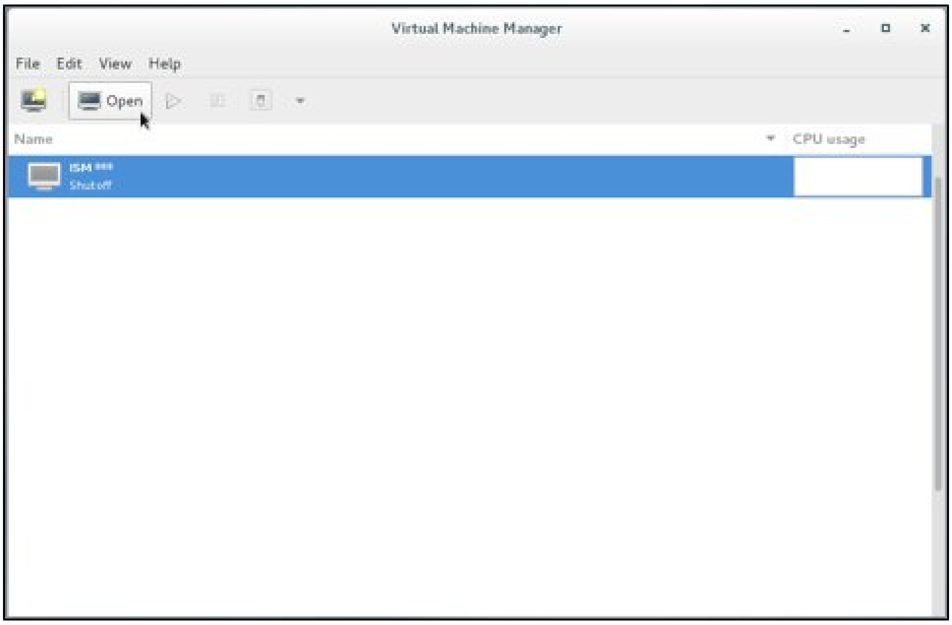
3. Specify the xml file to register ISM-VA.

```
# virsh define /etc/libvirt/qemu/ISM<Version>.xml
```

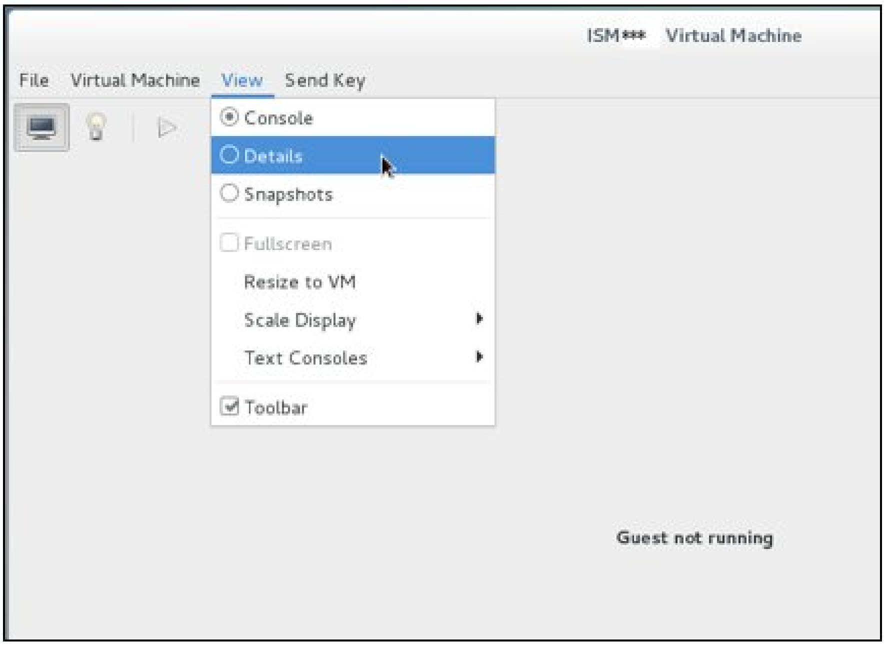
4. Select [Virtual Machine Manager] to open Virtual Machine Manager.



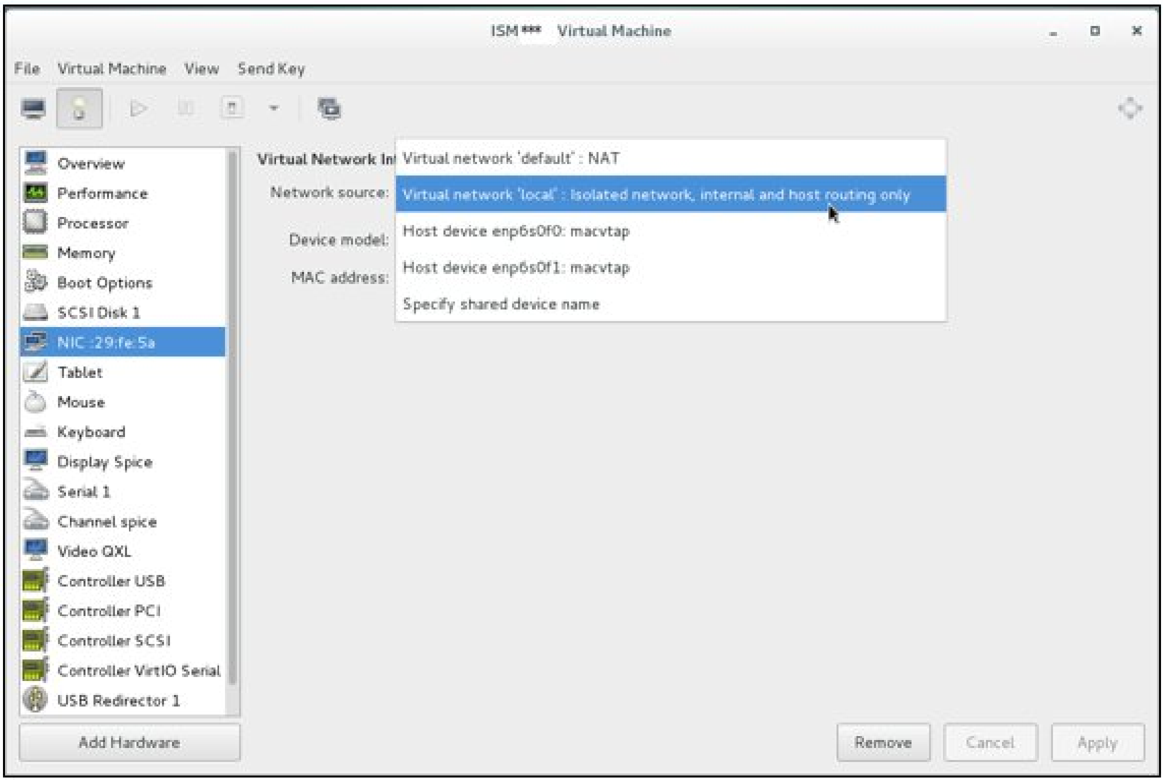
5. In Virtual Machine Manager, select ISM-VA, and then select [Open].



6. On the ISM-VA Virtual Machine screen, select [Details] from the [View] menu.



7. On the detailed screen for ISM-VA Virtual Machine, select [NIC] and the virtual network or host device to which to connect ISM-VA, and then select [Apply].



2.1.2 Export ISM-VA

Backup ISM-VA with the procedure depending on the hypervisor on which the ISM-VA is operating.

ISM-VA is backed up by using the exporting function of the hypervisor.

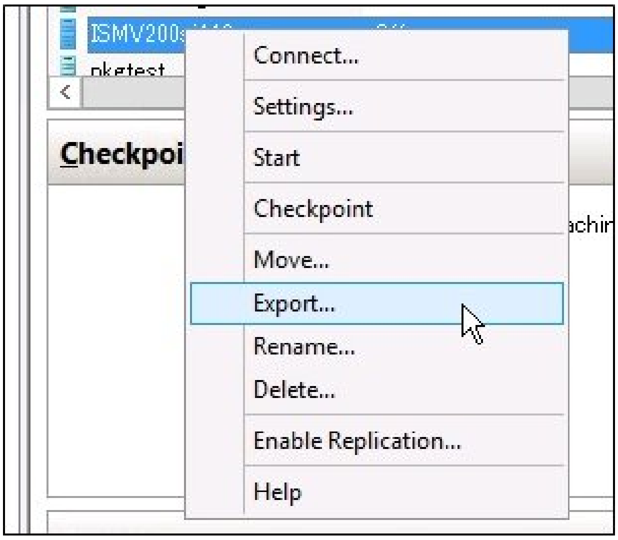
The following procedures describe the procedure to backup ISM-VA from Microsoft Windows Server Hyper-V, VMware vSphere Hypervisor, and KVM.

Note

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."

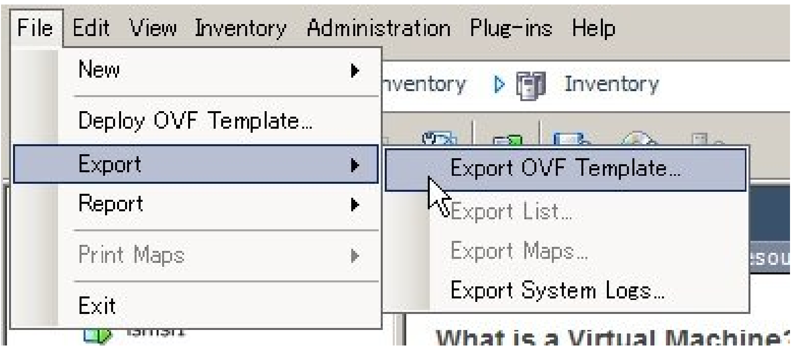
2.1.2.1 Back up ISM-VA running on Microsoft Windows Server Hyper-V

In Hyper-V Manager, right-click on the installed ISM-VA, and then select [Export].



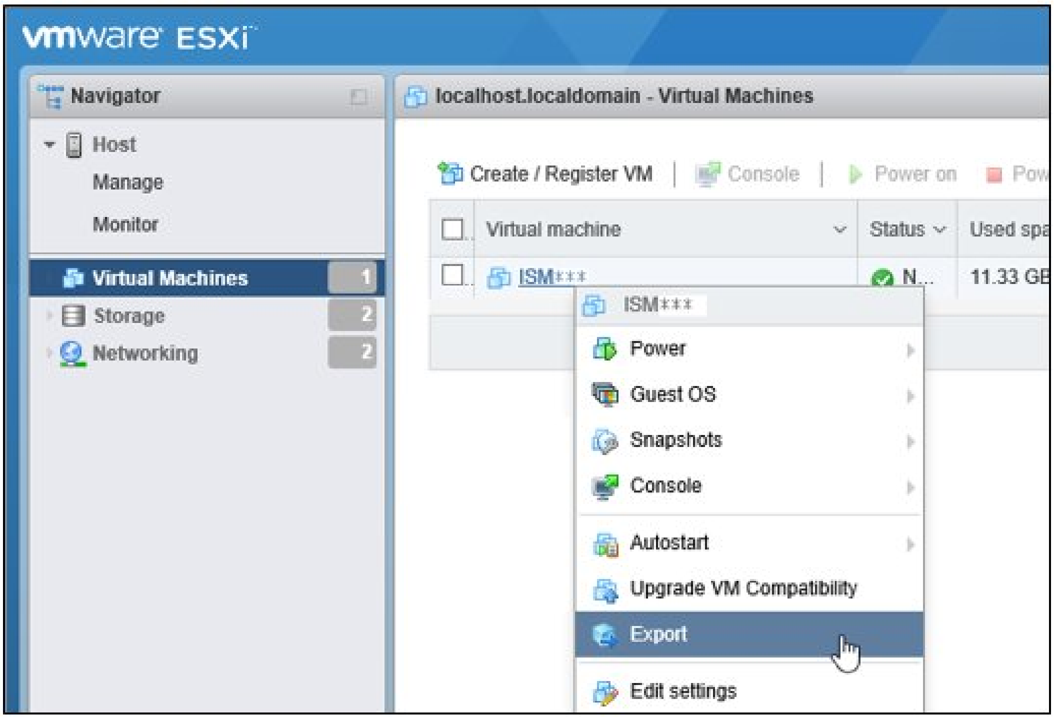
2.1.2.2 Back up ISM-VA running on VMware vSphere Hypervisor 5.5 or VMware vSphere Hypervisor 6.0

In vSphere Client, right-click on the installed ISM-VA, and then select [Export] - [Export OVF Template] from the [File] menu.



2.1.2.3 Back up ISM-VA running on VMware vSphere Hypervisor 6.5

In vSphere Client (HTML5), right-click on the installed ISM-VA, and then select [Export].



2.1.2.4 Back up ISM-VA running on KVM

Back up the KVM files that are stored in the following locations to arbitrary other locations as required.

- /etc/libvirt/qemu
- /var/lib/libvirt/images

2.1.3 Connect Virtual Disks

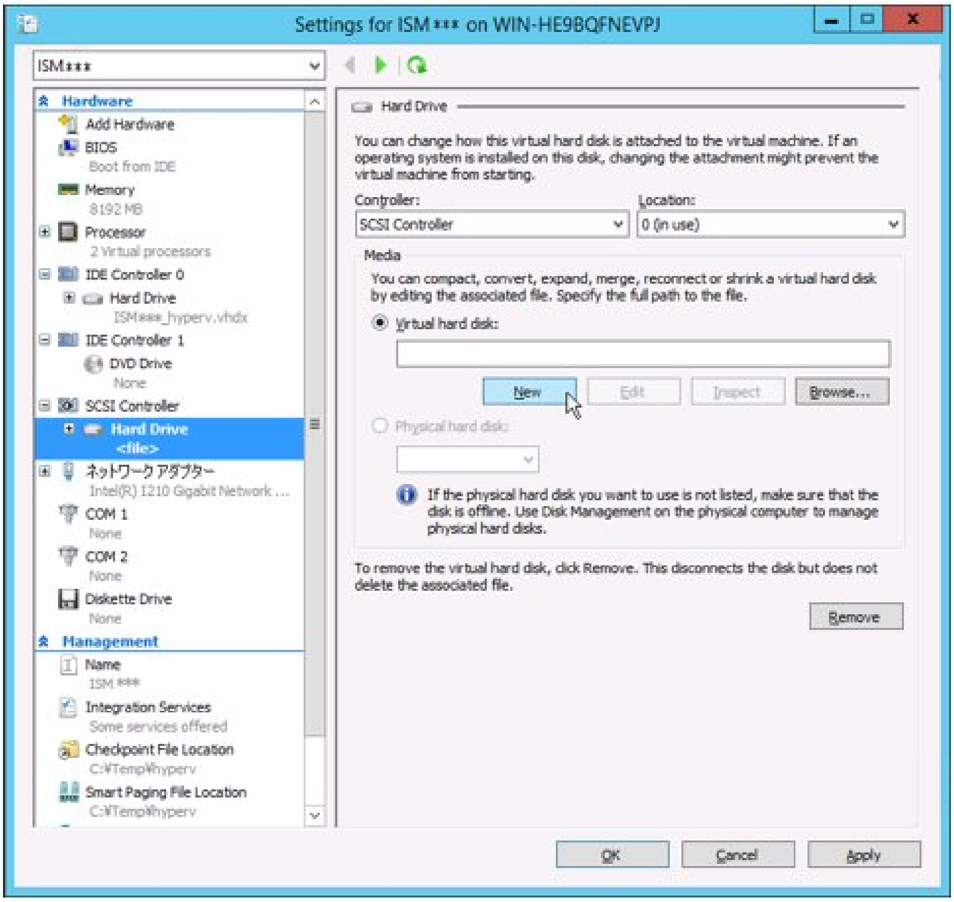
Virtual disks are resources for adding ISM-VA disk capacities. The storage of logs, repositories, and backups requires large capacities of disk resources. Moreover, these capacities vary with the respective operating procedures and scales of managed nodes. Allocating voluminous resources to virtual disks allows for avoiding any effects on ISM-VA from disk capacities or increased loads. Securing sufficient space on virtual disks ensures smooth operation of logs, repositories, and backups.

Virtual disks can be allocated to the entire ISM-VA or to user groups.

2.1.3.1 Allocate virtual disks to entire ISM-VA

1. After stopping ISM-VA, create a virtual disk on the hypervisor settings screen and connect it to ISM-VA (virtual machine).

   For Microsoft Windows Server Hyper-V



Settings for ISM*** on WIN-HE9BQFNEVPJ

Hard Drive

You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.

Controller: SCSI Controller

Location: 0 (in use)

Media

You can compact, convert, expand, merge, reconnect or shrink a virtual hard disk by editing the associated file. Specify the full path to the file.

● Virtual hard disk:

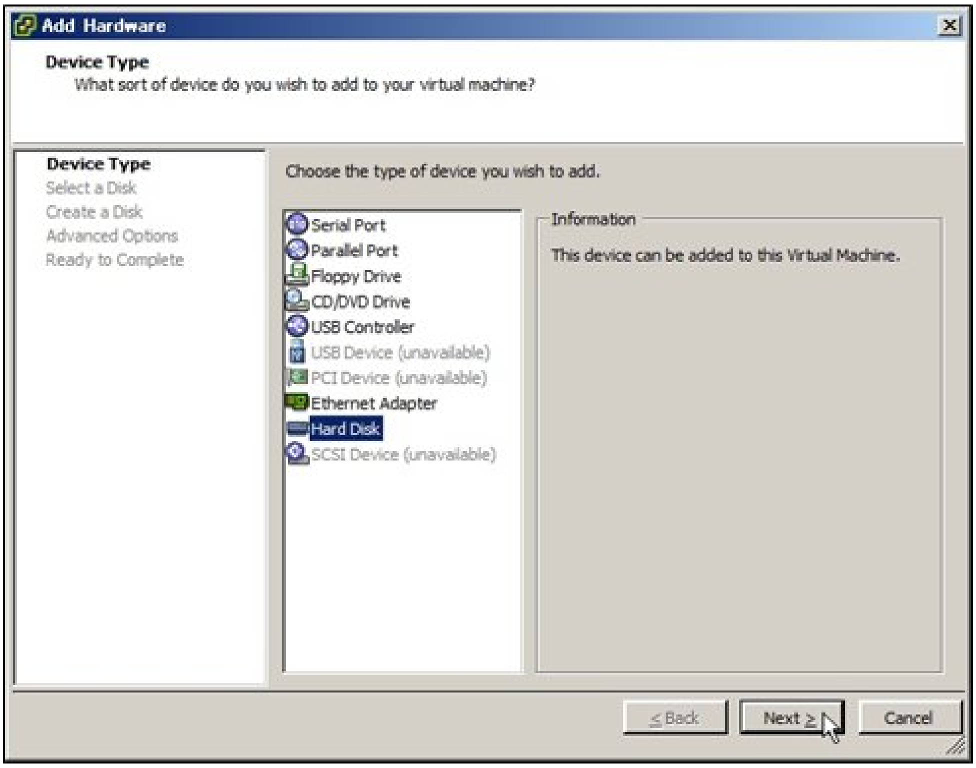
○ Physical hard disk:

If the physical hard disk you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disks.

To remove the virtual hard disk, click Remove. This disconnects the disk but does not delete the associated file.

Create the virtual disks so as to be controlled by SCSI controllers.

For VMware vSphere Hypervisor 5.5 or VMware vSphere Hypervisor 6.0



Add Hardware

Device Type

What sort of device do you wish to add to your virtual machine?

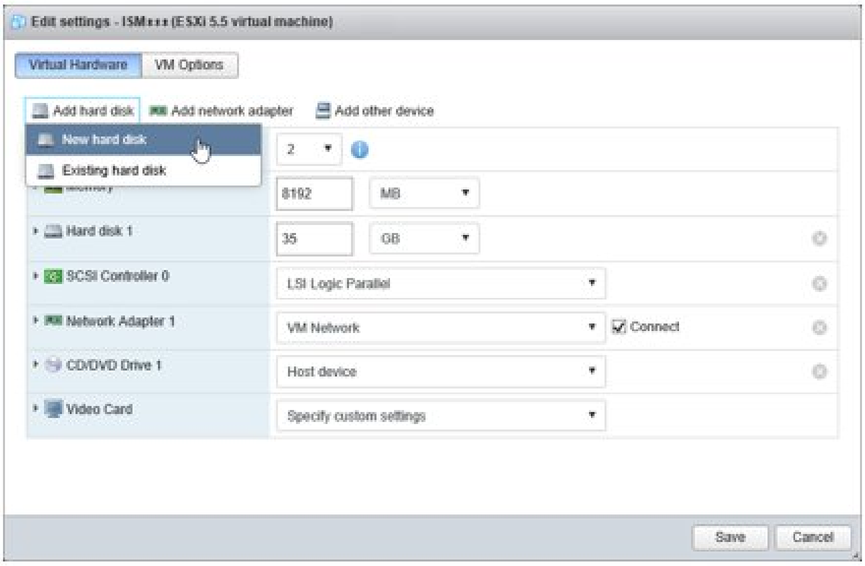
Choose the type of device you wish to add.

Information

This device can be added to this Virtual Machine.

In the virtual device node selection that comes up on the "Detail Option" screen during disk creation, select SCSI.

For VMware vSphere Hypervisor 6.5



Edit settings - ISM*** (ESXi 5.5 virtual machine)

Hard disk 1: 35 GB

SCSI Controller 0: LSI Logic Parallel

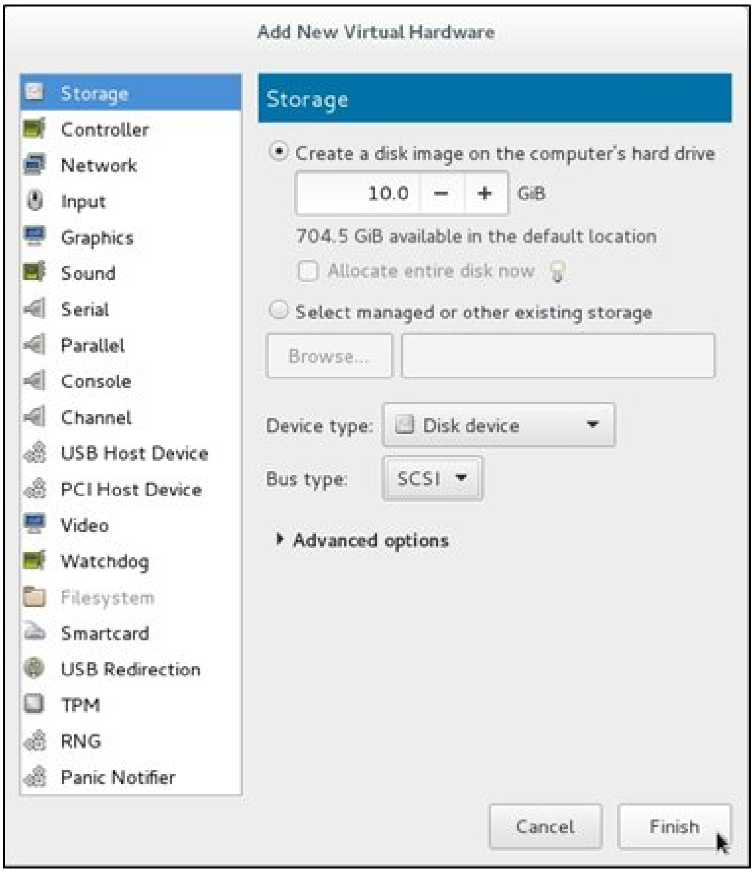
Network Adapter 1: VM Network ☑ Connect

CD/DVD Drive 1: Host device

Video Card: Specify custom settings

In the virtual device node selection that comes up on the "Detail Option" screen during disk creation, select SCSI.

For KVM



● Create a disk image on the computer's hard drive

10.0 − + GiB

704.5 GiB available in the default location

□ Allocate entire disk now

○ Select managed or other existing storage

Device type: Disk device

Bus type: SCSI

For Bus type, select SCSI.

2. After starting up ISM-VA, log in to ISM-VA from the console as an administrator.
3. In order to allocate the virtual disks, stop the ISM service temporarily.

```
# ismadm service stop ism
```

4. Confirm that the virtual disks you added in Step 1 are correctly recognized.

   Example:

```
# ismadm volume show -disk
Filesystem                 Size  Used  Avail Use% Mounted on
/dev/mapper/centos-root     16G  2.6G   13G   17% /
devtmpfs                   1.9G     0  1.9G    0% /dev
tmpfs                      1.9G  4.0K  1.9G    1% /dev/shm
tmpfs                      1.9G  8.5M  1.9G    1% /run
tmpfs                      1.9G     0  1.9G    0% /sys/fs/cgroup
/dev/sda1                  497M  170M  328M   35% /boot
tmpfs                      380M     0  380M    0% /run/user/1001
/dev/sdb                                           (Free)

  PV         VG     Fmt  Attr PSize  PFree
  /dev/sda2  centos lvm2 a--  19.51g    0
```

   In this example, /dev/sdb is recognized as an area that was added but is not yet in use.

5. Allocate the added virtual disks to the system volume of the entire ISM-VA.

```
# ismadm volume sysvol-extend -disk /dev/sdb
```

6. Confirm the virtual disk settings.

   Confirm that the newly added volume (/dev/sdb) is set for use by the system volume (centos).

```
# ismadm volume show -disk
Filesystem                Size  Used  Avail Use% Mounted on
/dev/mapper/centos-root    26G  2.5G   23G   10% /
devtmpfs                  1.9G     0  1.9G    0% /dev
tmpfs                     1.9G  4.0K  1.9G    1% /dev/shm
tmpfs                     1.9G  8.5M  1.9G    1% /run
tmpfs                     1.9G     0  1.9G    0% /sys/fs/cgroup
/dev/sda1                 497M  170M  328M   35% /boot
tmpfs                     380M     0  380M    0% /run/user/1001
tmpfs                     380M     0  380M    0% /run/user/0

  PV         VG       Fmt  Attr PSize   PFree
  /dev/sda2  centos   lvm2 a--  19.51g    0
  /dev/sdb1  centos   lvm2 a--  10.00g    0
```

7. Restart ISM-VA.

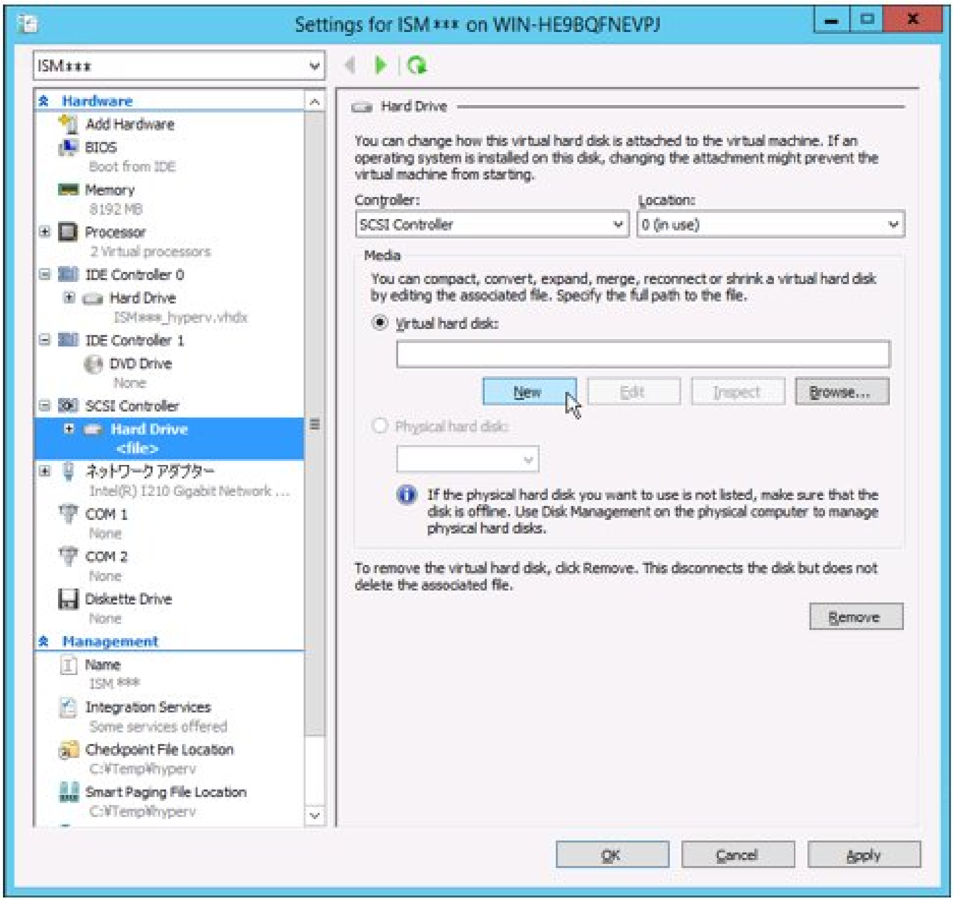
```
# ismadm power restart
```

2.1.3.2 Allocate virtual disks to user groups

The following example uses the Administrator user group to show you the procedure for allocating virtual disks.

1. After stopping ISM-VA, create a virtual disk on the hypervisor settings screen and connect it to ISM-VA (virtual machine).

   For Microsoft Windows Server Hyper-V



Settings for ISM*** on WIN-HE9BQFNEVPJ

Hard Drive

You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.

Controller: SCSI Controller

Location: 0 (in use)

Media

You can compact, convert, expand, merge, reconnect or shrink a virtual hard disk by editing the associated file. Specify the full path to the file.

● Virtual hard disk:

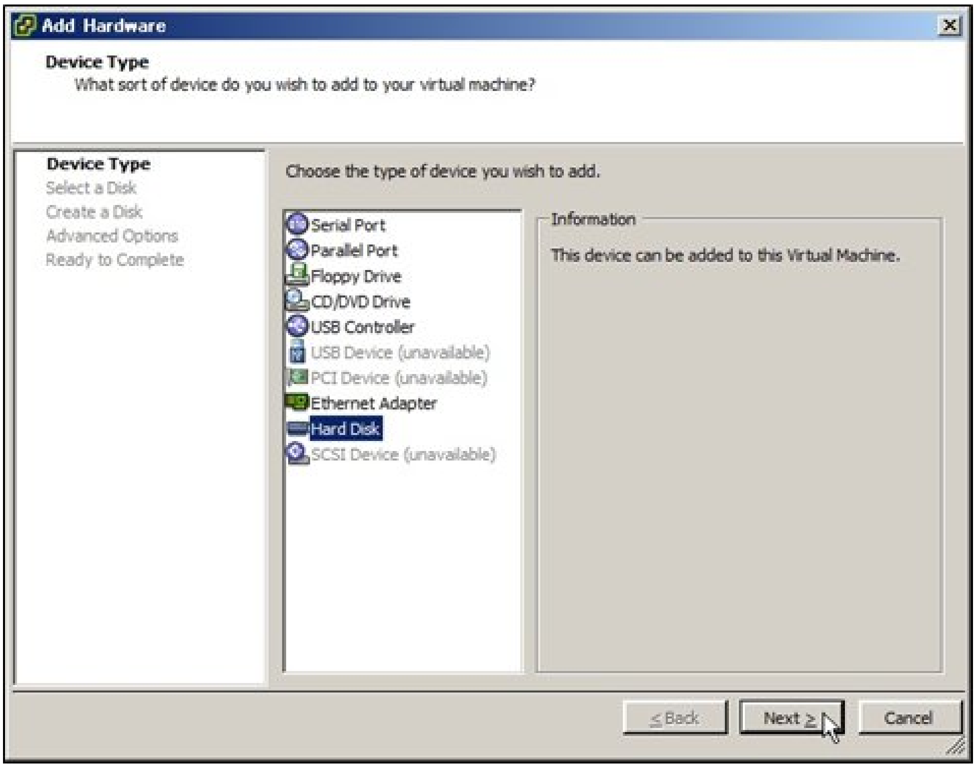
○ Physical hard disk:

If the physical hard disk you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disks.

To remove the virtual hard disk, click Remove. This disconnects the disk but does not delete the associated file.

   Create the virtual disks so as to be controlled by SCSI controllers.

For VMware vSphere Hypervisor 5.5 or VMware vSphere Hypervisor 6.0


Add Hardware

Device Type

What sort of device do you wish to add to your virtual machine?

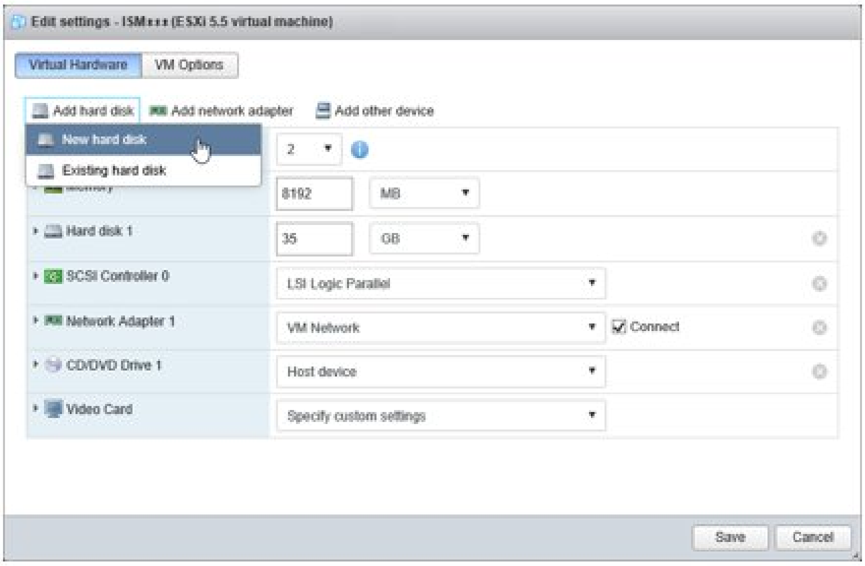
Choose the type of device you wish to add.

Information

This device can be added to this Virtual Machine.

In the virtual device node selection that comes up on the "Detail Option" screen during disk creation, select SCSI.

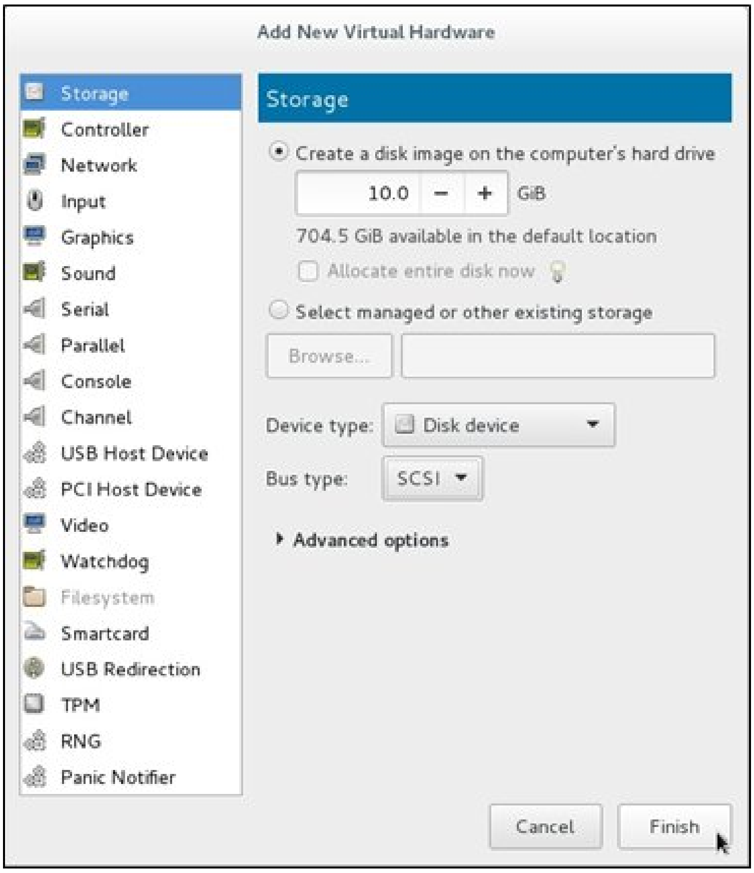
For VMware vSphere Hypervisor 6.5


Edit settings - ISM*** (ESXi 5.5 virtual machine)

	2	
Memory	8192 MB	
Hard disk 1	35 GB	
SCSI Controller 0	LSI Logic Parallel	
Network Adapter 1	VM Network	☑ Connect
CD/DVD Drive 1	Host device	
Video Card	Specify custom settings	

In the virtual device node selection that comes up on the "Detail Option" screen during disk creation, select SCSI.

For KVM



Add New Virtual Hardware

Storage

● Create a disk image on the computer's hard drive

10.0 GiB

704.5 GiB available in the default location

□ Allocate entire disk now

○ Select managed or other existing storage

Device type: Disk device

Bus type: SCSI

For Bus type, select SCSI.

2. After starting up ISM-VA, log in to ISM-VA from the console as an administrator.

3. In order to allocate the virtual disks, stop the ISM service temporarily.

```
# ismadm service stop ism
```

4. Confirm that the virtual disks you added in Step 1 are correctly recognized.

   Example:

```
# ismadm volume show -disk
Filesystem                Size  Used  Avail Use% Mounted on
/dev/mapper/centos-root    16G  2.6G   13G   17% /
devtmpfs                  1.9G     0  1.9G    0% /dev
tmpfs                     1.9G  4.0K  1.9G    1% /dev/shm
tmpfs                     1.9G  8.5M  1.9G    1% /run
tmpfs                     1.9G     0  1.9G    0% /sys/fs/cgroup
/dev/sda1                 497M  170M  328M   35% /boot
tmpfs                     380M     0  380M    0% /run/user/1001
/dev/sdb                                          (Free)

  PV         VG     Fmt  Attr PSize  PFree
  /dev/sda2  centos lvm2 a--  19.51g    0
```

In this example, /dev/sdb is recognized as an area that was added but is not yet in use.

5. Create an additional volume name for Administrator group with an arbitrary name (Example: "adminvol"), and correlate it with the newly added virtual disk (/dev/sdb).

```
# ismadm volume add -vol adminvol -disk /dev/sdb
Logical volume "/dev/mapper/adminvol-lv" created.
```

6. Enable the additional volume (in the following example "adminvol") you created in Step 5 so that it can be actually used by the Administrator group.

```
# ismadm volume mount -vol adminvol -gdir /Administrator
```

7. Confirm the virtual disk settings.

   Confirm that the newly added volume (/dev/sdb) is set for use by the Administrator group.

```
# ismadm volume show -disk
Filesystem                Size  Used  Avail Use% Mounted on
/dev/mapper/centos-root    16G  2.6G   13G   17% /
devtmpfs                  1.9G     0  1.9G    0% /dev
tmpfs                     1.9G  4.0K  1.9G    1% /dev/shm
tmpfs                     1.9G  8.6M  1.9G    1% /run
tmpfs                     1.9G     0  1.9G    0% /sys/fs/cgroup
/dev/sda1                 497M  170M  328M   35% /boot
tmpfs                     380M     0  380M    0% /run/user/1001
tmpfs                     380M     0  380M    0% /run/user/0
/dev/mapper/adminvol-lv   8.0G   39M  8.0G    1% 'RepositoryRoot'/Administrator

  PV         VG       Fmt  Attr PSize  PFree
  /dev/sda2  centos   lvm2 a--  19.51g    0
  /dev/sdb1  adminvol lvm2 a--   8.00g    0
```

8. Restart ISM-VA.

```
# ismadm power restart
```

2.1.4 Register Licenses

There are the following two types of licenses. ISM requires registration of both server licenses and node licenses.

Register the licenses with ISM-VA Management after installing ISM-VA.

- Server licenses

  These licenses are required for using ISM.

- Node licenses

  These licenses are related to the number of nodes that can be registered in ISM. You cannot register a number of nodes that exceeds the number of licenses you have registered with ISM-VA Management. If you want to register additional nodes in ISM, register additional node licenses beforehand.

For details on the types of ISM licenses, refer to "1.2 Product System and Licenses" in "First Step Guide."

There are two procedures to register licenses, the first is to register from the console, and the second is to register from the GUI operating in a web browser.

Procedure for registering from the console

Log in to ISM-VA from the console as an administrator.

1. Register the server licenses.

```
# ismadm license set -key <License key>
```

2. Register the node licenses.

```
# ismadm license set -key <License key>
```

3. Confirm the results of license registration.

```
# ismadm license show
```

Example of command execution:

```
# ismadm license show
Operation Mode: Advanced
#   [Type]  [Edition]   [#Node]  [Exp.Date]  [Reg.Date]  [Licensekey]
1   Server  Adv.              -           -  2018-01-01  **********************==
2   Node    Adv.             10           -  2018-01-01  **********************==
```

Table 2.1 Description on output for "license show" command results

Item	Description
[Operation Mode]	Operation Mode (ISM 2.4.0.b or later) - Essential - Advanced - Advanced for PRIMEFLEX
[Type]	Displays "Server" for a server license and "Node" for a node license.
[Edition]	The type of the license is displayed. - Adv.: ISM License - I4P: ISM for PRIMEFLEX License
[#Node]	The number of nodes that can be managed with the license is displayed. When the license type is "Server," "-" is always displayed.
[Exp.Date]	The expiration date of the license is displayed. For licenses with the perpetual term, "-" is always displayed.
[Reg.Date]	The registration date of the license is displayed.
[Licensekey]	The character string of the registered license key is displayed.

4. Restart ISM-VA.

```
# ismadm power restart
```

Procedure for registering from the GUI operating on a web browser

When registering a license for the first time

1. Execute the initial setup of ISM.

   For details, refer to "3.4.2 Initial Setup of ISM-VA" in "User's Guide."

2. Restart ISM-VA.
3. Start the GUI operating in a web browser.
4. From the GUI, log in as an administrator.

   The "Fujitsu End User Software License Agreement" screen is displayed.

5. Check the contents, and then check [Above contents are correct.].
6. Select the [Agree] button.

7. Follow the procedure below and register a license key.

    a. Specify the license key in the entry field.

    b. Select the [Apply] button.

    c. Select the [Add] button to add entry fields if adding other license keys.

    d. Repeat Step a to c and register all licenses, then select the [Close] button.

Point

If the [Registered licenses] button is selected, a list of all the registered licenses is displayed.

8. Select the [Restart ISM-VA] button and restart ISM-VA.

When registering additional node licenses

From the GUI, log in as an administrator and use the following procedure to register new licenses.

1. From the Global Navigation Menu on the GUI of ISM, select [Settings] - [General].

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

    The "License List" screen is displayed.

3. Select the [Register] button.

4. Follow the procedure below and register a license key.

    a. Specify the license key in the entry field.

    b. Select the [Add] button to add entry fields if adding other license keys.

    c. Repeat Step a to b and after specifying all the licenses, select the [Apply] button.

Note

Licenses cannot be deleted from the GUI. Delete licenses from the console. For details, refer to deleting licenses in "4.8 License Settings" in "User's Guide."

2.2 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 GUI of ISM, select [Management] - [Datacenters].

    The "Datacenter List" screen is displayed.

2. Select the ➕ button.

    The "Register Datacenter/Floor/Rack" screen will be 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.
    Procedure to display the help screen: Select the [?] in the upper right side on the screen.

    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 "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.
   Procedure to display the help screen: Select the [?] in the upper right side on the screen.
3. Confirm that the datacenter to be deleted is correct, and then select [Delete].

2.3 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 will be 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 "2.2 Register/Delete Datacenters."

   Refer to the help screen regarding other setting items.
   Procedure to display the help screen: Select the [?] in the upper right side on the screen.

   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.
   Procedure to display the help screen: Select the [?] in the upper right side on the screen.
3. Confirm that the floor to be deleted is correct, and then select [Delete].

2.4 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 will be 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 "2.2 Register/Delete Datacenters" and "2.3 Register/Delete Floors."

   Refer to the help screen regarding other setting items.
   Procedure to display the help screen: Select the [?] in the upper right side on the screen.

   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 GUI of ISM, 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.
   Procedure to display the help screen: Select the [?] in the upper right side on the screen.

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

2.5 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.
   Procedure to display the help screen: Select the [?] in the upper right side on the screen.

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.

2.6 Set an Alarm (ISM internal events)

By setting alarms, it becomes possible to send notifications to the ISM external devices when the ISM detects errors or events in ISM.

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

1. Action settings (notification method) (Refer to "2.6.1 Execute Action Settings (notification method).")
2. Test of Action (notification method) (Refer to "2.6.2 Execute Test for Action (notification method).")
3. Alarm settings (Refer to "2.6.3 Set an Alarm to the ISM Internal Event.")

2.6.1 Execute Action Settings (notification method)

Set a notification method for communication with ISM externals.

The followings 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.
  Procedure to display the help screen: Select the [?] in the upper right side on the screen.

Preparations are required before Action settings (notification method).

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

2.6.1.1 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)
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 setting procedures, 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 GUI of ISM, 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.

2.6.1.2 Send mail

Pre-settings

1. From the Global Navigation Menu on the GUI of ISM, 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 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 GUI of ISM, 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 action addition is finished, the set action will be displayed on the "Action List" screen.

2.6.1.3 Execute sending/forwarding a trap

Pre-settings

1. From the Global Navigation Menu on the GUI of ISM, 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 GUI of ISM, 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 action addition is finished, the set action will be displayed on the "Action List" screen.

2.6.1.4 Execute Syslog forwarding

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

The following OSes are supported as external Syslog servers.

- RHEL 6, RHEL 7
- CentOS 6, CentOS 7
- SLES 11, SLES 12, SLES 15

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.

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

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

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

2. Add the following content.

```
$ModLoad imtcp
$InputTCPServerRun 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 RHEL 7, CentOS 7, SLES 12, SLES 15

   ```
   # systemctl restart rsyslog
   ```

   - For RHEL 6, CentOS 6

   ```
   # service rsyslog restart
   ```

For SLES 11

1. Execute the following command to start editing "/etc/syslog-ng/syslog-ng.conf."

```
# vi /etc/syslog-ng/syslog-ng.conf
```

2. Add the following content.

```
source src {

      -Omitted-

tcp(ip("0.0.0.0") port(514));        *Add the left line, use the IP address of ISM
}
```

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

```
# service syslog restart
```

Action settings

1. From the Global Navigation Menu on the GUI of ISM, 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 action addition is finished, the set action will be displayed on the "Action List" screen.

2.6.2 Execute Test for Action (notification method)

1. From the Global Navigation Menu on the GUI of ISM, 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 operated as it set.

2.6.3 Set an Alarm to the ISM Internal Event

1. From the Global Navigation Menu on the GUI of ISM, 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 "Target" screen in the "Add Alarm" wizard.

   Refer to the help screen for entering other setting items.
4. Confirm the contents on the "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.

2.7 Register Administrator 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 manage ISM in its entirety.

2.7.1 Manage ISM Users

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

- 2.7.1.1 Add users
- 2.7.1.2 Edit users
- 2.7.1.3 Delete users

2.7.1.1 Add users

Point

This operation can be executed only by users with Administrator privilege.

Add new users by the following procedure:

1. From the Global Navigation Menu on the GUI of ISM, 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:

- User Name

  Specify a user name that is unique across the entire ISM system.

  The following names cannot be used because they are used by ISM.

    - A name starting with _
    - Administrator
    - anonymous
    - svimcontent
- Password
- User Role

  For information on user roles, refer to "2.13.1 User Management" in "User's Guide."
- 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
- Authentication Method

  You can select one of the following.
    - Follow user group setting
    - Infrastructure Manager (ISM)
- 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
- Time Zone
- Select the user group

2.7.1.2 Edit users

Point

For this operation, the information that can be changed differ 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 GUI of ISM, 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, 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

User information	Administrator group		Group other than administrator group	
	Administrator role	Operator role Monitor role	Administrator role	Operator role Monitor role
Password	Y	Y	Y	Y
User Role	Y	N	Y	N
Link with ISM	Y	N	N	N
Authentication Method	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.

2.7.1.3 Delete users

Point

This operation can be executed only by users with Administrator privilege.

Delete any users as required by the following procedure.

1. From the Global Navigation Menu on the GUI of ISM, 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, 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].

2.7.2 Manage User Groups

The following types of user group management are available:

- 2.7.2.1 Add user groups
- 2.7.2.2 Edit user groups
- 2.7.2.3 Delete user groups

Point

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

2.7.2.1 Add user groups

ISM administrators add new user groups by the following procedure:

1. From the Global Navigation Menu on the GUI of ISM, 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:

- User Group Name

  Specify a user group name that is unique across the entire ISM system.

  The following names cannot be used because they are used by ISM.

  - A name starting with _
  - Administrator
  - AbstractionLayer
  - anonymous
  - svimcontent

- Link with Microsoft AD Group (ISM 2.4.0.b or later)

  Specify when linking with users on a directory server. For details, refer to "2.7.3.2 Manage users and passwords on directory servers (ISM 2.4.0.b or later)."

- User roles (ISM 2.4.0.b or later)

  Specify when linking with users on directory servers. Specify the user roles for the users to be linked. For details, refer to "2.7.3.2 Manage users and passwords on directory servers (ISM 2.4.0.b or later)."

- Description

  Enter a description of the user group (comment). You can freely enter any contents as required.

- Directory size

  You can specify the alert of the upper limit for the total size of the files used by the user group and the notification threshold value.

Utilization	Size Restriction	Threshold Monitoring
Across user group	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	You cannot specify the value.

Utilization	Size Restriction	Threshold Monitoring
	executed import to the Repository results in error and an error message is exported to the Operation Log.	
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."

- Managed nodes

  Create correlations between user groups and node groups as required by selecting a node group.

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.

2.7.2.2 Edit user groups

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

1. From the Global Navigation Menu on the GUI of ISM, 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, 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.

- User group name
- Authentication Method
- User roles (ISM 2.4.0.b or later)
- Description
- 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.

- Directory size

  For the edited contents, refer to "Directory size" in "2.7.2.1 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.

2.7.2.3 Delete user groups

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

1. From the Global Navigation Menu on the GUI of ISM, 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, 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.

2.7.3 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 (ISM 2.4.0.b or later)

  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.

2.7.3.1 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 up the following information in the LDAP server settings of ISM.

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

Item	Setting contents
LDAP Server 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:

Item	Setting contents
	- 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.

4. Prepare the user groups for which you set Microsoft Active Directory or LDAP as the authentication method.

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

6. From the menu on the left side of the screen, select [Users] and add the user registered in Step 1.

   The information to be registered is as follows.

Item	Setting contents
User Name	Specify the names of the users you registered in Step 1.
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.

7. Confirm that the users you registered in Step 6 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

Procedure for disabling the settings

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

- Changing 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.

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

- Changing user groups

  Edit the user group to change the authentication method to "Infrastructure Manager (ISM)."

Both of the above operations enable the passwords you set during user registration or modified at a later stage.

2.7.3.2 Manage users and passwords on directory servers (ISM 2.4.0.b or later)

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 following information in the LDAP server settings of ISM.

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

Item	Setting contents
LDAP Server 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
Search Attribute	Specify the account attribute for searching accounts. 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 Microsoft Active Directory: ldap_search@company.com "anonymous" is not supported. "CN=ldap_search,OU=user_group,DC=company,DC=com" format 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.

4. Create the ISM user group that corresponds to the group on the directory server.

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

   b. From the menu on the left side of the screen, select [User Groups], and then add the user group that has the same name as the group on the directory server.

   The information to be registered is as follows.

Item	Setting contents
User Group Name	Specify the same name as the group on the directory server.
Link with Microsoft AD Group	Specify "Enable."
User Role	Specify the user role.

   For information other than the above, refer to "2.7.2.1 Add user groups."

5. Confirm that the users that belong to the group on the directory server registered in Step 4 are able to log in with the following.

   - User Name

     User name on the directory server

   - 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.

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.

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 GUI of ISM, select [Settings] - [Users].
3. Delete all users from the user group that has the same name as the group that you want to disable.

   For details, refer to "2.7.1.3 Delete users."
4. The user group that has the same name as the group that you want to disable is deleted.

   For details, refer to "2.7.2.3 Delete user groups."

2.7.4 Manage Node Groups

The following types of node group management are available:

- 2.7.4.1 Add node groups
- 2.7.4.2 Edit node groups
- 2.7.4.3 Delete node groups

Point

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

2.7.4.1 Add node groups

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

1. From the Global Navigation Menu on the GUI of ISM, 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 GUI of ISM, 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

  Specify a user name that is unique across the entire ISM system.

- 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.

2.7.4.2 Edit node groups

ISM administrators can edit node groups with the following procedure:

1. From the Global Navigation Menu on the GUI of ISM, 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 GUI of ISM, 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

  Specify a user name that is unique across the entire ISM system.

- 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 GUI of ISM, 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 2.2 Models in which tree structures are set between nodes."

Table 2.2 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	-	└
ETERNUS DX	-	Drive Enclosure	└
Drive Enclosure	ETERNUS DX	-	└
ETERNUS NR (NetApp) Cluster	-	ETERNUS NR (NetApp) Chassis	└
ETERNUS NR (NetApp) Chassis	ETERNUS NR (NetApp) Cluster	External Attached Disk Shelf	└
External Attached Disk Shelf	ETERNUS NR (NetApp) Chassis	-	└
VCS Fabric	-	VDX Switch	└
VDX Switch	VCS Fabric	-	└
C-Fabric	-	CFX2000 series/PY CB Eth Switch 10/40Gb 18/8+2 (Fabric mode)	└

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

2.7.4.3 Delete node groups

ISM administrators can delete node groups with the following procedure:

1. From the Global Navigation Menu on the GUI of ISM, 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 GUI of ISM, 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

2.8 Upload Files to ISM-VA

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

1. From the Global Navigation Menu on the GUI of ISM, 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 select other than "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 GUI of ISM. 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.

2.9 Delete Files Uploaded to ISM-VA

This section describes the operations to delete files uploaded to ISM-VA by using the GUI of ISM.

1. From the Global Navigation Menu on the GUI of ISM, 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. Check the checkbox of 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 3 Register/Set/Delete a Managed Node

This chapter describes various settings such as registration/deletion of the 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.

3.1.1 Discover Nodes in the Network and Register Nodes

1. From the Global Navigation Menu on the GUI of ISM, 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, contact your local Fujitsu customer service partner.

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.

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 or the FQDN name (the FQDN name is for ISM 2.4.0.b or later).
Discovery target	Select from the following items. - Server (iRMC/BMC + HTTPS) Select when you want to discover the server or PRIMEQUEST 3800B. - PRIMERGY CX1430 M1 or PRIMERGY GX2580 M5 (BMC + HTTPS) Select when you want to discover PRIMERGY CX1430 M1 or PRIMERGY GX2580 M5 (ISM 2.4.0.c or later). - 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)

Setting items	Setting contents
	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 + HTTPS) 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 CX1430M1 or PRIMERGY GX2580 M5 (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 3.4 When selecting PRIMEQUEST2000, PRIMEQUEST3000E (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 3.5 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 3.6 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 3.7 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 in local. - 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. - 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]. Check 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","HttpsPor
t"
"192.168.10.11"," admin1","********",""," admin1","********",""
"192.168.10.12"," admin2","********",""," 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].

8. Select the checkbox of 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 input the setting items.

    Refer to the help screen for descriptions on the setting items.
    Procedure to display the help screen: Select the [?] in the upper right side on the wizard screen.

    - Entering node information

Table 3.8 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 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.
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.

Setting items	Setting contents
	Select the [Edit] button, 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, contact your local Fujitsu customer service partner.
Web i/f URL	Enter the URL when you access Web i/f on the node.
Description	Enter the descriptions.

- Entering communication methods

  When registering nodes which are discovered with Auto Discovery, you must set the communication methods. Select [Settings] for each node and enter the communication method.

11. After entering the registration information of the discovered node has been finished, select the [Registration] button.

    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 procedures.

12. On the "Node List" screen, select the target node to select the Details of Node screen - [OS] tab.

13. Select [OS Actions] - [Edit OS Information].

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

Table 3.9 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. When using Windows, it is the port number of the WinRM service (Default: 5986), when using Linux it is the port number of the SSH service (Default: 22). When not entered, the default port number will be set.

14. 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.

3.1.2 Register a Node Directly

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

   The "Node Registration" screen is displayed.

2. From the [Actions] button, select [Register].

   The "Node Manual Registration" wizard is displayed.

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

   Refer to the help screen for descriptions on the setting items.
   Procedure to display the help screen: Select the [?] in the upper right side on the wizard screen.

Below is the description for the [Communication methods] setting items on the "1. Node Information" screen in the "Node Manual Registration" wizard.

Table 3.10 When "server" was selected in [Node Type] and PRIMERGY RX/TX series, PRIMERGY CX series (other than PRIMERGY CX1430 M1), PRIMERGY BX series (other than PRIMERGY BX900 S2), PRIMEQUEST 3800B, or IPCOM VX2 series was selected in [Model Name]

Setting items		Description
iRMC		When not accessing the node with iRMC, uncheck the checkbox (Default: Checked).
	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 3.11 When "server" was selected in [Node Type] and PRIMERGY CX1430 M1 or PRIMERGY GX2580 M5 was selected in [Model Name]

Setting items		Description
BMC		When not accessing the node with BMC, uncheck the checkbox (Default: Checked).
	User Name	BMC User Name
	Password	BMC Password
	Port Number	BMC Port Number (Default: 623)
HTTPS		When not accessing the node with HTTPS, uncheck the checkbox (Default: Checked).
	User Name	HTTPS User Name
	Password	HTTPS Password
	Port Number	HTTPS Port Number (Default: 443)

Table 3.12 When "server" was selected in [Node Type] and PRIMEQUEST 2000 series and PRIMEQUEST 3000 series except PRIMEQUEST 3800B was selected in [Model Name]

Setting items		Description
MMB		When not accessing the node with MMB, uncheck the checkbox (Default: Checked).
	User Name	MMB User Name
	Password	MMB Password
	Port Number	MMB Port Number (Default: 623)
SSH		When not accessing the node with SNMP, uncheck the checkbox (Default: Checked).
	User Name	User Name of PRIMEQUEST
	Password	User Password of PRIMEQUEST
	Port Number	SSH Port Number (Default: 22)
SNMP [Note 1]		When not accessing the node with SNMP, uncheck the checkbox (Default: Checked).
	Version	SNMP Version
	Port Number	SNMP Port Number (Default: 161)
	Community	SNMP community name of PRIMEQUEST

[Note 1]: This is the setting item when selecting SNMPv1 or SNMPv2c for SNMP version. If you have selected SNMPv3, refer to "Table 3.26 When selecting "SNMPv3" for SNMP version."

Table 3.13 When "server" was selected in [Node Type] and PRIMERGY BX900 S2 was selected in [Model Name]

Setting items		Description
SSH		When not accessing the node with SNMP, uncheck the checkbox (Default: Checked).
	User Name	User Name of PRIMERGY BX900 S2
	Password	User Password of PRIMERGY BX900 S2
	Port Number	SSH Port Number (Default: 22)
SNMP [Note 1]		When not accessing the node with SNMP, uncheck the checkbox (Default: Checked).
	Version	SNMP Version
	Port Number	SNMP Port Number (Default: 161)
	Community	SNMP community name of PRIMERGY BX900 S2

[Note 1]: This is the setting item when selecting SNMPv1 or SNMPv2c for SNMP version. If you have selected SNMPv3, refer to "Table 3.26 When selecting "SNMPv3" for SNMP version."

Table 3.14 When "server" was selected in [Node Type] and Generic Server (IPMI) was selected in [Model Name]

Setting items		Description
iRMC/BMC		When not accessing the node with iRMC/BMC, uncheck the checkbox (Default: Checked).
	User Name	iRMC/BMC User Name
	Password	Password of iRMC/BMC
	Port Number	iRMC/BMC Port Number (Default: 623)

Table 3.15 When "server" was selected in [Node Type] and Generic Server (SNMP) was selected in [Model Name]

Setting items		Description
SNMP [Note 1]		When not accessing the node with SNMP, uncheck the checkbox (Default: Checked).
	Version	SNMP Version
	Port Number	SNMP Port Number (Default: 161)
	Community	SNMP community name of Generic Server (SNMP)

[Note 1]: This is the setting item when selecting SNMPv1 or SNMPv2c for SNMP version. If you have selected SNMPv3, refer to "Table 3.26 When selecting "SNMPv3" for SNMP version."

Table 3.16 When "server" was selected in [Node Type] and "other" was selected in [Model Name]

Setting items		Description
iRMC/BMC		When accessing the node with iRMC/BMC, check the checkbox (Default: Unchecked).
	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, check the checkbox (Default: Unchecked).
	User Name	HTTPS User Name
	Password	HTTPS Password
	Port Number	HTTPS Port Number (Default: 443)
SSH		When accessing the node with SSH, check the checkbox (Default: Unchecked).
	User Name	SSH User Name

Setting items		Description
	Password	SSH Password
	Port Number	SSH Port Number (Default: 22)
SNMP [Note 1]		When accessing the node with SNMP, check the checkbox (Default: Unchecked).
	Version	SNMP Version
	Port Number	SNMP Port Number (Default: 161)
	Community	SNMP community name of the node to register

[Note 1]: This is the setting item when selecting SNMPv1 or SNMPv2c for SNMP version. If you have selected SNMPv3, refer to "Table 3.26 When selecting "SNMPv3" for SNMP version."

Table 3.17 When "switch" was selected in [Node Type] and other than SH-E514TR1, ICX6430, Cisco Catalyst switch, Generic Switch (SNMP), Generic Switch (PING) or "other" was selected in [Model Name], or when "storage" was selected in [Node Type] and other than Generic Storage (SNMP), Generic Storage (PING) or "other" was selected in [Model Name]

Setting items		Description
SSH		When not accessing the node with SNMP, uncheck the checkbox (Default: Checked).
	User Name	User Name of the switch or storage
	Password	User Password of the switch or storage
	Port Number	SSH Port Number (Default: 22)
SNMP [Note 1]		When not accessing the node with SNMP, uncheck the checkbox (Default: Checked).
	Version	SNMP Version
	Port Number	SNMP Port Number (Default: 161)
	Community	SNMP community name of the switch or storage

[Note 1]: This is the setting item when selecting SNMPv1 or SNMPv2c for SNMP version. If you have selected SNMPv3, refer to "Table 3.26 When selecting "SNMPv3" for SNMP version."

Table 3.18 When "switch" was selected in [Node Type] and "Cisco Catalyst switch" was selected in [Model Name]

Setting items			Description
SSH			When not accessing the node with SNMP, uncheck the checkbox (Default: Checked).
	User Name		SSH User Name
	Password		SSH Password
	Port Number		SSH Port Number (Default: 22)
	Enable password		When not using the password, uncheck the checkbox (Default: Checked).
		Password	Enable password
SNMP [Note 1]			When not accessing the node with SNMP, uncheck the checkbox (Default: Checked).
	Version		SNMP Version
	Port Number		SNMP Port Number (Default: 161)
	Community		SNMP community name of Cisco Catalyst switch

[Note 1]: This is the setting item when selecting SNMPv1 or SNMPv2c for SNMP version. If you have selected SNMPv3, refer to "Table 3.26 When selecting "SNMPv3" for SNMP version."

Table 3.19 When "switch" was selected in [Node Type] and Generic Switch (SNMP) was selected in [Model Name]

Setting items		Description
SNMP [Note 1]		When not accessing the node with SNMP, uncheck the checkbox (Default: Checked).
	Version	SNMP Version
	Port Number	SNMP Port Number (Default: 161)
	Community	SNMP community name of Generic Switch (SNMP)

[Note 1]: This is the setting item when selecting SNMPv1 or SNMPv2c for SNMP version. If you have selected SNMPv3, refer to "Table 3.26 When selecting "SNMPv3" for SNMP version."

Table 3.20 When "switch" was selected in [Node Type] and "other" was selected in [Model Name]

Setting items		Description
iRMC/BMC		When accessing the node with iRMC/BMC, check the checkbox (Default: Unchecked).
	User Name	User Name of iRMC/BMC
	Password	iRMC/BMC Password
	Port Number	iRMC/BMC Port Number (Default: 623)
HTTPS		When accessing the node with HTTPS, check the checkbox (Default: Unchecked).
	User Name	HTTPS User Name
	Password	HTTPS Password
	Port Number	HTTPS Port Number (Default: 443)
SSH		When accessing the node with SSH, check the checkbox (Default: Unchecked).
	User Name	SSH User Name
	Password	SSH Password
	Port Number	SSH Port Number (Default: 22)
SNMP [Note 1]		When accessing the node with SNMP, check the checkbox (Default: Unchecked).
	Version	SNMP Version
	Port Number	SNMP Port Number (Default: 161)
	Community	SNMP community name of the node to register

[Note 1]: This is the setting item when selecting SNMPv1 or SNMPv2c for SNMP version. If you have selected SNMPv3, refer to "Table 3.26 When selecting "SNMPv3" for SNMP version."

Table 3.21 When "storage" was selected in [Node Type] and Generic Storage (SNMP) was selected in [Model Name]

Setting items		Description
SNMP [Note 1]		When not accessing the node with SNMP, uncheck the checkbox (Default: Checked).
	Version	SNMP Version
	Port Number	SNMP Port Number (Default: 161)
	Community	SNMP community name of Generic Storage (SNMP)

[Note 1]: This is the setting item when selecting SNMPv1 or SNMPv2c for SNMP version. If you have selected SNMPv3, refer to "Table 3.26 When selecting "SNMPv3" for SNMP version."

Table 3.22 When "storage" was selected in [Node Type] and "other" was selected in [Model Name]

Setting items		Description
iRMC/BMC		When accessing the node with iRMC/BMC, check the checkbox (Default: Unchecked).

Setting items		Description
	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, check the checkbox (Default: Unchecked).
	User Name	HTTPS User Name
	Password	HTTPS Password
	Port Number	HTTPS Port Number (Default: 443)
SSH		When accessing the node with SSH, check the checkbox (Default: Unchecked).
	User Name	SSH User Name
	Password	SSH Password
	Port Number	SSH Port Number (Default: 22)
SNMP [Note 1]		When accessing the node with SNMP, check the checkbox (Default: Unchecked).
	Version	SNMP Version
	Port Number	SNMP Port Number (Default: 161)
	Community	SNMP community name of the node to register

[Note 1]: This is the setting item when selecting SNMPv1 or SNMPv2c for SNMP version. If you have selected SNMPv3, refer to "Table 3.26 When selecting "SNMPv3" for SNMP version."

Table 3.23 When "facility" was selected in [Node Type] and other than Generic Facility (PING) and "other" was selected in [Model Name]

Setting items		Description
SNMP [Note 1]		When not accessing the node with SNMP, uncheck the checkbox (Default: Checked).
	Version	SNMP Version
	Port Number	SNMP Port Number (Default: 161)
	Community	SNMP community name of facility

[Note 1]: This is the setting item when selecting SNMPv1 or SNMPv2c for SNMP version. If you have selected SNMPv3, refer to "Table 3.26 When selecting "SNMPv3" for SNMP version."

Table 3.24 When "facility" was selected in [Node Type] and "other" was selected in [Model Name]

Setting items		Description
iRMC/BMC		When accessing the node with iRMC/BMC, check the checkbox (Default: Unchecked).
	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, check the checkbox (Default: Unchecked).
	User Name	HTTPS User Name
	Password	HTTPS Password
	Port Number	HTTPS Port Number (Default: 443)
SSH		When accessing the node with SSH, check the checkbox (Default: Unchecked).
	User Name	SSH User Name
	Password	SSH Password

Setting items		Description
	Port Number	SSH Port Number (Default: 22)
SNMP [Note 1]		When accessing the node with SNMP, check the checkbox (Default: Unchecked).
	Version	SNMP Version
	Port Number	SNMP Port Number (Default: 161)
	Community	SNMP community name of the node to register

[Note 1]: This is the setting item when selecting SNMPv1 or SNMPv2c for SNMP version. If you have selected SNMPv3, refer to "Table 3.26 When selecting "SNMPv3" for SNMP version."

Table 3.25 When "other" was selected in [Node Type]

Setting items		Description
iRMC/BMC		When accessing the node with iRMC/BMC, check the checkbox (Default: Unchecked).
	User Name	iRMC/BMC User Name
	Password	Password of iRMC/BMC
	Port Number	iRMC/BMC Port Number (Default: 623)
HTTPS		When accessing the node with HTTPS, check the checkbox (Default: Unchecked).
	User Name	HTTPS User Name
	Password	HTTPS Password
	Port Number	HTTPS Port Number (Default: 443)
SSH		When accessing the node with SSH, check the checkbox (Default: Unchecked).
	User Name	User Name of the node
	Password	User Password of the node
	Port Number	SSH Port Number (Default: 22)
SNMP [Note 1]		When accessing the node with SNMP, check the checkbox (Default: Unchecked).
	Version	SNMP Version
	Port Number	SNMP Port Number (Default: 161)
	Community	SNMP community name of the node to register

[Note 1]: This is the setting item when selecting SNMPv1 or SNMPv2c for SNMP version. If you have selected SNMPv3, refer to "Table 3.26 When selecting "SNMPv3" for SNMP version."

Table 3.26 When selecting "SNMPv3" for SNMP version

Setting items		Description
SNMP		When accessing the node with SNMP, check the checkbox. When not accessing the node with SNMP, uncheck 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

Setting items		Description
	Auth Password	Authentication Password of SNMPv3
	Privacy Protocol	Privacy Protocol of SNMPv3
	Privacy Password	Privacy Password of SNMPv3

4. From the Global Navigation Menu on the GUI of ISM, 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 procedures.

5. On the "Node List" screen, select the target node 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 3.27 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. When using Windows, it is the port number of the WinRM service (Default: 5986), when using Linux it is the port number of the SSH service (Default: 22). When not entered, the default port number will be set.

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.

3.1.3 Delete Nodes

Delete a registered node.

1. From the Global Navigation Menu on the GUI of ISM, 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, it becomes possible to send notifications to the ISM external devices when the ISM receives SNMP traps from managed devices or detects errors or events on the managed devices.

When setting the 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 followings 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 detailed setting procedure, refer to "2.6.1 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 GUI of ISM, 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 GUI of ISM, 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, select "Node" in "Applicable type" on the "Target" screen in the "Add Alarm" wizard to select an alarm setting target node.

   Refer to the help screen for entering other setting items.

4. Confirm the contents on the "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 GUI of ISM, 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."

Add MIB File

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

1. Prepare 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.

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 GUI of ISM, 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.

   - Check the [Enable schedule execution] box. When the check is disabled, 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, log 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] on the top of the Global Navigation Menu to confirm that the task has been completed.

3.3 Execute Settings on a Server/Install Server OS

When installing servers or adding new servers, you can specify hardware settings (BIOS, iRMC, MMB), OS installation, or virtual IO settings to the multiple servers together.

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 "3.3.3 Create a Policy to Simplify Profile Creation."

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

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

   "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.

   Point

   Refer to the help screen for entering the setting items.

   Procedure to display the help screen: Select the [?] in the upper right side on the wizard screen.

   [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 [Next].

      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 [Next].

       In 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 [Next].

       In 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 virtual IO]

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

    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. From the Global Navigation Menu on the GUI of ISM, 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.

7. In [Column Display], select [Profile].

8. From the node list, select the nodes where the profile should 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.
    Procedure to display the help screen: Select the [?] in the upper right side on the screen.

    After the BIOS/iRMC/MMB/virtual IO settings is complete, the [Status] field on the "Node List" 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.

3.3.2 Install OS on a Server with Profiles

Install OSes 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 GUI of ISM, select [Structuring] - [Profiles].

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

   "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.

   Point

   Refer to the help screen for entering the setting items.

   Procedure to display the help screen: Select the [?] in the upper right side on the wizard screen.

   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 [Next].

   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 [Next].

      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. From the Global Navigation Menu on the GUI of ISM, 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.

8. In [Column Display], select "Profile."

9. From the node list, select the nodes where the profile should be assigned.

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

    The "Profile Assignment" screen is displayed.

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

    Refer to the help screen for entering the setting items.
    Procedure to display the help screen: Select the [?] in the upper right side on the screen.

    After the OS installation is complete, the [Status] field on the "Node List" 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 Create a Policy to Simplify Profile Creation

The 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 need always create a policy when creating a profile.

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

   "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.

     On the "1. General Information" screen in the "Add Policy" wizard, select "Server-Common" in the [Category] field (ISM 2.4.0.b or later).

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

   Refer to the help screen for entering the setting items.
   Procedure to display the help screen: Select the [?] in the upper right side on the wizard screen.

   After policy addition is complete, the corresponding policy will be displayed on the "All Policies" 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 execute 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 GUI of ISM, select [Structuring] - [Profiles].

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

   "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.
   Procedure to display the help screen: Select the [?] in the upper right side on the wizard screen.

   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.

5. From the Global Navigation Menu on the GUI of ISM, 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.

6. In [Column Display], select "Profile."

7. From the node list, select the nodes where the profile should 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.

   Procedure to display the help screen: Select the [?] in the upper right side on the screen.

   After assignment of the profile is complete, the [Status] column of the node will be displayed as [Assigned] on the "Node List" 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, confirming visually on the Network Map.

Change in VLAN settings of LAN Switch

Change VLAN settings of LAN switch from the Network Map.

1. From the Global Navigation Menu on the GUI of ISM, 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] in upper right side 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] on the top of the Global Navigation Menu to confirm that the task has been completed.

   This finishes the VLAN setting changes.

Change in Link Aggregation of LAN switch

Change Link Aggregation of LAN switch from the Network Map.

1. From the Global Navigation Menu on the GUI of ISM, 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

In ISM 2.4.0.b or later, 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 GUI of ISM, 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 a 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 GUI of ISM, 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 the password of the target node.
5. From the [Actions] button, select [Edit].

   The "Edit" screen is displayed.
6. Change the password of the communication methods to the password that was changed in Step 4.

   For setting values other than the password, change if required.
7. Check the content of the change, 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 GUI of ISM, 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.
7. Change the password to the password that was changed in Step 4.

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

   This finishes the password change for 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 the link with Microsoft Active Directory or LDAP.

For details, refer to "2.7.3 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 GUI of ISM, 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.
   - User Role

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

Note

- CAS is rebooted after executing the following operations. Therefore, you cannot use CAS just after executing them. To use CAS, you must log in again after the following operations.
  - Setting of Enable / Disable of CAS
  - Setting of the CAS port number
  - Setting of the directory server
  - Switching of the directory server
- 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)."

2. User Settings

   - Directory server

     Set the user in the directory server set in "2.7.3 Link with Microsoft Active Directory or LDAP."

   - ISM

     a. User Name

        Set a user name existing in the directory server set in "2.7.3 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 3.28 User roles that can use CAS

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

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

  1. Check the check box [Always display Login Page].
  2. Displays behaviors when checked.

3. 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.

Note

- If you uncheck [Always display Login Page], 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.

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. Select the URL of "Web i/f URL" on the Details of Node screen.

   The login screen of iRMC is displayed.

3. 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. ISM Dashboard is displayed.

Chapter 4 Check the Status of a Managed Node

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

4.1 Operate Dashboard

The Dashboard displays the widget showing various information about status, logs etc. Select the widget according to the needs of the user. The required information can be referenced.

Refer to the help screen for the procedure to select the widget to be shown on the Dashboard.

Procedure to display the help screen: Select the [ⓘHelp] - [Help] - [Help for this screen] in upper right side on the screen while it is displayed.

4.2 Check 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 GUI of ISM, 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 GUI of ISM, 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 a Floor summary on the upper left side 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 Check the Status of a Node

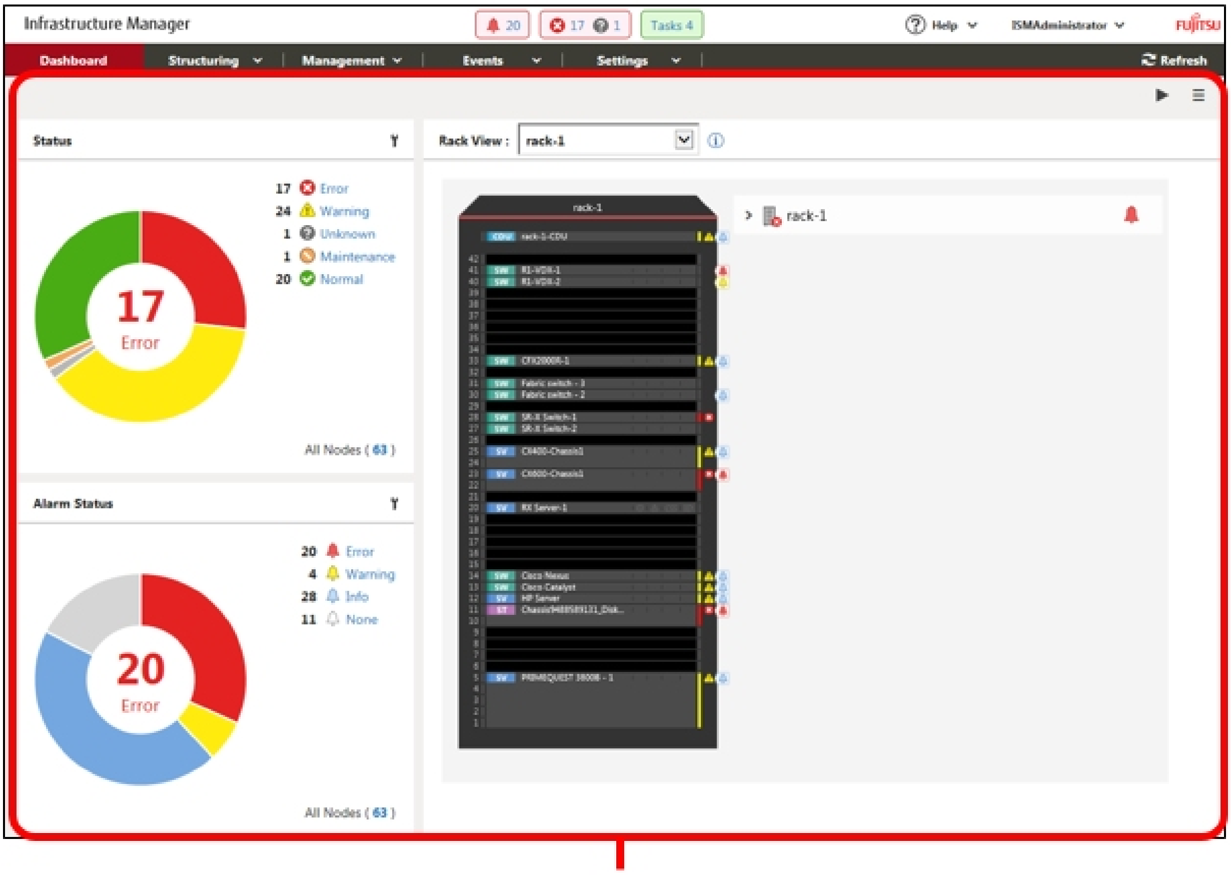
The node status can be checked in the [Status] widget on the Dashboard or on the "Node List" screen.

1. From the Global Navigation Menu on the GUI of ISM, 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.
   Procedure to display the help screen: Select the [ⓘHelp] - [Help] - [Help for this screen] in upper right side on the screen while it is displayed.



[Dashboard] screen

3. In the [Alarm Status] widget, select the status to check (Error, Warning, Maintenance, Normal, 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.
   Procedure to display the help screen: Select the [ⓘHelp] - [Help] - [Help for this screen] in upper right side on the screen while it is displayed.

   This finishes the node status display.

4.4 Display the Node Notification Information

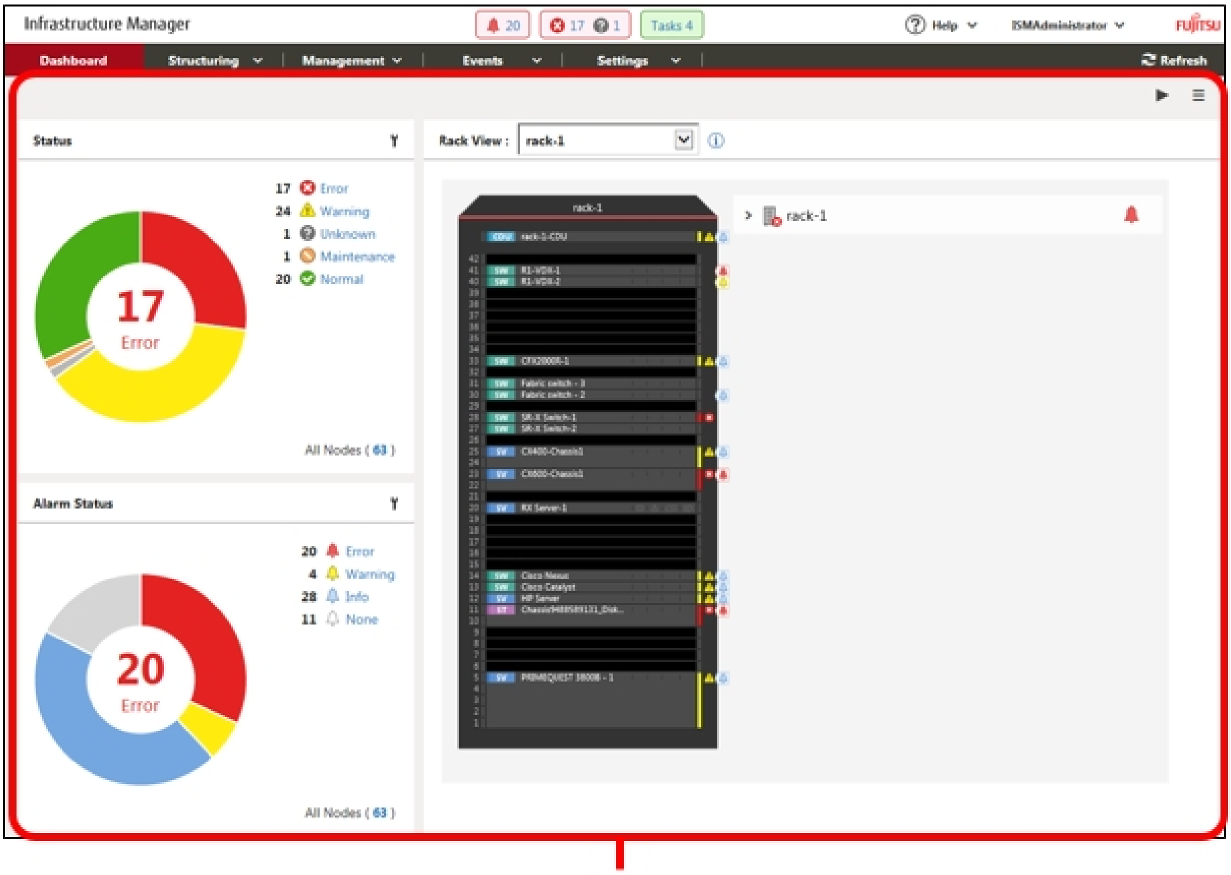
The node status, as well as whether an event has occurred on the node can be checked using either the [Alarm Status] widget on the Dashboard or by checking the "Node List" screen.

1. From the Global Navigation Menu on the GUI of ISM, 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.
   Procedure to display the help screen: Select the [?Help] - [Help] - [Help for this screen] in upper right side on the screen while it is displayed.



[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.
   Procedure to display the help screen: Select the [?Help] - [Help] - [Help for this screen] in upper right side on the screen while it is displayed.

   This finishes the display of the node notification information.

4.5 Display Monitoring History in a Graph

On the GUI of ISM, 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 GUI of ISM, 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 piled together.

Compare with other periods

From the [Compare with other periods] tab, graphs for the multiple periods of the same monitoring item can be displayed piled together. You can add 5 periods at a maximum and can display 6 graphs piled together. By piling 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 a graph.

   The multiple graphs are displayed piled together.

Compare with other item

From the [Compare with other item] tab, graphs for the multiple items of the same node can be displayed piled together. You can add one item at a maximum and can display two graphs piled together. By piling the graph of the other item 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.

   The multiple graphs are displayed piled together.

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 GUI of ISM, 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 top 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 Check Firmware Version

Displays the firmware version of the servers registered in ISM.

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

   The "Firmware" screen is displayed.

2. Select a 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 "Firmware" 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 retrieving the node information is completed, 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

Displays 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 to be displayed can be narrowed down.

1. From the Global Navigation Menu on the GUI of ISM, 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. When narrowing down the Node Logs displayed, select the [Filter] button.

   The "Filter" screen is displayed.

4. Enter the filtering requirements on the "Filter" screen, and then select the [Filter] button.

   Refer to the help screen for entering the filtering requirements.
   Procedure to display the help screen: Select the [?] in the upper right side on the screen.

   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 GUI of ISM, select [Structuring] - [Log Collection].

2. From the menu on the left side of the screen, select the [Log Management] - [Archived Log] tab.

3. Check the checkbox of 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.
   Procedure to display the help screen: Select the [?] in the upper right side on the screen.

   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 GUI of ISM, select [Management] - [Nodes].

2. Select the ⋮ button.

   The "Filter" screen is displayed.

3. Specify filtering items. When you want to execute filtering for all items, specify filtering conditions in [All Items] field. When you want to execute filtering 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 filtering conditions, the specified status button or pull down box on the top of the "Node List" screen becomes selected.

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 Check the Node where an Error Occurred

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 GUI of ISM, select [Dashboard].
2. In the [Status] widget, select the [Error] on the right side of ☒.

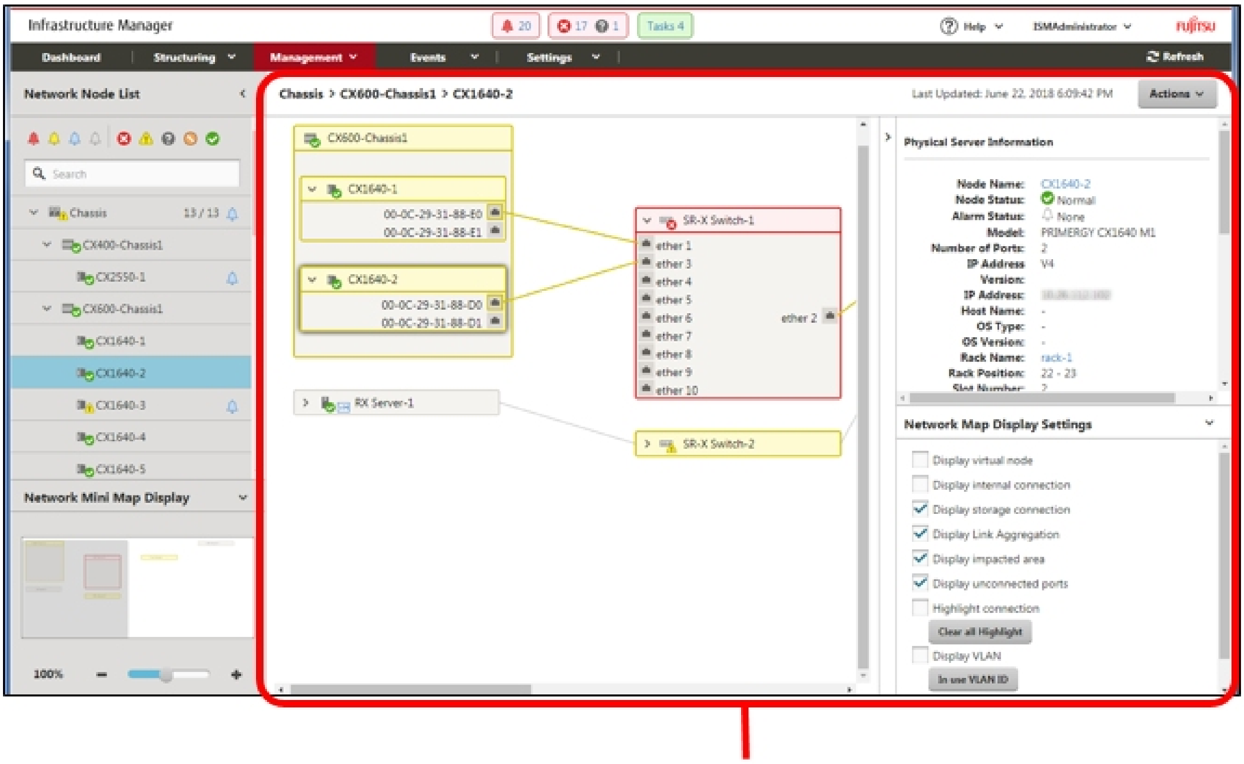
   Only the nodes where an error has occurred will be displayed.
3. Check the status for the error nodes displayed.

5.2 Check the Error Point/Affected Area on the Network

You can graphically check the error point on the network and its affected area with the Network Map.

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

   The "Network Map Display" screen is displayed.



Node Name: CX1640-2
Node Status: Normal
Alarm Status: None
Model: PRIMERGY CX1640 M1
Number of Ports: 2
IP Address Version: V4
IP Address: [redacted]
Host Name: -
OS Type: -
OS Version: -
Rack Name: rack-1
Rack Position: 22 - 23
Slot Number: 2

□ Display virtual node
□ Display internal connection
☑ Display storage connection
☑ Display Link Aggregation
☑ Display impacted area
☑ Display unconnected ports
□ Highlight connection
□ Display VLAN

[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, check [Display impacted area] 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 point on the network and its affected area.

5.3 Collect Logs of Managed Nodes

You can collect and accumulate Node Logs at any suitable time.

The following is a sample operation using the GUI for collecting logs.

1. From the Global Navigation Menu on the GUI of ISM, 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 all together.

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 of which you took a memo on the "Result" screen.

Point

The operations of manual log collection can be executed using the same operations for the screens displayed in the following procedure.

- From the Global Navigation Menu on the GUI of ISM, 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 GUI of ISM, 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.

Chapter 6 Other Functions to Manage/Operate Nodes

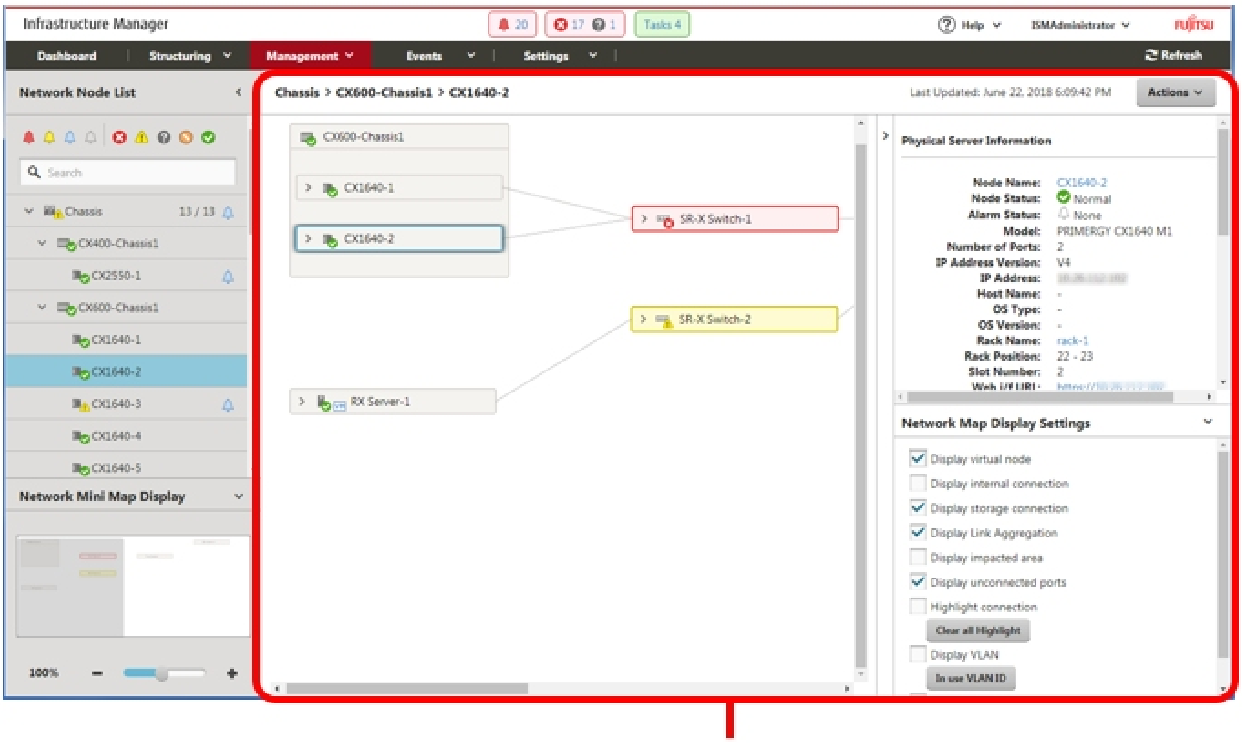
This chapter describes various operations for each node.

6.1 Set up Network Map

The Network Map displays the physical connections of LAN cables among the managed nodes. If LLDP (Link Layer Discovery Protocol) of the network port on the managed node is enabled, ISM retrieves the connection relation among the nodes and displays the connections on the Network Map. However, when the 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 GUI of ISM, select [Management] - [Network Map].

   The "Network Map Display" screen is displayed.



Node Name: CX1640-2
Node Status: Normal
Alarm Status: None
Model: PRIMERGY CX1640 M1
Number of Ports: 2
IP Address Version: V4
IP Address: [redacted]
Host Name: -
OS Type: -
OS Version: -
Rack Name: rack-1
Rack Position: 22 - 23
Slot Number: 2
Web I/F URL: [redacted]

☑ Display virtual node
□ Display internal connection
☑ Display storage connection
☑ Display Link Aggregation
□ Display impacted area
☑ Display unconnected ports
□ Highlight connection
□ Display VLAN

[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 2 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 the virtual machines and virtual switches running on the 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 a new cloud management software.

1. From the Global Navigation Menu on the GUI of ISM, 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 "Cloud Management Software Registration" 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.

   The cloud management software specified in the "Cloud Management Software List" screen is displayed.

   This finishes the registration of the cloud management software.

6.2.2 Confirm Information of Virtual Machines on the Managed Server

Retrieve the information of the cloud management software in order to display the information of the virtual machine.

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 GUI of ISM, select [Management] - [Nodes].

   The "Node List" screen is displayed.
2. Select 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 retrieval is complete.
4. From the Global Navigation Menu on the GUI of ISM, 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 retrieval of the cloud management software information is complete.

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

   The "Node List" screen is displayed.

8. Select the node that you retrieved its node information 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 Check the Status of Virtual Resource

By adding the information display screen (the widget) for the 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

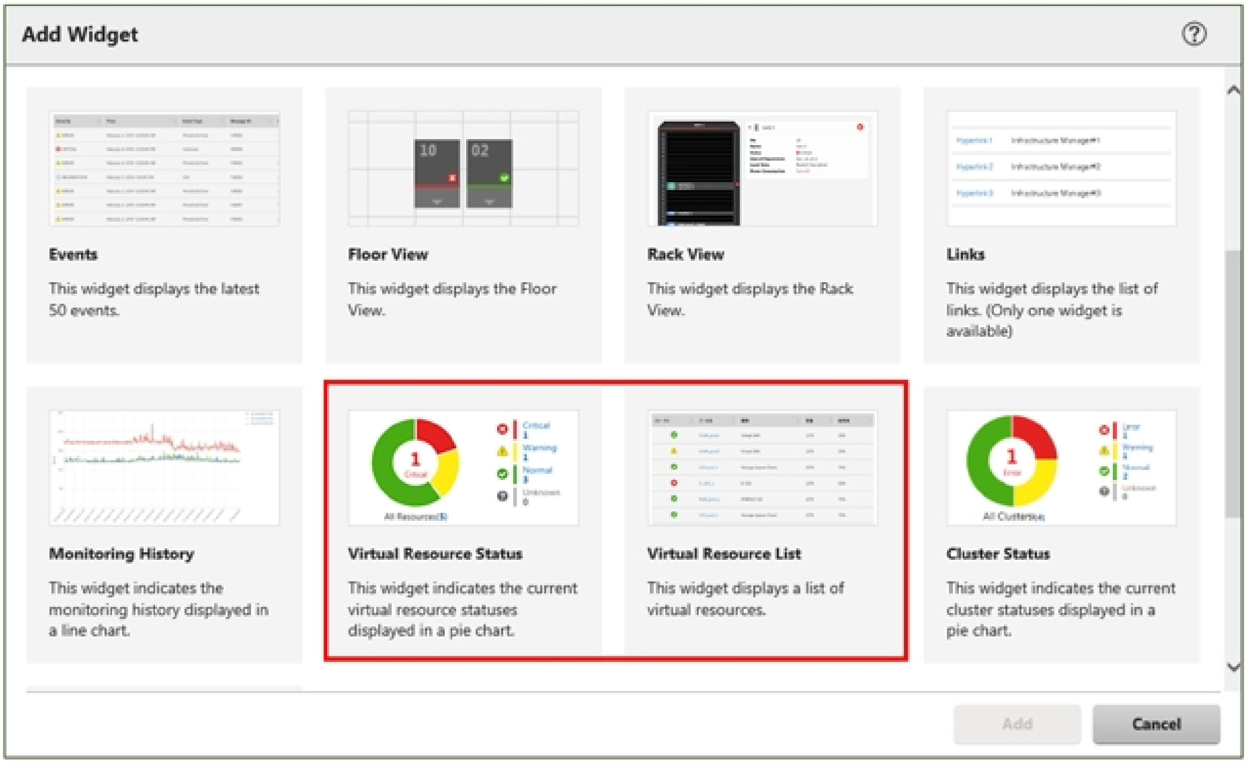
1. From the Global Navigation Menu on the GUI of ISM, select [Dashboard].

   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.



Add Widget

Events

This widget displays the latest 50 events.

Floor View

This widget displays the Floor View.

Rack View

This widget displays the Rack View.

Links

This widget displays the list of links. (Only one widget is available)

Monitoring History

This widget indicates the monitoring history displayed in a line chart.

Virtual Resource Status

This widget indicates the current virtual resource statuses displayed in a pie chart.

Virtual Resource List

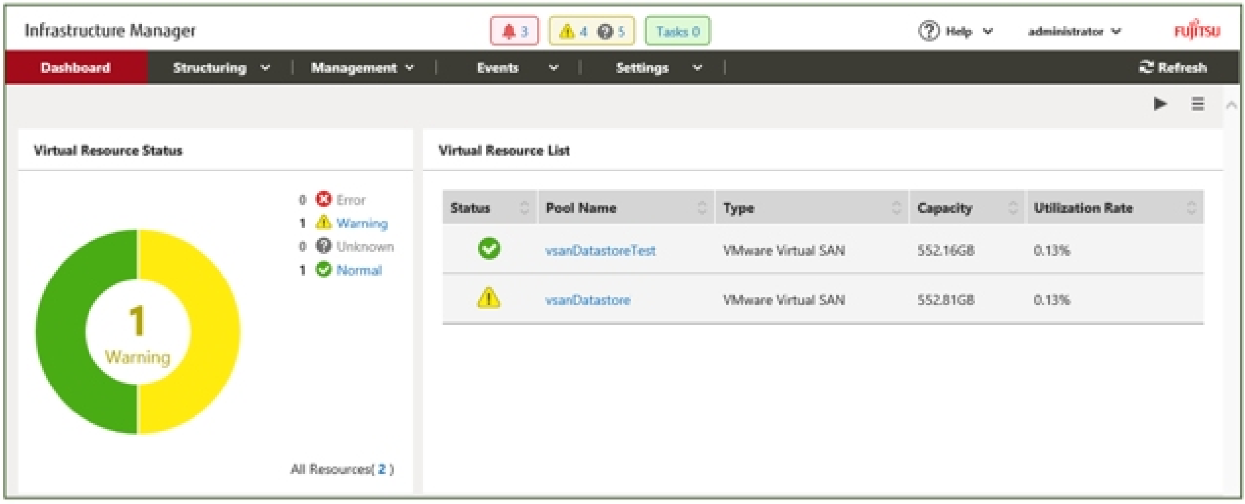
This widget displays a list of virtual resources.

Cluster Status

This widget indicates the current cluster statuses displayed in a pie chart.

3. Select either [Virtual Resource Status] or [Virtual Resource List], then select the [Add] button.

   The selected widget is displayed on the Dashboard.



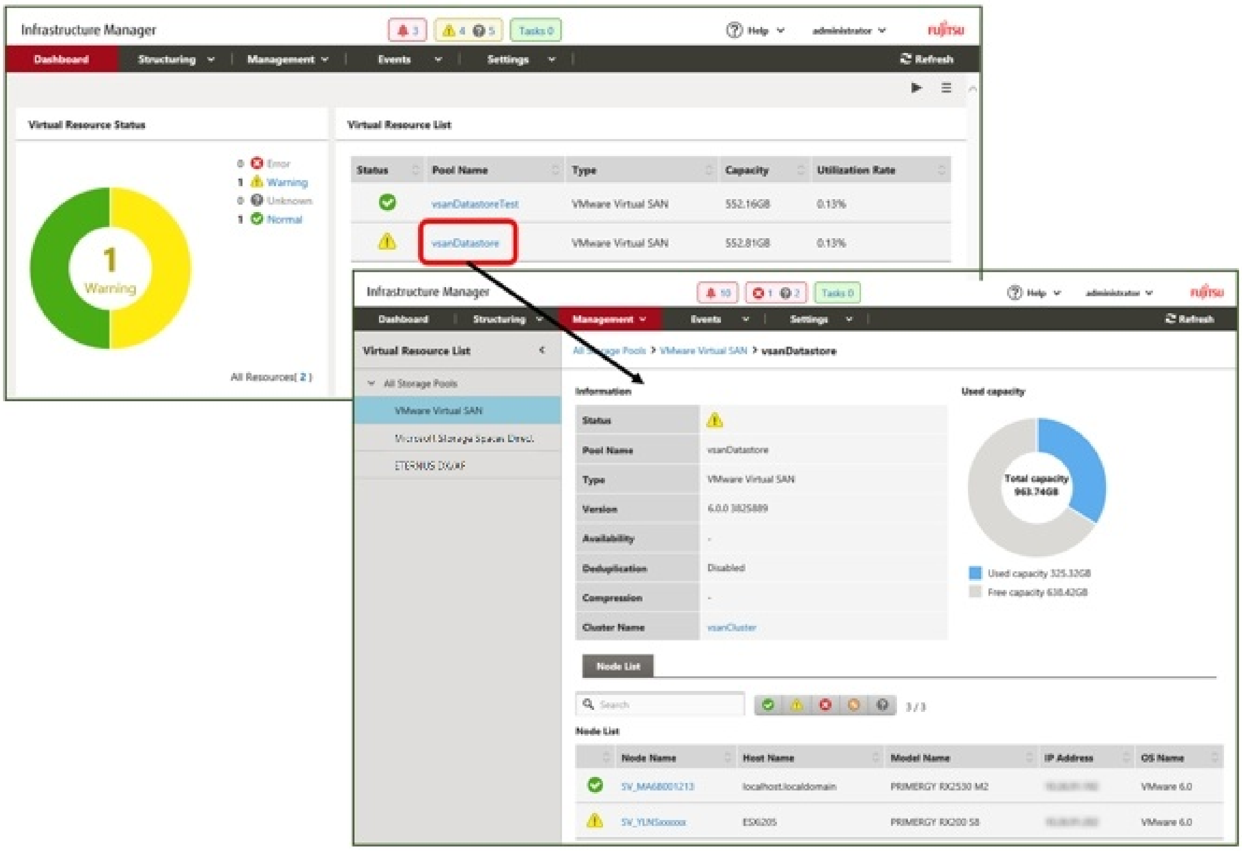
Status	Pool Name	Type	Capacity	Utilization Rate
✓	vsanDatastoreTest	VMware Virtual SAN	552.16GB	0.13%
⚠	vsanDatastore	VMware Virtual SAN	552.81GB	0.13%

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.
   Procedure to display the help screen: Select the [ⓘHelp] - [Help] - [Help for this screen] in upper right side on the screen while it is displayed.



Status	Pool Name	Type	Capacity	Utilization Rate
✓	vsanDatastoreTest	VMware Virtual SAN	552.16GB	0.13%
⚠	vsanDatastore	VMware Virtual SAN	552.81GB	0.13%

Information

Status	⚠
Pool Name	vsanDatastore
Type	VMware Virtual SAN
Version	6.0.0 3825889
Availability	-
Deduplication	Disabled
Compression	-
Cluster Name	vsanCluster

Node List

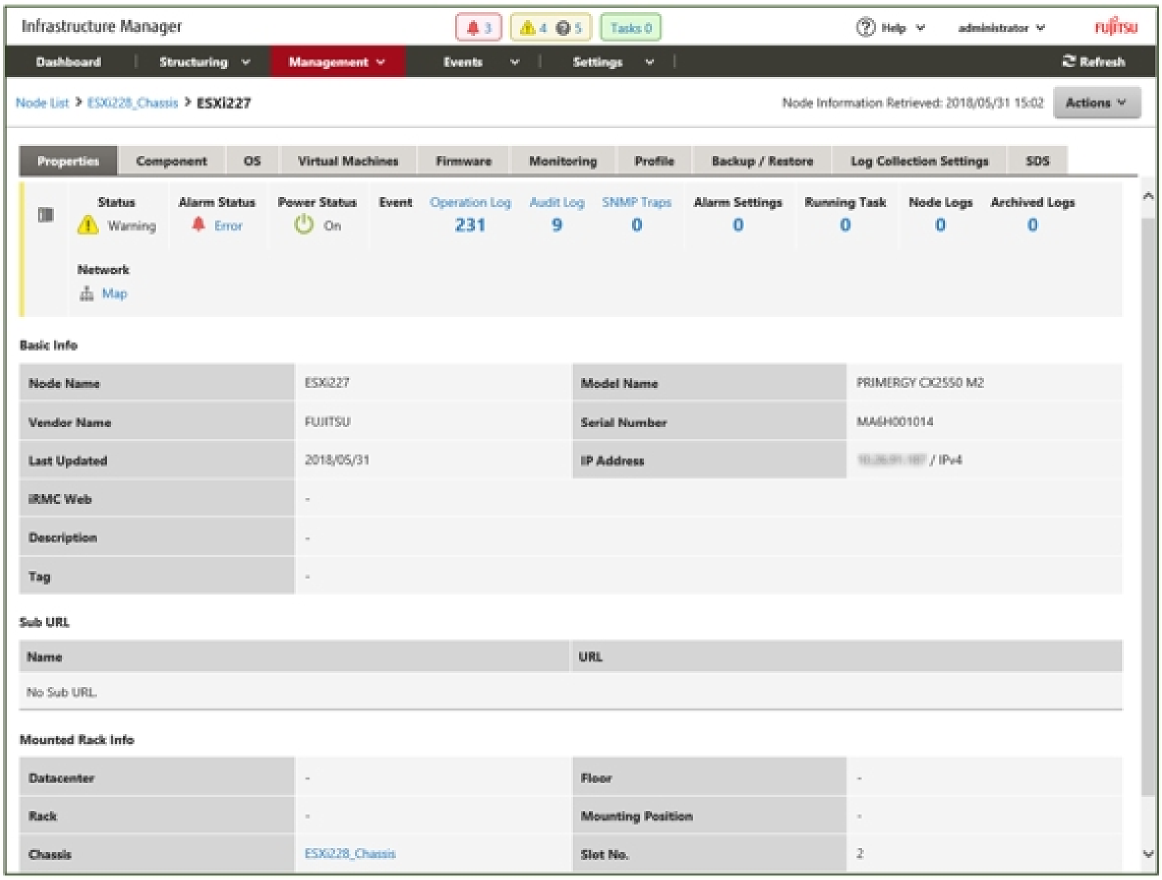
	Node Name	Host Name	Model Name	IP Address	OS Name
✓	SV_MA68001213	localhost.localdomain	PRIMERGY RX2530 M2	[redacted]	VMware 6.0
⚠	SV_YLNSxxxxx	ESX6205	PRIMERGY RX200 S8	[redacted]	VMware 6.0

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 GUI of ISM, select [Management] - [Nodes] to select the node name on the "Node List" screen.

   The Details of Node screen is displayed.



Status	Alarm Status	Power Status	Event	Operation Log	Audit Log	SNMP Traps	Alarm Settings	Running Task	Node Logs	Archived Logs
Warning	Error	On		231	9	0	0	0	0	0

Network
Map

Basic Info

Node Name	ESXi227	Model Name	PRIMERGY CX2550 M2
Vendor Name	FUJITSU	Serial Number	MA6H001014
Last Updated	2018/05/31	IP Address	[redacted] / IPv4
iRMC Web	-		
Description	-		
Tag	-		

Sub URL

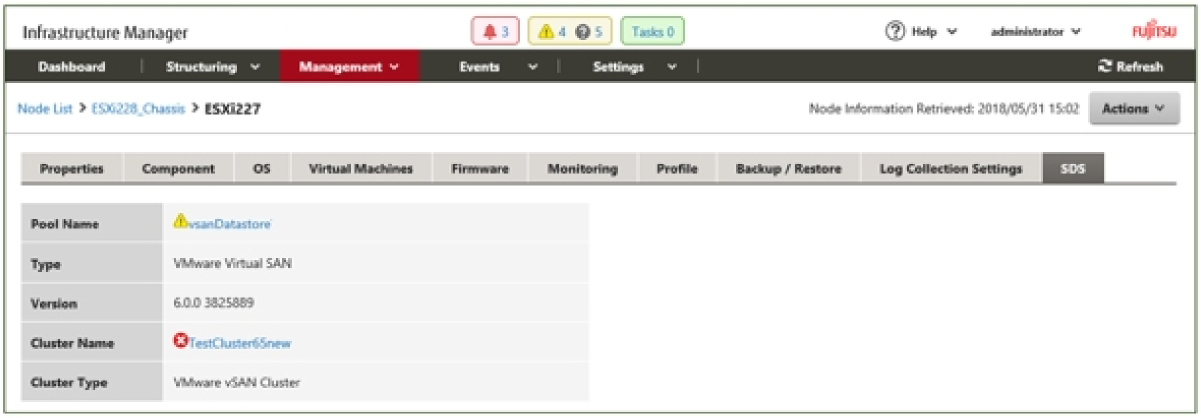
Name	URL
No Sub URL	

Mounted Rack Info

Datacenter	-	Floor	-
Rack	-	Mounting Position	-
Chassis	ESXi228_Chassis	Slot No.	2

2. Select the [SDS] tab.

   The storage pool information related to the node is displayed.



Pool Name	vsanDatastore
Type	VMware Virtual SAN
Version	6.0.0 3825889
Cluster Name	TestCluster65new
Cluster Type	VMware vSAN Cluster

When selecting [Pool Name], the details of the virtual resource screen is displayed.

6.3 Update the Firmware of the Server

Update the firmware of the servers registered in ISM.

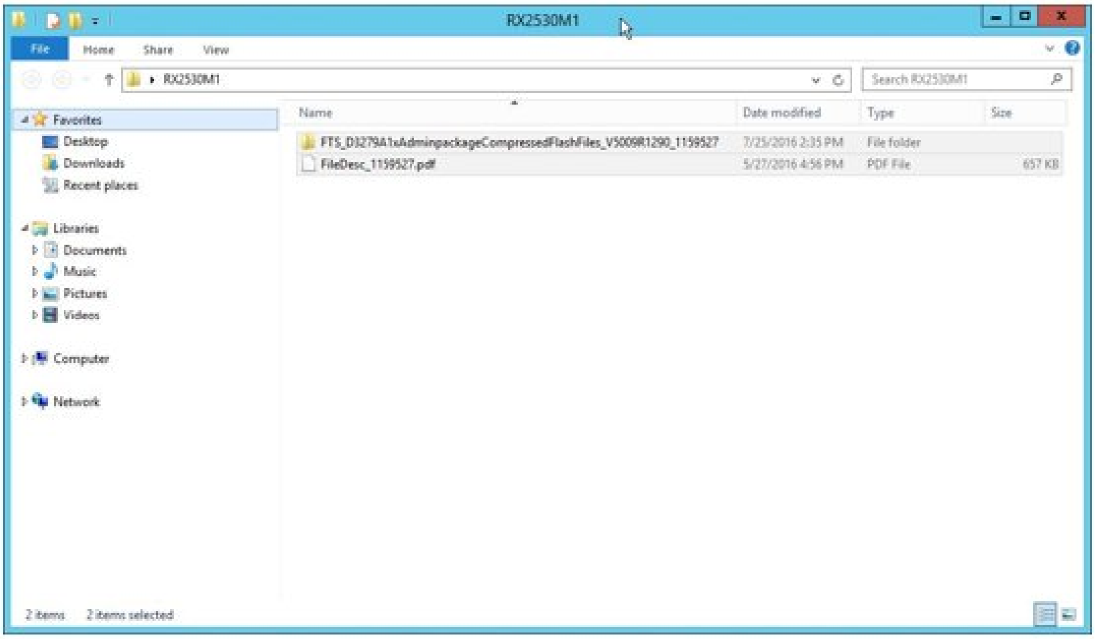
1. When the firmware to be updated is not imported yet, the firmware must first be imported. When it is already imported, proceed to Step 7.

2. Download the firmware of the iRMC/BIOS from the website.

   Download the firmware for the target model from the website below.

   http://support.ts.fujitsu.com/

3. Store the downloaded file in an arbitrary folder. When the downloaded file is compressed, decompress the file in the folder.



Name	Date modified	Type	Size
FTS_D3279A1xAdminpackageCompressedFlashFiles_V5009R1290_1159527	7/25/2016 2:35 PM	File folder	
FileDesc_1159527.pdf	5/27/2016 4:56 PM	PDF File	657 KB

4. Zip the folder in which the downloaded files are stored.

5. Import firmware.

   From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Firmware], and then select [Import] in the menu on the left side of the screen.

   In the [Import Data List] tab, from the [Actions] button, select [Import Firmware].

   Select "Local" in the [File selection method] and enter the [File Path], [Type], [Model Name] and [Version] according to the screen display, and then select the [Assign] button.

   Enter versions using the table below.

   Table 6.1 Versions to be entered

Type	Model	Version Entering Procedure
iRMC	RX100 S8, CX2550 M1, etc.	Refer to the release notes and specify the versions of iRMC and SDR.
BIOS	RX100 S8, CX2550 M1, etc.	Refer to the release notes and specify the BIOS version.

   After starting the import, the operations will be registered as ISM tasks. 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.

6. Confirm that the firmware has been imported.

   From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Firmware], and then select [Import] in the menu on the left side of the screen.

The "Import" screen is displayed.

Select the [Firmware Data] tab on the right side on the screen.

Confirm that the imported firmware is displayed on the list screen.

7. Select target server.

   On the "Firmware" screen, check the node to be executed firmware update.

   (When a firmware with a higher version than the current one is imported, you cannot check the box unless the version of this firmware is displayed in the Latest Version column.)

   From the [Actions] button, select [Update Firmware] to display the "Update Firmware" wizard.

8. Starting firmware update.

   Follow the instructions on the "Update Firmware" wizard and enter the setting items.

   Refer to the help screen for entering the setting items.

   Procedure to display the help screen: Select the [?] in the upper right side on the wizard screen.

   After starting the firmware update, the operations will be registered as ISM tasks.

   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.

9. When 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.

    From the Global Navigation Menu, select [Structuring] - [Firmware] to display the "Firmware" screen.

    Select a node name executed firmware update, retrieve node information from the "Node Information" screen - [Get Node Information].

    On the "Firmware" screen, the version number is displayed after 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 Execute Power Capping

In ISM, specifying the upper limit of power consumption by each rack enables to curb the power consumption of mounted devices.

The upper limit of the power consumption is configured by each of 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

A power capping setting is 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 at the following timing.

- Add a node to the rack

- Remove a node from the rack

- Move a node to another rack

6.4.1 Confirm the Current Power Capping Status

Confirm the power capping status of the target rack.

1. In 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 in the upper right side on the rack details screen.

Table 6.2 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.

6.4.2 Add/change the Power Capping Settings of the Rack

Register or edit the power capping definitions of the target rack.

1. In the "Datacenter List" screen, select the rack that you want to add or edit the power capping setting for.
2. From the [Actions] button, select the following.
   - When adding a new power capping setting: [Add Power Capping Setting]
   - When editing the set power capping setting: [Edit Power Capping Setting]

   The displayed content as well as the setting contents are displayed below.

   Rack power consumption column

   The current power capping status value is displayed.

   Table 6.3 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 6.4 [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 to the upper power value, it becomes the target for the 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 are 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 6.5 [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		
	All day	Check when not specifying operating time.

Item		Description
	Specify Time	Check when setting 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

6.4.3 Enable the Power Capping Policy of the Racks

Enable the Power Capping Policy for the applicable racks.

1. In 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 6.6 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 minimum is set it is executed with 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.

6.4.4 Delete Power Capping Settings for Racks

Delete all power capping settings information for the rack.

1. In 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.

6.5 Check the Traffic Status of the Network

Network Map displays the traffic status of virtual adapters of the virtual machines running on the managed nodes. This section describes procedures to check traffic status with Packet Analysis of Virtual Network.

Execute Packet Analysis of Virtual Network with the following procedures.

- 6.5.1 Obtain Analysis VM
- 6.5.2 Import Analysis VM
- 6.5.3 Set Virtual Adapter Threshold
- 6.5.4 Check Notification
- 6.5.5 Check Traffics
- 6.5.6 Start Packet Analysis
- 6.5.7 Check Packet Analysis Status
- 6.5.8 Check Packet Analysis Result
- 6.5.9 Stop Packet Analysis

6.5.1 Obtain Analysis VM

To obtain Analysis VM of virtual network, contact your local Fujitsu service partner.

6.5.2 Import Analysis VM

Deploy an Analysis VM image on ISM-VA.

Deploy the Analysis VM image in the file transferring area "/Administrator/ftp" within 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 "2.8 Upload Files to ISM-VA."

Note

The Analysis VM image to be used varies according to the type of hypervisor (VMware, KVM).

6.5.3 Set Virtual Adapter Threshold

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

   The "Network Map Display" screen is displayed.

2. From the [Actions] button, select [Setting Virtual Adapter Threshold].

3. Check the virtual adapter names and select the ports to be monitored.

4. Select the [Set Threshold] 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" for [Monitor Threshold] and after setting the threshold values, select the [Reflection] button.

   Point

   - When you enable [Monitor Threshold], monitoring the virtual adapters is started.
   - When you disable [Monitor Threshold], monitoring the virtual adapters is stopped.
   - When you enter threshold values, monitoring the threshold values is started.
   - When you delete threshold values, monitoring the threshold values is stopped. Obtaining information will continue.

Note

- The number of virtual adapters that can be monitored is maximum 1000.
- You can check the number of ports being monitored currently from "Monitoring Virtual Adapter" displayed on the upper side of the "Setting Virtual Adapter Threshold" screen.

6.5.4 Check Notification

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].

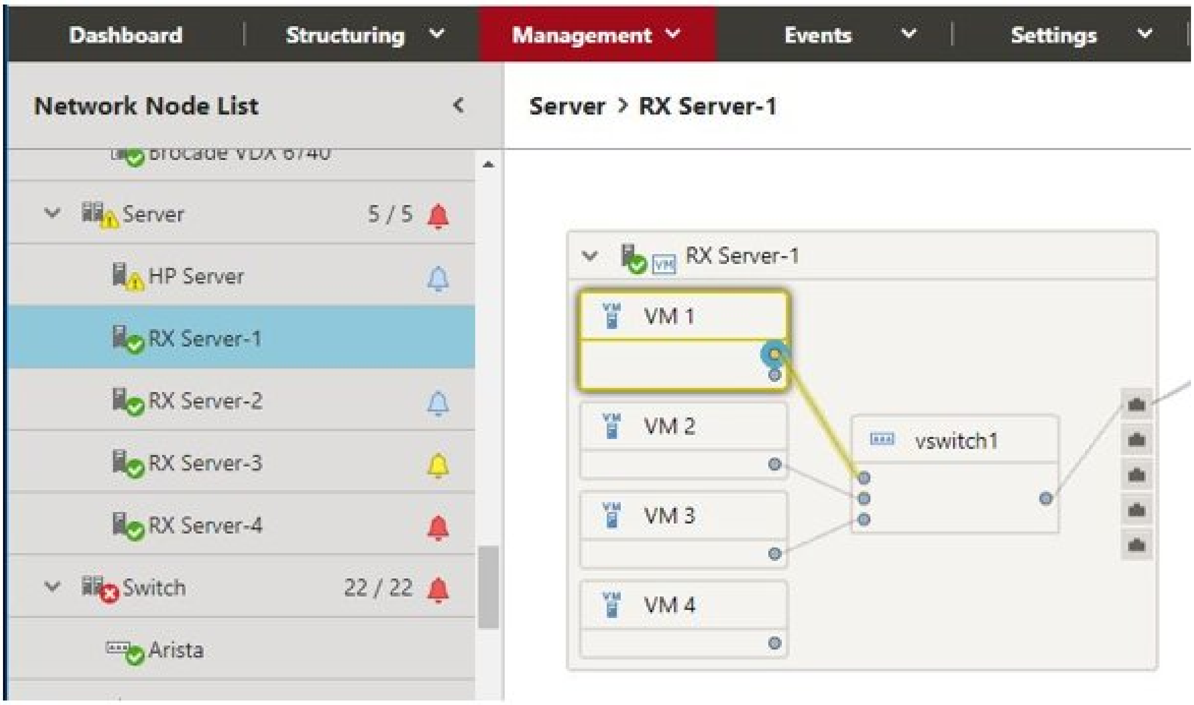
Event ID	Message
30030112	The upper warning threshold value was exceeded at the virtual adapter 'virtual adapter name' of the virtual machine 'virtual machine name'. The monitoring item 'monitoring item name' with value 'measured value' exceeded threshold 'value set by user'.
50030114	The upper abnormal 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'.

6.5.5 Check Traffics

1. Select an applicable [Virtual Network Adapter].

2. Select the node that was notified of in the event.

3. Select the virtual adapter name shown in the message of the event notified. Otherwise, select the virtual adapter name highlighted in the virtual machine that was notified of in the event.



4. Scroll the bar downward on the [Virtual Adapter Information] window displayed in the right pane to see [Traffic Information].

5. By selecting the [Graph] button located on the right of the information, you can check the transition of the monitored data in a graph.

6.5.6 Start Packet Analysis

If the cause of performance degradation cannot be identified even by completing up to traffic check, execute the packet analysis of the host where the event is occurring.

Deploy Analysis VM for the host OS where the performance failure is occurring.

1. Select the [Start Analysis] button.

2. Enter the parameters.

Table 6.7 Analysis VM IP Address Settings

Item	Description
IP Version	Select the IP version.
DHCP	Select whether to enable or disable DHCP.
IP address	Required if DHCP is disabled.
Prefix (when IPv6 is specified) Subnet Mask (when IPv4 is specified)	Required if DHCP is disabled.
Default Gateway	Required if DHCP is disabled. *vCenter will be shown only.
NTP server IP Address	Recommended to specify NTP server.

Table 6.8 Analysis VM Deploy Settings (vCenter)

Item	Description
Analysis VM Name	Specify the Analysis VM name.

Item	Description
Analysis VM Image Filename	Specify vmdk file of Analysis VM.
Analysis VM ovf Filename	Specify ovf file of Analysis VM.
Datastore Name	Specify a data store name.
Folder Name	Specify a folder to deploy the Analysis VM in.
Virtual Switch Type Connected to Management Port	Select the type of virtual switch for the connection destination of the management port.
Virtual Switch Name	Specify the name of switch that can communicate with ISM.
Network Label/Port Group	Specify a network label that can communicate with ISM or a port group name.

Table 6.9 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 a security group name that has SSH permission to be applied to Analysis VM.
Project Name	Specify a project name in which the Analysis VM belongs.
Network Name	Specify a network that can be communicated with ISM.
Floating IP Address Setting	Select if you use floating IP address.
Floating IP Address	Floating IP address is specified.

Note

- If the condition has been improved after addressing the cause as a result of checking the packet analysis outcome, stop the packet analysis.
- Once the packet analysis is started, do not delete or change the node OS account or cloud management software settings.
- Resources must be obtained in advance because Analysis VM will be deployed on the target host OS.

  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 target host automatically.
- 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 target host are depleted from analyzing packets.

  Keep in mind this before use.
- For vCenter, the virtual network adapter to be analyzed must be connected to the distributed virtual switch.
- For OpenStack, SSH must be authenticated in a security group applied to Analysis VM.

6.5.7 Check Packet Analysis Status

Check the Operation Log.

Event ID	Message	Action
10030037	Packet Analysis setting was completed (Analysis VM: analysis virtual machine name)	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: error message)	For the following error message, check the corresponding table for the ISM version and the Analysis VM version in "2.11.2 Check of Analysis VM" in "User's Guide." "The file 'file name' is not correct" "The version 'analysis VM version' is not support"
50035217	An error has occurred while deploying of packet analysis. Analysis virtual machine (analysis virtual machine name) setting was failed. (Error: error message) Refer to "Table 6.10 Event ID50035217 Error Message List."	Specify the correct input parameter and execute again. Or check the status of the cloud management software.

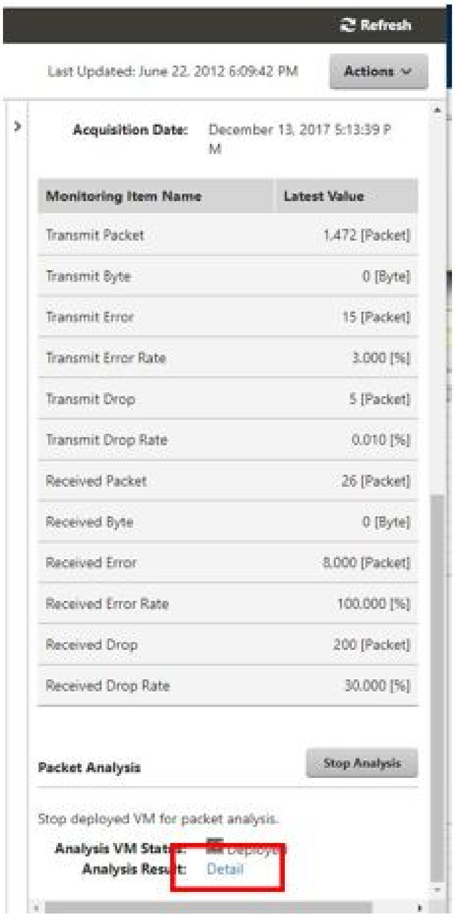
Table 6.10 Event ID50035217 Error Message List

Message	Action
"vCenter: xxxx"	Displays the message sent from vCenter. Check vCenter.
"OpenStack: xxxx"	Displays the message sent from OpenStack. Check OpenStack.
The file 'xxxx' is not correct.	Check the file name of the specified Analysis VM.
The version 'x.x.x' is not supported.	Check the version of Analysis VM.
The VM name 'xxxx' already exists.	Change the name of Analysis VM.
Unable to find the datastore 'xxxx'.	Check the datastore name.
Unable to find the VM folder 'xxxx'.	Check the VM folder name.
Unable to find the switch 'xxxx'.	Check the virtual switch name.
Unable to find the port group 'xxxx'.	Check the network label/port group name.
Unable to find security_group with name or id 'xxxx'.	Check the security group name or the security group ID.
The network 'xxxx' does not exist.	Check the network name.
Cannot complete login to vCenter due to an incorrect user name or password.	Check the user name and password for the vCenter in the cloud management software settings.
Cannot complete login to ESXi due to an incorrect user name or password.	Check the [OS] tab in the Details of Node screen, and check the user name and password of ESXi.
Cannot complete login due to an incorrect IP address.	Check the IP address of Analysis VM.
Unable to obtain IP address.	Check the IP version and IP address of the Analysis VM. Select enable or disable DHCP (ISM 2.4.0.b or later).
The request you have made requires authentication.	Check the authentication settings of OpenStack.
There may be insufficient memory	Check the resources of the server of the deployment location for Analysis VM.

6.5.8 Check Packet Analysis Result

Select "Detail" and check the information approximately ten minutes after packet analysis has started.

Figure 6.1 [Virtual Adapter Information] window



Last Updated: June 22, 2012 6:09:42 PM

Acquisition Date: December 13, 2017 5:13:39 PM

Monitoring Item Name	Latest Value
Transmit Packet	1,472 [Packet]
Transmit Byte	0 [Byte]
Transmit Error	15 [Packet]
Transmit Error Rate	3.000 [%]
Transmit Drop	5 [Packet]
Transmit Drop Rate	0.010 [%]
Received Packet	26 [Packet]
Received Byte	0 [Byte]
Received Error	8,000 [Packet]
Received Error Rate	100.000 [%]
Received Drop	200 [Packet]
Received Drop Rate	30.000 [%]

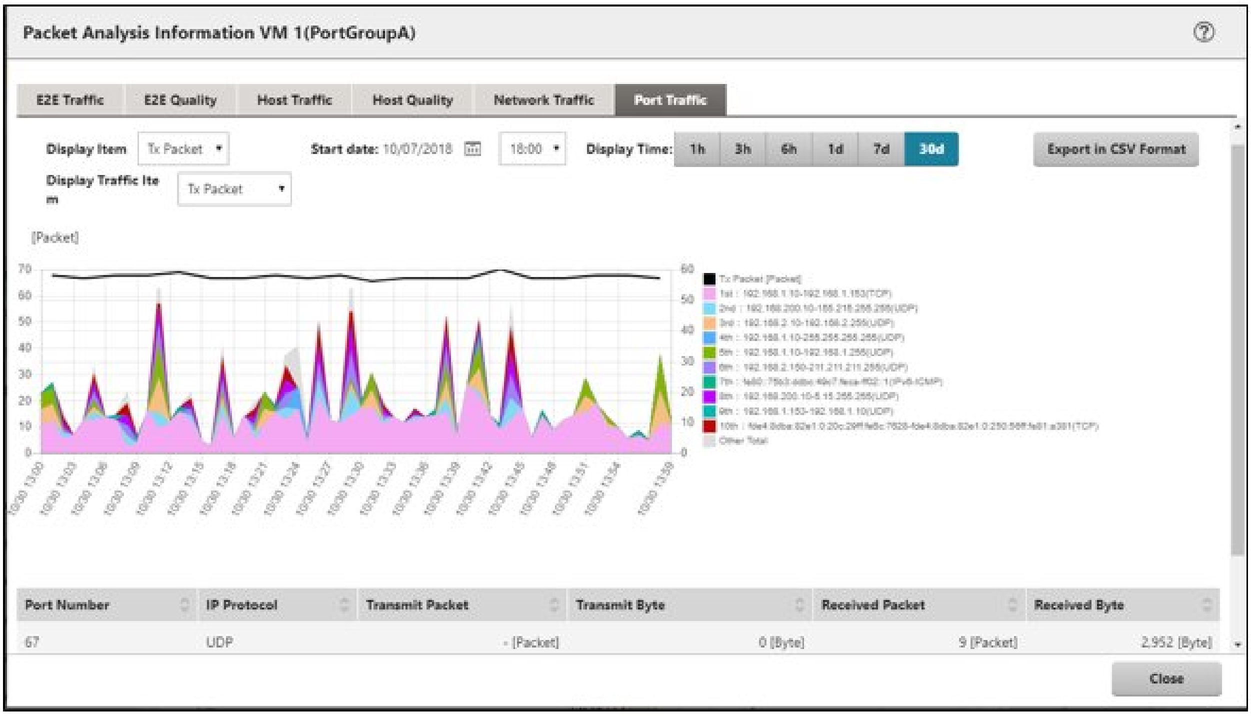
Packet Analysis

Stop deployed VM for packet analysis.

Analysis VM Status: Deployed

Analysis Result: Detail

Figure 6.2 Packet Analysis Result


E2E Traffic
E2E Quality
Host Traffic
Host Quality
Network Traffic
Port Traffic
1h
3h
6h
1d
7d
30d
Export in CSV Format
[Packet]
70
60
50
40
30
20
10
0
10/30 13:00
10/30 13:03
10/30 13:06
10/30 13:09
10/30 13:12
10/30 13:15
10/30 13:18
10/30 13:21
10/30 13:24
10/30 13:27
10/30 13:30
10/30 13:33
10/30 13:36
10/30 13:39
10/30 13:42
10/30 13:45
10/30 13:48
10/30 13:51
10/30 13:54
10/30 13:59
60
50
40
30
20
10
0
Tx Packet [Packet]
1st : 192.168.1.10-192.168.1.153(TCP)
2nd : 192.168.200.10-165.218.255.255(UDP)
3rd : 192.168.2.10-192.168.2.255(UDP)
4th : 192.168.1.10-255.255.255.255(UDP)
5th : 192.168.1.10-192.168.1.255(UDP)
6th : 192.168.2.150-211.211.211.255(UDP)
7th : fe80::75b3:ddbc:49e7:feca-ff02::1(IPv6-ICMP)
8th : 192.168.200.10-5.15.255.255(UDP)
9th : 192.168.1.153-192.168.1.10(UDP)
10th : fde4:8dba:82e1:0:20c:29ff:fe6c:7628-fde4:8dba:82e1:0:250:56ff:fe81:a391(TCP)
Other Total
Close

Packet Analysis Information VM 1(PortGroupA)

Display Item: Tx Packet

Display Traffic Item: Tx Packet

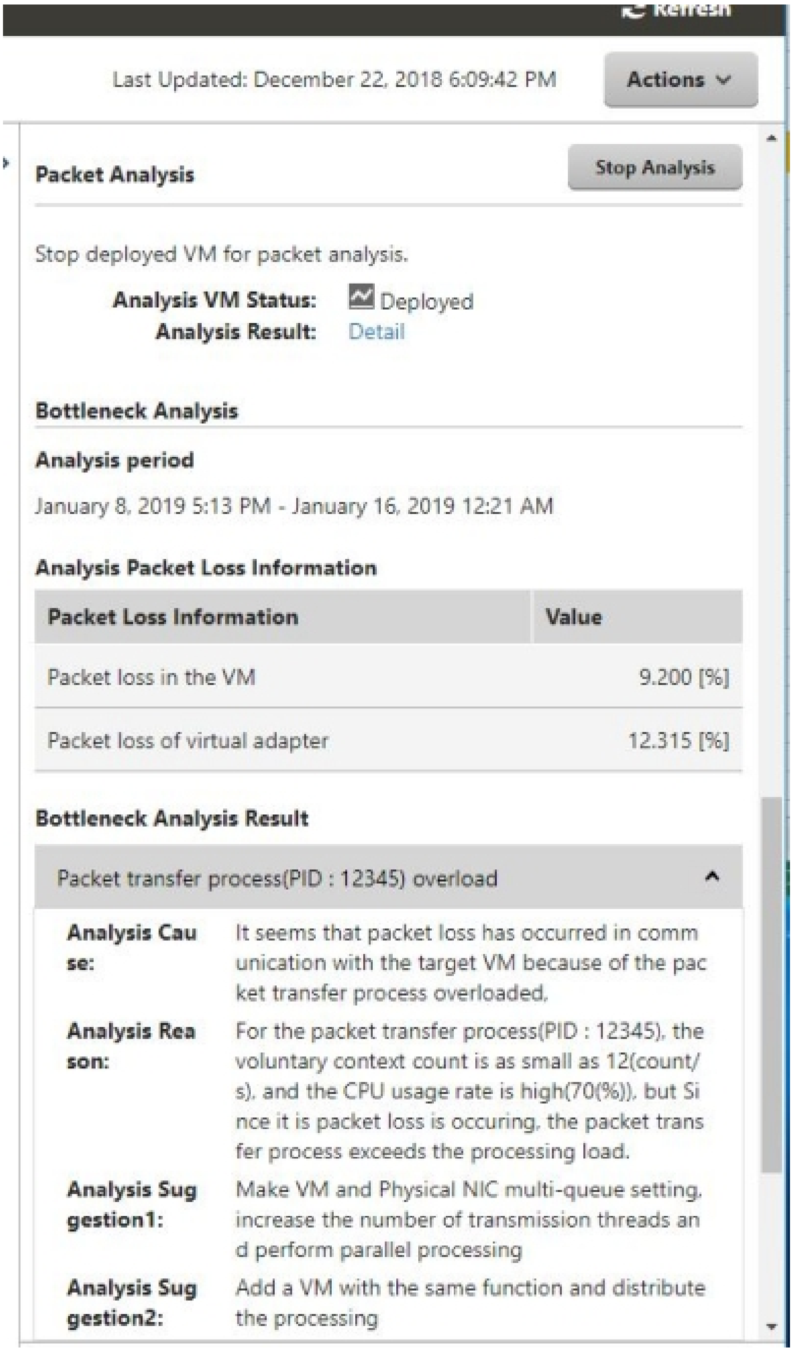
Start date: 10/07/2018 18:00

Display Time: 30d

Port Number	IP Protocol	Transmit Packet	Transmit Byte	Received Packet	Received Byte
67	UDP	- [Packet]	0 [Byte]	9 [Packet]	2,952 [Byte]

Continue to [Packet Analysis], [Analysis Packet Loss Information], [Bottleneck Analysis Result] (Analysis Cause, Analysis Reason, and Analysis Suggestion) is displayed. Consider the countermeasures, referring to the description (ISM 2.4.0.b or later).

Figure 6.3 Bottleneck analysis result (ISM 2.4.0.b or later)



Packet Analysis

Stop deployed VM for packet analysis.

Analysis VM Status: Deployed

Analysis Result: Detail

Bottleneck Analysis

Analysis period

January 8, 2019 5:13 PM - January 16, 2019 12:21 AM

Analysis Packet Loss Information

Packet Loss Information	Value
Packet loss in the VM	9.200 [%]
Packet loss of virtual adapter	12.315 [%]

Bottleneck Analysis Result

Packet transfer process(PID : 12345) overload

Analysis Cause:	It seems that packet loss has occurred in communication with the target VM because of the packet transfer process overloaded.
Analysis Reason:	For the packet transfer process(PID : 12345), the voluntary context count is as small as 12(count/s), and the CPU usage rate is high(70(%)), but Since it is packet loss is occuring, the packet transfer process exceeds the processing load.
Analysis Suggestion1:	Make VM and Physical NIC multi-queue setting, increase the number of transmission threads and perform parallel processing
Analysis Suggestion2:	Add a VM with the same function and distribute the processing

6.5.9 Stop Packet Analysis

Select the [Stop Analysis] button.

Analysis VM is deleted from the hypervisor.

6.6 Execute Firmware Rolling Update

This section describes the applicable procedure for Firmware Rolling Update 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 into operation.

This function can be used only with the license for ISM for PRIMEFLEX.

Firmware Rolling Update is executed according to the following work flow.

Table 6.11 Firmware Rolling Update work flow

Firmware Rolling Update procedure		Tasks
1	Preparations	- Obtaining of the firmware data to be applied - Import of the firmware to be applied into ISM - Selection of nodes on which to execute firmware updates - Selection of temporary nodes for virtual machines
2	Execute Firmware Rolling Update	
3	Follow-up processing	- Confirmation of firmware updates

6.6.1 Preparations

This section describes the preparations required before executing Firmware Rolling Update.

Obtain firmware data to be applied

Obtain firmware data to be applied.

For the procedure to obtain firmware data, refer to "6.3 Update the Firmware of the Server," and "2.13.2 Repository Management" in "User's Guide."

Also, for supported versions, refer to "2.12.4 Firmware Rolling Update" in "User's Guide."

Import firmware data to be applied into ISM-VA

Import firmware data to apply to ISM.

For the procedure to import firmware data, refer to "6.3 Update the Firmware of the Server," and "2.13.2 Repository Management" in "User's Guide."

Also, for supported versions, refer to "2.12.4 Firmware Rolling Update" in "User's Guide."

Add ISM-VA virtual disks as required. For information on the procedure to add virtual disks, refer to "3.7 Allocation of Virtual Disks" in "User's Guide."

Select target nodes for firmware updates

Select target nodes for firmware updates.

For node selection, refer to "6.6.2.1 Operation requirements for Firmware Rolling Update" to select nodes which satisfy the operation requirements.

Select temporary nodes for virtual machines

Select temporary nodes for virtual machines.

For selection of temporary nodes, refer to "6.6.2.1 Operation requirements for Firmware Rolling Update" to select temporary nodes which satisfy 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: Log in with VMware Web Client, check it from [Home] - [Hosts and Clusters] - [<Cluster Name>] - [Settings] - [Service] - [vSphere DRS].

6.6.2 Execute Firmware Rolling Update

By executing Firmware Rolling Update, you can apply rolling update to the firmware on the virtualized platform.

6.6.2.1 Operation requirements for Firmware Rolling Update

Common operation requirements for all configurations

- Use the latest firmware data that is already registered in ISM to apply firmware data. Upload/import the firmware data in ISM in advance.

- The applicable firmware data are as follow.

  Note: Y = Supported, N = Not supported

Type	Update procedure	
	Online update	Offline update [Note 1]
Server (iRMC)	Y	Y
Server (BIOS)	Y	Y
Server (LAN/CNA card) [Note 2] (ISM 2.4.0.b or later)	N	Y

[Note 1]: For Offline update, use the PXE boot function on the target node. Refer to "Offline Update" in "2.6.2.1 How to update firmware" in "User's Guide" to enable PXE booting from the management LAN.

[Note 2]: This is for LAN/CNA cards that are supported on PRIMEFLEX HS/PRIMEFLEX for VMware vSAN as well as PRIMEFLEX for Microsoft Storage Spaces Direct.

Note

Among the firmware data imported in advance, the latest firmware will be applied.

In ISM 2.4.0.b or later, if the firmware data of Online Update and Offline Update have been imported, the firmware of Online Update will be applied. If the firmware data for both Online Update and Offline Update is included on the UpdateDVD, Online Update will be given priority over Offline Update.

- Use the Virtual Resource Management. For the settings for using Virtual Resource Management, refer to "3.8 Pre-Settings for Virtual Resource Management" in "User's Guide."

- Update target nodes must be powered on. You can check if the nodes are powered on with the following procedure.

  1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Cluster] to display the "Cluster List" screen.
  2. From [<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."

- The statuses of the clusters and of the nodes are checked at the beginning of the processing. If an error has occurred, Firmware Rolling Update is not executed, since data integrity cannot be guaranteed.

- Firmware 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 will be migrated back from the temporary node to the node that was updated. When migrating virtual machines on other nodes, make sure to specify temporary nodes which have enough resources (CPU performance, memory capacity, and so on) to operate the virtual machines as temporary nodes.
  Set temporary nodes from the "FW Rolling Update" wizard - the "Temporary Node" screen - [Temporary Node].

- At least one ADVM must be running for configurations with link with Active Directory.

Note

- If the virtual machines that cannot be migrated to other nodes due to reasons related to system configurations or cluster settings are running, Firmware Rolling Update fails.

  Migration of virtual machines can be avoided with one of the following procedures.

  - Stop the target virtual machines manually before executing Firmware Rolling Update
  - From the "FW Rolling Update" wizard, set the nodes, on which the target virtual machines are running, not to be rebooted

- Firmware Rolling Update migrates the virtual machines to other nodes when rebooting the nodes if they are running, even if virtual machines that must actually not be migrated to other nodes due to license-related reasons exist. Be sure not to migrate virtual machines to other nodes and cause a licensing violation.

  Migration of virtual machines can be avoided with one of the following procedures.

  - Stop the target virtual machines manually before executing Firmware Rolling Update
  - From the "FW Rolling Update" wizard, set the nodes, on which the target virtual machines are running, not to be rebooted

Operation requirements for PRIMEFLEX HS/PRIMEFLEX for VMware vSAN configuration only

- Before executing Firmware Rolling Update, check the statuses of clusters and nodes for any errors.
  - Clusters

    Access the vCSA of the PRIMEFLEX from the vSphere Web Client and check that there are no warnings or error icons in the cluster names in the [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 Firmware Rolling Update for the configuration of three or less nodes.
- The vCSA of PRIMEFLEX must be registered in the Cloud Management Software of ISM.
- When the VMware Distributed Resource Scheduler (hereafter referred to as "DRS") is on, if you log in to the VMware Web Client, then from [Home] - [Hosts and Clusters] and move to [<Cluster name>] - [Settings] - [vSphere DRS] where under [Edit], you can set the automation level of VMware DRS, however, if you set the automation level to other than "Automatic" it might 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.
- Even if you set one node in Maintenance Mode, you must be able to secure 30% or more of vSAN data store.
- Set the ESXi host in Maintenance Mode because the update target nodes are rebooted during Firmware Rolling Update. In this case, the following Health errors may occur.
  - For vSAN 6.2 environment (VMware ESXi 6.0)
    - Virtual SAN Health alarm, "Virtual SAN Disk Balance"
    - General health summary, Virtual SAN Health service alarm
    - Virtual SAN Health alarm, "Cluster Health"
  - For vSAN 6.5 environment (VMware ESXi 6.5) or later
    - Virtual SAN Health alarm, "Virtual SAN Disk Balance"
    - Virtual SAN Health service alarm, "General health summary"
    - Virtual SAN Health alarm, "Cluster Health"

  Set these health errors to disabled in the alarm definition.

  You can set the alarm definition with the following procedure.

  - For vSAN 6.2 environment (VMware ESXi 6.0)

    From the "Top" screen, select [Inventories] - [Hosts and Clusters] - [<vCSA Name>] - [Manage] - [Alarm Definitions]
  - For vSAN 6.5 environment (VMware ESXi 6.5) or later

    From the "Top" screen, select [Inventories] - [Hosts and Clusters] - [<vCSA Name>] - [Monitor] - [Issues] - [Alarm Definitions]

    After executing Firmware Rolling Update, reverse the alarm definition if required.

Point

- If you do not set these Health errors to disabled with the alarm definition and a Health error occurs, Firmware Rolling Update ends in an error before completion.

- If you set these Health errors to disabled with the alarm definition, confirm that even if you set one node in Maintenance Mode, you can secure 30% or more of the vSAN data store.

- If you reverse the alarm definition after executing Firmware Rolling Update, these Health errors may occur. Take countermeasures, referring to the following KB.

  https://kb.vmware.com/s/article/2144278

Note

In PRIMEFLEX HS/PRIMEFLEX for VMware vSAN configuration, 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.

Operation requirements only for Microsoft Storage Spaces Direct configuration

- Before executing Firmware 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 Firmware Rolling Update for the configuration of two or less of nodes.

- Register the cluster name of the target Microsoft Failover Cluster in Cloud Management Software of ISM. System Center can be registered, but it is not used with Firmware Rolling Update.
- Virtual machine migration is supported only for high availability virtual 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

- For the PRIMEFLEX for Microsoft Storage Spaces Direct configuration, 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.
- For the PRIMEFLEX for Microsoft Storage Spaces Direct configuration, if a CPU Internal Error (CPU IERR) or other error occurs during the execution of the Firmware Rolling Update, all virtual machines might fail over.

6.6.2.2 Firmware Rolling Update procedure

This section describes the procedure for executing Firmware Rolling Update of ISM for PRIMEFLEX.

Point

Before executing Firmware 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 GUI of ISM 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 GUI of ISM, 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.
  4. 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 GUI of ISM, select [Management] - [Cluster].

     The "Cluster List" screen is displayed.

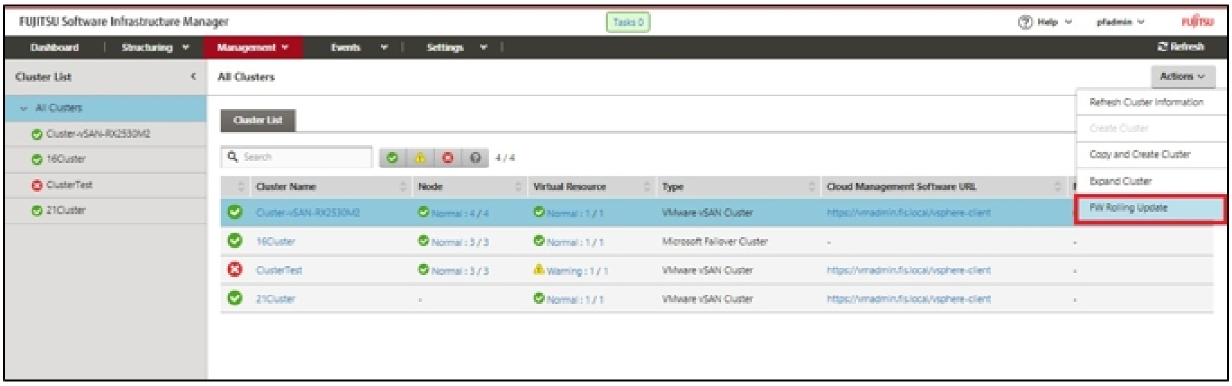
  2. From the [Actions] button, select [Refresh Cluster Information].
  3. Check that the update of the cluster information has become "Complete."

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 GUI of ISM, select [Management] - [Cluster].

   The "Cluster List" screen is displayed.

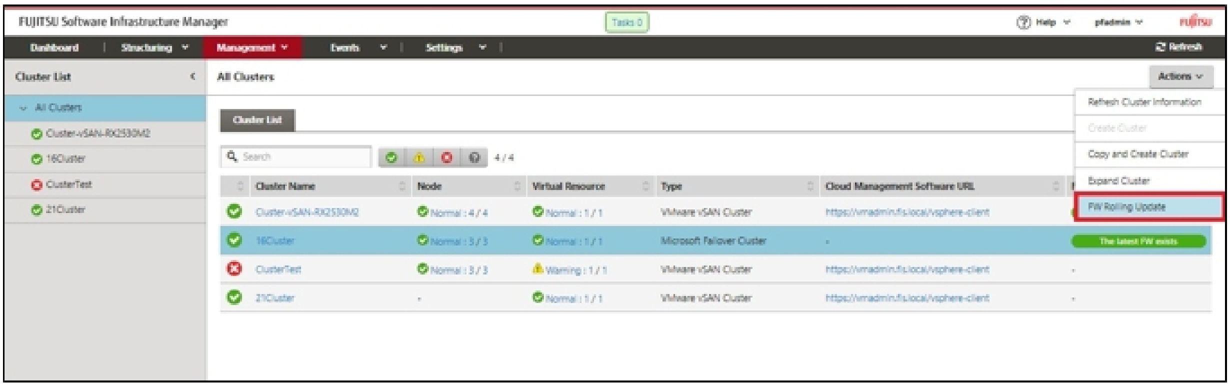
3. Select [<Target Cluster>], from the [Actions] button, select [FW Rolling Update].

   For PRIMEFLEX HS/PRIMEFLEX for VMware vSAN



Cluster Name	Node	Virtual Resource	Type	Cloud Management Software URL	
Cluster-vSAN-RX2530M2	Normal : 4 / 4	Normal : 1 / 1	VMware vSAN Cluster	https://vmadmin.fis.local/vsphere-client	
16Cluster	Normal : 3 / 3	Normal : 1 / 1	Microsoft Failover Cluster	-	-
ClusterTest	Normal : 3 / 3	Warning : 1 / 1	VMware vSAN Cluster	https://vmadmin.fis.local/vsphere-client	-
21Cluster	-	Normal : 1 / 1	VMware vSAN Cluster	https://vmadmin.fis.local/vsphere-client	-

   For PRIMEFLEX for Microsoft Storage Spaces Direct



Cluster Name	Node	Virtual Resource	Type	Cloud Management Software URL	
Cluster-vSAN-RX2530M2	Normal : 4 / 4	Normal : 1 / 1	VMware vSAN Cluster	https://vmadmin.fis.local/vsphere-client	
16Cluster	Normal : 3 / 3	Normal : 1 / 1	Microsoft Failover Cluster	-	The latest FW exists
ClusterTest	Normal : 3 / 3	Warning : 1 / 1	VMware vSAN Cluster	https://vmadmin.fis.local/vsphere-client	-
21Cluster	-	Normal : 1 / 1	VMware vSAN Cluster	https://vmadmin.fis.local/vsphere-client	-

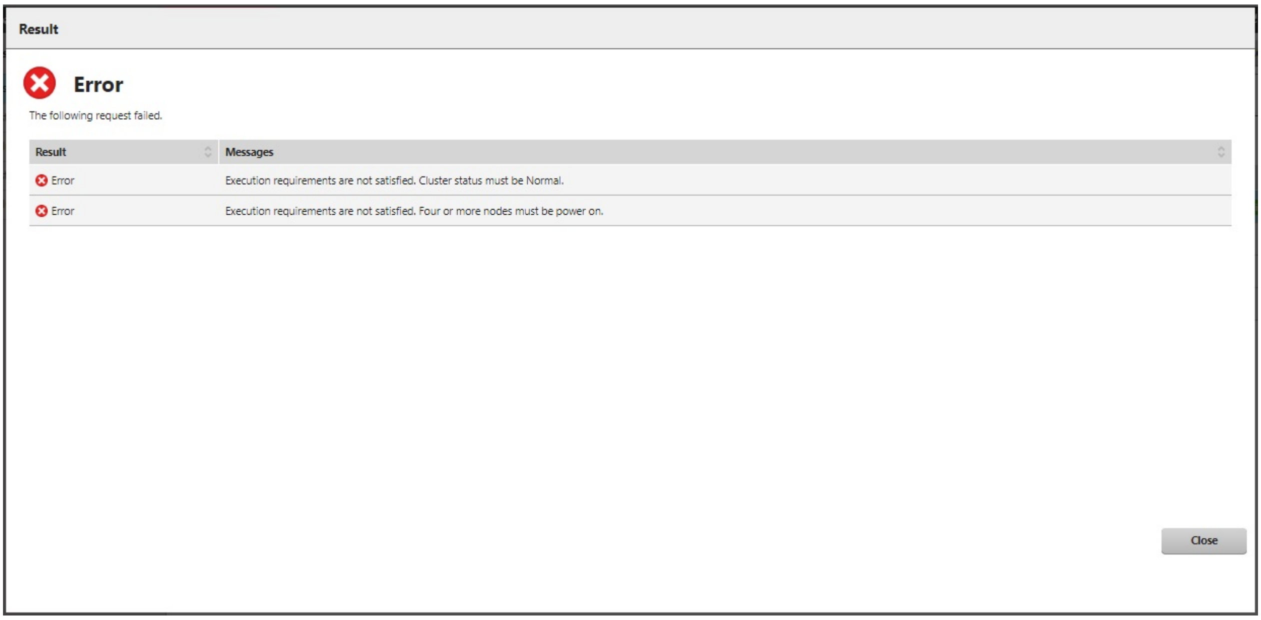
   The "FW Rolling Update" wizard is displayed.

   Select an operation option using the following procedure.

Point

Only for the clusters whose FW Update Status of the "Cluster List" screen is [The latest FW exists], Firmware Rolling Update can be executed.

If the execution conditions are not satisfied, the following "Result" screen is displayed. Read the message and take countermeasures to satisfy the execution conditions, and then execute again. For details on the execution conditions, refer to "6.6.2.1 Operation requirements for Firmware Rolling Update."



Result

Error

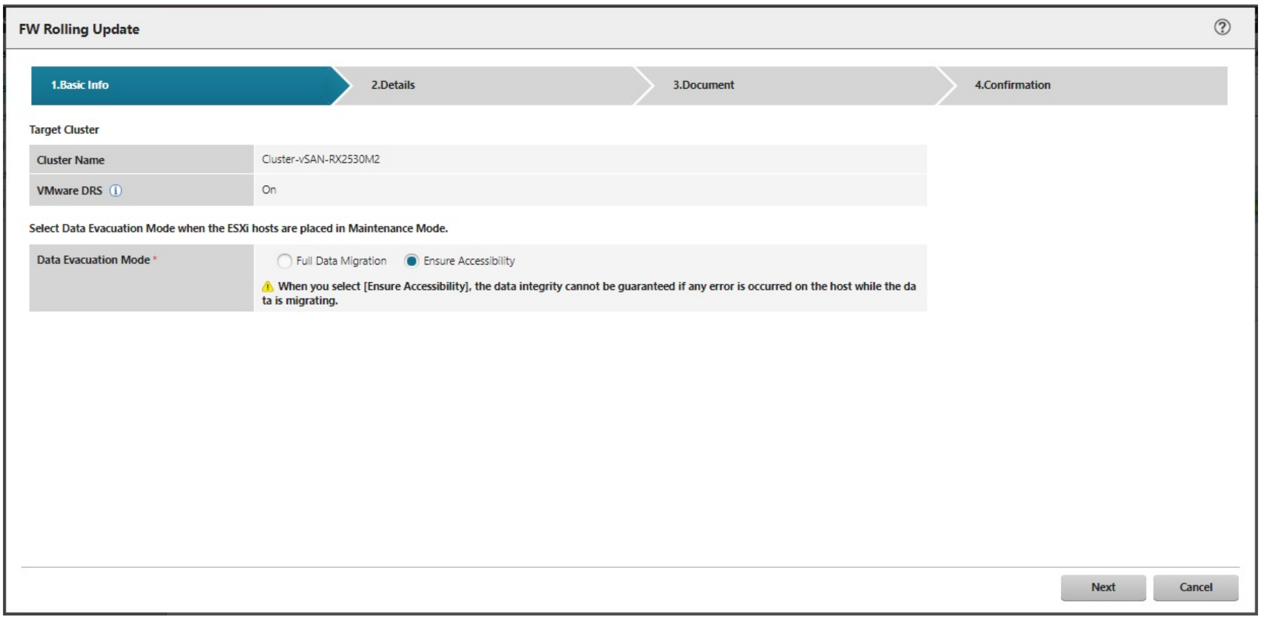
The following request failed.

Result	Messages
✖ Error	Execution requirements are not satisfied. Cluster status must be Normal.
✖ Error	Execution requirements are not satisfied. Four or more nodes must be power on.

4. Set the basic information from the "Basic Info" screen for Firmware Rolling Update execution.

   If executing again, select the [Next] button to proceed to Step 5 if no settings are required.

   For PRIMEFLEX HS/PRIMEFLEX for VMware vSAN



FW Rolling Update

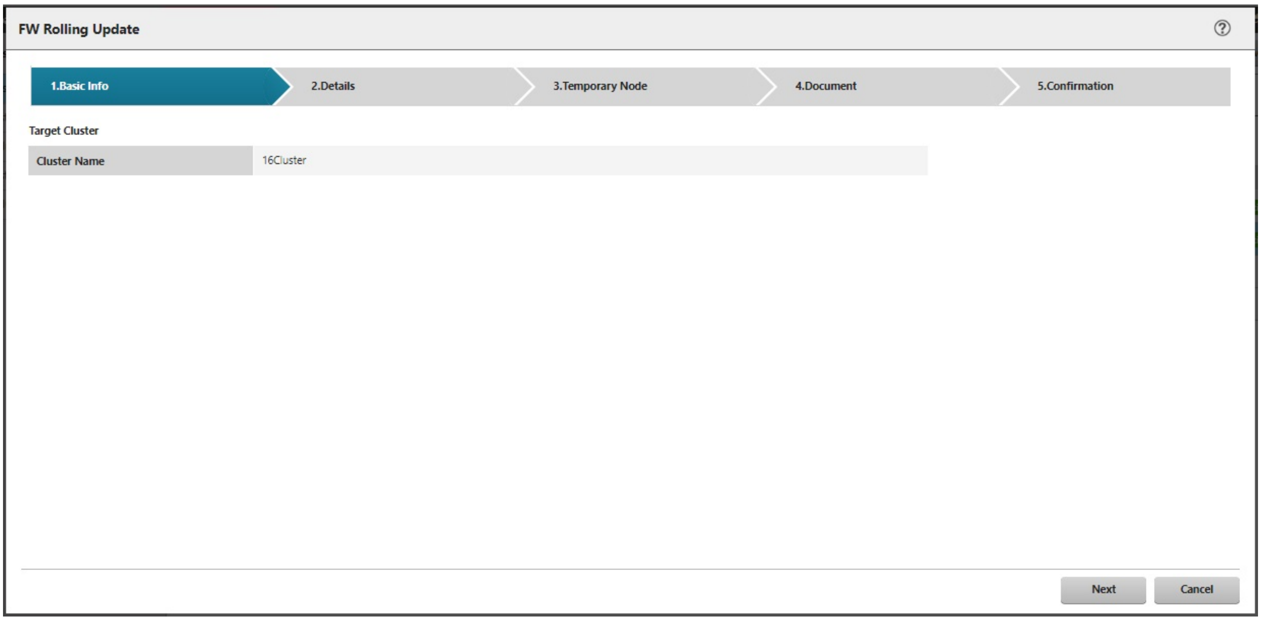
Target Cluster

Cluster Name	Cluster-vSAN-RX2530M2
VMware DRS ⓘ	On

Select Data Evacuation Mode when the ESXi hosts are placed in Maintenance Mode.

Data Evacuation Mode *	○ Full Data Migration ● Ensure Accessibility ⚠ When you select [Ensure Accessibility], the data integrity cannot be guaranteed if any error is occurred on the host while the da ta is migrating.

For PRIMEFLEX for Microsoft Storage Spaces Direct



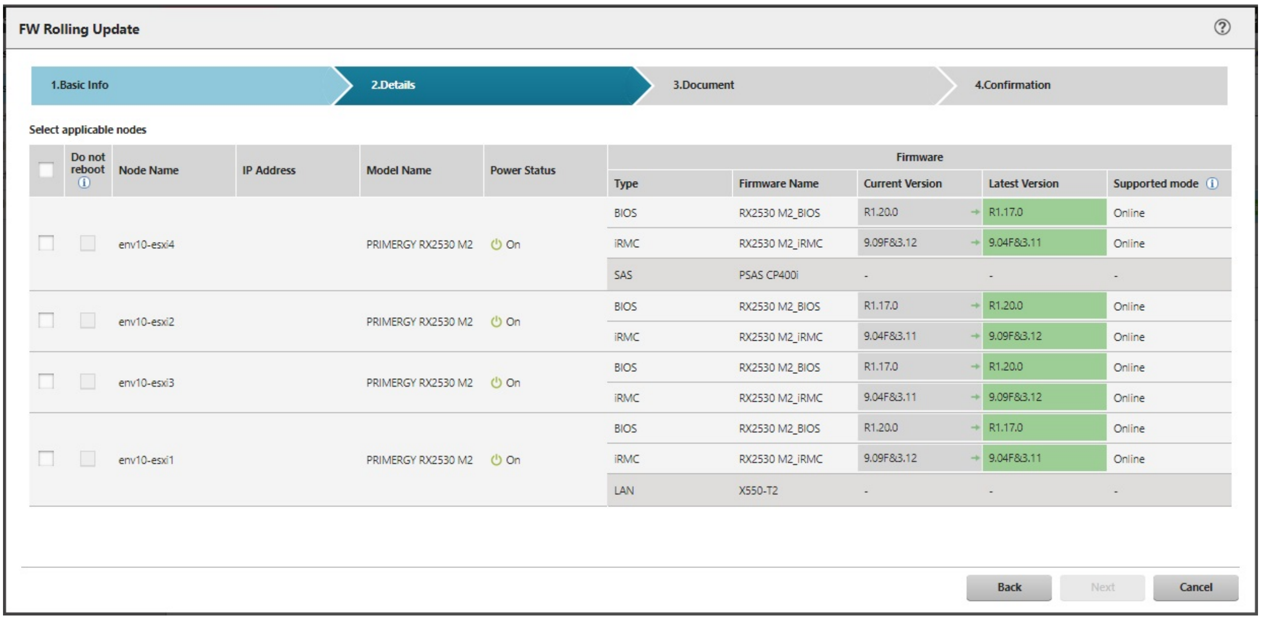
FW Rolling Update

Target Cluster

Cluster Name	16Cluster

5. From the "Details" screen, select the applicable nodes and check the checkbox of [Do not reboot] if required.

   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.



FW Rolling Update

Select applicable nodes

□	Do not reboot ⓘ	Node Name	IP Address	Model Name	Power Status	Firmware				
						Type	Firmware Name	Current Version	Latest Version	Supported mode ⓘ
□	□	env10-esxi4		PRIMERGY RX2530 M2	⏻ On	BIOS	RX2530 M2_BIOS	R1.20.0 →	R1.17.0	Online
						iRMC	RX2530 M2_iRMC	9.09F&3.12 →	9.04F&3.11	Online
						SAS	PSAS CP400i	-	-	-
□	□	env10-esxi2		PRIMERGY RX2530 M2	⏻ On	BIOS	RX2530 M2_BIOS	R1.17.0 →	R1.20.0	Online
						iRMC	RX2530 M2_iRMC	9.04F&3.11 →	9.09F&3.12	Online
□	□	env10-esxi3		PRIMERGY RX2530 M2	⏻ On	BIOS	RX2530 M2_BIOS	R1.17.0 →	R1.20.0	Online
						iRMC	RX2530 M2_iRMC	9.04F&3.11 →	9.09F&3.12	Online
□	□	env10-esxi1		PRIMERGY RX2530 M2	⏻ On	BIOS	RX2530 M2_BIOS	R1.20.0 →	R1.17.0	Online
						iRMC	RX2530 M2_iRMC	9.09F&3.12 →	9.04F&3.11	Online
						LAN	X550-T2	-	-	-

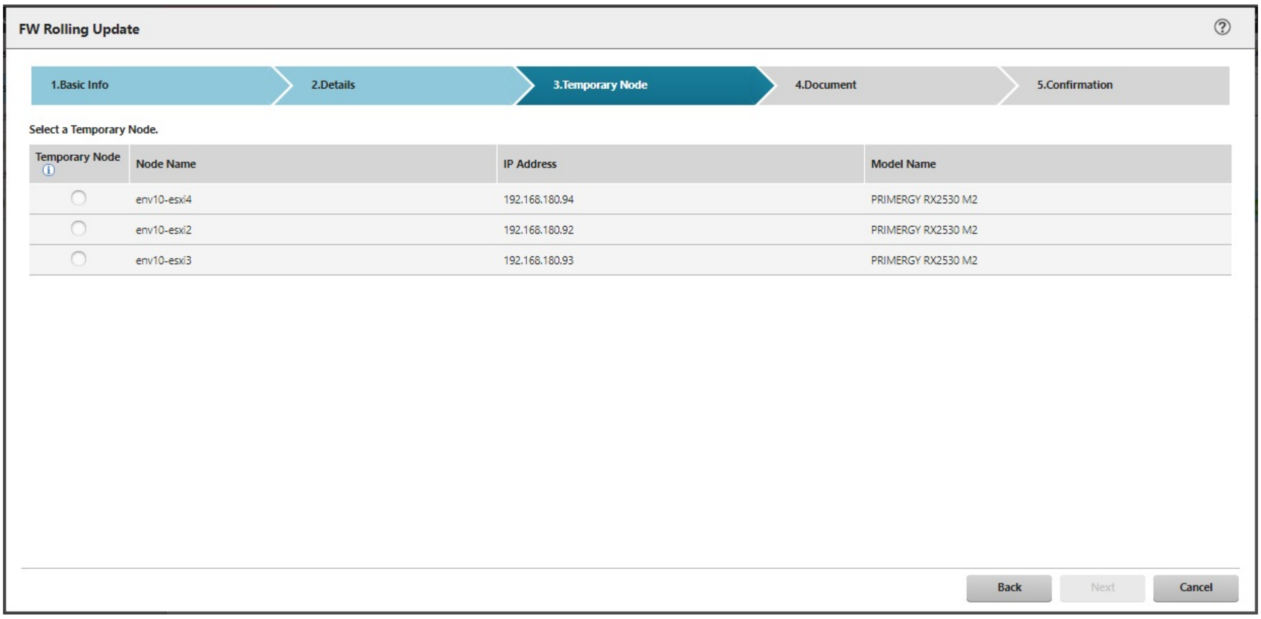
Note

- Firmware updates of iRMC does not require restarting of the nodes. You can set not to reboot nodes by checking the checkbox of [Do not reboot] for the applicable nodes for the firmware update, which are selected on the "Details" screen.

- For firmware updates for BIOS, do not check the check box of [Do not reboot] for the applicable nodes for firmware update, which are selected on the "Details" screen. If there are some nodes that must not be rebooted, check the check box of [Do not reboot], and then reboot manually after executing Firmware Rolling Update.

6. Select the temporary node on the "Temporary Node" screen.

   If executing again, select the [Next] button to proceed to Step 7 if re-selection of the temporary node is not required.



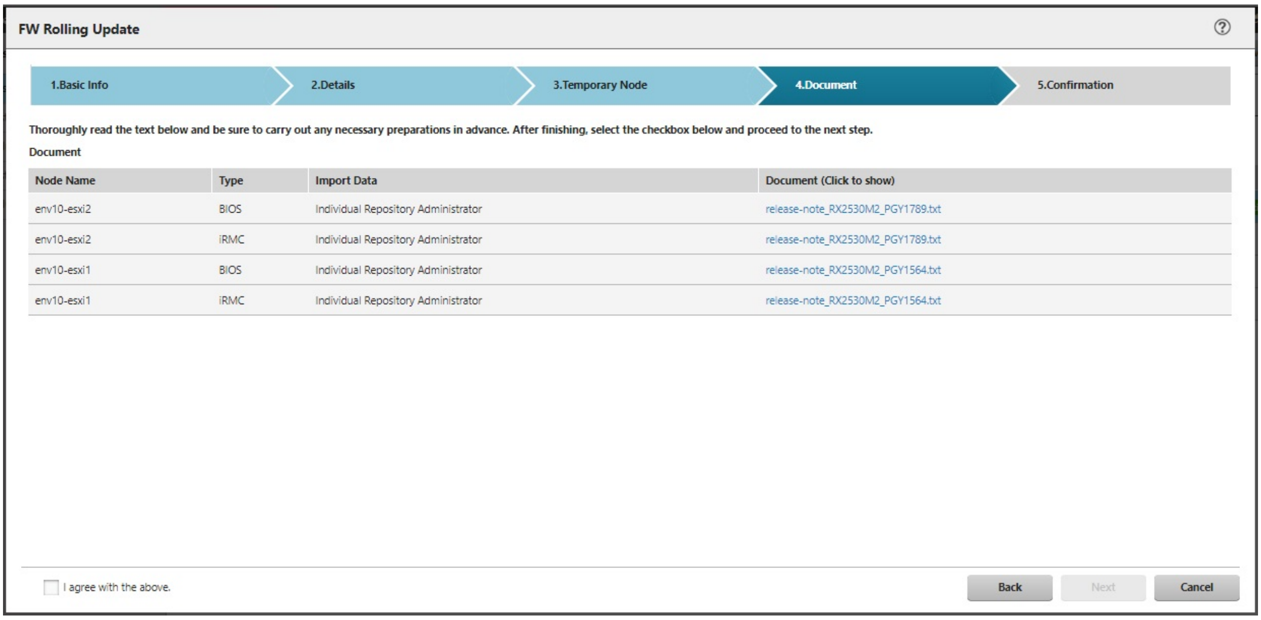
Select a Temporary Node.

Temporary Node	Node Name	IP Address	Model Name
○	env10-esxi4	192.168.180.94	PRIMERGY RX2530 M2
○	env10-esxi2	192.168.180.92	PRIMERGY RX2530 M2
○	env10-esxi3	192.168.180.93	PRIMERGY RX2530 M2

Point

The "Temporary Node" screen is not displayed when the target cluster is PRIMEFLEX HS/PRIMEFLEX for VMware vSAN and DRS is ON. Proceed to Step 7. You can check the DRS status, ON or OFF, from the "Basic Info" screen in Step 4.

7. On the "Document" screen, check the document of the firmware to apply.



Thoroughly read the text below and be sure to carry out any necessary preparations in advance. After finishing, select the checkbox below and proceed to the next step.

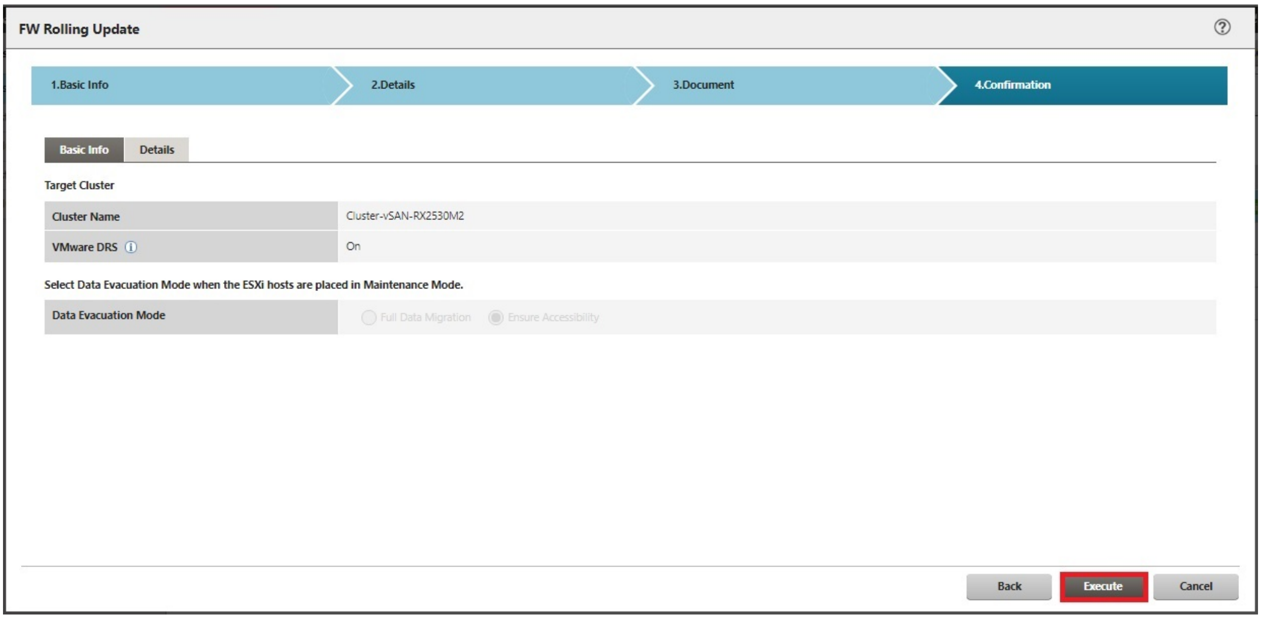
Document

Node Name	Type	Import Data	Document (Click to show)
env10-esxi2	BIOS	Individual Repository Administrator	release-note_RX2530M2_PGY1789.txt
env10-esxi2	iRMC	Individual Repository Administrator	release-note_RX2530M2_PGY1789.txt
env10-esxi1	BIOS	Individual Repository Administrator	release-note_RX2530M2_PGY1564.txt
env10-esxi1	iRMC	Individual Repository Administrator	release-note_RX2530M2_PGY1564.txt

□ I agree with the above.

8. Check the parameters on the "Confirmation" screen, then select the [Execute] button.

For PRIMEFLEX HS/PRIMEFLEX for VMware vSAN



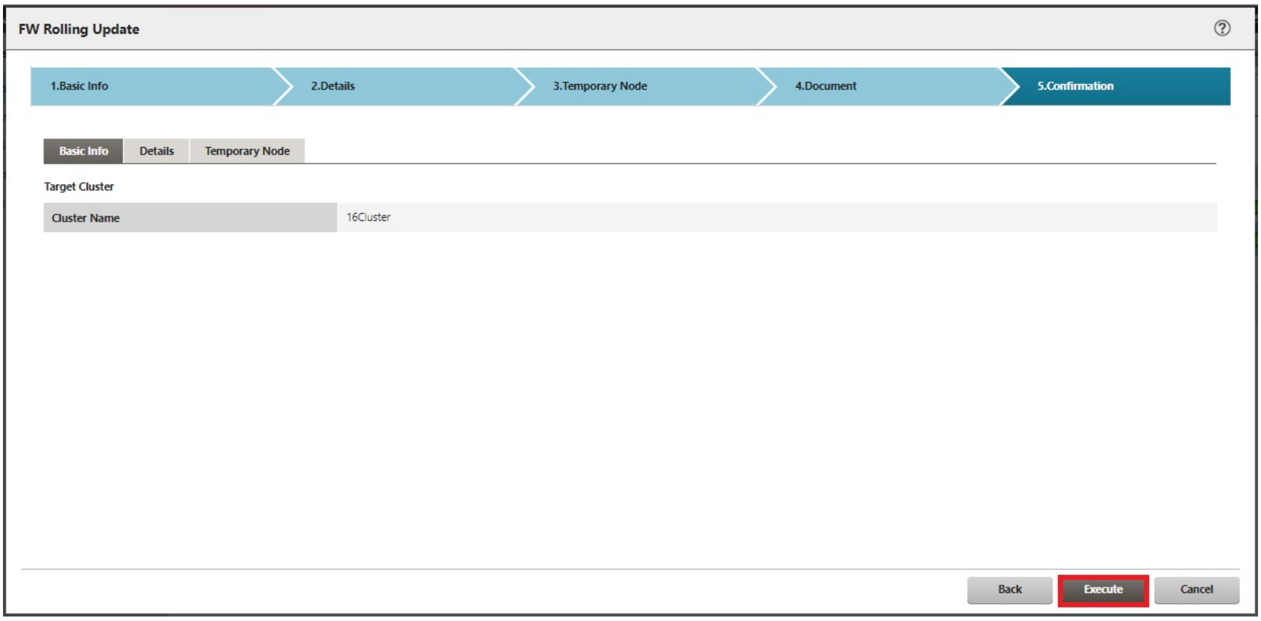
Target Cluster

Cluster Name	Cluster-vSAN-RX2530M2
VMware DRS	On

Select Data Evacuation Mode when the ESXi hosts are placed in Maintenance Mode.

Data Evacuation Mode	○ Full Data Migration ● Ensure Accessibility

For PRIMEFLEX for Microsoft Storage Spaces Direct

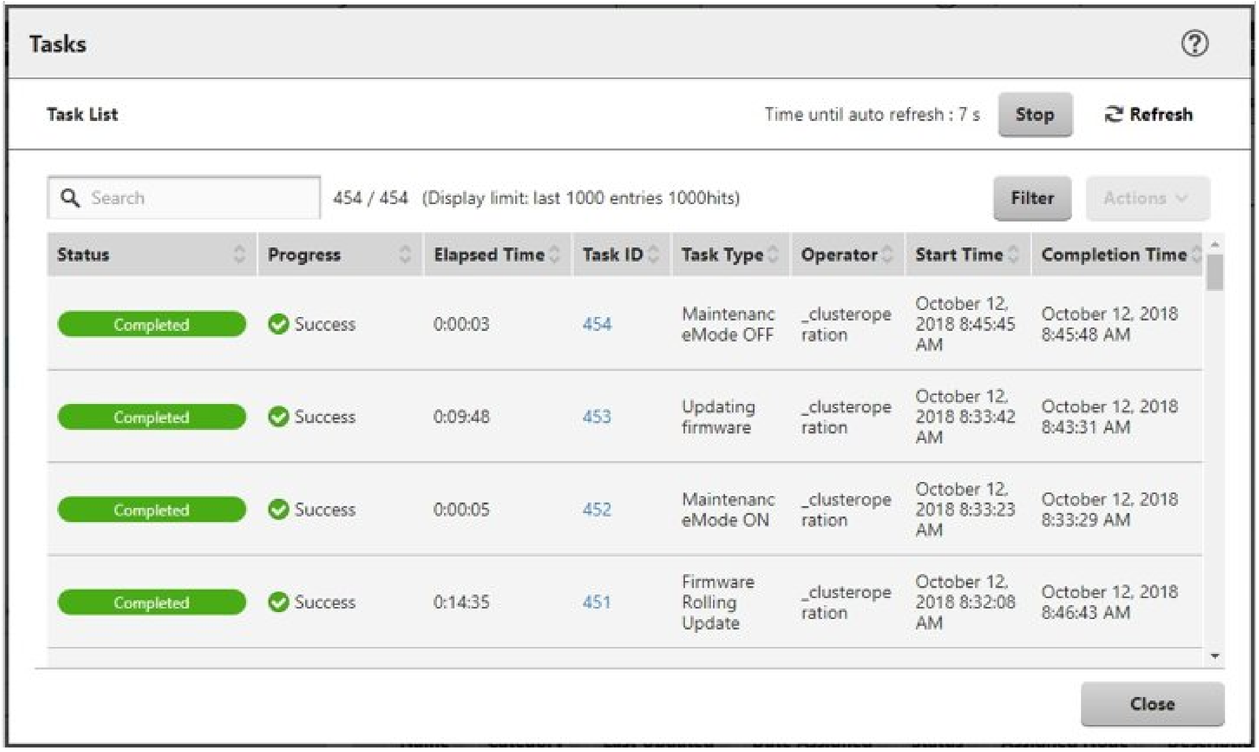


Target Cluster

Cluster Name	16Cluster

The execution of Firmware Rolling Update is registered as an ISM task.

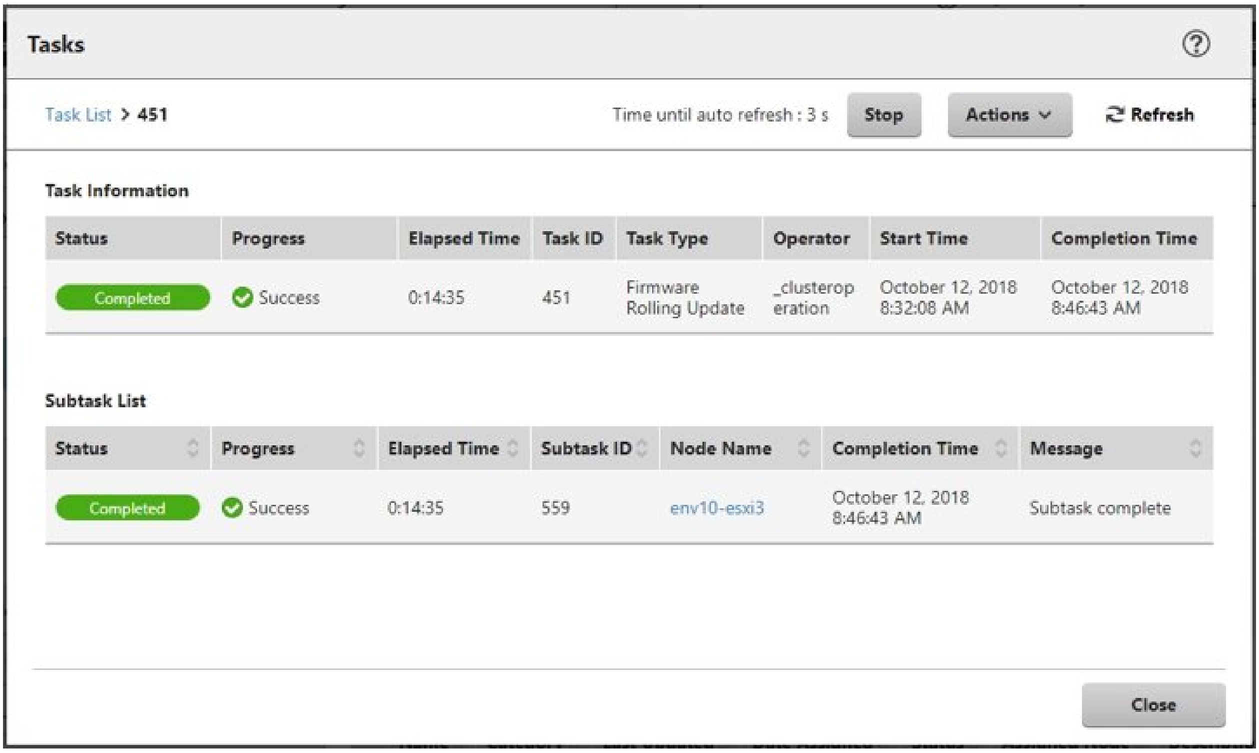
At the top of the Global Navigation Menu, select [Tasks], then the tasks in the task list displayed in the "Tasks" screen whose task type has become "Firmware Rolling Update" are the Firmware Rolling Update tasks.


Tasks
Task List
Time until auto refresh : 7 s
Stop
Refresh
Search
454 / 454 (Display limit: last 1000 entries 1000hits)
Filter
Actions
Close

Status	Progress	Elapsed Time	Task ID	Task Type	Operator	Start Time	Completion Time
Completed	✓ Success	0:00:03	454	MaintenanceMode OFF	_clusteroperation	October 12, 2018 8:45:45 AM	October 12, 2018 8:45:48 AM
Completed	✓ Success	0:09:48	453	Updating firmware	_clusteroperation	October 12, 2018 8:33:42 AM	October 12, 2018 8:43:31 AM
Completed	✓ Success	0:00:05	452	MaintenanceMode ON	_clusteroperation	October 12, 2018 8:33:23 AM	October 12, 2018 8:33:29 AM
Completed	✓ Success	0:14:35	451	Firmware Rolling Update	_clusteroperation	October 12, 2018 8:32:08 AM	October 12, 2018 8:46:43 AM

Point

From the task list on the "Tasks" screen, select [Task ID] from "Firmware Rolling Update," and then the "Tasks" screen of the "Firmware Rolling Update" is displayed. In this screen, a subtask list is displayed for each target node for Firmware Rolling Update. You can check the progress status of each task by checking the message column.



Task Information

Status	Progress	Elapsed Time	Task ID	Task Type	Operator	Start Time	Completion Time
Completed	✓ Success	0:14:35	451	Firmware Rolling Update	_clusteroperation	October 12, 2018 8:32:08 AM	October 12, 2018 8:46:43 AM

Subtask List

Status	Progress	Elapsed Time	Subtask ID	Node Name	Completion Time	Message
Completed	✓ Success	0:14:35	559	env10-esxi3	October 12, 2018 8:46:43 AM	Subtask complete

9. Check that the status of "Firmware Rolling Update" has become "Completed."

Note

- If an error is displayed on the ISM "Tasks" screen, refer to "ISM for PRIMEFLEX Messages" and take the countermeasures. After solving the error, and execute Firmware Rolling Update again.

- During execution of Cluster Creation or Cluster Expansion, do not execute Firmware Rolling Update.

- If the BIOS Firmware 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 GUI of ISM, 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] tab, select the [Actions] button - [Get Node Information].
       The firmware information is refreshed.

    5. Check the Current Version of the node to be updated and check that the firmware has not been applied.

- If you set the target nodes for firmware updates to reboot in the "FW 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. Firmware 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, access vSphere Web Client, execute the test again with the following procedure, and check that the status has returned to normal. From the "Top" screen, select [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Monitor] - [vSAN] - [Health]. 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 rolling update firmware. An error occurred during verification of the
  Firmware Rolling Update task. (Cluster status is abnormal; cluster name = Cluster; 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 GUI of ISM, 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] tab, select the [Actions] button - [Get Node Information].
       The firmware information is refreshed.

    5. Check the 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.

- In the PRIMEFLEX for Microsoft Storage Spaces Direct, if a warning is displayed in the cluster event of [<Cluster name>] of the failover cluster manager after completing Firmware 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.

6.6.3 Follow-up Processing

This section describes the follow-up processing required after executing Firmware Rolling Update of ISM for PRIMEFLEX.

6.6.3.1 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 GUI of ISM, select [Structuring] - [Firmware].
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 [Do not reboot] is checked have been applied, proceed to Step 4.

   b. For nodes that firmware has not been applied except for the nodes for which [Do not reboot] is checked, refer to "Appendix E Troubleshooting" in "User's Guide" and solve the error.

      After that, execute one of the following operations.

      - From the "FW Rolling Update" wizard, change the settings, and then restart Firmware Rolling Update.
      - From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Firmware].
        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].

4. From the Global Navigation Menu on the GUI of ISM, 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 Firmware Rolling Update, these Health errors may occur. Take countermeasures, referring to the following KB.

   - Virtual SAN Disk Balance

     https://kb.vmware.com/s/article/2144278

5. For firmware (BIOS) Online update, you must reboot the nodes. When you check the checkbox of [Do not reboot] for the applicable nodes for firmware update which are selected in the "FW Rolling Update" wizard - "Details" screen, reboot the nodes at your convenient timing.

   When reboot of the nodes has been completed successfully, execute Step 4 and check the "Cluster List" screen.

6. Log in to the iRMC and confirm that any errors are not output in the System Event Log.

6.7 Create a Cluster for PRIMEFLEX HS/PRIMEFLEX for VMware vSAN

This section describes the cluster creating procedure for PRIMEFLEX HS/PRIMEFLEX for VMware vSAN.

This function can be used only with the license for ISM for PRIMEFLEX.

Cluster Creation is executed according to the following work flow.

Table 6.12 Cluster Creation work flow

Cluster Creation procedure		Tasks
1	Preparations	- Creating ADVM certificates - Registering host records in DNS - DHCP settings - Importing the ISO image of the OS installation media to ISM-VA - Upload of the VMware ESXi patch file. - Upload of VMware SMIS Provider - Creating profiles - Installing and Wiring - Setting the IP address of iRMC - BIOS settings - Registering nodes in ISM
2	Execute Cluster Creation	
3	Follow-up processing	- Confirming the created cluster - Restrictions/Precautions for VMware vSphere - Registering in ServerView RAID Manager - Deleting unnecessary files

Note

PRIMERGY M5 series is available in ISM 2.4.0.c or later.

6.7.1 Preparations

This section describes the preparations required before the cluster creation.

6.7.1.1 Create ADVM certificates

This setting is required only when configuring an ADVM dedicated to PRIMEFLEX HS/PRIMEFLEX for VMware vSAN, and the first time Cluster Creation is used. This is not required if Cluster Expansion has been already executed.

Certificate registration is required because Cluster Creation does settings to 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 without using SSL encrypted communication. In this case this setting is not required.
Proceed to "6.7.1.2 Register host records in DNS."

Note

- If using Cluster Creation without using SSL encrypted communication, as the settings are executed using http communication, there are security risks such that setting parameters are intercepted. 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 Setting Items Lists for Cluster Definition Parameters" in "ISM for PRIMEFLEX Parameter List."

- If an error message is displayed and you cannot connect while using remote desktop connection, the error could 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 remote desktop connection destination.

https://blogs.technet.microsoft.com/mckittrick/unable-to-rdp-to-virtual-machine-credssp-encryption-oracle-remediation/

- 6.7.1.1.1 Check WinRM service startup
- 6.7.1.1.2 Set up WinRM service
- 6.7.1.1.3 Open the port of the firewall
- 6.7.1.1.4 Change the Windows PowerShell script execution policy

6.7.1.1.1 Check 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 might 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.

6.7.1.1.2 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."

WinRM is not set up to permit remote access to this computer for administration purposes. is displayed, which means 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 as that 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 file 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)

(3-1) Creating certificate and private key file

Open the command prompt (administrator) on the management terminal and execute the following command.

This is a command example where the target ADVM server name is "192.168.10.10" and the certificate expiration date is March 30, 2018.

```
>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 <file name of the certificate file.cer> -sv <file name of the private
key.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 <file name of the certificate file.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 <file name of the certificate
file.cer> -pfx <file name of the service certificate.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 <file name of the service certificate.pfx>.

```
>dir
```

Note

Create two certificates for ADVM#1 and ADVM#2.

(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 [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 <name of certificate file.cer>

   [Console Root] - [Certificate (local computer)] - right click on [Trusted Root Certification Authorities]. From [All tasks] - [Import], select <name of certificate file.cer> and close the "Certificate Import Wizard" screen.

2. Check that <name of certificate file.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 <name of service certificate file.pfx> as personal.

   [Console root] - [Certificate (local computer)] - right click on [Personal]. From [All tasks] - [Import], select the <name of service certificate file.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 <name of service certificate file.pfx> file, you must specify it from the pull-down.

4. Check that the <Name of service certificate file.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) Register 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 "6.7.1.1.2 Set up WinRM service," replacing ADVM#1 to ADVM#2.

6.7.1.1.3 Open the port of the firewall

To enable 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 "6.7.1.1.3 Open the port of the firewall" to ADVM#2 as well, replacing ADVM#1 to ADVM#2.

6.7.1.1.4 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 "6.7.1.2 Register host records in DNS" or "6.7.1.3 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

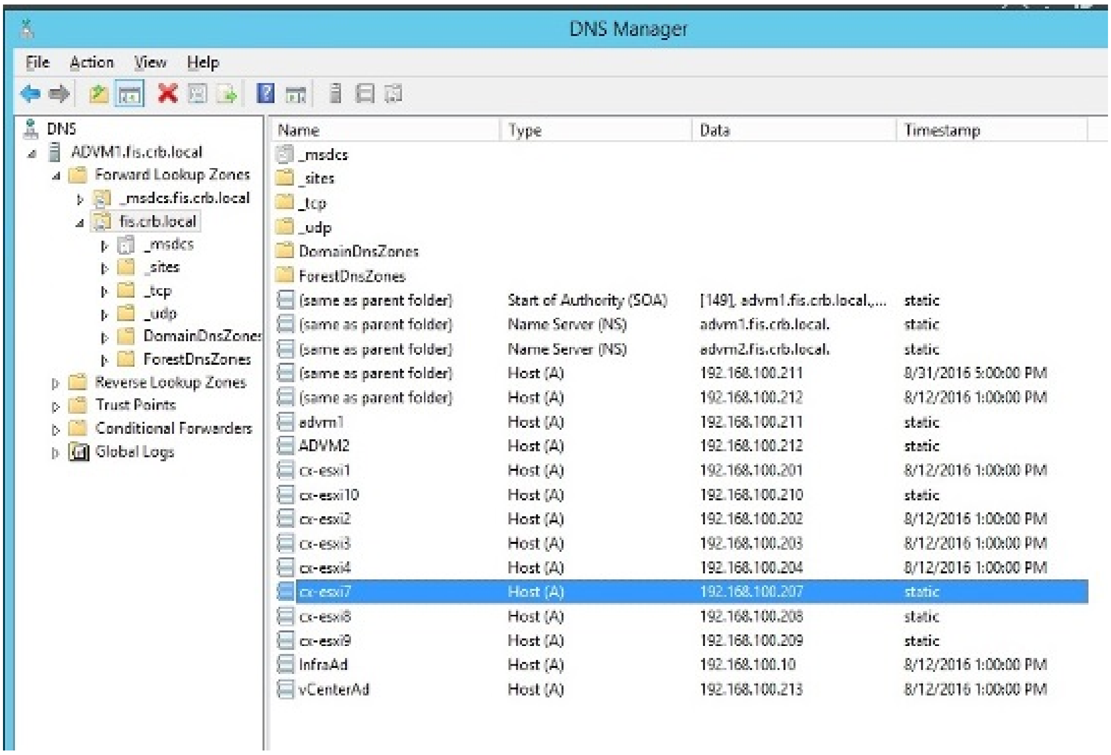
Execute "6.7.1.1.4 Change the Windows PowerShell script execution policy" to ADVM#2 as well, replacing ADVM#1 to ADVM#2.

6.7.1.2 Register host records in DNS

This section is required only when you use DNS servers already setup in your environment. Before executing Cluster Creation, make sure that name resolution is possible for the OS of the servers for creating a new cluster used for DNS forward lookup zones and reverse lookup zones.

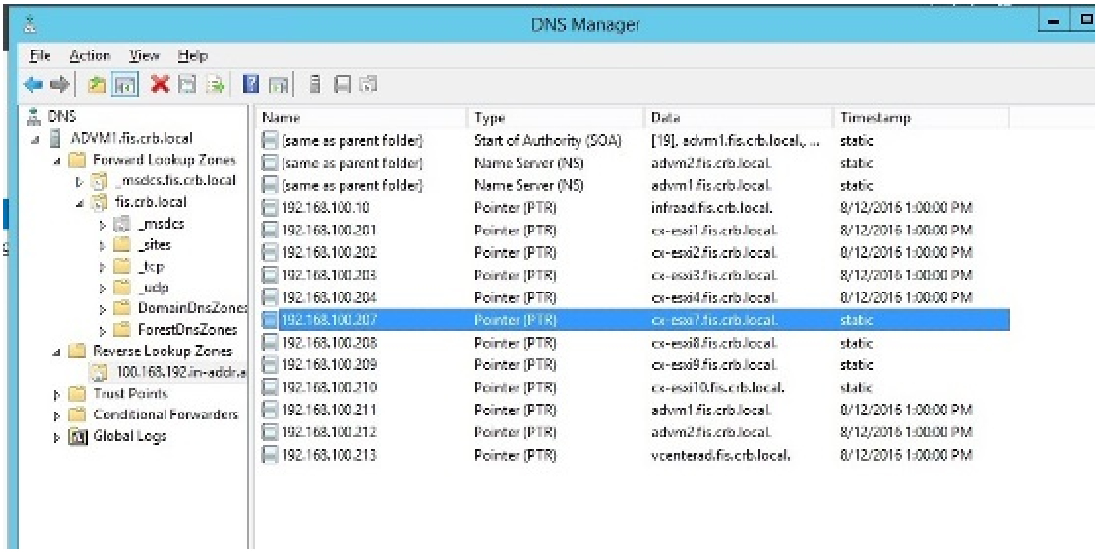
Execute for all servers for creating a new cluster.

Figure 6.4 Example for registration of forward lookup zones



Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[149], advm1.fis.crb.local.,...	static
(same as parent folder)	Name Server (NS)	advm1.fis.crb.local.	static
(same as parent folder)	Name Server (NS)	advm2.fis.crb.local.	static
(same as parent folder)	Host (A)	192.168.100.211	8/31/2016 5:00:00 PM
(same as parent folder)	Host (A)	192.168.100.212	8/12/2016 1:00:00 PM
advm1	Host (A)	192.168.100.211	static
ADVM2	Host (A)	192.168.100.212	static
cx-esxi1	Host (A)	192.168.100.201	8/12/2016 1:00:00 PM
cx-esxi10	Host (A)	192.168.100.210	static
cx-esxi2	Host (A)	192.168.100.202	8/12/2016 1:00:00 PM
cx-esxi3	Host (A)	192.168.100.203	8/12/2016 1:00:00 PM
cx-esxi4	Host (A)	192.168.100.204	8/12/2016 1:00:00 PM
cx-esxi7	Host (A)	192.168.100.207	static
cx-esxi8	Host (A)	192.168.100.208	static
cx-esxi9	Host (A)	192.168.100.209	static
InfraAd	Host (A)	192.168.100.10	8/12/2016 1:00:00 PM
vCenterAd	Host (A)	192.168.100.213	8/12/2016 1:00:00 PM

Figure 6.5 Example for registration of reverse lookup zones



Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[19], advm1.fis.crb.local., ...	static
(same as parent folder)	Name Server (NS)	advm2.fis.crb.local.	static
(same as parent folder)	Name Server (NS)	advm1.fis.crb.local.	static
192.168.100.10	Pointer (PTR)	infraad.fis.crb.local.	8/12/2016 1:00:00 PM
192.168.100.201	Pointer (PTR)	cx-esxi1.fis.crb.local.	8/12/2016 1:00:00 PM
192.168.100.202	Pointer (PTR)	cx-esxi2.fis.crb.local.	8/12/2016 1:00:00 PM
192.168.100.203	Pointer (PTR)	cx-esxi3.fis.crb.local.	8/12/2016 1:00:00 PM
192.168.100.204	Pointer (PTR)	cx-esxi4.fis.crb.local.	8/12/2016 1:00:00 PM
192.168.100.207	Pointer (PTR)	cx-esxi7.fis.crb.local.	static
192.168.100.208	Pointer (PTR)	cx-esxi8.fis.crb.local.	static
192.168.100.209	Pointer (PTR)	cx-esxi9.fis.crb.local.	static
192.168.100.210	Pointer (PTR)	cx-esxi10.fis.crb.local.	static
192.168.100.211	Pointer (PTR)	advm1.fis.crb.local.	8/12/2016 1:00:00 PM
192.168.100.212	Pointer (PTR)	advm2.fis.crb.local.	8/12/2016 1:00:00 PM
192.168.100.213	Pointer (PTR)	vcenterad.fis.crb.local.	8/12/2016 1:00:00 PM

6.7.1.3 Set up DHCP

For Cluster Creation, 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 servers for creating a new cluster.

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 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 multiple ports. Make the settings so that there are always IP addresses that can be leased.
- 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."

6.7.1.4 Import the ISO image of the OS installation media to ISM-VA

Import the ServerView Suite DVD and the installation media into ISM.

If you are going to use existing installation media, the import is not required.

For information on import operations, refer to "2.13.2 Repository Management" in "User's Guide."

For the support version, refer to "Setting Items for Profile Management."

Add ISM-VA virtual disks as required. For information on the procedure to add virtual disks, refer to "3.7 Allocation of Virtual Disks" in "User's Guide."

6.7.1.5 Upload the VMware ESXi patch file

Execute this when you want to apply the VMware ESXi patch by using Cluster Creation. When you upload the VMware ESXi patch file, the patch application processing will be executed.

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 ends with an error.
- Do not decompress the uploaded VMware ESXi patch file (zip file). If you decompress, Cluster Creation ends with an error.

Upload the VMware ESXi patch file, checking the following items and referring to "2.8 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 1] Example: ESXi650-201704001.zip

[Note 1]: Upload the VMware ESXi patch file without renaming it.

6.7.1.6 Upload VMware SMIS provider

This is a required operation when the servers for creating a cluster 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

- Offline bundle example:

  VMW-ESX-5.5.0-lsiprovider-500.04.V0.63-0005-offline_bundle-5240997.zip

Add ISM-VA virtual disks as required. 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 ends with an error.
- Do not decompress the uploaded offline bundle (zip file) of the VMware SMIS Provider. If you decompress, Cluster Creation ends with an error.

Upload the Offline bundle of the VMware SMIS Provider, checking the following items and referring to "2.8 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 1] Example: VMW-ESX-5.5.0-lsiprovider-500.04.V0.63-0005-offline_bundle-5240997.zip

[Note 1]: Upload the Offline bundle file name of the VMware SMIS Provider without renaming it.

6.7.1.7 Create a profile

Use ISM Profile Management to create the profiles for the servers for creating a new cluster. Create profiles by creating references from existing profiles.

Note

Create a profile for all servers for creating a new cluster.

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Profiles].
2. Select the current profile to be used to create a reference, from the [Actions] button, select [Duplicate Profile].
3. Set each item.

   Point

   If the servers for creating a new cluster are the same as the servers of the existing cluster environment, specify the existing ones. If they are different from the servers in the existing cluster environment, create a new profile.

   For profile creation, refer to "3.3 Execute Settings on a Server/Install Server OS."

   Note

   - Do not check the following items.
     - In the [OS] tab, [Network] - [Setup]
     - In the [OS] tab, [Register to Cloud Management Software]
     - In the [OS (for each node)] tab, [DHCP]
   - Set the following in the [OS] tab - [Management LAN network port settings] items.
     - Check [Network port specification]
     - For [Method to specify], select [MAC Address].
     - For [MAC Address], specify a MAC address with port 0 of the port expansion option with 10 Gbps communication available
   - 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]
   - The following item is automatically set by Cluster Creation. If you select the item before Cluster Creation is executed, it will not cause any errors but the setting value will be overwritten during the execution of Cluster Creation.
     - In the [OS] tab, [Execute Script after Installation]

6.7.1.8 Execute installation and wiring

Install a server for creating a new cluster at its physical location and connect the cables. For details, refer to the "Operating Manual" of the server for creating a new cluster. Execute the settings for your network switches as appropriate, referring to the manual for the switches.

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 servers for creating a new cluster.

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 "6.7.1.9 Set the IP address of iRMC."

- For Auto Discovery of nodes

  Execute "Node registration with Auto Discovery" in "6.7.1.11 Register a node to ISM."

6.7.1.9 Set the IP address of iRMC

When you register a server for creating a new cluster by using Manual Discovery, set a static IP address for the iRMC.

Boot the BIOS of the server for creating a new cluster and, on the "BIOS setup" screen, set a static IP address. To execute this operation, you must execute "6.7.1.8 Execute installation and wiring." Moreover, to display and operate the "BIOS setup" screen, connect a display and keyboard to the server for creating a new cluster.

For information on booting the BIOS and setting the IP address for the iRMC, refer to the "BIOS Setup Utility Reference Manual" for the server for creating a new cluster.

Set for all servers for creating a new cluster.

Also, execute "6.7.1.10 Set up BIOS" as well as setting of the IP address.

You can obtain the "BIOS Setup Utility Reference Manual" for each server for creating a new cluster from the following website:

http://manuals.ts.fujitsu.com/index.php?l=en

6.7.1.10 Set up BIOS

Specify the BIOS settings.

When you select "For Manual Discovery of nodes" in "6.7.1.8 Execute installation and wiring," set this item together with "6.7.1.9 Set the IP address of iRMC."

When you select "For Auto Discovery of nodes" in "6.7.1.8 Execute installation and wiring," you can set BIOS settings remotely with iRMC Video Redirection. Start BIOS, then specify the following settings from the "BIOS setup" screen.

Execute for all servers for creating a new cluster.

Table 6.13 BIOS settings

Item		Setting Value
Server Mgmt - iRMC LAN Parameters Configuration [Note 1]	iRMC IPv6 LAN Stack	Disabled
Advanced - CPU Configuration [Note 1]	Override OS Energy Performance	Enabled
	Energy Performance	Performance
	Package C State Limit	C0
Advanced - Network Stack Configuration [Note 1]	Network Stack	Enabled
	IPv6 PXE Support	Disabled
Management - iRMC LAN Parameters Configuration [Note 2]	iRMC IPv6 LAN Stack	Disabled
Configuration - CPU Configuration [Note 2]	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
Configuration - UEFI Network Stack Configuration [Note 2]	Network Stack	Enabled

Item		Setting Value
	IPv6 PXE Support	Disabled

[Note 1]: This item is displayed for the "BIOS setup" screen of the PRIMERGY RX M4 series/PRIMERGY RX M5 series.

[Note 2]: This item is displayed for the "BIOS setup" screen of the PRIMERGY CX M4 series/PRIMERGY CX M5 series.

When you select "For Manual Discovery of nodes" in "6.7.1.8 Execute installation and wiring," continue to execute "Registering a node using Manual Discovery" in "6.7.1.11 Register a node to ISM."

When you select "For Auto Discovery of nodes" in "6.7.1.8 Execute installation and wiring," continue to execute "6.7.2 Execute Cluster Creation."

6.7.1.11 Register a node to ISM

In order to use ISM to install an OS, register the server for creating a new cluster in ISM.

To register a node in the ISM, you can use both Manual Discovery and Auto Discovery.

Register all servers for creating a new cluster.

Point

- When you execute node registration in ISM, you must enter the iRMC user names and passwords for the servers for creating a new cluster. 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 Install ISM."
- For node registration, refer to "2.2.1.2 Registration of nodes" or "2.2.1.6 Discovery of nodes" in "User's Guide."

Node registration using Manual Discovery

For the procedure for registering a node with Manual Discovery, refer to "3.1.2 Register a Node Directly."

Specify the IP address set in "6.7.1.9 Set the IP address of iRMC" when registering.

By specifying the scope of the IP addresses, all servers for creating a new cluster can be registered simultaneously.

Continue to execute "6.7.2 Execute Cluster Creation."

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."

Set the static IP address of the iRMC in the "Node Registration" wizard.

Continue to execute "6.7.1.10 Set up BIOS."

6.7.2 Execute Cluster Creation

By executing Cluster Creation, you can create a cluster in the virtualized platform.

6.7.2.1 Operation requirements for Cluster Creation

To use Cluster Creation, the following requirements must be satisfied.

Check the following requirements before executing it.

- That the AD, DNS, and NTP are all running normally and can be used
- 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 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
- That the type of servers for creating a new cluster are the same
- That there are three or more servers for creating a new cluster
- That you register the server for creating a new cluster 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 physical NIC of the server for creating a new cluster using the storage network is 10 GbE
- That the port of the physical switch using the storage network is 10 GbE
- 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
- A profile has been created for the server for creating a new cluster with Profile Management of ISM
- The power of the server for creating a new cluster is off

Note

The following is an operation requirement when executing Cluster Creation again with the OS installation completed using profile assignment.

- The power of the server for creating a new cluster is on

To check if the OS installation has been completed, use the following procedure.

1. At the top of the Global Navigation Menu, 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."

- The SSD capacity device fulfill the following specifications when using an All Flash configuration

  If the two types of SSD, cache and capacity, is the one with the highest number of devices (if the number of SSDs is the same, it should be the largest one)

- The computer name of the servers configuring a new cluster 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 servers configuring a new cluster which you specify in the profile must be unique among all IP addresses of the OS of the nodes managed by ISM
- On the "Cluster Details" screen in the "Create Cluster" wizard, [Storage Pool Name] on the [Storage Pool] tab does not overlap the [Storage Pool Name] of an existing cluster
- On the "Cluster Details" screen in the "Create Cluster" wizard, [Port Group Name] on the [Network] tab does not overlap the [Port Group Name] of an existing cluster when creating a new vDS

- On the "Basic Information" screen in the "Create Cluster" wizard, the name in [Cluster Name] must be 15 characters or less

6.7.2.2 Cluster Creation procedure

This section describes the procedure for executing Cluster Creation of ISM for PRIMEFLEX.

Note

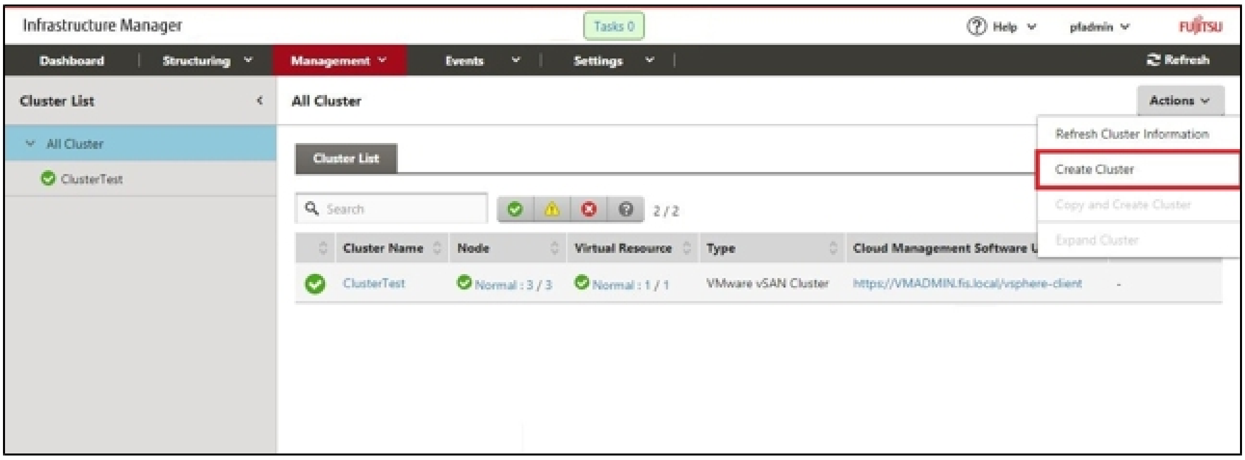
Before executing Cluster Creation, check the settings of [Add disks to storage].

If the setting is "Manual," execute disk addition manually after completing Cluster Creation.

If the setting is "Automatic," disks are added to the vSAN storage automatically.

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 GUI of ISM, select [Management] - [Cluster].

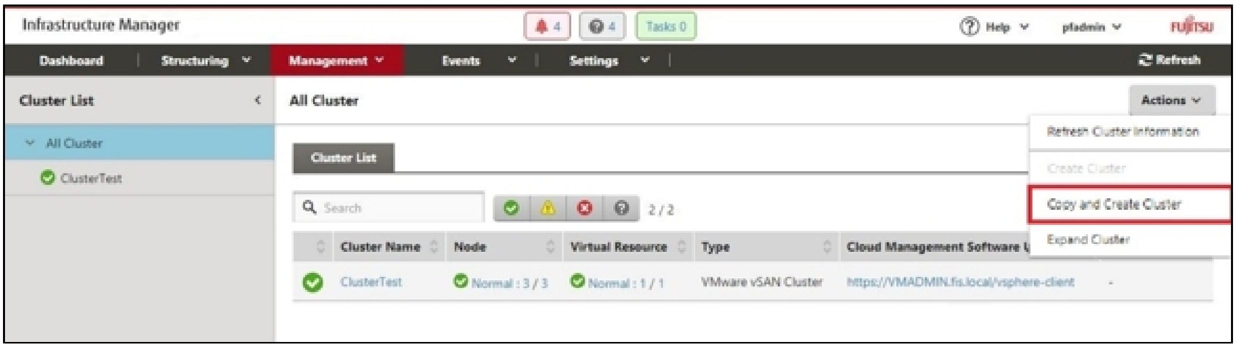
   The "Cluster List" screen is displayed.
3. From the [Actions] button, select [Create Cluster].



Cluster Name	Node	Virtual Resource	Type	Cloud Management Software U
ClusterTest	Normal : 3 / 3	Normal : 1 / 1	VMware vSAN Cluster	https://VMADMIN.fis.local/vsphere-client

   The "Create Cluster" wizard is displayed.

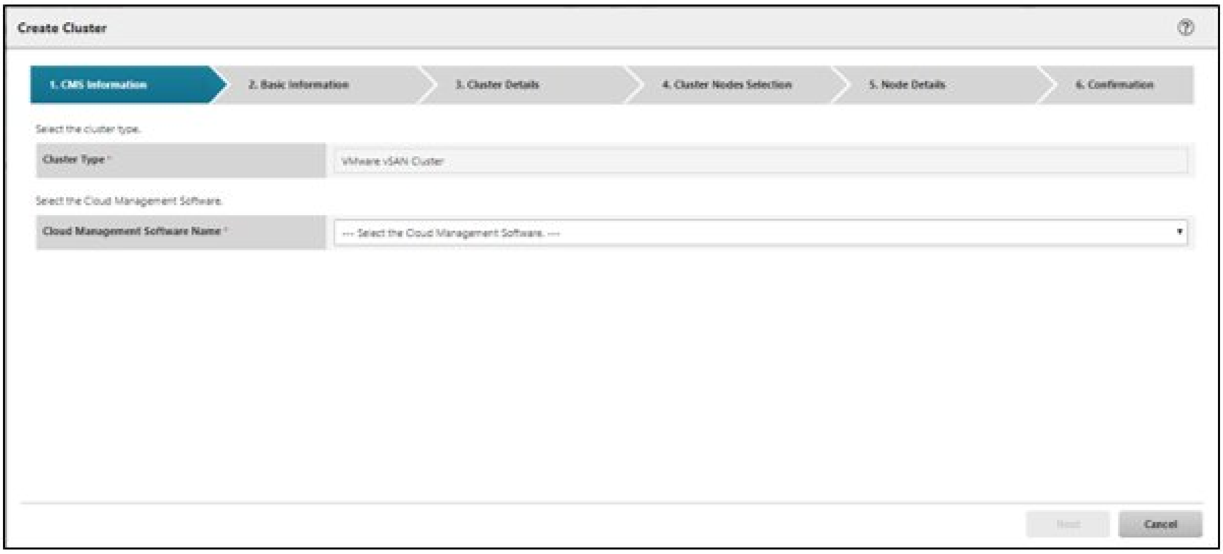
   If you create a cluster by referring the existing cluster, select the existing cluster, then from the [Actions] button, select [Copy and Create Cluster].



Cluster Name	Node	Virtual Resource	Type	Cloud Management Software U
ClusterTest	Normal : 3 / 3	Normal : 1 / 1	VMware vSAN Cluster	https://VMADMIN.fis.local/vsphere-client

4. Enter each parameter on the "CMS Information" screen.

   If executing again, select the [Next] button if no parameters must be entered again, and proceed to Step 5.



Select the cluster type.

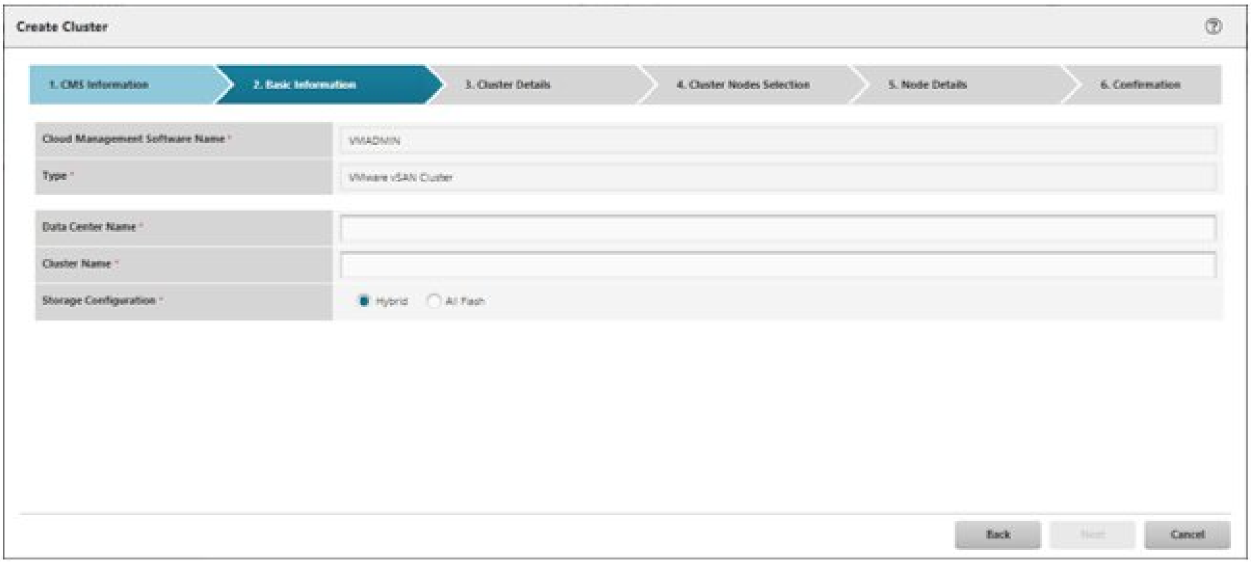
Cluster Type *	VMware vSAN Cluster

Select the Cloud Management Software.

Cloud Management Software Name *	--- Select the Cloud Management Software. ---

5. Enter each parameter on the "Basic Information" screen.

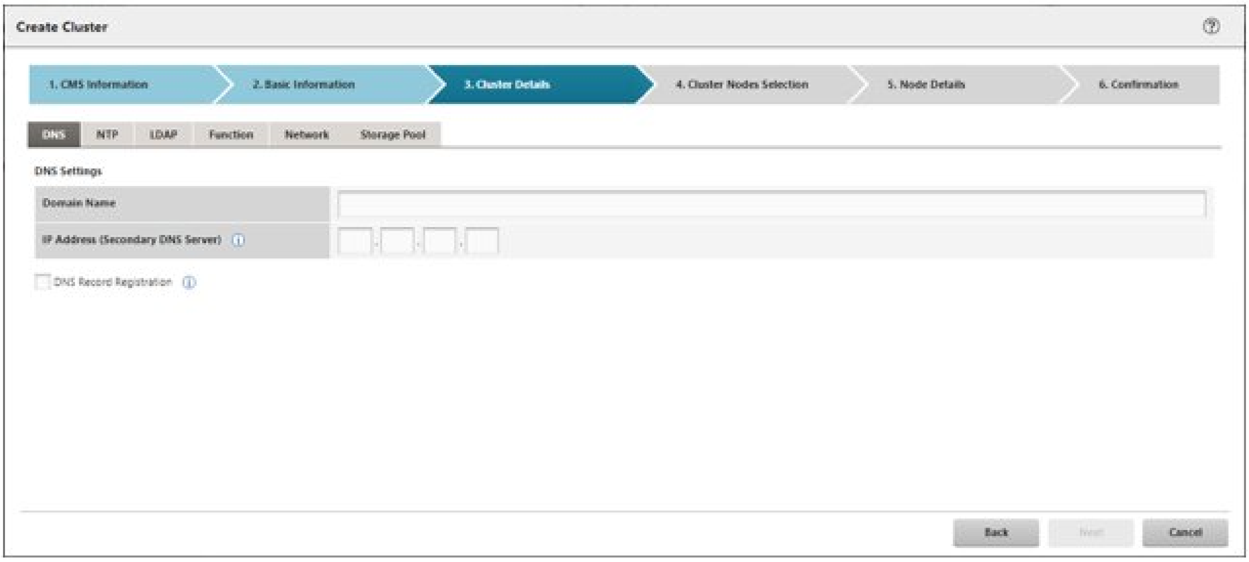
   If executing again, select the [Next] button if no parameters must be entered again, and proceed to Step 6.



Cloud Management Software Name *	VMADMIN
Type *	VMware vSAN Cluster
Data Center Name *	
Cluster Name *	
Storage Configuration *	● Hybrid ○ All Flash

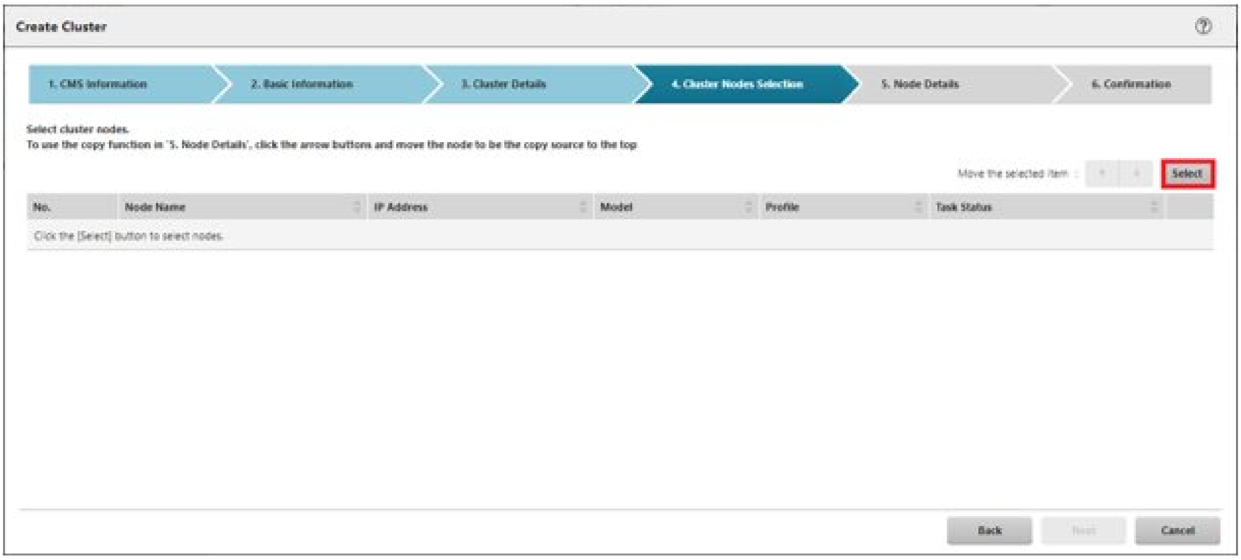
6. Enter each parameter on the "Cluster Details" screen.

   If executing again, select the [Next] button if no parameters must be entered again, and proceed to Step 7.



7. Select the [Select] button in the "Cluster Nodes Selection" screen, and then on the displayed "Target nodes selection" screen, select the server for creating a new cluster.

   If executing again, this procedure is not required. Select the [Next] button and proceed to Step 9.



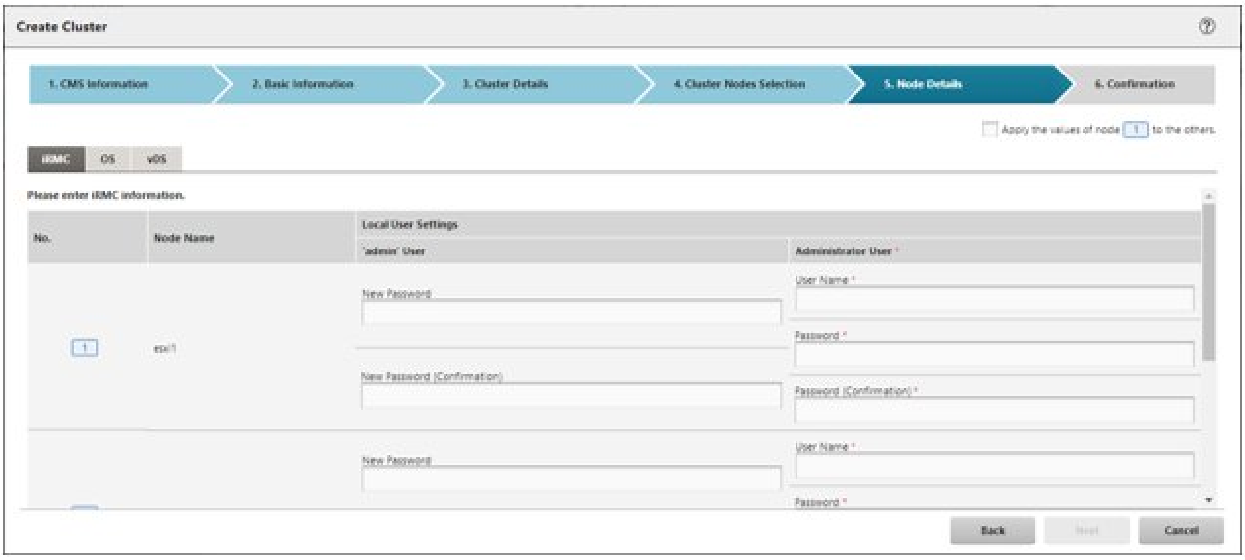
Select cluster nodes.
To use the copy function in '5. Node Details', click the arrow buttons and move the node to be the copy source to the top

Click the [Select] button to select nodes.

8. If a profile has not been assigned to the server for creating a new cluster, select the [Select] button in the [Profile] item, and then select the profile to be assigned.

9. Enter each parameter on the "Node Details" screen.

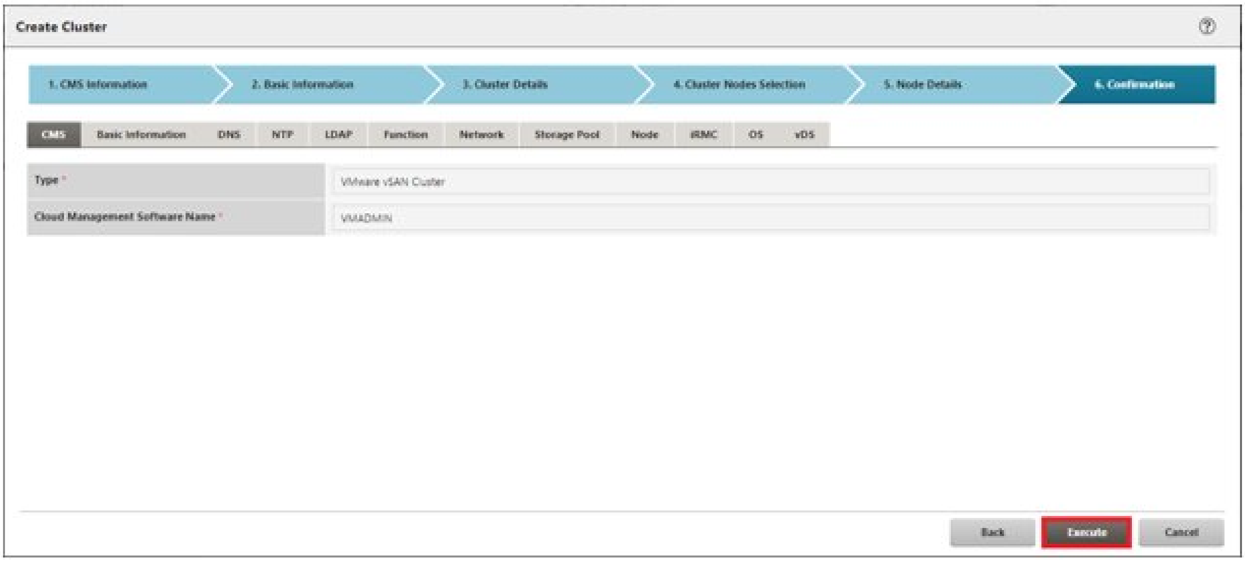
   If executing again, select the [Next] button if no parameters must be entered again, and proceed to Step 10.



Note

For details on Cluster Definition Parameters, refer to "Chapter 3 Setting Items Lists for Cluster Definition Parameters" in "ISM for PRIMEFLEX Parameter List."

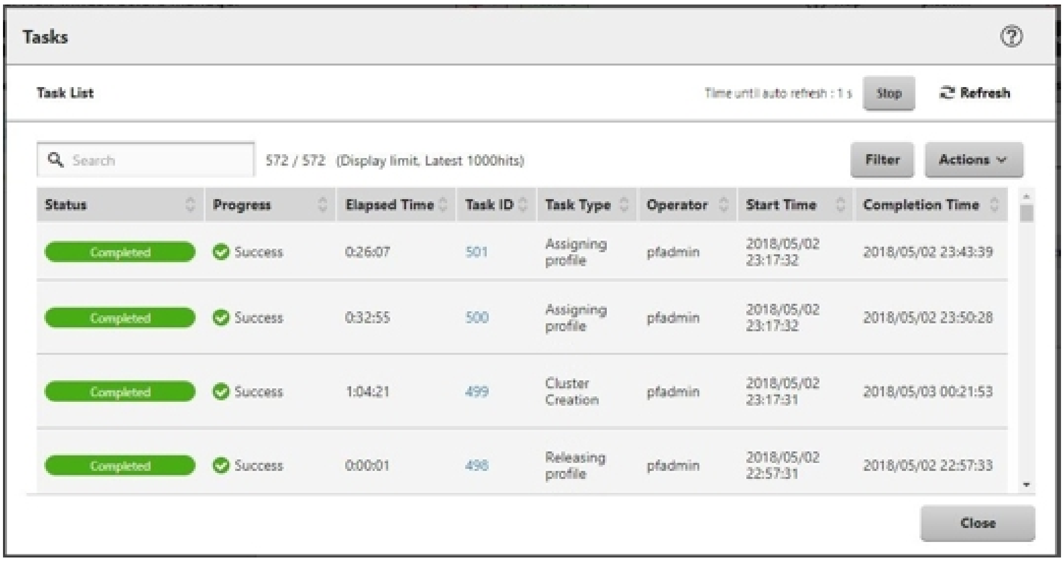
10. Check the parameters on the "Confirmation" screen, then select the [Execute] button.



Type *	VMware vSAN Cluster
Cloud Management Software Name *	VMADMIN

The execution of the cluster creation is registered as an ISM task.

At the top of the Global Navigation Menu, select [Tasks], then the tasks in the task list displayed in the "Tasks" screen whose task type has become "Cluster Creation" are the Cluster Creation tasks.

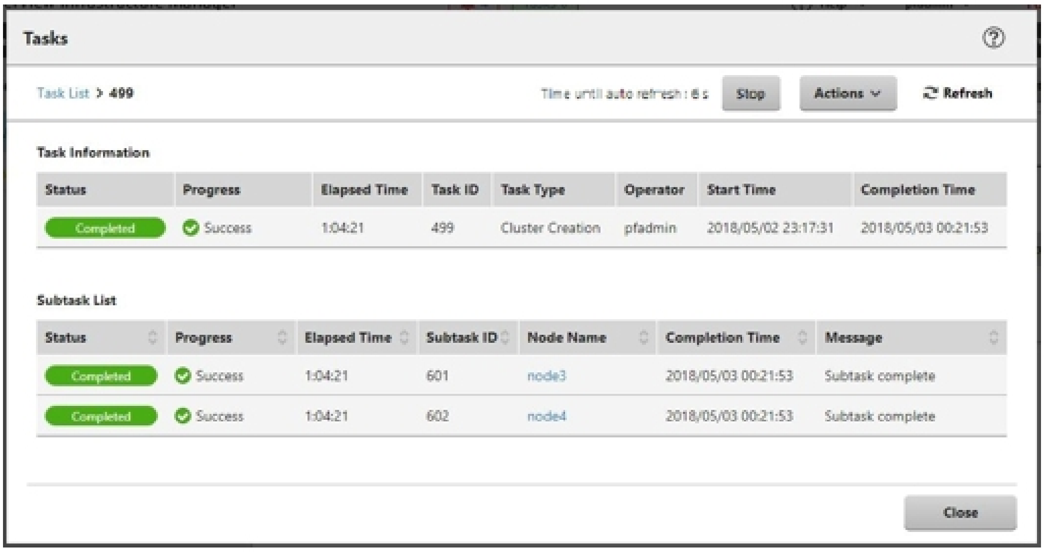


572 / 572 (Display limit, Latest 1000hits)

Status	Progress	Elapsed Time	Task ID	Task Type	Operator	Start Time	Completion Time
Completed	✓ Success	0:26:07	501	Assigning profile	pfadmin	2018/05/02 23:17:32	2018/05/02 23:43:39
Completed	✓ Success	0:32:55	500	Assigning profile	pfadmin	2018/05/02 23:17:32	2018/05/02 23:50:28
Completed	✓ Success	1:04:21	499	Cluster Creation	pfadmin	2018/05/02 23:17:31	2018/05/03 00:21:53
Completed	✓ Success	0:00:01	498	Releasing profile	pfadmin	2018/05/02 22:57:31	2018/05/02 22:57:33

Point

From the task list on the "Tasks" screen, select [Task ID] from "Cluster Creation," and then the "Tasks" screen of the "Cluster Creation" is displayed. In this screen, a subtask list is displayed for each server for creating a new cluster. You can check the progress status of each task by checking the message column.



Task Information

Status	Progress	Elapsed Time	Task ID	Task Type	Operator	Start Time	Completion Time
Completed	✓ Success	1:04:21	499	Cluster Creation	pfadmin	2018/05/02 23:17:31	2018/05/03 00:21:53

Subtask List

Status	Progress	Elapsed Time	Subtask ID	Node Name	Completion Time	Message
Completed	✓ Success	1:04:21	601	node3	2018/05/03 00:21:53	Subtask complete
Completed	✓ Success	1:04:21	602	node4	2018/05/03 00:21:53	Subtask complete

11. Check that the status of "Cluster Creation" has become "Completed."

Note

- If an error is displayed on the ISM "Tasks" screen, refer to "ISM for PRIMEFLEX Messages" and tale the countermeasures. Solve the error, then execute the operation again.

  If the OS installation with Profile Management of ISM (Assigning profile tasks) ends normally, do not power off the server for creation a new cluster when executing again.

- Even when the execution of Cluster Creation is complete, the processing of "Updating vSAN configuration" and "Configuring vSphere HA" may be under execution. Proceed to "6.7.3 Follow-up Processing" after the processing of these tasks is completed.

  Access 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 the settings of the virtual network for service on the server for creating a new cluster, set them according to your environment.

- Do not execute the Cluster Creation during execution of Firmware Rolling Update.

6.7.3 Follow-up Processing

This section describes the follow-up processing required after the cluster creation.

6.7.3.1 Confirm Cluster Creation

Confirm the created vSAN cluster with the following procedure.

1. Access vSphere Web Client to confirm the following.

   - Confirm that the created cluster is displayed from the "Top" screen - [Home] tab - [Inventories] - [Hosts and Clusters].

   - Confirm that the disks of the server for creating a new cluster 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.

   Sometimes a warning may be issued 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 vSAN6.6.1 environment (VMware ESXi 6.5 Update 1), health errors and the countermeasures are described below.

   - Virtual SAN Disk Balance

     Execute proactive balancing for the disks.

   - 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 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

   - To check the fault domain host of the server for expanding a cluster, move from "Top" screen - [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Settings] - [Fault Domains & Stretched Cluster] - [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 servers configuring a current cluster or the servers for creating a new cluster. If the result of checking is that they overlap, refer to "2.6 Action Examples for when a Cluster Creation Error Occurs" - "Actions example 23" in "ISM for PRIMEFLEX Messages" and take the action.

- When the setting in [Add disks to storage] is "Manual," the disks of the server for creating a new cluster are not displayed in [Top screen] - [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Monitor] - [vSAN] - [Physical Disk].

  Add disks manually.

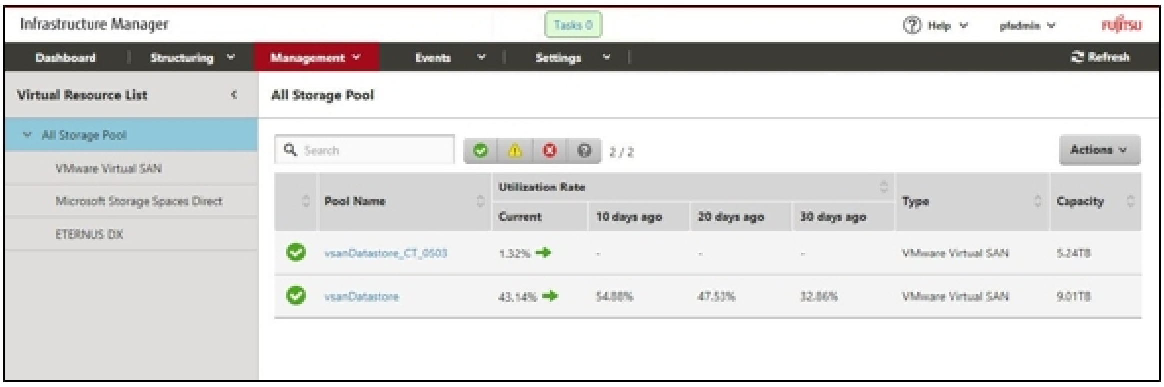
  To check the settings, access vSphere Web Client and select the "Top" screen - [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Configure] - [vSAN] - [General] - [Add disks to storage].

  If you want to add disks manually, follow the procedure below. Execute it for all servers for creating a new cluster.

  1. Log in to vCSA with vSphere Web Client.
  2. From "Top" screen, select [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster Name>] - [Configure] - [Disk Management].
  3. Select the server for creating a new cluster and select [Create Disk Group].
  4. On the "Create Disk Group" screen, select "disk to serve as cache tier" and "disk to serve as capacity tier," and then select the [OK] button.

     When the task is complete, the disk addition is complete.

2. Access the GUI of ISM, and in the "All Storage Pool" screen in [Management] - [Virtual Resource], execute [Actions] - [Refresh Virtual Resource Information] to refresh. After the update, confirm that the target vSAN datastore is displayed.



All Storage Pool

	Pool Name	Utilization Rate				Type	Capacity
		Current	10 days ago	20 days ago	30 days ago		
✓	vsanDatastore_CT_0503	1.32% →	-	-	-	VMware Virtual SAN	5.24TB
✓	vsanDatastore	43.14% →	54.88%	47.53%	32.86%	VMware Virtual SAN	9.01TB

Note

Even when the task completed successfully, if the vSAN storage is not displayed, or the vSAN storage capacity is less than expected, the following causes can be considered.

- Communication for the vSAN network failed.

  Check the settings and the wiring of the switch.

- The setting of [Add disks to storage] is "Manual."

  Add disks manually.

  To check the settings, access vSphere Web Client and select the "Top" screen - [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Configure] - [vSAN] - [General] - [Adds disks to storage].

  If you want to add disks manually, follow the following procedure. Execute it for all servers for creating a new cluster.

  1. Log in to vCSA with vSphere Web Client.
  2. From "Top" screen, select [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster Name>] - [Configure] - [Disk Management].
  3. Select the server for creating a new cluster and select [Create Disk Group].

4. On the "Create Disk Group" screen, select "disk to serve as cache tier" and "disk to serve as capacity tier," and then select the [OK] button.

   When the task is complete, the disk addition is complete.

6.7.3.2 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 servers for creating a new cluster.

http://support.ts.fujitsu.com/Index.asp?lng=COM

6.7.3.3 Register a server for creating a new cluster to ServerView RAID Manager

To execute Monitoring of SSD lifetime, you must register the server for creating a new cluster 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

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 servers for creating a new cluster.

```
>amCLI -e 21/0 add_server name=<IP address of ESXi of the server for creating a new cluster>
port=5989 username=root password=<root password>
```

3. Execute the following command to check that all servers for creating a new cluster 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.

6.7.3.4 Delete unnecessary files

Delete unnecessary files with the following procedure after completing Cluster Creation.

(1) Deleting certificates

The certificate created in "6.7.1.1 Create ADVM certificates" is not required after once registered.

Note

The certificates uploaded to ADVM#1 and ADVM#2 in "6.7.1.1 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. If you are using the files that you uploaded to ISM-VA, 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 the unnecessary files, checking the following items and referring to "2.9 Delete Files Uploaded to ISM-VA."

Item	Value
Root Directory	Administrator/ftp
Directory Name	kickstart
File Name	- VMware ESXi patch files in "6.7.1.5 Upload the VMware ESXi patch file" - Offline bundle of the VMware SMIS Provider in "6.7.1.6 Upload VMware SMIS provider"

6.8 Create a Cluster for Microsoft Storage Spaces Direct

This section describes the cluster creating procedure for PRIMEFLEX for Microsoft Storage Spaces Direct.

This function can be used only with the license for ISM for PRIMEFLEX.

Cluster Creation is executed according to the following work flow.

Table 6.14 Cluster Creation work flow

Cluster Creation procedure		Tasks
1	Preparations	- Creating certificates for servers for creating a new cluster - DHCP settings - Importing the ISO image of the OS installation media to ISM-VA - Creating profiles - Installing and Wiring - Setting the IP address of iRMC - BIOS settings - Creating system disk (RAID1) - Registering nodes in ISM
2	Execute Cluster Creation	
3	Follow-up processing	- Refresh cluster information - Confirm Cluster Creation - Registering to the virtual switch for service - Setting the system volume name - Setting the browser - Deleting unnecessary files

6.8.1 Preparations

This section describes the preparations required before the cluster creation.

6.8.1.1 Create certificates for servers for creating a new cluster

You must create and register certificates for the servers for creating a new cluster because Cluster Creation 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.

- 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 as that 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.

This is a command example where the name of the server for creating a new cluster is "192.168.10.10" and the certificate expiration date is March 30, 2018.

```
>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 <file name of the certificate file.cer> -sv <file name of the private
key.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 <file name of the certificate file.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 <file name of the certificate
file.cer> -pfx <file name of the service certificate.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 <file name of the service certificate.pfx>.

```
>dir
```

Note

- Create certificates for all servers for creating a new cluster.
- For the name of the certificate files, specify "Computer name set in ISM's profiles."

  Example:

  - hv-host4.cer
  - hv-host4.pfx

(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 "2.8 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)

6.8.1.2 Set up DHCP

For Cluster Creation, 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 there are leases for all servers and that leases are possible for all servers for creating a new cluster.

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 operation is in progress.
- Since the management network is made redundant in the configuration of this product, IP addresses are leased to multiple ports. Execute the settings so that there are always IP addresses that can be leased.
- 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."

6.8.1.3 Import the ISO image of the OS installation media to ISM-VA

Import the ServerView Suite DVD and the installation media into ISM.

If you are going to use existing installation media, the import is not required.

For information on import operations, refer to "2.13.2 Repository Management" in "User's Guide."

For the support version, refer to "Setting Items for Profile Management."

Add ISM-VA virtual disks as required. For information on the procedure to add virtual disks, refer to "3.7 Allocation of Virtual Disks" in "User's Guide."

6.8.1.4 Create a profile

Use ISM Profile Management to create the profiles for the servers for creating a new cluster. Create profiles by creating references from existing profiles.

Note

Create a profile for all servers for creating a new cluster.

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Profiles].
2. Select the current profile to be used to create a reference, from the [Actions] button, select [Duplicate Profile].
3. Set each item.

   Point

   If the servers for creating a new cluster are the same as the servers of the existing cluster environment, specify the existing ones. If they are different from the servers in the existing cluster environment, create a new profile.

   For profile creation, refer to "3.3 Execute Settings on a Server/Install Server OS."

   Note

   - Do not check the following items.
     - In the [OS (for each node)] tab, [DHCP]
   - 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]
   - The following item is automatically set by Cluster Creation. If you select the item before Cluster Creation is executed, it will not cause any errors but the setting value will be overwritten during the execution of Cluster Creation.
     - In the [OS] tab, [Execute Script after Installation]

6.8.1.5 Execute installation and wiring

Install a server for creating a new cluster at its physical location and connect the cables. For details, refer to the "Operating Manual" of the server for creating a new cluster. Execute the settings for your network switches as appropriate, referring to the manual for the switches.

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 servers for creating a new cluster.

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 "6.8.1.6 Set the IP address of iRMC."

- For Auto Discovery of nodes

  Execute "Node registration using Auto Discovery" in "6.8.1.9 Register a node to ISM."

6.8.1.6 Set the IP address of iRMC

When you register a server for creating a new cluster by using Manual Discovery, set a static IP address for the iRMC.

Boot the BIOS of the server for creating a new cluster and, on the "BIOS setup" screen, set a static IP address. To execute this operation, you must execute "6.8.1.5 Execute installation and wiring." Moreover, to display and operate the "BIOS setup" screen, connect a display and keyboard to the server for creating a new cluster.

For information on booting the BIOS and setting the IP address for the iRMC, refer to the "BIOS Setup Utility Reference Manual" for the server for creating a new cluster.

Set for all servers for creating a new cluster.

Also, execute "6.8.1.7 Set up BIOS" as well as setting of the IP address.

You can obtain the "BIOS Setup Utility Reference Manual" for each server for creating a new cluster from the following website:

http://manuals.ts.fujitsu.com/index.php?l=en

6.8.1.7 Set up BIOS

Specify the BIOS settings.

When you select "For Manual Discovery of nodes" in "6.8.1.5 Execute installation and wiring," set this item together with "6.8.1.6 Set the IP address of iRMC."

When you select "For Auto Discovery of nodes" in "6.8.1.5 Execute installation and wiring," you can set BIOS settings remotely with iRMC Video Redirection. Start BIOS, then specify the following settings from the "BIOS setup" screen.

Execute for all servers for creating a new cluster.

Table 6.15 BIOS settings

Item		Setting Value
Main	System Date	Local date
	System Time	Local date
Advanced - CPU Configuration	Override OS Energy Performance	Enabled
	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

After completing the BIOS settings, in the "BIOS setup" screen - the [Save & Exit] tab, execute "Save Changes and Exit," then power off after several minutes.

Continue to execute "6.8.1.8 Create system disk (RAID1)."

6.8.1.8 Create system disk (RAID1)

The logical disk to be used as a system disk (Configure 2 HDD as RAID 1) is created in the "UEFI" screen in PRIMERGY. Execute for all servers for creating a new cluster.

1. Start the "BIOS setup" screen.

2. Select [Advanced] tab, then select "LSI SAS3 MPT Controller SAS3008" and press the [Enter] key.
3. Select "LSI SAS3 MPT Controller X.XX.XX.XX" and press the [Enter] key.
4. Select "Controller Management" and press the [Enter] key.
5. Select "Create Configuration" and press the [Enter] key.
6. In "Select RAID level" select "RAID 1," select "Select Physical Disks" and then press the [Enter] key.
7. Select the type of the system disk prepared in "Select Interface Type."
8. In "Select Media Type" select the media of the system disk (HDD).

   Select two system disks for your OS booting from the disk list displayed in "Select Media Type."
9. Change the two disks to be used as system disk to "Enabled," select "Apply Changes" and press the [Enter] key.
10. The "Confirmation" screen displayed and after changing "Confirm" to "Enabled," select "Yes" and press the [Enter] key.
11. In "Operation completed successfully," select "OK" and press the [Enter] key.
12. Press the [Esc] key several times, in "Exit Without Saving," select "Yes" and press the [Enter] key.
13. The power of the server is turned off.

When you select "For Manual Discovery of nodes" in "6.8.1.5 Execute installation and wiring," continue to execute "Node registration using Manual Discovery" in "6.8.1.9 Register a node to ISM."

When you select "For Auto Discovery of nodes" in "6.8.1.5 Execute installation and wiring," continue to execute "6.8.2 Execute Cluster Creation."

6.8.1.9 Register a node to ISM

In order to use ISM to install an OS, register the server for creating a new cluster in ISM.

To register a node in the ISM, you can use both Manual Discovery and Auto Discovery.

Register all servers for creating a new cluster.

Point

- When you execute node registration in ISM, you must enter the iRMC user names and passwords for the servers for creating a new cluster. 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 Install ISM."
- For node registration, refer to "2.2.1.2 Registration of nodes" or "2.2.1.6 Discovery of nodes" in "User's Guide."

Node registration using Manual Discovery

For the procedure for registering a node with Manual Discovery, refer to "3.1.2 Register a Node Directly."

Specify the IP address set in "6.8.1.6 Set the IP address of iRMC" when registering.

By setting the scope of IP addresses, the servers for creation a cluster can be registered simultaneously.

Continue to execute "6.8.2 Execute Cluster Creation."

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."

Set the static IP address of the iRMC on the "Node Registration" wizard.

Continue to execute "6.8.1.7 Set up BIOS."

6.8.2 Execute Cluster Creation

By executing Cluster Creation, you can create a cluster in the virtualized platform.

6.8.2.1 Operation requirements for Cluster Creation

To use Cluster Creation, the following requirements must be satisfied.

- Check the following requirements before executing it.
  - That the AD, DNS and NTP are all running normally and can be used
  - That the information of the DNS server is registered in ISM-VA
  - That the existing cluster is operating normally
  - That the type of servers for creating a new cluster are the same
  - That there are two or more servers for creating a new cluster

    If you created a new cluster with two nodes, you need to configure a quorum.
  - That you register the server for creating a new cluster 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.
  - An Intel or Mellanox Ethernet adapter must be installed in the server for creating a new cluster
  - The Ethernet adapter can handle over 10 GB traffic
  - BIOS settings for the server for creating a new cluster are specified as described in "6.8.1.7 Set up BIOS"
  - The devices for PRIMEFLEX for Microsoft Storage Spaces Direct are configured as below

Device	Default	Utilization
PCI card 1 (Port1), PCI card 2 (Port1)	Workload virtual switch	Production LAN
PCI card 1 (Port0), PCI card 2 (Port0)	Management virtual switch	Management LAN Storage_1 LAN, Storage_2 LAN (for Heart Beat and Live Migration of the failover cluster)

  - A profile has been created for the server for creating a new cluster in Profile Management of ISM
  - The power of the server for creating a new cluster is off

Note

The following is an operation requirement when executing Cluster Creation again with the OS installation completed using profile assignment.

- The power of the server for creating a new cluster is on

To check if the OS installation has been completed, use the following procedure.

1. At the top of the Global Navigation Menu, 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."

- When configuring an ADVM dedicated to PRIMEFLEX for Microsoft Storage Spaces Direct, that the following files for PRIMEFLEX for Microsoft Storage Spaces Direct 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

- The computer name of the servers configuring a new cluster 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 servers configuring a new cluster which you specify in the profile must be unique among all IP addresses of the OS of the nodes managed by ISM.

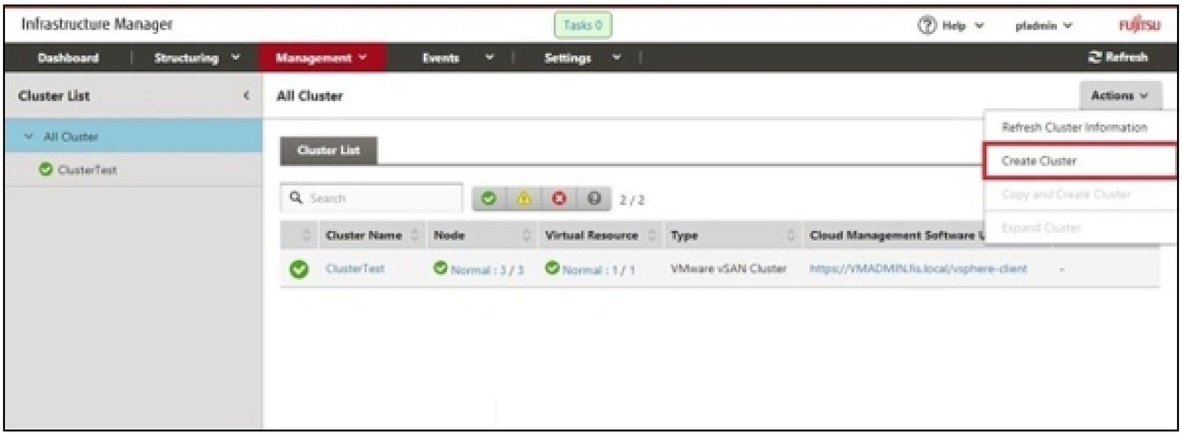
- On the "Basic Information" screen in the "Create Cluster" wizard, the name in [Cluster Name] must be 15 characters or less.

6.8.2.2 Cluster Creation procedure

This section describes the procedure for executing Cluster Creation of ISM for 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 GUI of ISM, select [Management] - [Cluster].

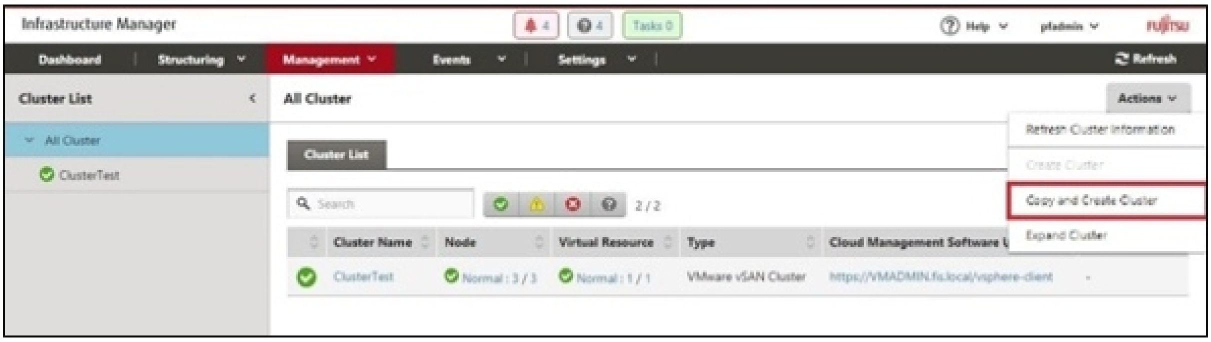
   The "Cluster List" screen is displayed.
3. From the [Actions] button, select [Create Cluster].



Cluster Name	Node	Virtual Resource	Type	Cloud Management Software U	
ClusterTest	Normal : 3 / 3	Normal : 1 / 1	VMware vSAN Cluster	https://VMADMIN.fis.local/vsphere-client	-

The "Create Cluster" wizard is displayed.

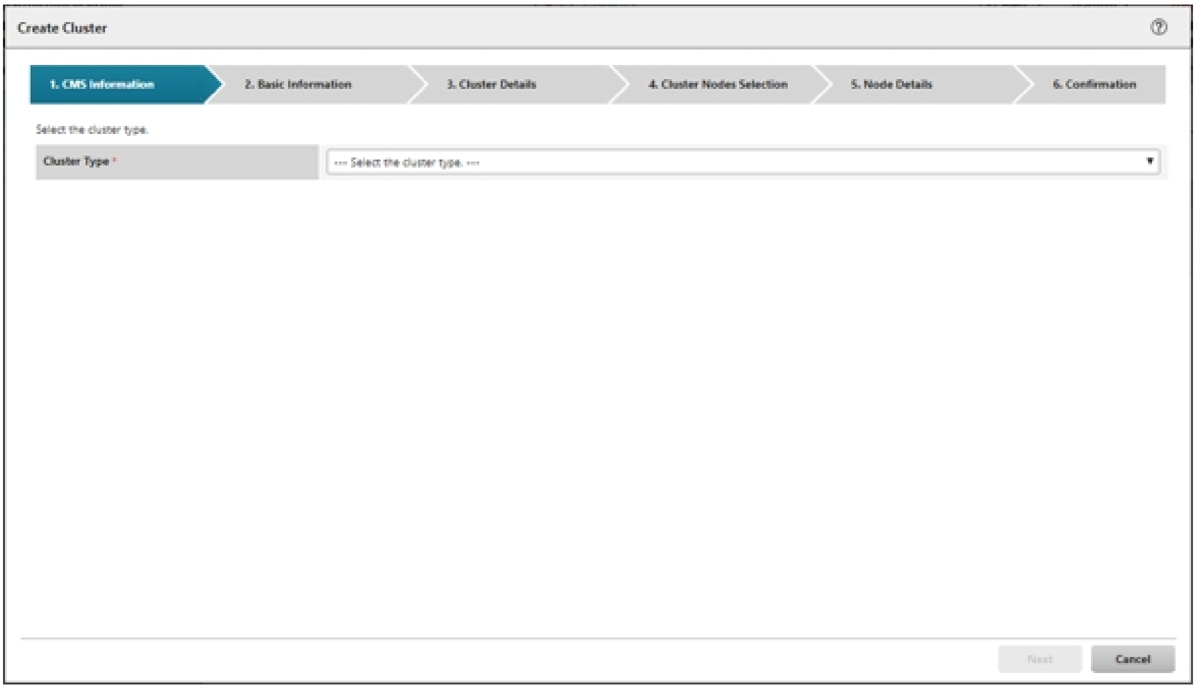
If you create a cluster by referring the existing cluster, select the existing cluster, then from the [Actions] button, select [Copy and Create Cluster].



Cluster Name	Node	Virtual Resource	Type	Cloud Management Software U	
ClusterTest	Normal : 3 / 3	Normal : 1 / 1	VMware vSAN Cluster	https://VMADMIN.fis.local/vsphere-client	-

4. Enter each parameter on the "CMS Information" screen.

   If executing again, select the [Next] button if no parameters must be entered again, and proceed to Step 5.



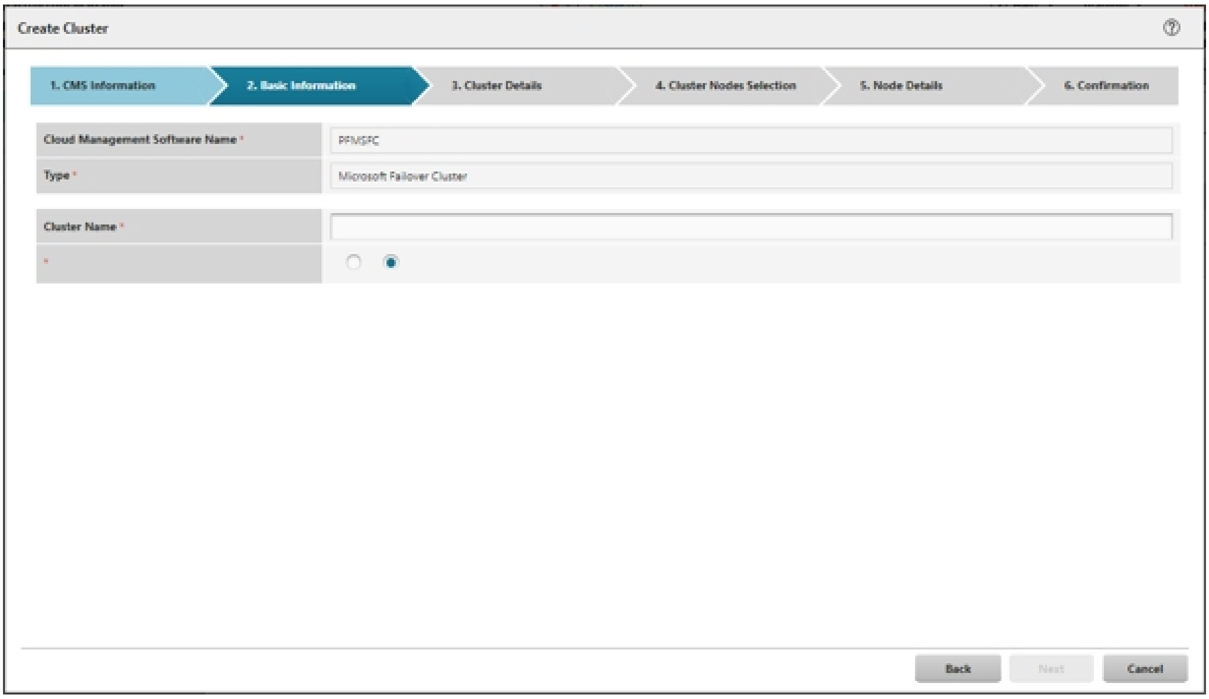
Create Cluster

Select the cluster type.

Cluster Type *	--- Select the cluster type. --- ▾

5. Enter each parameter on the "Basic Information" screen.

   If executing again, select the [Next] button if no parameters must be entered again, and proceed to Step 6.

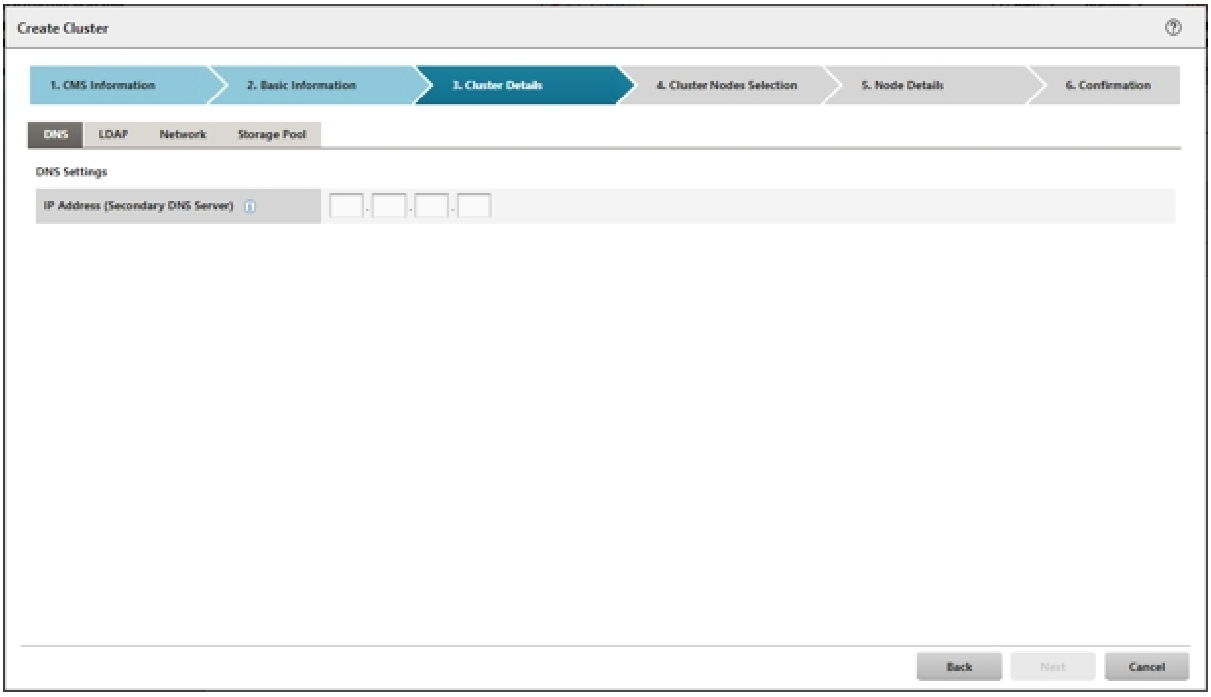


Create Cluster

Cloud Management Software Name *	PFMSFC
Type *	Microsoft Failover Cluster
Cluster Name *	
*	○ ●

6. Enter each parameter on the "Cluster Details" screen.

   If executing again, select the [Next] button if no parameters must be entered again, and proceed to Step 7.

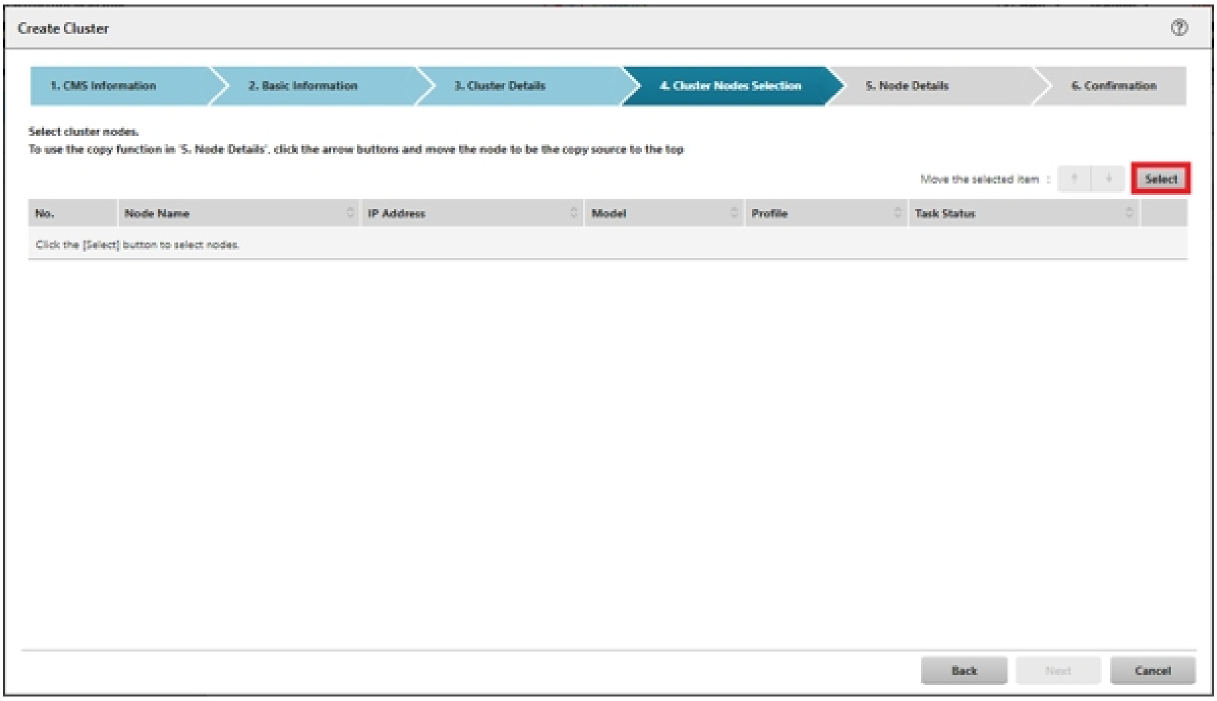


DNS Settings

IP Address (Secondary DNS Server): . . .

7. Select the [Select] button in the "Cluster Nodes Selection" screen, and then on the displayed "Target nodes selection" screen, select the server for creating a new cluster.

   If executing again, this procedure is not required. Select the [Next] button and proceed to Step 9.



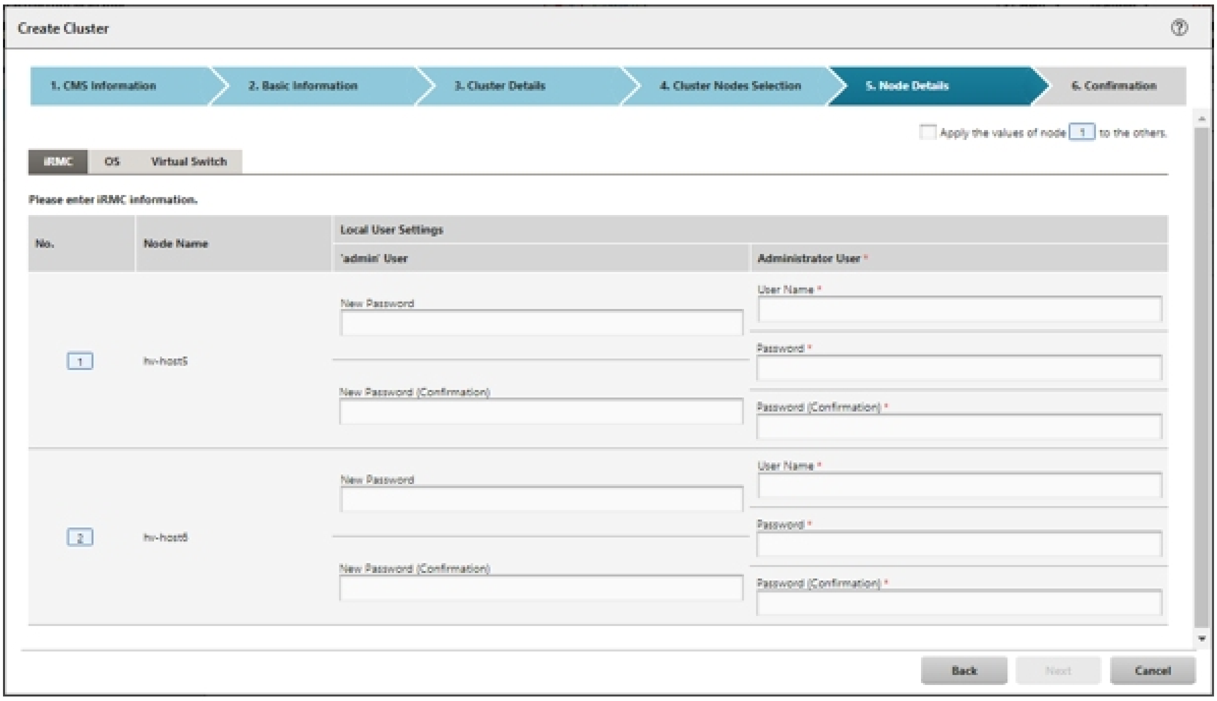
Select cluster nodes.
To use the copy function in '5. Node Details', click the arrow buttons and move the node to be the copy source to the top

No.	Node Name	IP Address	Model	Profile	Task Status
Click the [Select] button to select nodes.					

8. If a profile has not been assigned to the server for creating a new cluster, select the [Select] button in the [Profile] item and select the profile to be assigned.

9. Enter each parameter on the "Node Details" screen.

   If executing again, select the [Next] button if no parameters must be entered again, and proceed to Step 10.



Create Cluster

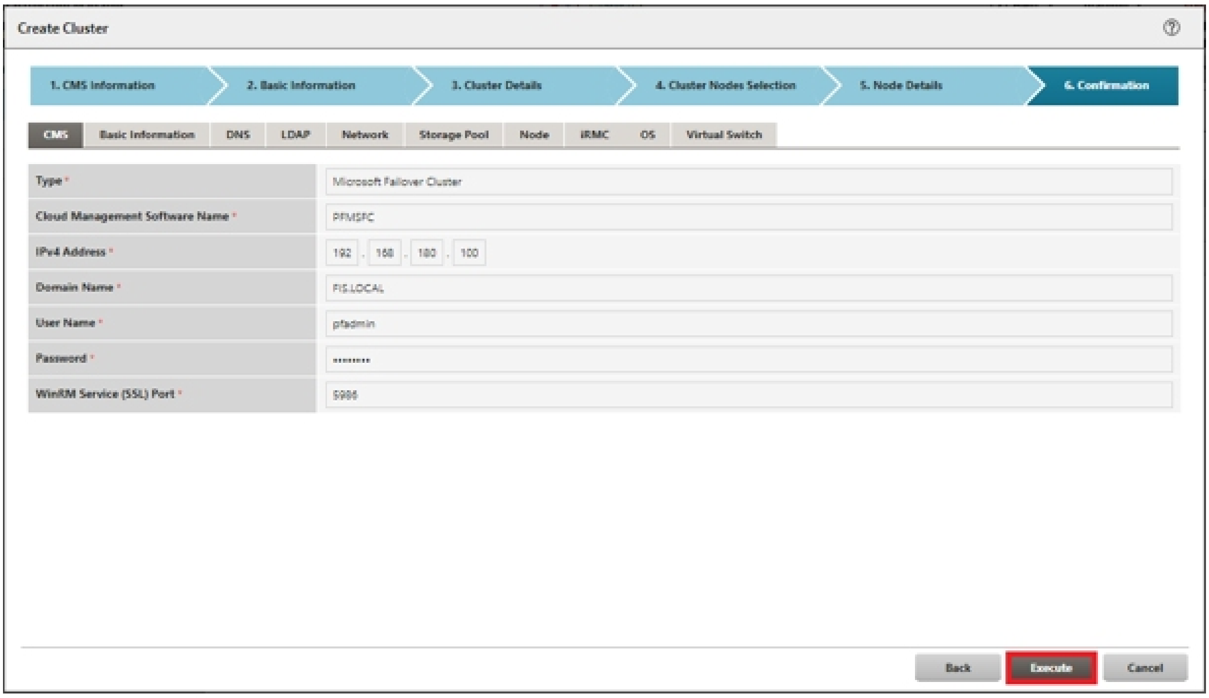
Please enter iRMC information.

No.	Node Name	Local User Settings	
		'admin' User	Administrator User *
1	hv-host5	New Password New Password (Confirmation)	User Name * Password * Password (Confirmation) *
2	hv-host6	New Password New Password (Confirmation)	User Name * Password * Password (Confirmation) *

Note

For details on Cluster Definition Parameters, refer to "Chapter 3 Setting Items Lists for Cluster Definition Parameters" in "ISM for PRIMEFLEX Parameter List."

10. Check the parameters on the "Confirmation" screen, then select the [Execute] button.

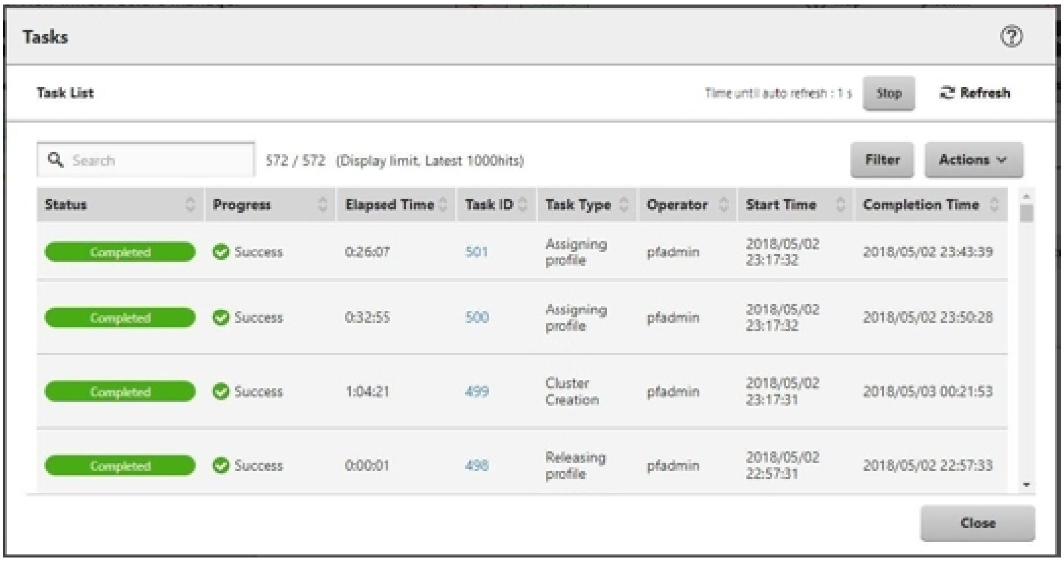


Create Cluster

Type *	Microsoft Failover Cluster
Cloud Management Software Name *	PFMSFC
IPv4 Address *	192 . 168 . 180 . 100
Domain Name *	FIS.LOCAL
User Name *	pfadmin
Password *	********
WinRM Service (SSL) Port *	5986

The execution of Cluster Creation is registered as an ISM task.

At the top of the Global Navigation Menu, select [Tasks], then the tasks in the task list displayed in the "Tasks" screen whose task type has become "Cluster Creation" are the Cluster Creation tasks.


Tasks
Task List
Time until auto refresh : 1 s
Stop
Refresh
Search
572 / 572 (Display limit, Latest 1000hits)
Filter
Actions
Close

Status	Progress	Elapsed Time	Task ID	Task Type	Operator	Start Time	Completion Time
Completed	Success	0:26:07	501	Assigning profile	pfadmin	2018/05/02 23:17:32	2018/05/02 23:43:39
Completed	Success	0:32:55	500	Assigning profile	pfadmin	2018/05/02 23:17:32	2018/05/02 23:50:28
Completed	Success	1:04:21	499	Cluster Creation	pfadmin	2018/05/02 23:17:31	2018/05/03 00:21:53
Completed	Success	0:00:01	498	Releasing profile	pfadmin	2018/05/02 22:57:31	2018/05/02 22:57:33

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, you must accept the conditions of the license.

Also, in order to ensure stable operation, apply the latest Windows update programs.

Execute the following Steps 12 to 26 within 180 minutes after completing profile assignment. Please 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.

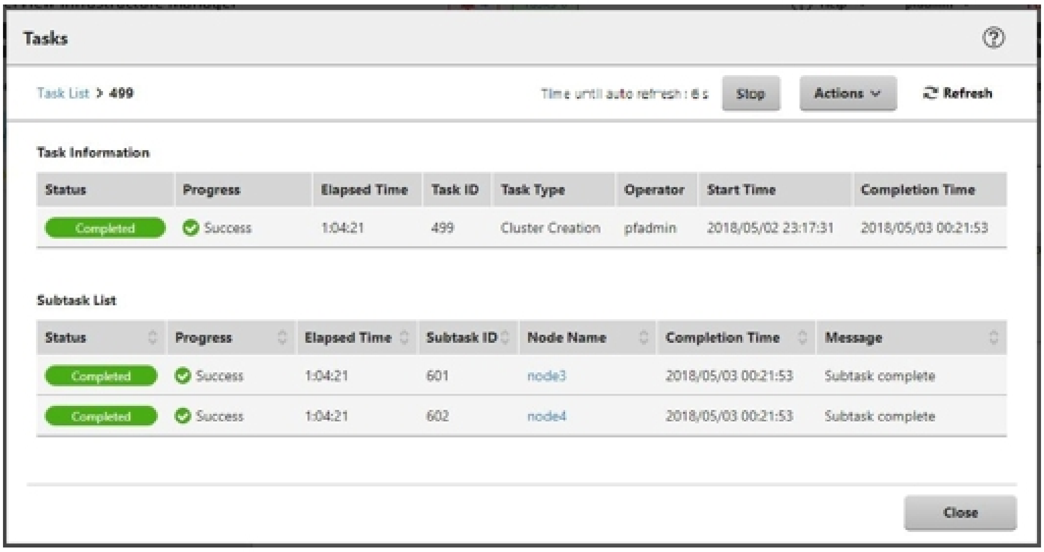
```
50215309: Subtask error : Failed to create cluster. An error occurred during the setting process
of the Cluster Creation task. (The task type setting process retried out; task type = Cluster
Creation; id = 20; task item set name = OS Installation; task item name = Wait Hyperv OS Boot;
detail code = E010205)
```

If Cluster Creation times out and finishes with an error, execute up to Step 26, and then execute Cluster Creation again.

Even if Cluster Creation times out and ends with an error during the execution of Step 12 to 26, continue and execute to Step 26.

Point

From the task list on the "Tasks" screen, select [Task ID] from "Cluster Creation," and then the "Tasks" screen of the "Cluster Creation" is displayed. In this screen, a subtask list is displayed for each server for creating a new cluster. You can check the progress status of each task by checking the message column.



Task Information

Status	Progress	Elapsed Time	Task ID	Task Type	Operator	Start Time	Completion Time
Completed	✓ Success	1:04:21	499	Cluster Creation	pfadmin	2018/05/02 23:17:31	2018/05/03 00:21:53

Subtask List

Status	Progress	Elapsed Time	Subtask ID	Node Name	Completion Time	Message
Completed	✓ Success	1:04:21	601	node3	2018/05/03 00:21:53	Subtask complete
Completed	✓ Success	1:04:21	602	node4	2018/05/03 00:21:53	Subtask complete

12. After the status of [Assigning profile] task turned to [Completed], display iRMC screen of the server for creating a new cluster to log in and select [Video Redirection].

    When the security warning is displayed, check [I accept the risk and want to run this application] and select the [Run] button.

    The Video redirection screen of the server is displayed.

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

    In the video redirection screen, do not select the [Restart system] button in the "ServerView Installation Manager" screen and do not restart Windows.

    It will not be possible to apply the Windows update program and Mellanox LAN driver.

16. Use a user with Administrator privileges on the remote desktop to access the Windows OS of the server for creating a new cluster.

    Note

    If an error message is displayed and you cannot connect while using remote desktop connection, the error could 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 remote desktop connection destination.

    https://blogs.technet.microsoft.com/mckittrick/unable-to-rdp-to-virtual-machine-credssp-encryption-oracle-remediation/

17. Transfer the latest Windows update program to the server for creating a new cluster.

18. If you are using a Mellanox LAN card and if the SVIM version used during construction is earlier than 12.08.04, transfer Mellanox LAN driver to the server for creating a new cluster.

    For the Mellanox LAN driver, download the driver package from the following website.

http://support.ts.fujitsu.com/

If you already applied the Mellanox LAN driver, this procedure is not required. Proceed to Step 19.

Point

You can check if Mellanox LAN driver is installed by checking that "MLNX_WinOF2" is "Installed" in [Control panel] - [Programs] - [Programs and Functions] - [Uninstall or Change programs].

Note

If you use a Mellanox LAN card, install the driver for the Mellanox LAN card in Step 20.

19. Apply the Windows update program transferred to the servers for creating a new cluster.

20. If you are using a Mellanox LAN card and if the SVIM version used during construction is earlier than 12.08.04, apply the Mellanox LAN driver transferred to the servers for creating a new cluster.

    If you already applied the Mellanox LAN driver, this step is not required. Proceed to Step 21.

21. 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.

22. If Server Manager is displayed at the front, minimize it to display the "ServerView Installation Manager" screen.

23. Select the [Restart system] button when the "ServerView Installation Manager" screen is displayed.

    The "Sign out" screen is displayed and the server is restarted.

24. After restarting, log in with a user that has Administrator privilege.

25. Delete the Windows update program transferred in Step 17.

26. Delete the Mellanox LAN driver transferred in Step 18.

27. Repeat Step 12 to 26 for all servers for creating a new cluster.

28. Check that the status of "Cluster Creation" has become "Completed."

Note

- If an error is displayed on the ISM "Tasks" screen, refer to "ISM for PRIMEFLEX Messages" and solve the error. Solve the error, then execute the operation again.

  If the OS installation with Profile Management of ISM (Assigning profile tasks) ends normally, do not power off the server for creation a new cluster when executing again.

- For the settings of the virtual network for service on the server for creating a new cluster, set them according to your environment.

- Do not execute Cluster Creation during execution of Firmware Rolling Update.

6.8.3 Follow-up Processing

This section describes the follow-up processing required after the cluster creation.

6.8.3.1 Refresh cluster information

Execute the settings to monitor new clusters with Cluster Management. After that, refresh the cluster information.

(1)Add the Service Principal Name for Active Directory

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>
```

(2) Configure Kerberos delegation for Active Directory

The Kerberos delegation of all servers for creating a new cluster is configured in Active Directory.

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, check the checkbox of [Trust this computer for delegation to any service (Kerberos only)] if it is not checked.
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 GUI of ISM, 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," then after waiting a while, refresh the ISM GUI screen (select the Refresh button on the top right side on the screen).
4. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Cluster].
5. 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 at the upper right side of the screen) and repeat until it is displayed.

6.8.3.2 Confirm Cluster Creation

Use the following procedure to check the status of Cluster Creation to the PRIMEFLEX for Microsoft Storage Spaces Direct.

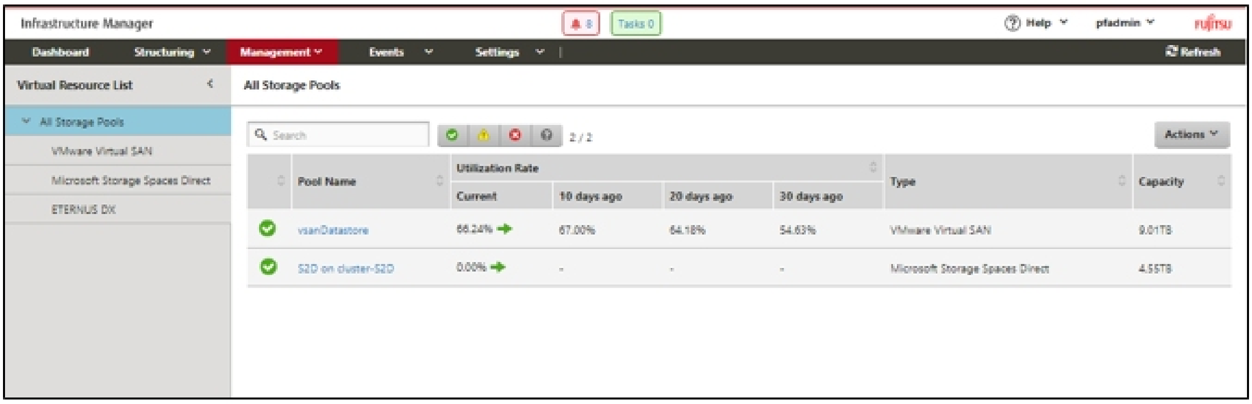
1. Access the Failover Cluster Manager and check that the created cluster is displayed in [<Cluster name>] - [Nodes]. Check the following points.

   - 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"

   Note

   If you cannot confirm the points above, collect maintenance data and contact your local Fujitsu customer service partner.

2. Access the GUI of ISM, and in the "All Storage Pool" screen in [Management] - [Virtual Resource], execute [Actions] - [Refresh Virtual Resource Information] to refresh. After refreshing, check that the target storage pool is displayed.



	Pool Name	Utilization Rate				Type	Capacity
		Current	10 days ago	20 days ago	30 days ago		
✓	vsanDatastore	66.24% →	67.00%	64.18%	54.63%	VMware Virtual SAN	9.01TB
✓	S2D on cluster-S2D	0.00% →	-	-	-	Microsoft Storage Spaces Direct	4.55TB

Note

- Even when the task completed successfully, if the storage pool is not displayed, communication for the PRIMEFLEX for Microsoft Storage Spaces Direct network could fail. Check the settings and the wiring of the switch.
- 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.

6.8.3.3 Register to the virtual switch for workload

Execute for all servers for creating a new cluster.

Set up a Service adapter. Open PowerShell from the command prompt with administrator privilege and execute the following commands.

```
>Add-VMNetworkAdapter -SwitchName <Virtual Switch Name> -Name "Service" -ManagementOS [Note 1]
>Set-VMNetworkAdapterVlan -VMNetworkAdapterName "Service" -VlanId <VLAN ID> -Access -ManagementOS
[Note 2]
>Set-VMNetworkAdapterTeamMapping -VMNetworkAdapterName "Service" -ManagementOS -
PhysicalNetAdapterName "Slot <Slot Number>  port 2" [Note 3]
>Set-VMNetworkAdapterTeamMapping -VMNetworkAdapterName "Service" -ManagementOS -
PhysicalNetAdapterName "Slot <Slot Number>  port 2" [Note 4]
```

[Note 1]: Specify the Virtual switch name of the production LAN in < Virtual Switch Name>.

[Note 2]: Specify the VLAN ID of the production LAN in <VLAN ID>.

[Note 3]: Specify the slot number of the network adapter name of the first PCI card set in the service adapter in <Slot Number>.

[Note 4]: Specify the slot number of the network adapter name of the second PCI card set in the service adapter in <Slot Number>.

Point

If the slot number is not known, check it using the following command.

```
> Get-NetAdapterHardwareInfo | select Name,InterfaceDescription,Slot,Function | Sort-Object Name
```

Example of command output

```
:Name                            InterfaceDescription                                  Slot Function
----                            --------------------                                  ---- --------
Onboard Flexible LOM port 1  Intel(rainbow)  Ethernet Connection X722 for 10GBASE-T             0
Onboard Flexible LOM port 2  Intel(rainbow)  Ethernet Connection X722 for 10GBASE-T #2          1
Onboard LAN port 1           Intel(rainbow)  I350 Gigabit Network Connection #2                 0
Onboard LAN port 2           Intel(rainbow)  I350 Gigabit Network Connection                    1
Slot 03 port 1               Intel(R) Ethernet Converged Network Adapter X550-T2 #4    3        0
Slot 03 port 2               Intel(R) Ethernet Converged Network Adapter X550-T2 #2    3        1
Slot 07 port 1               Intel(R) Ethernet Converged Network Adapter X550-T2       7        0
Slot 07 port 2               Intel(R) Ethernet Converged Network Adapter X550-T2 #3    7        1
```

6.8.3.4 Set a system volume name

Execute for all servers for creating a new cluster.

Set a system volume name to "system" according to the following procedure.

1. Log in to the host added when configuring a new cluster.
2. Start the explorer, select C drive and right-click to select [Change name].
3. Enter "system" to the drive name.
4. Repeat Step 1 to 3 for all the hosts.

6.8.3.5 Set the browser for the servers for creating a new cluster

To execute Monitoring of SSD lifetime in ServerView RAID Manager, you must set a browser for the servers for creating a new cluster.

Refer to "2.2.1 Client/Browser Settings" in "FUJITSU Software ServerView Suite ServerView RAID Manager" and set up the web browser of the server for creating a new cluster.

6.8.3.6 Delete unnecessary files

Delete unnecessary files with the following procedure after competing Cluster Creation.

(1) Deleting certificates

The certificates created in "6.8.1.1 Create certificates for servers for creating a new cluster" are transferred and registered to the servers for creating a new cluster when installing OS. Use the following procedure to delete the certificate.

Execute for all servers for creating a new cluster.

1. Use remote desktop to access the Windows OS of the server for creating a new cluster.
2. Open Explorer and delete the following files.
    - C:\PostInstall\UserApplication\postscript_ClusterOperation\<certificate file name.cer>
    - C:\PostInstall\UserApplication\postscript_ClusterOperation\<service certificate file name.pfx>
    - C:\DeploymentRepository\Add-on\UserApplication\postscript_ClusterOperation\<certificate file name.cer>
    - C:\DeploymentRepository\Add-on\UserApplication\postscript_ClusterOperation\<service certificate file name.pfx>

Note

The certificates uploaded to ISM-VA in "6.8.1.1 Create certificates for servers for creating a new cluster" have security risks. If you cannot accept this risk, delete the certificate.

(2) Deleting unnecessary files of the server for creating a new cluster

Execute for all servers for creating a new cluster.

1. Use remote desktop to access the Windows OS of the server for creating a new cluster.
2. Open Explorer and delete all files and directories under the following directories.
    - C:\PostInstall\UserApplication\postscript_ClusterOperation
    - C:\FISCRB\PowershellScript
    - C:\FISCRB\log

(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 the unnecessary files, checking the following items and referring to "2.9 Delete Files Uploaded to ISM-VA."

Item	Value
Root Directory	Administrator/ftp
Directory Name	postscript_ClusterOperation
File Name	The certificate created in (1) in "6.8.1.1 Create certificates for servers for creating a new cluster"

6.9 Expand a Cluster for PRIMEFLEX HS/PRIMEFLEX for VMware vSAN

This section describes the Cluster Expansion procedure for PRIMEFLEX HS/PRIMEFLEX for VMware vSAN.

This function can be used only with the license for ISM for PRIMEFLEX.

Cluster Expansion is executed according to the following work flow.

Table 6.16 Work flow for Cluster Expansion

Cluster Expansion procedure		Tasks
1	Preparations	- vCenter Server VMware EVC settings - Creating ADVM certificates - Registering host records in DNS - DHCP settings - Importing the ISO image of the OS installation media to ISM-VA - Upload of the VMware ESXi patch file. - Upload of VMware SMIS Provider - Creating profiles - Creating and editing Cluster Definition Parameters - Installation and Wiring - Setting the IP address of iRMC - BIOS settings - Registering nodes in ISM
2	Execute Cluster Expansion	
3	Follow-up processing	- Confirmation of the cluster expansion - Restrictions/Precautions for VMware vSphere

Cluster Expansion procedure		Tasks
		- Registering in ServerView RAID Manager - Deleting unnecessary files

Note

PRIMERGY M5 series is available in ISM 2.4.0.c or later.

6.9.1 Preparations

This section describes the preparations required before the cluster expansion.

6.9.1.1 Set up vCenter Server VMware EVC

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 VMware EVC (Enhanced vMotion Compatibility) function.

Note

- You must set VMware EVC mode before using a successor server to expand a PRIMEFLEX vSAN cluster.

  To set VMware EVC mode after you have added a successor server to the cluster, you must stop all virtual machines in the vSAN cluster after migrating vCSA out of the vSAN cluster.

- 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 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 version that supports the CPU generations in advance.

  https://kb.vmware.com/s/article/1003212

  Example: vCSA 6.5 or later is required for the PRIMERGY M2 series (Intel (R) "Broadwell" Generation).

Set VMware EVC according to the following procedure.

1. Access vSphere Web Client, and select the "Top" screen - [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Configure] - [Configuration] - [VMware EVC] - [Edit the EVC configuration of the cluster].

2. On the screen to change the EVC mode, select the [Enable EVC for Intel(R) Hosts] check box 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

3. Select the [OK] button.

6.9.1.2 Create ADVM certificates

This setting is required only when configuring an ADVM dedicated to PRIMEFLEX HS/PRIMEFLEX for VMware vSAN, and the first time Cluster Expansion is used.

Certificate registration is required because Cluster Expansion makes settings to ADVM from ISM with SSL encrypted communication.

For ADVM#1 and ADVM#2, follow the following operations flow and register authentication for SSL communication and execute the settings to permit communication.

Cluster Expansion can be used without using SSL encrypted communication. In this case, this setting is not required. Proceed to "6.9.1.3 Register host records in DNS."

Note

- If using 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.
- The settings depending on whether you use SSL encrypted communication or not are as follows.
  - Use SSL encrypted communication

    Enter the [Cluster] - [DNS Information] - [WinRM Service (SSL) Port Number] of Cluster Definition Parameters and set it so that communication between ADVM and WinRM is done with SSL.
  - Do not use SSL encrypted communication

    Enter the [Cluster] - [DNS Information] - [WinRM Service Port Number] of Cluster Definition Parameters and set it so that communication between ADVM and WinRM does not use SSL.

  For details on Cluster Definition Parameters, refer to "Chapter 3 Setting Items Lists for Cluster Definition Parameters" in "ISM for PRIMEFLEX Parameter List."
- If an error message is displayed and you cannot connect while using remote desktop connection, the error could 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 remote desktop connection destination.

  https://blogs.technet.microsoft.com/mckittrick/unable-to-rdp-to-virtual-machine-credssp-encryption-oracle-remediation/

- 6.9.1.2.1 Check WinRM service startup
- 6.9.1.2.2 Set up WinRM service
- 6.9.1.2.3 Open the port of the firewall
- 6.9.1.2.4 Change the Windows PowerShell script execution policy

6.9.1.2.1 Check 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 might 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.

6.9.1.2.2 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, which means 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 as that 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 file 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)

(3-1) Creating certificate and private key file

Open the command prompt (administrator) on the management terminal and execute the following command.

This is a command example where the target ADVM server name is "192.168.10.10" and the certificate expiration date is March 30, 2018.

```
>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 <file name of the certificate file.cer> -sv <file name of the private
key.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 <file name of the certificate file.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 <file name of the certificate
file.cer> -pfx <file name of the service certificate.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 <file name of the service certificate.pfx>.

```
>dir
```

Note

Create two certificates for ADVM#1 and ADVM#2.

(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 [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 <name of certificate file.cer>

   [Console Root] - [Certificate (local computer)] - right click on [Trusted Root Certification Authorities]. From [All tasks] - [Import], select <name of certificate file.cer> and close the "Certificate Import Wizard" screen.

2. Check that <name of certificate file.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 <name of service certificate file.pfx> as personal.

   [Console root] - [Certificate (local computer)] - right click on [Personal]. From [All tasks] - [Import], select the <name of service certificate file.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 <name of service certificate file.pfx> file, you must specify it from the pull-down.

4. Check that the <Name of service certificate file.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) Register 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 "6.9.1.2.2 Set up WinRM service," replacing ADVM#1 to ADVM#2.

6.9.1.2.3 Open the port of the firewall

To enable 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 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 of the 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 "6.9.1.2.3 Open the port of the firewall" to ADVM#2 as well, replacing ADVM#1 to ADVM#2.

6.9.1.2.4 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 "6.9.1.3 Register host records in DNS" or "6.9.1.4 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

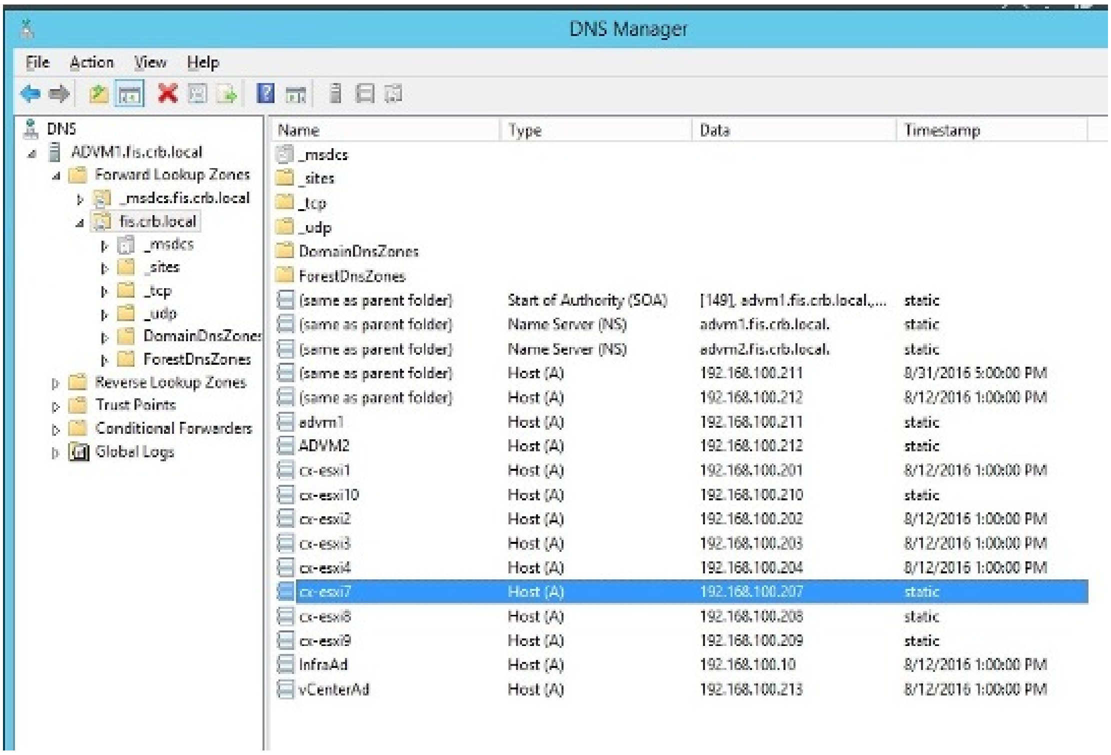
Execute "6.9.1.2.4 Change the Windows PowerShell script execution policy" to ADVM#2 as well, replacing ADVM#1 to ADVM#2.

6.9.1.3 Register host records in DNS

This section is required only when you use DNS servers already setup in your environment. Before executing OS installation, make sure that name resolution is possible for the servers for expanding a cluster used for DNS forward lookup zones and reverse lookup zones.

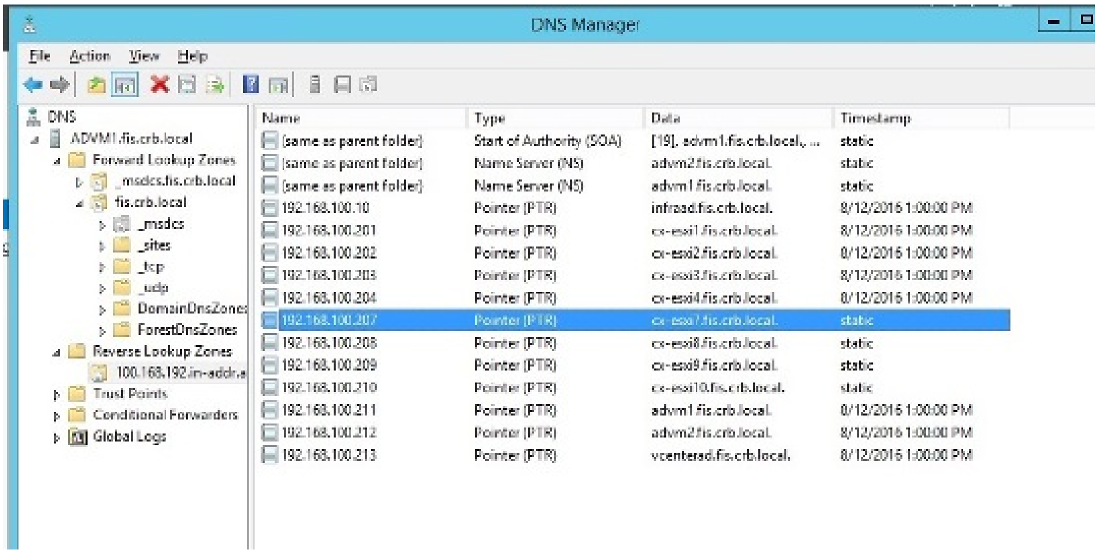
If there are multiple servers for expanding a cluster, create parameters for all the servers to be added.

Figure 6.6 Example for registration of forward lookup zones



Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[149], advm1.fis.crb.local.,...	static
(same as parent folder)	Name Server (NS)	advm1.fis.crb.local.	static
(same as parent folder)	Name Server (NS)	advm2.fis.crb.local.	static
(same as parent folder)	Host (A)	192.168.100.211	8/31/2016 5:00:00 PM
(same as parent folder)	Host (A)	192.168.100.212	8/12/2016 1:00:00 PM
advm1	Host (A)	192.168.100.211	static
ADVM2	Host (A)	192.168.100.212	static
cx-esxi1	Host (A)	192.168.100.201	8/12/2016 1:00:00 PM
cx-esxi10	Host (A)	192.168.100.210	static
cx-esxi2	Host (A)	192.168.100.202	8/12/2016 1:00:00 PM
cx-esxi3	Host (A)	192.168.100.203	8/12/2016 1:00:00 PM
cx-esxi4	Host (A)	192.168.100.204	8/12/2016 1:00:00 PM
cx-esxi7	Host (A)	192.168.100.207	static
cx-esxi8	Host (A)	192.168.100.208	static
cx-esxi9	Host (A)	192.168.100.209	static
InfraAd	Host (A)	192.168.100.10	8/12/2016 1:00:00 PM
vCenterAd	Host (A)	192.168.100.213	8/12/2016 1:00:00 PM

Figure 6.7 Example for registration of reverse lookup zones



Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[19], advm1.fis.crb.local., ...	static
(same as parent folder)	Name Server (NS)	advm2.fis.crb.local.	static
(same as parent folder)	Name Server (NS)	advm1.fis.crb.local.	static
192.168.100.10	Pointer (PTR)	infraad.fis.crb.local.	8/12/2016 1:00:00 PM
192.168.100.201	Pointer (PTR)	cx-esxi1.fis.crb.local.	8/12/2016 1:00:00 PM
192.168.100.202	Pointer (PTR)	cx-esxi2.fis.crb.local.	8/12/2016 1:00:00 PM
192.168.100.203	Pointer (PTR)	cx-esxi3.fis.crb.local.	8/12/2016 1:00:00 PM
192.168.100.204	Pointer (PTR)	cx-esxi4.fis.crb.local.	8/12/2016 1:00:00 PM
192.168.100.207	Pointer (PTR)	cx-esxi7.fis.crb.local.	static
192.168.100.208	Pointer (PTR)	cx-esxi8.fis.crb.local.	static
192.168.100.209	Pointer (PTR)	cx-esxi9.fis.crb.local.	static
192.168.100.210	Pointer (PTR)	cx-esxi10.fis.crb.local.	static
192.168.100.211	Pointer (PTR)	advm1.fis.crb.local.	8/12/2016 1:00:00 PM
192.168.100.212	Pointer (PTR)	advm2.fis.crb.local.	8/12/2016 1:00:00 PM
192.168.100.213	Pointer (PTR)	vcenterad.fis.crb.local.	8/12/2016 1:00:00 PM

6.9.1.4 Set up DHCP

For Cluster Expansion, execute OS installation by using profile assignment. To execute OS installation with profile assignment, DHCP servers are 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."

If there are multiple servers for expanding a cluster, set it so that multiple leases are possible.

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 operation is in progress.
- Since the management network is made redundant in the configuration of this product, IP addresses are leased to multiple ports. Execute the settings so that there are always IP addresses that can be leased.
- 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."

6.9.1.5 Import the ISO image of the OS installation media to ISM-VA

Import the ServerView Suite DVD and the installation media into ISM.

If you are going to use existing installation media, the import is not required.

For information on import operations, refer to "2.13.2 Repository Management" in "User's Guide."

For the support version, refer to "Setting Items for Profile Management."

Add ISM-VA virtual disks as required. For information on the procedure to add virtual disks, refer to "3.7 Allocation of Virtual Disks" in "User's Guide."

6.9.1.6 Upload the VMware ESXi patch file

Execute this when you want to apply the VMware ESXi patch by using Cluster Expansion. When you upload the VMware ESXi patch file, the processing of patch application will be executed.

Execute the operations depending on your environment so that the version of VMware ESXi of the new cluster becomes the same version as that of the existing cluster.

Add ISM-VA virtual disks as required. 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 Expansion ends with an error.
- Do not decompress uploaded VMware ESXi patch file (zip file). If you decompress, Cluster Expansion ends with an error.

Upload the VMware ESXi patch file, checking the following items and referring to "2.8 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 1] Example: ESXi650-201704001.zip

[Note 1]: Upload the VMware ESXi patch file without renaming it.

6.9.1.7 Upload VMware SMIS provider

This is the required operation when the servers for expanding a cluster 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

- Offline bundle example:

  VMW-ESX-5.5.0-lsiprovider-500.04.V0.63-0005-offline_bundle-5240997.zip

Add ISM-VA virtual disks as required. 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 Expansion ends with an error.
- Do not decompress the uploaded offline bundle (zip file) of the VMware SMIS Provider. If you decompress, Cluster Expansion ends with an error.

Upload the offline bundle of the VMware SMIS Provider, checking the following items and referring to "2.8 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 1] Example: VMW-ESX-5.5.0-lsiprovider-500.04.V0.63-0005-offline_bundle-5240997.zip

[Note 1]: Upload the offline bundle of the VMware SMIS Provider file without renaming it.

6.9.1.8 Create a profile

Use ISM Profile Management to add the profiles for the servers for expanding a cluster. Create profiles by creating references from existing profiles.

Note

If there are multiple servers for expanding a cluster, create profiles for all the servers for expansion.

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Profiles].
2. Select the current profile to be used to create a reference, from the [Actions] button, select [Duplicate Profile].
3. Set each item.

   Point

   For profile creation, refer to "3.3 Execute Settings on a Server/Install Server OS."

   Note

   - Do not check the following items.
     - In the [OS] tab, [Network] - [Setup]
     - In the [OS] tab, [Register to Cloud Management Software]
     - In the [OS (for each node)] tab, [DHCP]
   - For PRIMERGY M2 series, do not check the following items.
     - In the [OS] tab, [Network port specification]
   - For PRIMERGY M4 series/PRIMERGY M5 series, set the following in the [OS] tab - [Management LAN network port settings] items
     - Check [Network port specification]
     - For [Method to specify], select [MAC Address].
     - For [MAC Address], specify a MAC address with port 0 of the port expansion option with 10 Gbps communication available
   - 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]
   - The following item is automatically set by Cluster Expansion. If you select the item before Cluster Expansion is executed, it will not cause any errors but the setting value will be overwritten during the execution of Cluster Expansion.
     - In the [OS] tab, [Execute Script after Installation]

6.9.1.9 Create and edit Cluster Definition Parameters

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 GUI of ISM, select [Management] - [Cluster] - [<Target Cluster>] - [Cluster Definition Parameters] tab.

- If creating a new one

  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 Setting Items Lists for Cluster Definition Parameters" in "ISM for PRIMEFLEX Parameter List."

6.9.1.10 Execute installation and wiring

Install a server for expanding a cluster at its physical location and connect the cables. For details, refer to the "Operating Manual" of the server for Cluster Expansion. Execute the settings for your network switches as appropriate, referring to the manual of the switches.

If there are multiple servers for expanding a cluster, create parameters for all the servers to be added.

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 "6.9.1.11 Set the IP address of iRMC."

- For Auto Discovery of nodes

  Execute "Node registration using Auto Discovery" in "6.9.1.13 Register a node to ISM."

6.9.1.11 Set the IP address of iRMC

When you register a server for expanding a cluster by using Manual Discovery, set the static IP address to the iRMC.

Boot the BIOS of the server for expanding a cluster, and on the "BIOS setup" screen, set a static IP address. To execute this operation, you must execute "6.9.1.10 Execute installation and wiring." Moreover, to display and operate the "BIOS setup" screen, connect a display and keyboard to the server for Cluster Expansion.

For information on booting the BIOS and setting the IP address for the iRMC, refer to the "BIOS Setup Utility Reference Manual" of the server for expanding a cluster.

If there are multiple servers for expanding a cluster, specify parameters for all the servers to be added.

Also, execute "6.9.1.12 Set up BIOS" as well as setting of the IP address.

You can obtain the "BIOS Setup Utility Reference Manual" for each server for expanding a cluster from the following website:

http://manuals.ts.fujitsu.com/index.php?l=en

6.9.1.12 Set up BIOS

Specify the BIOS settings.

When you select "For Manual Discovery of nodes" in "6.9.1.10 Execute installation and wiring," set this item together with "6.9.1.11 Set the IP address of iRMC."

When you select "For Auto Discovery of nodes" in "6.9.1.10 Execute installation and wiring," you can set BIOS settings remotely with iRMC Video Redirection. Start BIOS, then specify the following settings from the "BIOS setup" screen.

If there are multiple servers for expanding a cluster, create parameters for all the servers to be added.

Table 6.18 BIOS settings

Item		Setting Value
Server Mgmt - iRMC LAN Parameters Configuration [Note 1]	iRMC IPv6 LAN Stack	Disabled
Advanced - CPU Configuration [Note 1]	Override OS Energy Performance	Enabled
	Energy Performance	Performance
	Package C State Limit	C0
Advanced - Network Stack Configuration [Note 1]	Network Stack	Enabled
	IPv6 PXE Support	Disabled
Management - iRMC LAN Parameters Configuration [Note 2]	iRMC IPv6 LAN Stack	Disabled
Configuration - CPU Configuration [Note 2]	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
Configuration - UEFI Network Stack Configuration [Note 2]	Network Stack	Enabled
	IPv6 PXE Support	Disabled

[Note 1]: This item is displayed for the "BIOS setup" screen of the PRIMERGY RX M4 series/PRIMERGY RX M5 series.

[Note 2]: This item is displayed for the "BIOS setup" screen of the PRIMERGY CX M4 series/PRIMERGY CX M5 series.

When you select "For Manual Discovery of nodes" in "6.9.1.10 Execute installation and wiring" continue to execute "Node registration using Manual Discovery" in "6.9.1.13 Register a node to ISM."

When you select "For Auto Discovery of nodes" in "6.9.1.10 Execute installation and wiring," continue to execute "6.9.2 Execute Cluster Expansion."

6.9.1.13 Register a node to ISM

In order to use ISM to install OS, register the server for expanding a cluster in ISM.

To register a node to the ISM, you can use both Manual Discovery and Auto Discovery. Register all servers for expanding a cluster.

Point

- When you register a node in ISM, you must enter the iRMC user name and password for the servers for expanding a cluster. 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 Install ISM."
- For node registration, refer to "2.2.1.2 Registration of nodes" or "2.2.1.6 Discovery of nodes" in "User's Guide."

Node registration using Manual Discovery

For the procedure for registering a node with Manual Discovery, refer to "3.1.2 Register a Node Directly."

Specify the IP address set in "6.9.1.11 Set the IP address of iRMC" when registering.

If there are multiple servers for expanding a cluster, you can register them at the same time by specifying an IP address range.

Continue to execute "6.9.2 Execute 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."

Set the static IP address of the iRMC on the "Node Registration" wizard.

Continue to execute "6.9.1.12 Set up BIOS."

6.9.2 Execute Cluster Expansion

By executing Cluster Expansion, you can expand a cluster in the virtualized platform.

6.9.2.1 Operation requirements for Cluster Expansion

To use Cluster Expansion, the following requirements must be met.

- Check the following requirements before executing it.
    - That the AD, DNS, and NTP are all running normally and can be used
    - 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 cluster is operating normally
    - That the type of servers for expanding a cluster are the same

    Point

    For successor cluster expansion, refer to "Appendix D Successor Cluster Expansion" in "User's Guide."

    - That you register the server for expanding a cluster in AD in advance when configuring an AD that already exist in your environment, since registering a computer in AD is restricted by policies etc.
    - That the physical NIC of the server for expanding a cluster using the storage network is 10 GbE
    - That the port of the physical switch using the storage network is 10 GbE
    - That the settings of [Add disks to storage] is confirmed

      If "Automatic" selected, disks will be added to vSAN storage automatically.

      If "Manual" selected, add disks manually after completing expansion.

      To check the settings, access vSphere Web Client and select "Top" screen - [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Configure] - [vSAN] - [General] - [Add disks to storage].
    - 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 might occur after executing Cluster Expansion.
    - 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

    - A profile has been created for the server for expanding a cluster in Profile Management of ISM

    - Cluster Definition Parameters have been set

      For details, refer to "6.9.1.9 Create and edit Cluster Definition Parameters."

    - The power of the server for expanding a cluster is off

      Note

      The following is an operation requirement when executing Cluster Expansion again with the OS installation completed using profile assignment.

        - The power of the server for expanding a cluster is on

      To check if the OS installation has been completed, use the following procedure.

      1. At the top of the Global Navigation Menu, 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."

    - The SSD capacity device fulfill the following specifications when using an All Flash configuration

      PRIMEFLEX HS: If the size is another than 160 - 210 GB, 320 - 420 GB

      PRIMEFLEX for VMware vSAN: If the two types of SSD, cache and capacity, is the one with the highest number of devices (if the number of SSDs is the same, it should be the largest one)

    - The computer name of the servers for expanding a cluster 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 servers for expanding a cluster which you specify in the profile must be unique among all IP addresses of the OS of the nodes managed by ISM.

    - On the "Cluster Details" screen in the "Expand Cluster" wizard, [Storage Pool Name] on the [Storage Pool] tab does not overlap the [Storage Pool Name] of an existing cluster

    - On the "Cluster Details" screen in the "Expand Cluster" wizard, [Port Group Name] on the [Network] tab does not overlap the [Port Group Name] of an existing cluster when creating a new vDS

- Confirm the current vSAN storage capacity in advance. For the procedure to confirm, refer to "6.9.3.1 Confirm Cluster Expansion."

- To use Cluster Expansion, you must set Virtual Resource Management to the cluster to be expanded.

  For settings of Virtual Resource Management, refer to "3.9 Pre-Settings for Cluster Management" in "User's Guide."

6.9.2.2 Cluster Expansion procedure

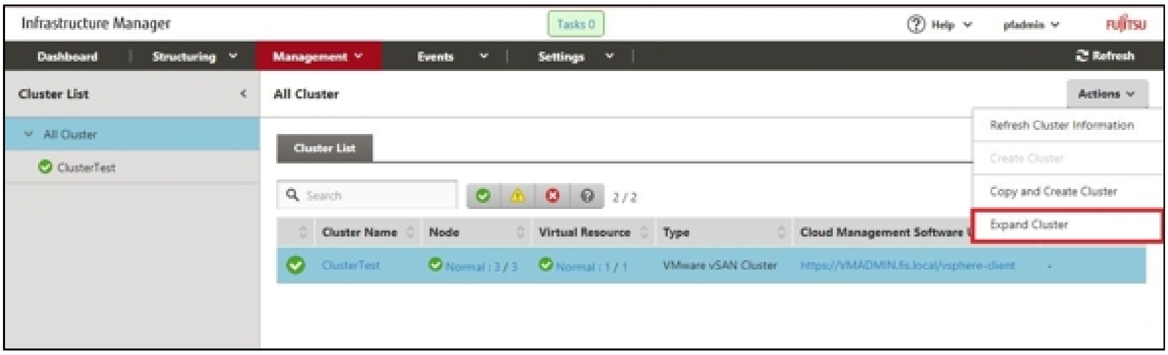
This section describes the procedure for executing Cluster Expansion of ISM for PRIMEFLEX.

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 GUI of ISM, select [Management] - [Cluster].

   The "Cluster List" screen is displayed.

3. Select [<Target cluster>] from the [Actions] button, select [Expand Cluster].

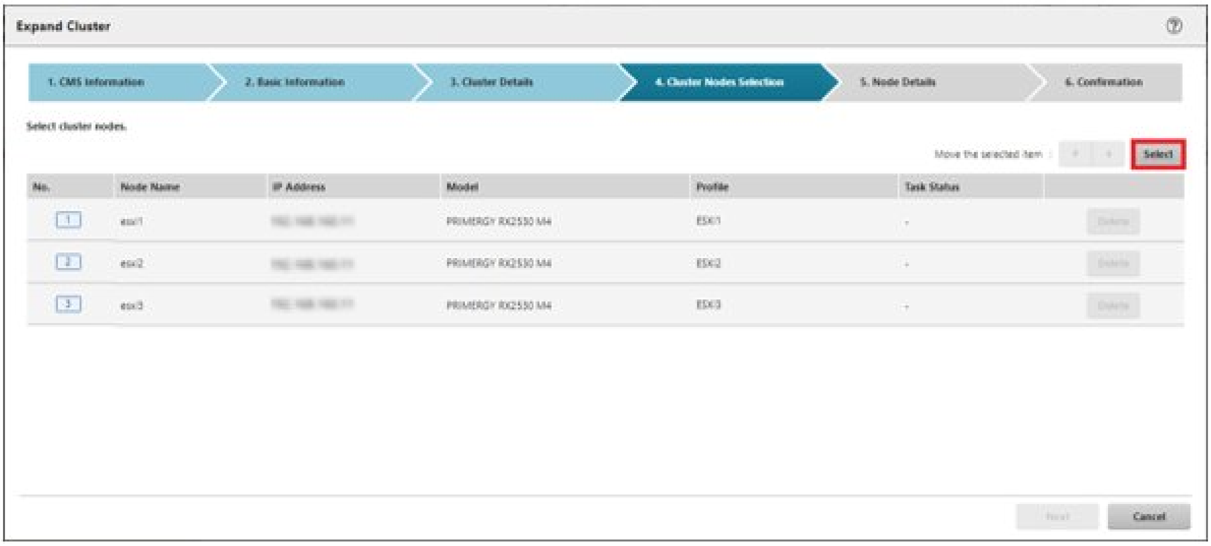


	Cluster Name	Node	Virtual Resource	Type	Cloud Management Software
✓	ClusterTest	✓ Normal : 3 / 3	✓ Normal : 1 / 1	VMware vSAN Cluster	https://VMADMIN.fis.local/vsphere-client -

The "Expand Cluster" wizard is displayed.

4. Select the [Select] button in the "Cluster Nodes Selection" screen, and then on the displayed "Target nodes selection" screen, select the server for expanding a cluster.

   If executing again, this procedure is not required. Select the [Next] button and proceed to Step 6.



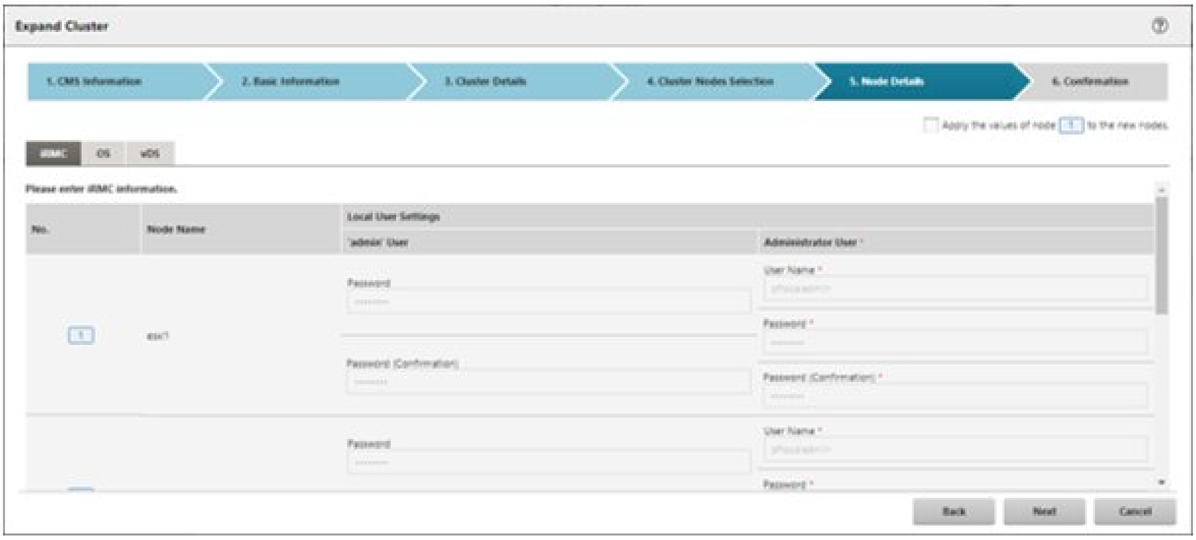
Select cluster nodes.

No.	Node Name	IP Address	Model	Profile	Task Status	
1	esxi1	[redacted]	PRIMERGY RX2530 M4	ESXi1	-	Delete
2	esxi2	[redacted]	PRIMERGY RX2530 M4	ESXi2	-	Delete
3	esxi3	[redacted]	PRIMERGY RX2530 M4	ESXi3	-	Delete

5. If a profile has not been assigned to the server for expanding a cluster, select the [Select] button in the [Profile] item and then select the profile to be assigned.

6. Enter each parameter of the server for expanding a cluster on the "Node Details" screen.

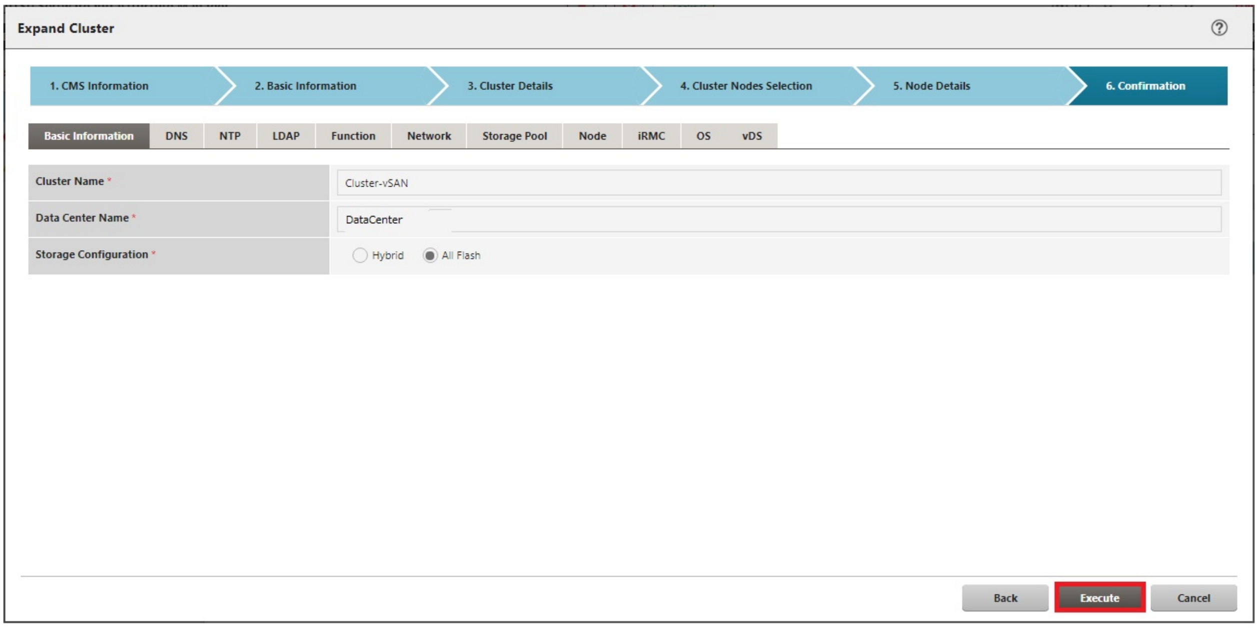
   If executing again, select the [Next] button if no parameters must be entered again and proceed to Step 7.



Note

For details on Cluster Definition Parameters, refer to "Chapter 3 Setting Items Lists for Cluster Definition Parameters" in "ISM for PRIMEFLEX Parameter List."

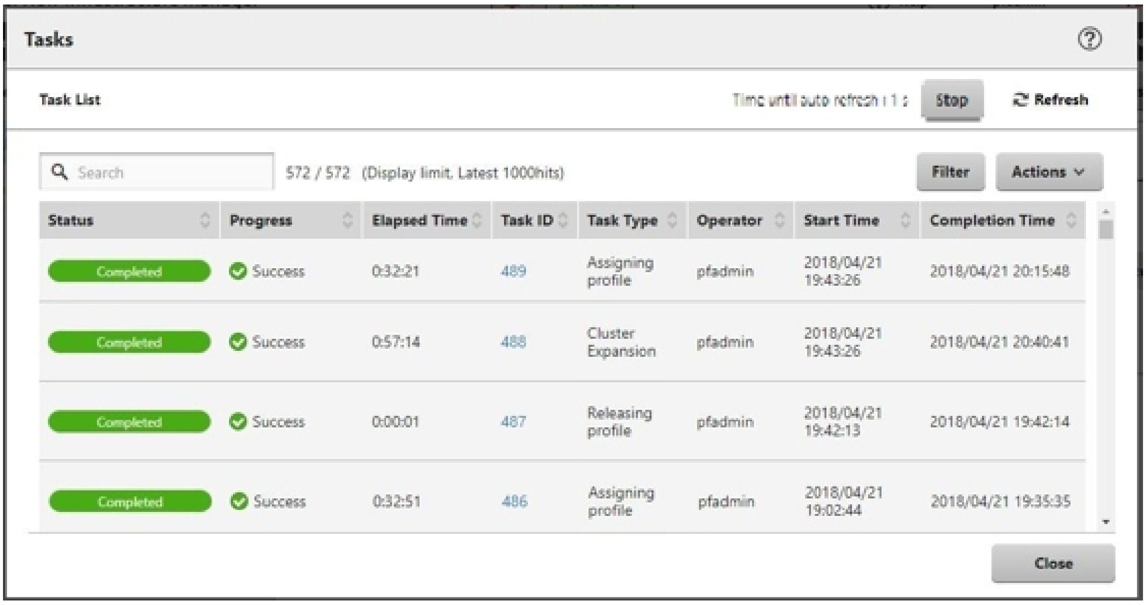
7. Check the parameters on the "Confirmation" screen, then select the [Execute] button.



Cluster Name *	Cluster-vSAN
Data Center Name *	DataCenter
Storage Configuration *	○ Hybrid ● All Flash

The execution of Cluster Expansion is registered as an ISM task.

At the top of the Global Navigation Menu, select [Tasks], then the tasks in the task list displayed in the "Tasks" screen whose task type has become "Cluster Expansion" are the Cluster Expansion tasks.



Tasks

Task List

Time until auto refresh : 1 s Stop Refresh

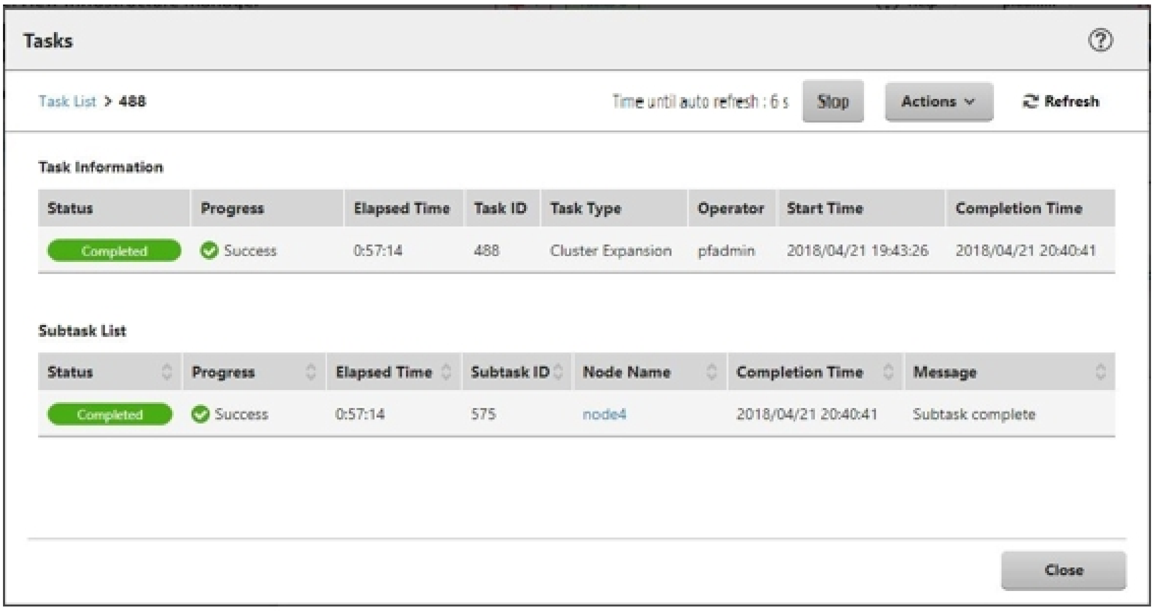
Search 572 / 572 (Display limit. Latest 1000hits) Filter Actions

Status	Progress	Elapsed Time	Task ID	Task Type	Operator	Start Time	Completion Time
Completed	Success	0:32:21	489	Assigning profile	pfadmin	2018/04/21 19:43:26	2018/04/21 20:15:48
Completed	Success	0:57:14	488	Cluster Expansion	pfadmin	2018/04/21 19:43:26	2018/04/21 20:40:41
Completed	Success	0:00:01	487	Releasing profile	pfadmin	2018/04/21 19:42:13	2018/04/21 19:42:14
Completed	Success	0:32:51	486	Assigning profile	pfadmin	2018/04/21 19:02:44	2018/04/21 19:35:35

Close

Point

From the task list on the "Tasks" screen, select [Task ID] from "Cluster Expansion," and then the "Tasks" screen of the "Cluster Expansion" is displayed. In this screen, a subtask list is displayed for each server for expanding a cluster. You can check the progress status of each task by checking the message column.



Tasks

Task List > 488

Time until auto refresh : 6 s Stop Actions Refresh

Task Information

Status	Progress	Elapsed Time	Task ID	Task Type	Operator	Start Time	Completion Time
Completed	Success	0:57:14	488	Cluster Expansion	pfadmin	2018/04/21 19:43:26	2018/04/21 20:40:41

Subtask List

Status	Progress	Elapsed Time	Subtask ID	Node Name	Completion Time	Message
Completed	Success	0:57:14	575	node4	2018/04/21 20:40:41	Subtask complete

Close

8. Check that the status of "Cluster Expansion" has become "Completed."

Note

- If an error is displayed on the ISM "Tasks" screen, refer to "ISM for PRIMEFLEX Messages" and solve the error. Solve the error, then execute the operation again.

  If the OS installation with Profile Management of ISM (Assigning profile tasks) ends normally, do not power off the server for expanding a cluster when executing again.

- For the settings of the virtual network for service on the server for expanding a cluster according to your environment.

- Do not execute Cluster Expansion during execution of Firmware Rolling Update.

6.9.3 Follow-up processing

This section describes the follow-up processing required after the cluster expansion.

6.9.3.1 Confirm Cluster Expansion

Confirm the cluster expansion to vSAN with the following procedure.

1. Confirm that the disks of the server for expanding a cluster 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.

   Sometimes a warning may be issued 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 vSAN6.6.1 environment (VMware ESXi 6.5 Update 1), health errors and the countermeasures are described below.

   - Virtual SAN Disk Balance

     Execute proactive balancing for the disks.

   - 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 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

   - To check the fault domain host of the server for expanding a cluster, from the "Top" screen, select the [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Settings] - [Fault Domains & Stretched Cluster] - [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 servers configuring a current cluster or servers for expanding a cluster. If the result of checking is that they overlap, refer to "3.16 Action Examples for when a Cluster Expansion Error Occurs" - "Actions example 19" in "ISM for PRIMEFLEX Messages" and take the action.

- When the setting in [Add disks to storage] is "Manual," the disks of the server for expanding a cluster are not displayed on the "Top" screen - [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Monitor] - [vSAN] - [Physical Disk].

  Add disks manually.

  To check the settings, access vSphere Web Client and from the "Top" screen, select the [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Configure] - [vSAN] - [General] - [Add disks to storage].

  If you want to add disks manually, follow the procedure below. Execute for all servers for expanding a cluster.

  1. Log in to vCSA with vSphere Web Client.

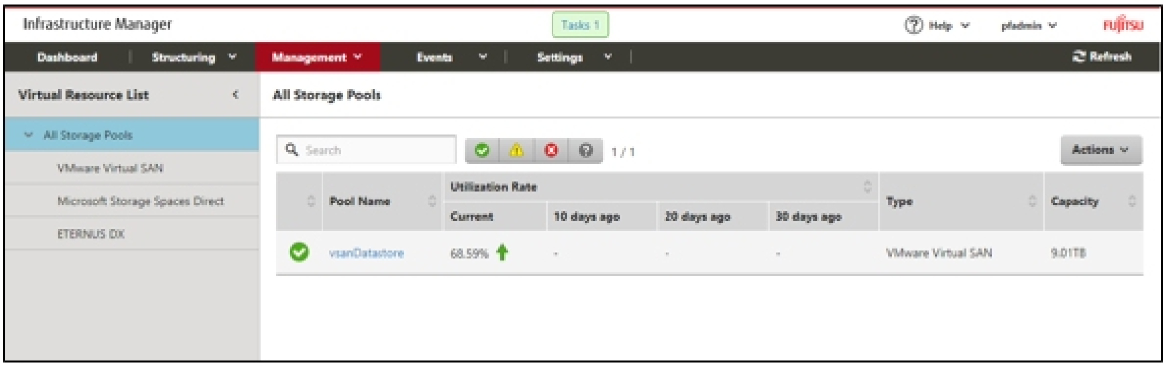
  2. From the "Top" screen, select [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster Name>] - [Configure] - [Disk Management].

  3. Select the server for expanding a cluster, and then select [Create Disk Group].

  4. On the "Create Disk Group" screen, select "disk to serve as cache tier" and "disk to serve as capacity tier," and then select the [OK] button.

     When the task is complete, the disk addition is complete.

2. Access the GUI of ISM, and in the "All Storage Pool" screen in [Management] - [Virtual Resource], execute [Actions] - [Refresh Virtual Resource Information] to refresh. After the update, confirm that the [Capacity] of the target vSAN datastore has increased.



All Storage Pools

	Pool Name	Utilization Rate				Type	Capacity
		Current	10 days ago	20 days ago	30 days ago		
✓	vsanDatastore	68.59% ↑	-	-	-	VMware Virtual SAN	9.01TB

Note

Even when the task completed successfully, if the previously checked vSAN storage has not been expanded, the following causes can be thought.

- Communication for the vSAN network failed

  Check the settings and the wiring of the switch.

- The setting of [Add disks to storage] is "Manual"

  Add disks manually.

  To check the settings, access vSphere Web Client and from the "Top" screen, select the [Home] tab - [Inventories] - [Hosts and Clusters] - [<Cluster name>] - [Configure] - [vSAN] - [General] - [Adds disks to storage].

  If you want to add disks manually, follow the following procedure. Execute for all servers for expanding a cluster.

  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] - [Disk Management].

  3. Select the server for expanding a cluster, and then select [Create Disk Group].

  4. On the "Create Disk Group" screen, select "disk to serve as cache tier" and "disk to serve as capacity tier," and then select the [OK] button.

     When the task is complete, the disk addition is complete.

In order to confirm that the expansion is actually implemented, first check the current vSAN storage capacity in advance.

6.9.3.2 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 servers for expanding a cluster.

http://support.ts.fujitsu.com/Index.asp?lng=COM

6.9.3.3 Register a server for expanding a cluster to ServerView RAID Manager

Register a server for expanding a cluster to ServerView RAID Manager to execute Monitoring of SSD lifetime.

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

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 servers for expanding a cluster.

```
>amCLI -e 21/0 add_server name=<IP address of ESXi of the server for expanding a cluster>
port=5989 username=root password=<root password>
```

3. Execute the following command to check that all servers for expanding a cluster 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.

6.9.3.4 Delete unnecessary files

Delete unnecessary files with the following procedure after competing Cluster Expansion.

(1) Deleting certificates

The certificate created in "6.9.1.2 Create ADVM certificates" is not required after once registered.

Note

The certificates uploaded to ADVM#1 and ADVM#2 in "6.9.1.2 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. If you are using the files that you uploaded to ISM-VA, 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 the unnecessary files, checking the following items and referring to "2.9 Delete Files Uploaded to ISM-VA."

Item	Value
Root Directory	Administrator/ftp
Directory Name	kickstart
File Name	- VMware ESXi patch files in "6.9.1.6 Upload the VMware ESXi patch file" - Offline bundle of the VMware SMIS Provider in "6.9.1.7 Upload VMware SMIS provider"

6.10 Expand a Cluster for Microsoft Storage Spaces Direct

This section describes the cluster expansion procedure for PRIMEFLEX for Microsoft Storage Spaces Direct.

This function can be used only with the license for ISM for PRIMEFLEX.

Cluster Expansion is executed according to the following work flow.

Table 6.19 Work flow for Cluster Expansion

Cluster Expansion procedure		Tasks
1	Preparations	- Creating certificates for servers for expanding a cluster - DHCP settings - Importing 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) - Registering nodes in ISM
2	Execute Cluster Expansion	
3	Follow-up processing	- Refresh cluster information - Confirmation of the cluster expansion - Registering to the virtual switch for service - Setting the system volume name - Setting the browser - Deleting unnecessary files

6.10.1 Preparations

This section describes the preparations required before the cluster expansion.

6.10.1.1 Create certificates for servers for expanding a cluster

You must create and register certificates for the servers for expanding a cluster because Cluster Expansion execute settings from ISM with SSL encrypted communication.

(1) Creating certificates

Use the tool to create certificates (makecert.exe) and the tool to create file 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)

(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 as that 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.

This is a command example where the name of the server for expanding a cluster is "192.168.10.10" and the certificate expiration date is March 30, 2018.

```
>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 <file name of the certificate file.cer> -sv <file name of the private
key.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 <file name of the certificate file.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 <file name of the certificate
file.cer> -pfx <file name of the service certificate.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 <file name of the service certificate.pfx>.

```
>dir
```

Note

- If there are multiple servers for expanding a cluster, create certificates for all the servers for expansion.
- For the name of the certificate files, specify "Computer name set in ISM's profiles."

  Example:

  - hv-host4.cer
  - hv-host4.pfx

(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 "2.8 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)

6.10.1.2 Set up DHCP

For Cluster Expansion, execute OS installation by using profile assignment. To execute OS installation with profile assignment, DHCP servers are 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."

If there are multiple servers for expanding a cluster, set it so that multiple leases are possible.

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 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 multiple ports. Execute settings so that there are always IP addresses that can be leased.
- 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."

6.10.1.3 Import the ISO image of the OS installation media to ISM-VA

Import the ServerView Suite DVD and the installation media into ISM.

If you are going to use existing installation media, the import is not required.

For information on import operations, refer to "2.13.2 Repository Management" in "User's Guide."

For the support version, refer to "Setting Items for Profile Management."

Add ISM-VA virtual disks as required. For information on the procedure to add virtual disks, refer to "3.7 Allocation of Virtual Disks" in "User's Guide."

6.10.1.4 Create a profile

Use ISM Profile Management to add the profiles for the servers for expanding a cluster. Create profiles by creating references from existing profiles.

Note

If there are multiple servers for expanding a cluster, create profiles for all the servers for expansion.

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Profiles].
2. Select the current profile to be used to create a reference, from the [Actions] button, select [Duplicate Profile].
3. Set each item.

   Point

   For profile creation, refer to "3.3 Execute Settings on a Server/Install Server OS."

   Note

   - Do not check the following items.
     - In the [OS (for each node)] tab, [DHCP]
   - 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]
   - The following item is automatically set by Cluster Expansion. If you select the item before Cluster Expansion is executed, it will not cause any errors but the setting value will be overwritten during the execution of Cluster Expansion.
     - In the [OS] tab, [Execute Script after Installation]

6.10.1.5 Create and edit Cluster Definition Parameters

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 don 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 GUI of ISM, select [Management] - [Cluster] - [<Target Cluster>] - [Cluster Definition Parameters] tab.

- If creating a new one

  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 Setting Items Lists for Cluster Definition Parameters" in "ISM for PRIMEFLEX Parameter List."

6.10.1.6 Execute installation and wiring

Install a server for expanding a cluster at its physical location and connect the cables. For details, refer to the "Operating Manual" of the server for Cluster Expansion. Execute the settings for your network switches as appropriate, referring to the manual of the switches.

If there are multiple servers for expanding a cluster, create parameters for all the servers to be added.

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 "6.10.1.7 Set the IP address of iRMC."

- For Auto Discovery of nodes

  Execute "Node registration using Auto Discovery" in "6.10.1.10 Register a node to ISM."

6.10.1.7 Set the IP address of iRMC

When you register a server for expanding a cluster by using Manual Discovery, set the static IP address to the iRMC.

Boot the BIOS of the server for expanding a cluster, and on the "BIOS setup" screen, set a static IP address. To execute this operation, you must execute "6.10.1.6 Execute installation and wiring." Moreover, to display and operate the "BIOS setup" screen, connect a display and keyboard to the server for Cluster Expansion.

For information on booting the BIOS and setting the IP address for the iRMC, refer to the "BIOS Setup Utility Reference Manual" of the server for expanding a cluster.

If there are multiple servers for expanding a cluster, specify parameters for all the servers to be added.

Also, execute "6.10.1.8 Set up BIOS" as well as setting of the IP address.

You can obtain the "BIOS Setup Utility Reference Manual" for each server for expanding a cluster from the following website:

http://manuals.ts.fujitsu.com/index.php?l=en

6.10.1.8 Set up BIOS

Specify the BIOS settings.

When you select "For Manual Discovery of nodes" in "6.10.1.6 Execute installation and wiring," set this item together with "6.10.1.7 Set the IP address of iRMC."

When you select "For Auto Discovery of nodes" in "6.10.1.6 Execute installation and wiring," you can set BIOS settings remotely with iRMC Video Redirection. Start BIOS, then specify the following settings from the "BIOS setup" screen.

If there are multiple servers for expanding a cluster, create parameters for all the servers to be added.

Table 6.20 BIOS settings

Item		Setting Value
Main	System Date	Local date
	System Time	Local date
Advanced - CPU Configuration	Override OS Energy Performance	Enabled
	Energy Performance	Performance
	Package C State Limit	C0
Advanced - Network Stack Configuration	Network Stack	Enabled

Item		Setting Value
	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

After completing the BIOS settings, in the "BIOS setup" screen - the [Save & Exit] tab, execute "Save Changes and Exit," then power off after several minutes.

Continue to execute "6.10.1.9 Create system disk (RAID1)."

6.10.1.9 Create system disk (RAID1)

The logical disk to be used as a system disk (Configure 2 HDD as RAID 1) is created in the "UEFI" screen in PRIMERGY.

If there are multiple servers for expanding a cluster, create parameters for all the servers to be added.

1. Start the "BIOS setup" screen.
2. Select [Advanced] tab, then select "LSI SAS3 MPT Controller SAS3008" and press the [Enter] key.
3. Select "LSI SAS3 MPT Controller X.XX.XX.XX" and press the [Enter] key.
4. Select "Controller Management" and press the [Enter] key.
5. Select "Create Configuration" and press the [Enter] key.
6. In "Select RAID level" select "RAID 1," select "Select Physical Disks" and then press the [Enter] key.
7. Select the type of the system disk prepared in "Select Interface Type."
8. In "Select Media Type" select the media of the system disk (HDD).

   Select 2 system disks for your OS booting from the disk list displayed in "Select Media Type."
9. Change the 2 disks to be used as system disk to "Enabled," select "Apply Changes" and press the [Enter] key.
10. The confirmation screen displayed and after changing "Confirm" to "Enabled," select "Yes" and press the [Enter] key.
11. In "Operation completed successfully," select "OK" and press the [Enter] key.
12. Press the [Esc] key several times, in "Exit Without Saving," select "Yes" and press the [Enter] key.
13. The power of the server is turned off.

When you select "For Manual Discovery of nodes" in "6.10.1.6 Execute installation and wiring" continue to execute "Node registration using Manual Discovery" in "6.10.1.10 Register a node to ISM."

When you select "For Auto Discovery of nodes" in "6.10.1.6 Execute installation and wiring," continue to execute "6.10.2 Execute Cluster Expansion."

6.10.1.10 Register a node to ISM

In order to use ISM to install OS, register the server for expanding a cluster in ISM.

To register a node to the ISM, you can use both Manual Discovery and Auto Discovery. Register all servers for expanding a cluster.

Point

- When you register a node in ISM, you must enter the iRMC user name and password for the servers for expanding a cluster. 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 Install ISM."
- For node registration, refer to "2.2.1.2 Registration of nodes" or "2.2.1.6 Discovery of nodes" in "User's Guide."

Node registration using Manual Discovery

For the procedure for registering a node with Manual Discovery, refer to "3.1.2 Register a Node Directly."

Specify the IP address set in "6.10.1.7 Set the IP address of iRMC" when registering.

If there are multiple servers for expanding a cluster, you can register them at the same time by specifying an IP address range.

Continue to execute "6.10.2 Execute 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."

Set the static IP address of the iRMC on the "Node Registration" wizard.

Continue to execute "6.10.1.8 Set up BIOS."

6.10.2 Execute Cluster Expansion

By executing Cluster Expansion, you can expand a cluster in the virtualized platform.

6.10.2.1 Operation requirements for Cluster Expansion

To use Cluster Expansion, the following requirements must be met.

- Check the following requirements before executing it.
  - That the AD, DNS, and NTP are all running normally and can be used
  - That the information of the DNS server is registered in ISM-VA
  - That the cluster is operating normally
  - That the type of servers for expanding a cluster are the same

    Point

    For successor cluster expansion, refer to "Appendix D Successor Cluster Expansion" in "User's Guide."

  - That you register the server for expanding a cluster 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.
  - An Intel or Mellanox Ethernet adapter must be installed in the server for expanding a cluster
  - The Ethernet adapter can handle over 10 GB traffic
  - BIOS settings for the server for expanding a cluster are specified as described in "6.10.1.8 Set up BIOS."
  - That the virtual networks for PRIMEFLEX for Microsoft Storage Spaces Direct are configured as below

Setting items	Setting Value
Switch Embedded Teaming	Workload virtual switch
	Management virtual switch
Virtual Network Adapter	- vEthernet (Management) - vEthernet (Storage_1) - vEthernet (Storage_2)

The configuration of the virtual network for PRIMEFLEX for Microsoft Storage Spaces Direct 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 are configured as below

Device	Default	Utilization
PCI card 1 (Port1), PCI card 2 (Port1)	Workload virtual switch	Production LAN
PCI card 1 (Port0), PCI card 2 (Port0)	Management virtual switch	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 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."

- A profile has been created for the server for expanding a cluster in Profile Management of ISM
- Cluster Definition Parameters have been set

  For details, refer to "6.10.1.5 Create and edit Cluster Definition Parameters."
- The power of the server for expanding a cluster is off

Note

The following is an operation requirement when executing Cluster Expansion again with the OS installation completed using profile assignment.

- The power of the server for expanding a cluster is on

To check if the OS installation has been completed, use the following procedure.

1. At the top of the Global Navigation Menu, 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."

- The computer name of the servers for expanding a cluster 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 servers for expanding a cluster which you specify in the profile must be unique among all IP addresses of the OS of the nodes managed by ISM.

- First check the current PRIMEFLEX for Microsoft Storage Spaces Direct storage capacity. For the procedure to confirm, refer to "6.10.3.2 Confirm Cluster Expansion."

- To use Cluster Expansion, you must set Virtual Resource Management to the cluster to be expanded.

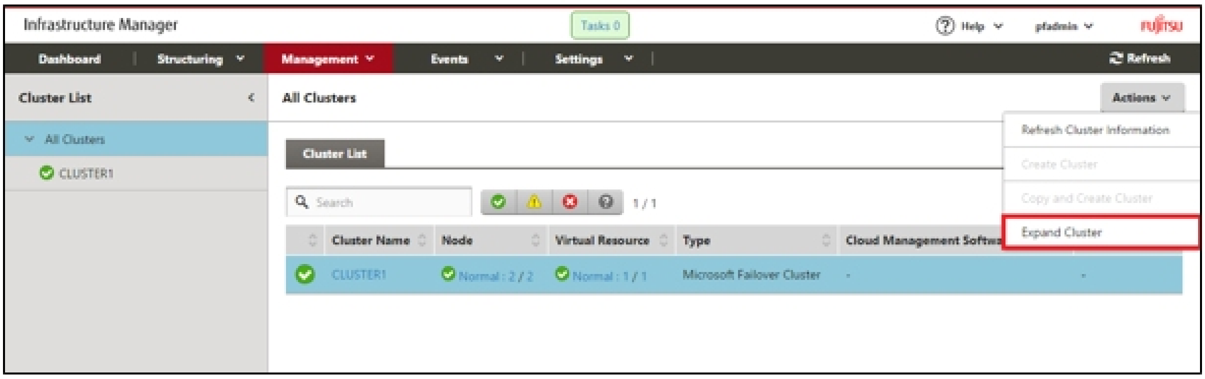
  For settings of Virtual Resource Management, refer to "3.9 Pre-Settings for Cluster Management" in "User's Guide."

6.10.2.2 Cluster Expansion procedure

This section describes the procedure for executing Cluster Expansion of ISM for 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 GUI of ISM, select [Management] - [Cluster].

   The "Cluster List" screen is displayed.
3. Select [<Target cluster>], and then from the [Actions] button, select [Expand Cluster].

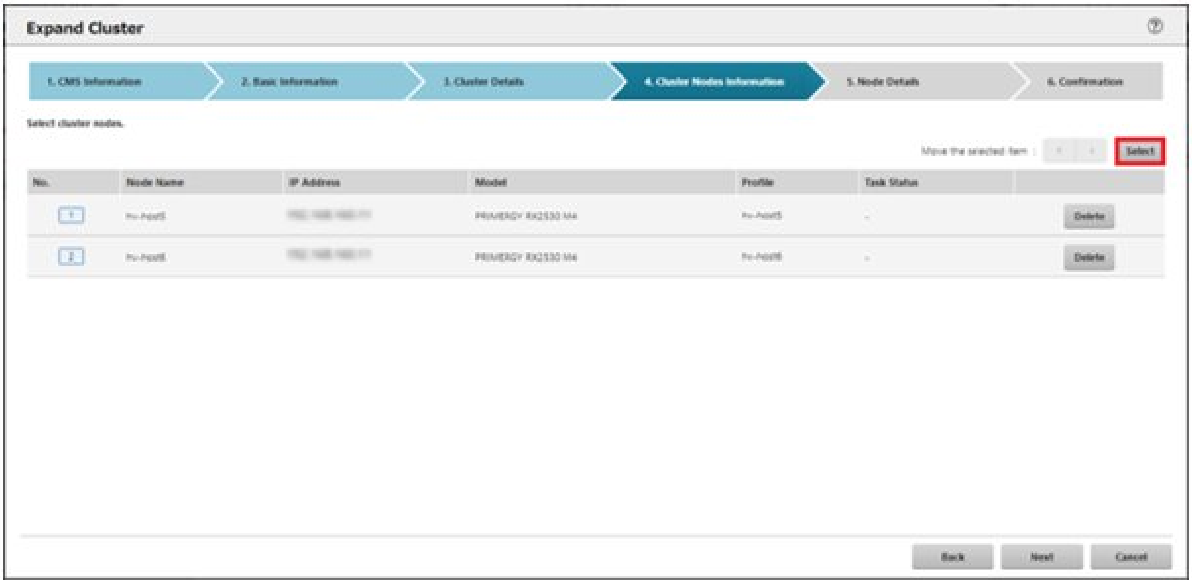


	Cluster Name	Node	Virtual Resource	Type	Cloud Management Softw
✓	CLUSTER1	✓ Normal : 2 / 2	✓ Normal : 1 / 1	Microsoft Failover Cluster	-

The "Expand Cluster" wizard is displayed.

4. Select the [Select] button in the "Cluster Nodes Selection" screen, and then on the displayed "Target nodes selection" screen, select the server for expanding a cluster.

   If executing again, this procedure is not required. Select the [Next] button and proceed to Step 6.



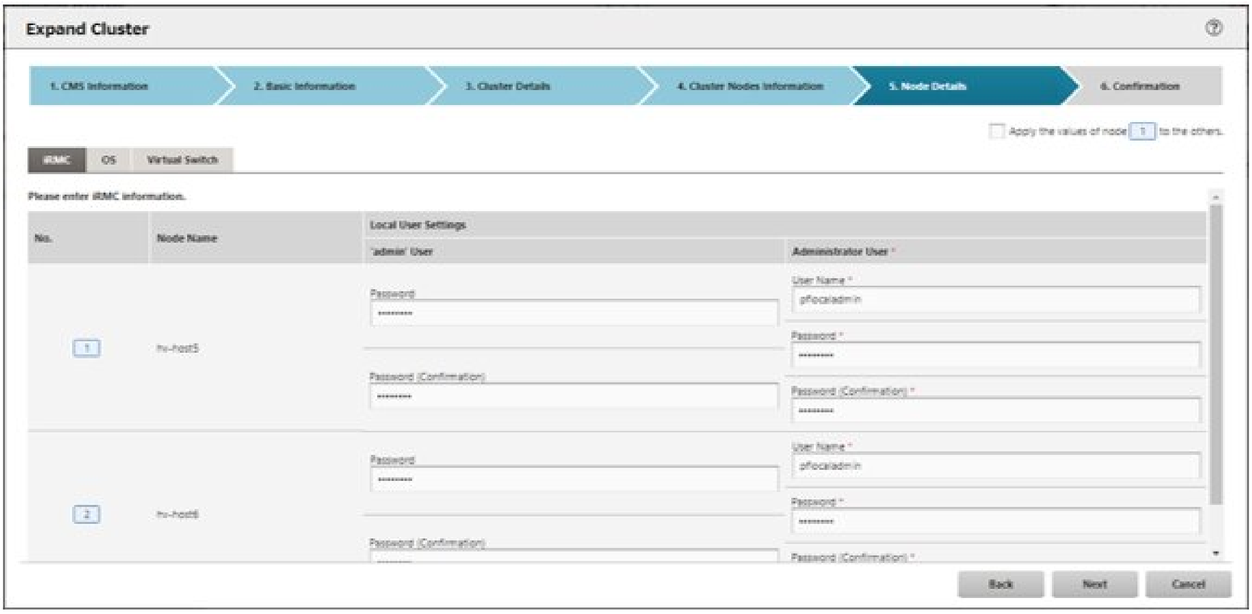
Select cluster nodes.

No.	Node Name	IP Address	Model	Profile	Task Status
1	hv-host5	[redacted]	PRIMERGY RX2530 M4	hv-host5	-
2	hv-host6	[redacted]	PRIMERGY RX2530 M4	hv-host6	-

5. If a profile has not been assigned to the server for expanding a cluster, select the [Select] button in the [Profile] item, and then select the profile to be assigned.

6. Enter each parameter of the server for expanding a cluster on the "Node Details" screen.

   If executing again, select the [Next] button if no parameters must be entered again and proceed to Step 7.



□ Apply the values of node 1 to the others.

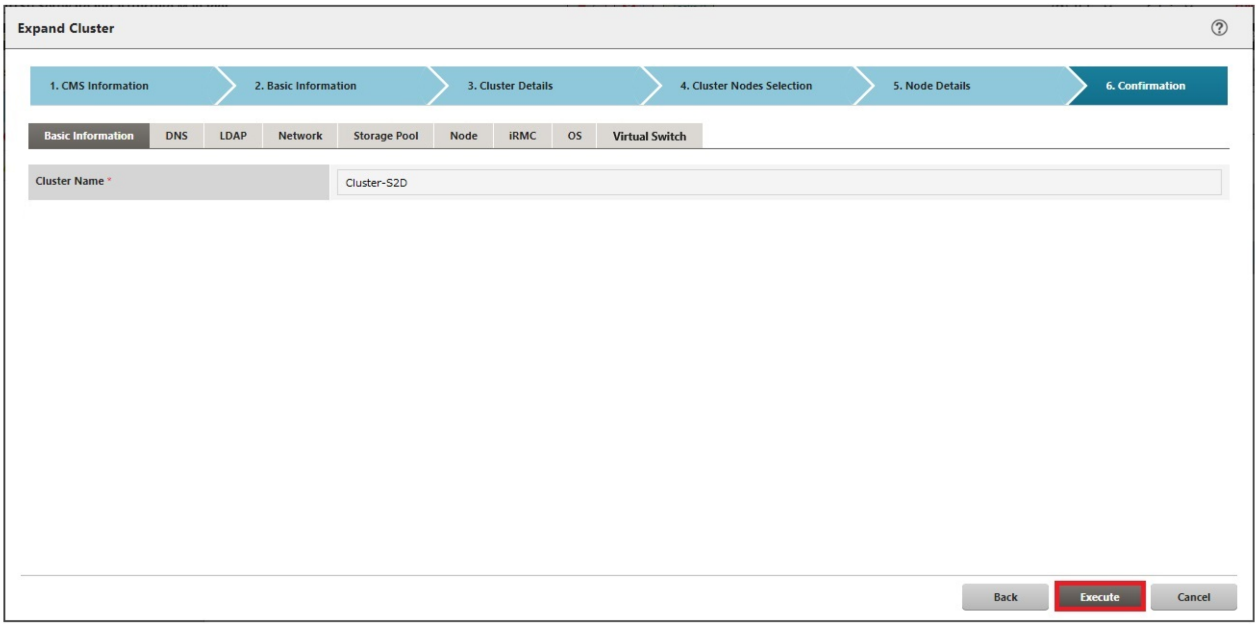
Please enter iRMC information.

No.	Node Name	Local User Settings 'admin' User	 Administrator User *
1	hv-host5	Password: ******** Password (Confirmation): ********	User Name *: pflocaladmin Password *: ******** Password (Confirmation) *: ********
2	hv-host6	Password: ******** Password (Confirmation): ********	User Name *: pflocaladmin Password *: ******** Password (Confirmation) *

Note

For details on Cluster Definition Parameters, refer to "Chapter 3 Setting Items Lists for Cluster Definition Parameters" in "ISM for PRIMEFLEX Parameter List."

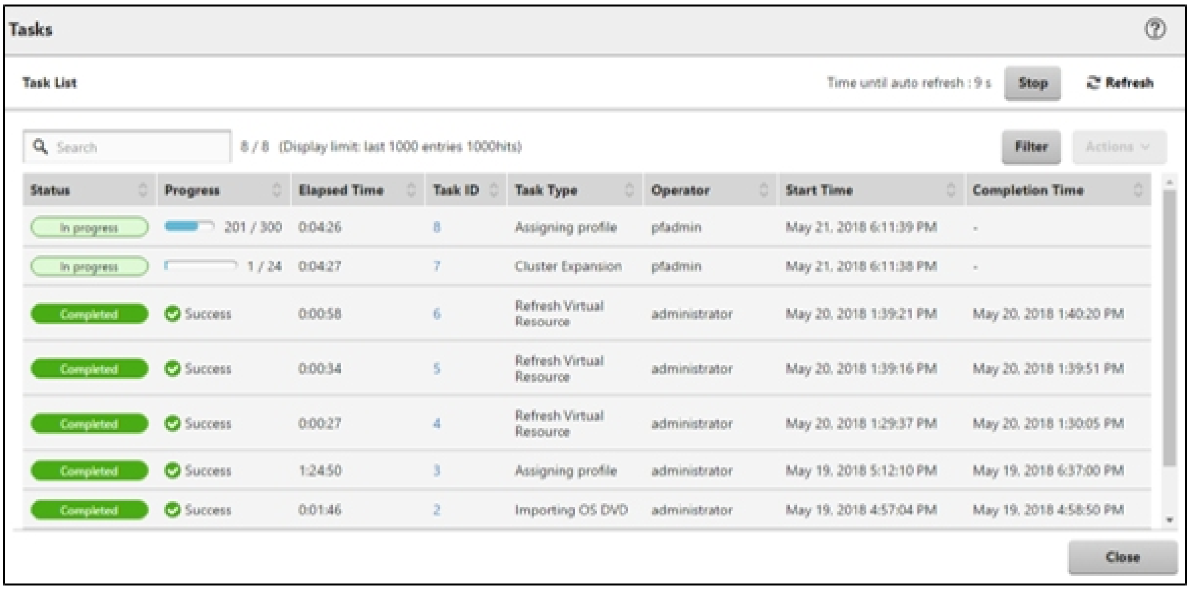
7. Check the parameters on the "Confirmation" screen, then select the [Execute] button.



Cluster Name * Cluster-S2D

The execution of Cluster Expansion is registered as an ISM task.

At the top of the Global Navigation Menu, select [Tasks], then the tasks in the task list displayed in the "Tasks" screen whose task type has become "Cluster Expansion" are the Cluster Expansion tasks.



8 / 8 (Display limit: last 1000 entries 1000hits)

Status	Progress	Elapsed Time	Task ID	Task Type	Operator	Start Time	Completion Time
In progress	201 / 300	0:04:26	8	Assigning profile	pfadmin	May 21, 2018 6:11:39 PM	-
In progress	1 / 24	0:04:27	7	Cluster Expansion	pfadmin	May 21, 2018 6:11:38 PM	-
Completed	Success	0:00:58	6	Refresh Virtual Resource	administrator	May 20, 2018 1:39:21 PM	May 20, 2018 1:40:20 PM
Completed	Success	0:00:34	5	Refresh Virtual Resource	administrator	May 20, 2018 1:39:16 PM	May 20, 2018 1:39:51 PM
Completed	Success	0:00:27	4	Refresh Virtual Resource	administrator	May 20, 2018 1:29:37 PM	May 20, 2018 1:30:05 PM
Completed	Success	1:24:50	3	Assigning profile	administrator	May 19, 2018 5:12:10 PM	May 19, 2018 6:37:00 PM
Completed	Success	0:01:46	2	Importing OS DVD	administrator	May 19, 2018 4:57:04 PM	May 19, 2018 4:58:50 PM

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, you must accept the conditions of the license.

Also, in order to ensure stable operation, apply the latest Windows update programs.

Execute the following Steps 9 to 23 within 180 minutes after completing profile assignment. Please 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.

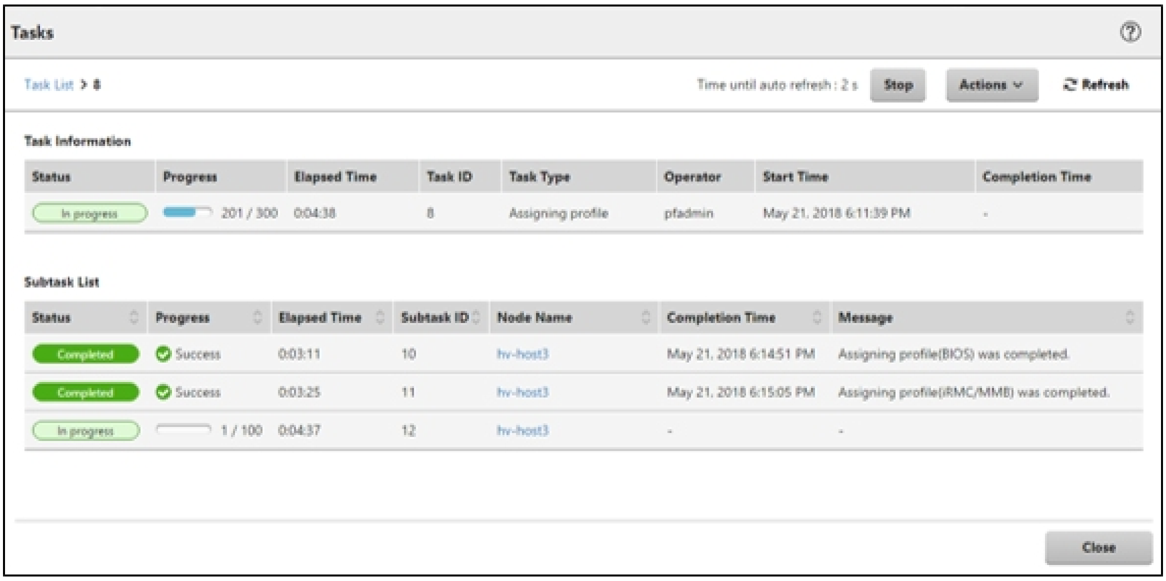
```
50215109: Subtask error : Failed to add server. An error occurred during the setting process of
the Cluster Expansion task. (The task type setting process retried out; task type = Cluster
Expansion; id = 20; task item set name = OS Installation; task item name = Wait Hyperv OS Boot;
detail code = E010205)
```

If Cluster Expansion times out and finishes with an error, execute up to Step 23, and then execute Cluster Expansion again.

Even if Cluster Expansion times out and ends with an error during the execution of Step 9 to 23, continue and execute to Step 23.

Point

From the task list on the "Tasks" screen, select [Task ID] from "Cluster Expansion," and then the "Tasks" screen of the "Cluster Expansion" is displayed. In this screen, a subtask list is displayed for each server for expanding a cluster. You can check the progress status of each task by checking the message column.



Task Information

Status	Progress	Elapsed Time	Task ID	Task Type	Operator	Start Time	Completion Time
In progress	201 / 300	0:04:38	8	Assigning profile	pfadmin	May 21, 2018 6:11:39 PM	-

Subtask List

Status	Progress	Elapsed Time	Subtask ID	Node Name	Completion Time	Message
Completed	✓ Success	0:03:11	10	hv-host3	May 21, 2018 6:14:51 PM	Assigning profile(BIOS) was completed.
Completed	✓ Success	0:03:25	11	hv-host3	May 21, 2018 6:15:05 PM	Assigning profile(iRMC/MMB) was completed.
In progress	1 / 100	0:04:37	12	hv-host3	-	-

9. After the status of [Assigning profile] task turned to [Completed], display iRMC screen of the server for expanding a cluster to log in, and then select [Video Redirection].

   When the security warning is displayed, check [I accept the risk and want to run this application], 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

In the video redirection screen, do not select the [Restart system] button in the "ServerView Infrastructure Manager" screen and do not restart Windows.

It will not be possible to apply the Windows update program and Mellanox LAN driver.

13. Use a user with Administrator privileges on the remote desktop to access the Windows OS of the server for expanding a cluster.

Note

If an error message is displayed and you cannot connect while using remote desktop connection, the error could 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 remote desktop connection destination.

https://blogs.technet.microsoft.com/mckittrick/unable-to-rdp-to-virtual-machine-credssp-encryption-oracle-remediation/

14. Transfer the same Windows update program as that of the current cluster to the server for expanding a cluster.

15. If you are using a Mellanox LAN card and if the SVIM version used during construction is earlier than 12.08.04, transfer Mellanox LAN driver to the server for expanding a cluster.

    For the Mellanox LAN driver, download the driver package from the following website.

    http://support.ts.fujitsu.com/

    If you already applied the Mellanox LAN driver, this procedure is not required. Proceed to Step 16.

Point

You can check if Mellanox LAN driver is installed by checking that "MLNX_WinOF2" is "Installed" in [Control panel] - [Programs] - [Programs and Functions] - [Uninstall or Change programs].

Note

If you use a Mellanox LAN card, install the driver for the Mellanox LAN card in Step 17.

16. Apply the Windows update program transferred to the servers for expanding a cluster.

17. If you are using a Mellanox LAN card and if the SVIM version used during construction is earlier than 12.08.04, apply the Mellanox LAN driver transferred to the servers for expanding a cluster.

    If you already applied the Mellanox LAN driver, this step is not required. Proceed to Step 18.

18. 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.

19. If Server Manager is displayed at the front, minimize it to display the "ServerView Installation Manager" screen.

20. Select the [Restart system] button when the ServerView Installation Manager screen is displayed.

    The sign out screen is displayed and the server is restarted.

21. After restarting, log in with a user that has Administrator privilege.

22. Delete the Windows update program transferred in Step 14.

23. Delete the Mellanox LAN driver transferred in Step 15.

24. Repeat Step 9 to 23 for all servers for expanding a cluster.

25. Check that the status of "Cluster Expansion" has become "Completed."

Note

- If an error is displayed on the ISM "Tasks" screen, refer to "ISM for PRIMEFLEX Messages" and solve the error. Solve the error, then execute the operation again.

  If the OS installation with Profile Management of ISM (Assigning profile tasks) ends normally, do not power off the server for expanding a cluster when executing again.

- For the settings of the virtual network for service on the server for expanding a cluster according to your environment.

- Do not execute Cluster Expansion during execution of Firmware Rolling Update.

6.10.3 Follow-up processing

This section describes the follow-up processing required after the cluster expansion.

6.10.3.1 Refresh cluster information

Execute the settings to monitor the servers for creating a new cluster with Cluster Management. After that, refresh the cluster information.

(1) Configure Kerberos delegation for Active Directory

The Kerberos delegation of all the servers for expanding a cluster are configured in Active Directory.

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>, then select [Properties].
6. In the [Delegation] tab, check the checkbox of [Trust this computer for delegation to any service (Kerberos only)] if it is not checked.
7. Select the [OK] button, then repeat Step 5 to 6 for all the nodes configuring the cluster.

(2) 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 GUI of ISM, 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," then after waiting a while, refresh the ISM GUI screen (select the Refresh button on the top right side on the screen).

6.10.3.2 Confirm Cluster Expansion

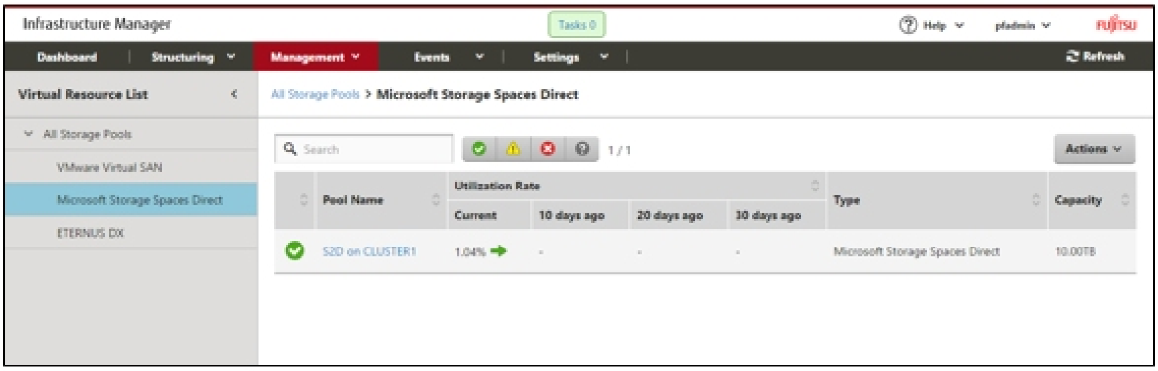
Use the following procedure to check the status of Cluster Expansion to the PRIMEFLEX for Microsoft Storage Spaces Direct.

1. Access the Failover Cluster Manager and check that the node of the server for expanding a cluster is displayed in [<Cluster name>] - [Nodes]. Check the following points.

   - 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 [<Cluster name>] - [Storage] - [Pool] - [<Pool name>] - [Virtual disk] is "Normal"
   - That the health status of all the disks in [<Cluster name>] - [Storage] - [Pool] - [<Pool name>] - [Physical disks] is "Normal"

2. Access the GUI of ISM, and in the "Storage Pool" screen in [Management] - [Virtual Resource], execute [Actions] - [Refresh Virtual Resource Information] to refresh.

   After refreshing, check that the [Capacity] of the target storage pool has been expanded.



	Pool Name	Utilization Rate				Type	Capacity
		Current	10 days ago	20 days ago	30 days ago		
✓	S2D on CLUSTER1	1.04%	-	-	-	Microsoft Storage Spaces Direct	10.00TB

Note

- Whether the task completed successfully or not, if the previously checked storage pool has not been expanded, communication for the PRIMEFLEX for Microsoft Storage Spaces Direct 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.

6.10.3.3 Register to the virtual switch for workload

Execute for all servers added when expanding a cluster.

Set up a Service adapter. Open PowerShell from the command prompt with administrator privilege and execute the following commands.

```
>Add-VMNetworkAdapter -SwitchName <Virtual Switch Name> -Name "Service" -ManagementOS [Note 1]
>Set-VMNetworkAdapterVlan -VMNetworkAdapterName "Service" -VlanId <VLAN ID> -Access -ManagementOS
[Note 2]
>Set-VMNetworkAdapterTeamMapping -VMNetworkAdapterName "Service" -ManagementOS -
PhysicalNetAdapterName "Slot <Slot Number>  port 2" [Note 3]
>Set-VMNetworkAdapterTeamMapping -VMNetworkAdapterName "Service" -ManagementOS -
PhysicalNetAdapterName "Slot <Slot Number>  port 2" [Note 4]
```

[Note 1]: Specify the Virtual switch name of the production LAN in <Virtual Switch Name>.

[Note 2]: Specify the VLAN ID of the production LAN in <VLAN ID>.

[Note 3]: Specify the slot number of the network adapter name of the first PCI card set in the service adapter in <Slot Number>.

[Note 4]: Specify the slot number of the network adapter name of the second PCI card set in the service adapter in <Slot Number>.

Point

If the slot number is not known, check it using the following command.

```
> Get-NetAdapterHardwareInfo | select Name,InterfaceDescription,Slot,Function | Sort-Object Name
```

Example of command output

```
:Name                            InterfaceDescription                                  Slot Function
----                            --------------------                                  ---- --------
Onboard Flexible LOM port 1  Intel(rainbow)  Ethernet Connection X722 for 10GBASE-T             0
Onboard Flexible LOM port 2  Intel(rainbow)  Ethernet Connection X722 for 10GBASE-T #2          1
Onboard LAN port 1           Intel(rainbow)  I350 Gigabit Network Connection #2                 0
Onboard LAN port 2           Intel(rainbow)  I350 Gigabit Network Connection                    1
Slot 03 port 1               Intel(R) Ethernet Converged Network Adapter X550-T2 #4    3        0
Slot 03 port 2               Intel(R) Ethernet Converged Network Adapter X550-T2 #2    3        1
Slot 07 port 1               Intel(R) Ethernet Converged Network Adapter X550-T2       7        0
Slot 07 port 2               Intel(R) Ethernet Converged Network Adapter X550-T2 #3    7        1
```

6.10.3.4 Set a system volume name

Execute for all servers added when expanding a cluster.

Set a system volume name to "system" according to the following procedure.

1. Log in to the host added when expanding a cluster.
2. Start the explorer, select C drive and right-click to select [Change name].
3. Enter "system" to the drive name.
4. Repeat Step 1 to 3 for all the hosts.

6.10.3.5 Set the browser for the servers for expanding a cluster

Set a browser for the servers for expanding a cluster to execute Monitoring of SSD lifetime in ServerView Raid Manager.

Refer to "2.2.1 Client/Browser Settings" in "FUJITSU Software ServerView Suite ServerView RAID Manager" and set up the web browser of the server for expanding a cluster.

6.10.3.6 Delete unnecessary files

Delete unnecessary files with the following procedure after competing Cluster Expansion.

(1) Deleting certificates

The certificates created in "6.10.1.1 Create certificates for servers for expanding a cluster" are transferred and registered to the servers for expanding a cluster when installing OS. Use the following procedure to delete the certificate.

Execute for all servers added when expanding a cluster.

1. Use remote desktop to access the Windows OS of the server for expanding a cluster.
2. Open Explorer and delete the following files.
    - C:\PostInstall\UserApplication\postscript_ClusterOperation\<certificate file name.cer>
    - C:\PostInstall\UserApplication\postscript_ClusterOperation\<service certificate file name.pfx>
    - C:\DeploymentRepository\Add-on\UserApplication\postscript_ClusterOperation\<certificate file name.cer>
    - C:\DeploymentRepository\Add-on\UserApplication\postscript_ClusterOperation\<service certificate file name.pfx>

Note

The certificates uploaded to ISM-VA in "6.10.1.1 Create certificates for servers for expanding a cluster" have security risks. If you cannot accept this risk, delete the certificate.

(2) Deleting unnecessary files for servers for expanding a cluster

Execute for all servers added when expanding a cluster.

1. Use remote desktop to access the Windows OS of the server for expanding a cluster.
2. Open Explorer and delete all files and directories under the following directories.
   - C:\PostInstall\UserApplication\postscript_ClusterOperation
   - C:\FISCRB\PowershellScript
   - C:\FISCRB\log

(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 the unnecessary files, checking the following items and referring to "2.9 Delete Files Uploaded to ISM-VA."

Item	Value
Root Directory	Administrator/ftp
Directory Name	postscript_ClusterOperation
File Name	The certificate created in (1) in "6.10.1.1 Create certificates for servers for expanding a cluster"

6.11 Export/Import/Delete Cluster Definition Parameters

This section describes the procedures to export/import/delete Cluster Definition Parameters.

This function can be used only with the license for ISM for PRIMEFLEX.

6.11.1 Export Cluster Definition Parameters

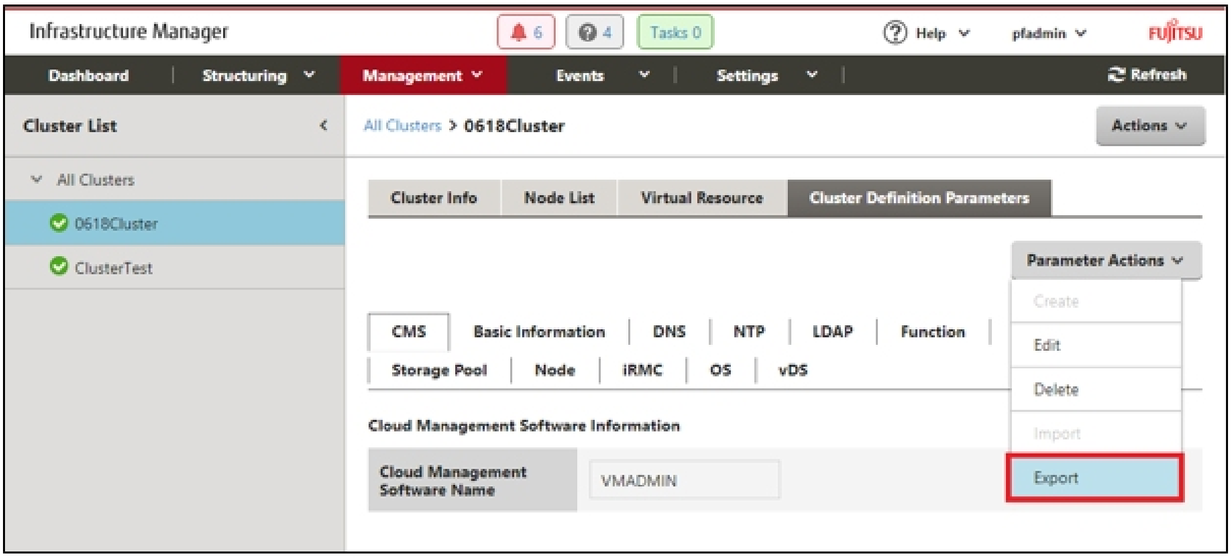
This section describes the procedure to export Cluster Definition Parameters.

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 GUI of ISM, select [Management] - [Cluster].

   The "Cluster List" screen is displayed.
3. Select the [<Target Cluster>] - [Cluster Definition Parameters] tab of the export target.

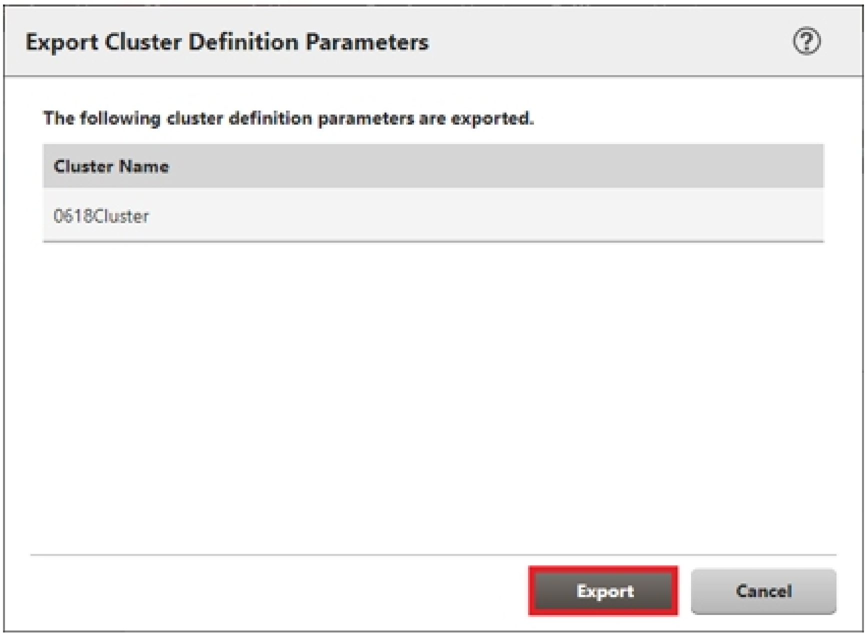
4. From the [Parameter Actions] button, select [Export].



Cloud Management Software Information

Cloud Management Software Name: VMADMIN

5. Select the [Export] button.

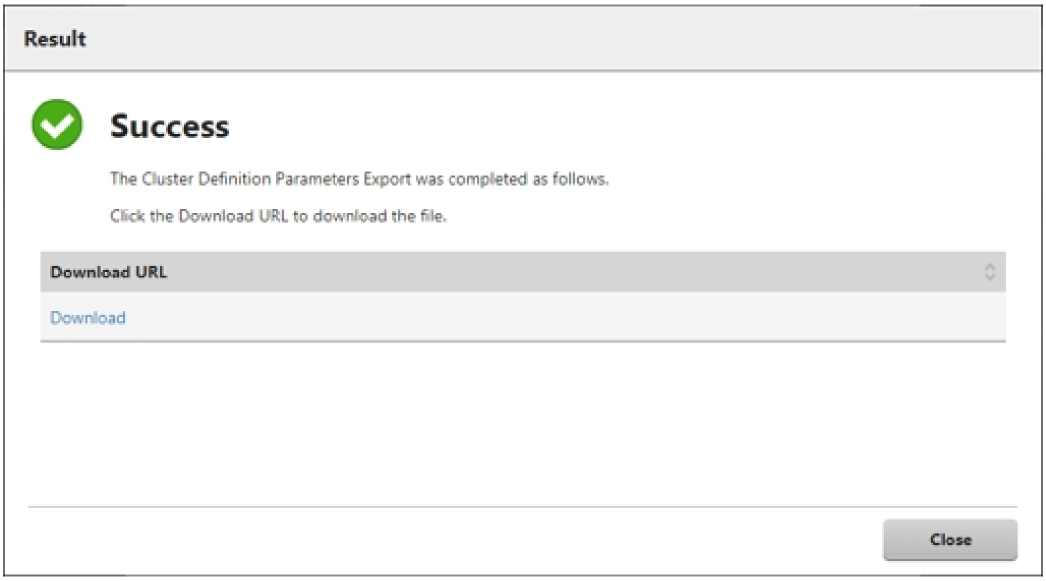

Export Cluster Definition Parameters

The following cluster definition parameters are exported.

Cluster Name
0618Cluster

When the export has been completed, the Result screen is displayed.

6. Select the link displayed in [Download URL] to download the file.



Result

Success

The Cluster Definition Parameters Export was completed as follows.

Click the Download URL to download the file.

Download URL
Download

If the file download is complete, the export of the Cluster Definition Parameters is complete.

6.11.2 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.

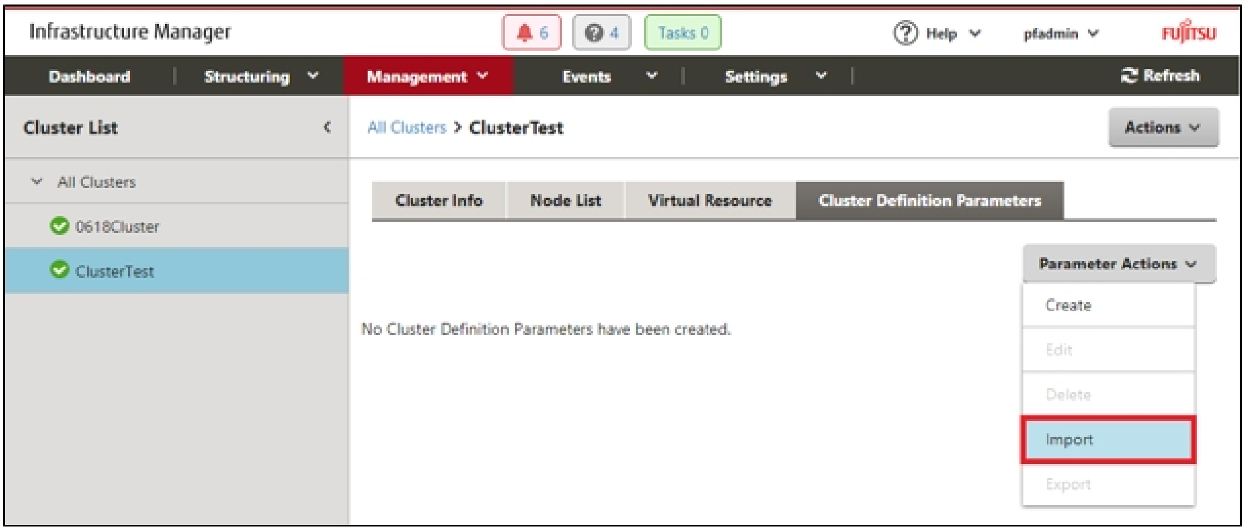
Note

If Cluster Definition Parameters are already created in the import target cluster, they cannot be imported. Delete Cluster Definition Parameters in advance.

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 GUI of ISM, select [Management] - [Cluster].

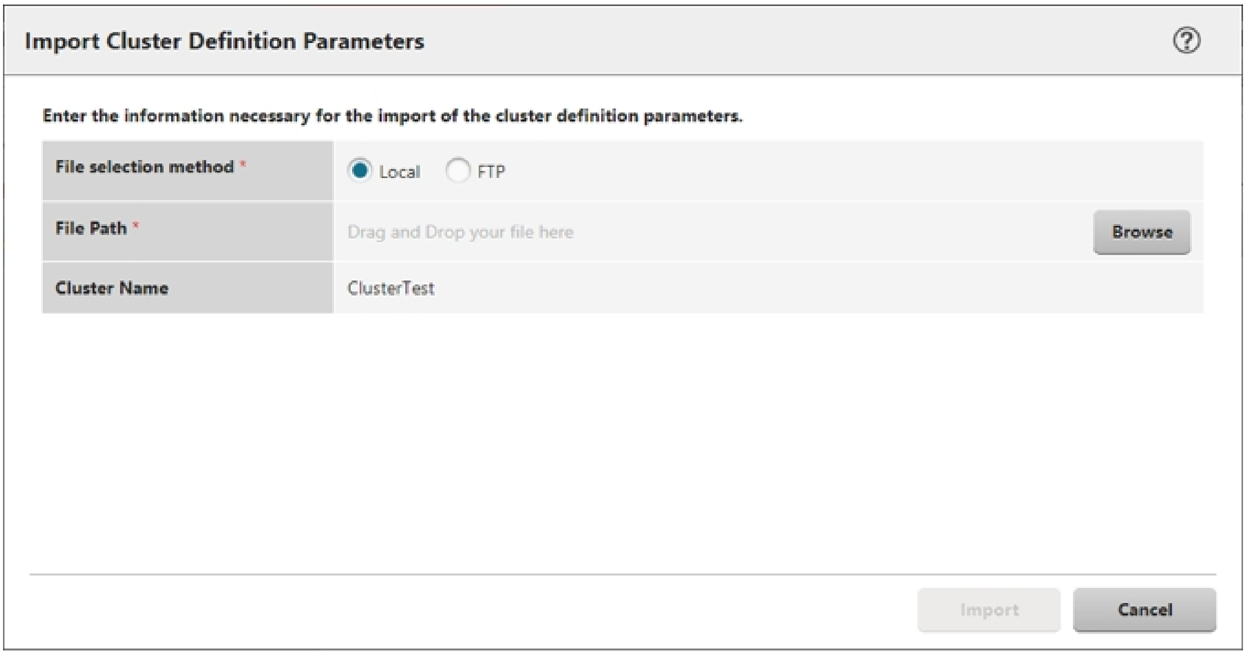
   The "Cluster List" screen is displayed.
3. Select the [<Target Cluster>] - [Cluster Definition Parameters] tab of the import target.

4. From the [Parameter Actions] button, select [Import].



No Cluster Definition Parameters have been created.

5. Select the file selection method in [File selection method], then set the file of the import target in [File Path].

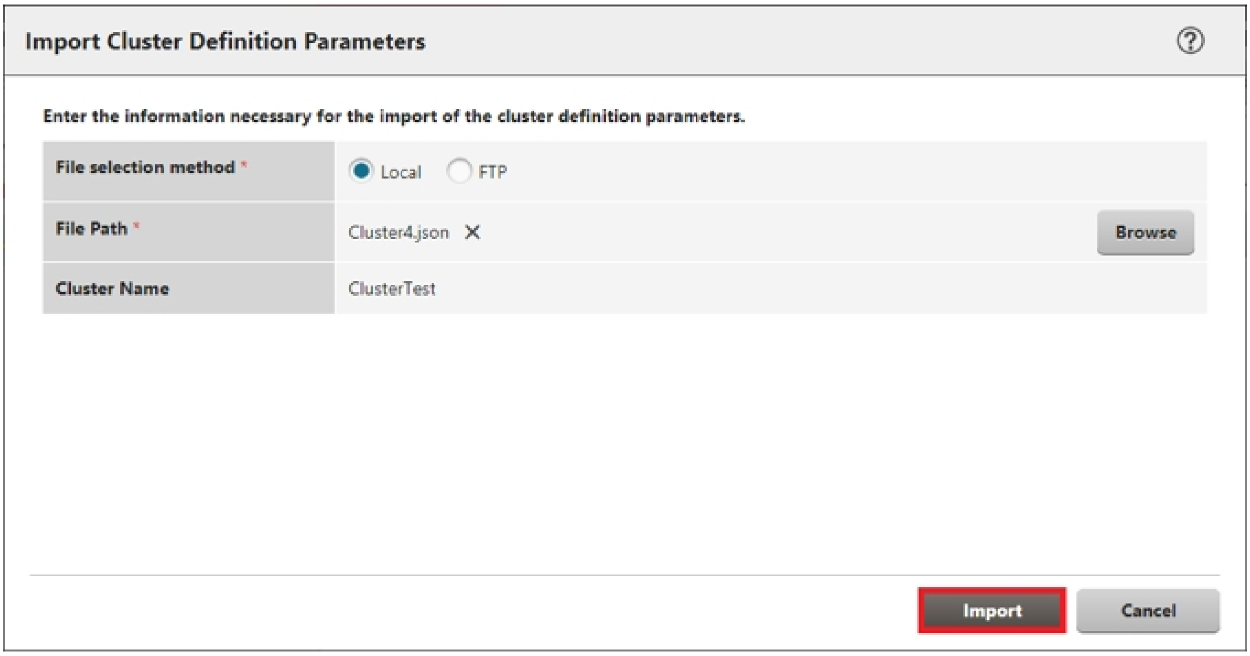


Import Cluster Definition Parameters

Enter the information necessary for the import of the cluster definition parameters.

File selection method *	● Local ○ FTP
File Path *	Drag and Drop your file here
Cluster Name	ClusterTest

6. Select the [Import] button.



Import Cluster Definition Parameters

Enter the information necessary for the import of the cluster definition parameters.

File selection method *	● Local ○ FTP
File Path *	Cluster4.json ✕
Cluster Name	ClusterTest

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 GUI of ISM, select [Management] - [Cluster].

2. Select the [<Target Cluster>] - [Cluster Definition Parameters] tab.

3. From the [Parameter Actions] button, select [Edit].

   Passwords and other parameters that are set according to your environment are not specified, and you may change the setting values as required.

For details on Cluster Definition Parameters, refer to "Chapter 3 Setting Items Lists for Cluster Definition Parameters" in "ISM for PRIMEFLEX Parameter List."

6.11.3 Delete Cluster Definition Parameters

This section describes the procedures to delete Cluster Definition Parameters.

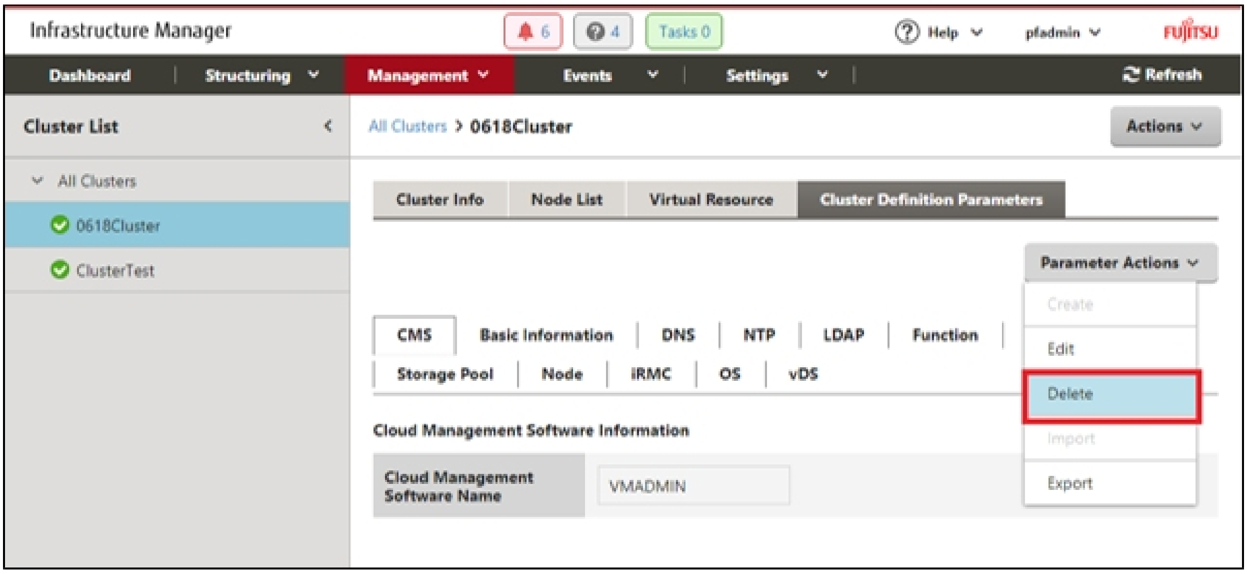
1. Log in to ISM as an ISM administrator who belongs to an Administrator group and has an Administrator role.

2. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Cluster].

   The "Cluster List" screen is displayed.

3. Select the [<Target Cluster>] - [Cluster Definition Parameters] tab of the one to be deleted.

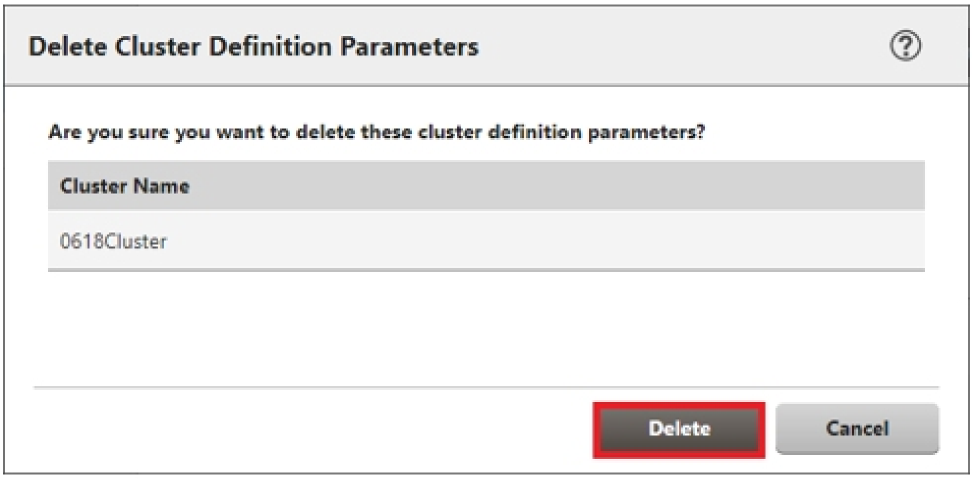
4. From the [Parameter Actions] button, select [Delete].



Cloud Management Software Information

Cloud Management Software Name	VMADMIN

5. Select the [Delete] button.



Are you sure you want to delete these cluster definition parameters?

Cluster Name
0618Cluster

6. From the "Cluster List" screen, select the [<Target Cluster>] - [Cluster Definition Parameters] tab of the delete 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.

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 GUI of ISM, 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 GUI of ISM, 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.

P Point

You can select multiple nodes and hardware settings for backing up and exporting.

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 GUI of ISM, 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.
   Procedure to display the help screen: Select the [?] in the upper right side on the wizard screen.

Point

You can select multiple hardware settings for creating profiles.

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 GUI of ISM, 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.
   Procedure to display the help screen: Select the [?] in the upper right side on the wizard screen.

Point

You can select multiple hardware settings for creating policies.

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 GUI of ISM, 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 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 GUI of ISM, 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 checkbox "Above contents are correct." and then select the [Execute] button.

Point

You can select multiple nodes for restoring.

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 GUI of ISM, 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 of [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

1. From the Global Navigation Menu on the GUI of ISM, 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 GUI of ISM, 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 will be displayed.
4. Select the file location in [File selection method].
   - Local

     Import a backup file kept in local.
   - FTP

     Import a backup file from 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 saved in "7.2.1 Backup Settings of Switches and Storages" or files imported in "7.2.3 Import Settings of Switches" to the switches registered in ISM.

1. Before restoring, power on the hardware.
2. From the Global Navigation Menu on the GUI of ISM, 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 checkbox "Above contents are correct." 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 contents of 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

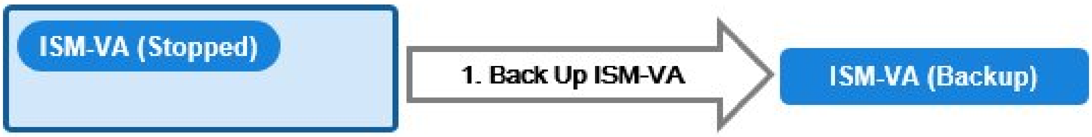
This section describes the procedure to Backup/Restore ISM.

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.

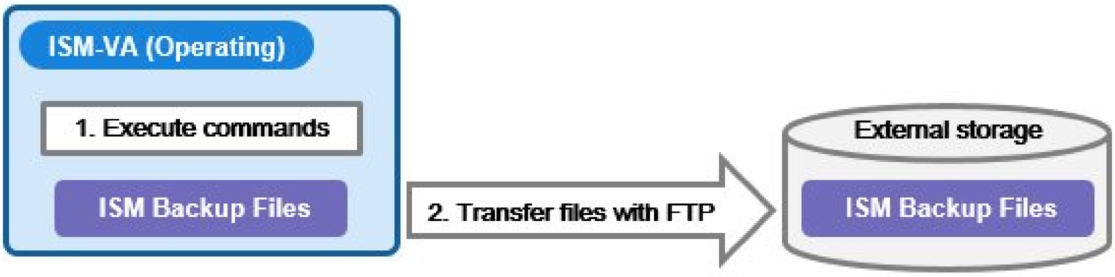
1. As a preparation, back up the ISM-VA on which you are going to restore ISM.

   Refer to "8.1.1 Prepare to Backup/Restore ISM."



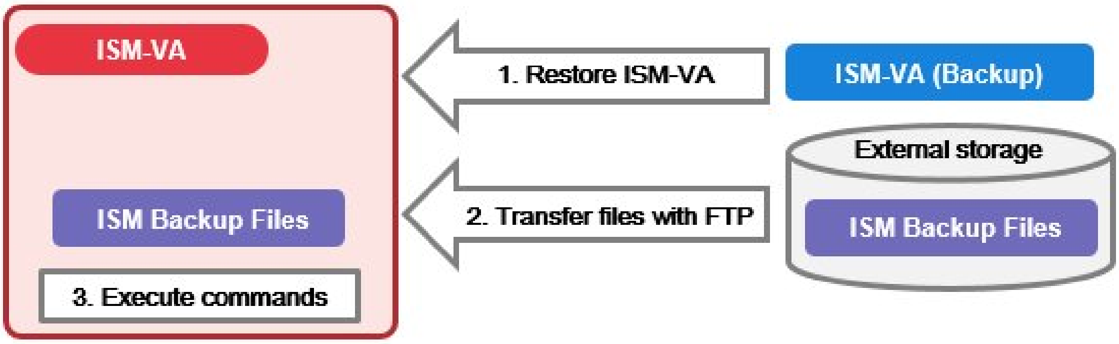
2. Back up the ISM.

   Refer to "8.1.2 Back up ISM."



3. Restore the ISM.

   Refer to "8.1.3 Restore ISM."



8.1.1 Prepare to Backup/Restore ISM

Back up the ISM-VA on which you are going to restore backup files of the ISM.

Back up the ISM-VA of the version that you intend to use.

For information on the ISM-VA backup procedures, refer to "2.1.2 Export ISM-VA."

Note

Be sure to back up ISM-VA after the following operations.

- ISM implementation
- ISM upgrade
- Patch application for ISM

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-VA.

```
# ismadm system backup
```

   Example of ISM backup command execution

```
# ismadm system backup
[System Information]
  Version : 2.4.0.x (S20190220-01)

[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: /Administrator/ftp/ism2.4.0.x-backup-20180801120000.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 which backed up in "8.1.1 Prepare to Backup/Restore ISM."

Note

- In the following cases, you cannot execute ISM restoring.
  - When the version of the backup file of ISM are different from the ISM-VA version at the restoration destination
    You need to restore the same version of the ISM-VA as of the ISM backup file.
  - 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 entire ISM-VA.
- Restore execution by using GUI, REST API or the workflow service is not provided.

1. Restore the ISM-VA backed up in "8.1.1 Prepare to Backup/Restore ISM."

   Restore the backups of the ISM-VA on which you created the ISM backup file.

   Use the restored ISM-VA as the restoration destination of the ISM.

   For information on restoring procedures, refer to "2.1.1 Import ISM-VA."

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 restoration destination with FTP. Access "ftp://<ISM-VA IP address of the restoration 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 restoration destination.

5. Execute a command for restoring the ISM-VA.

   ```
   # ismadm system restore -file <backup file name>
   ```

   Example of ISM restore command execution

   ```
   # ismadm system restore -file ism2.4.0.x-backup-20190801120000.tar.gz
   [System Information]
     Version : 2.4.0.x (S20190220-01)

   [Backup File Information]
     Version : 2.4.0.x (S20190220-01)

   [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.

7. After completing restoring, execute the following command to restart ISM-VA.

   ```
   # ismadm power restart
   ```

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 the entire ISM-VA is back the status of ISM-VA that had backed up.

   Confirm the allocation of the virtual disk and allocate new virtual disks to the system and user groups as required according to the procedure to allocate new virtual disks. For information on virtual disk allocation, refer to "2.1.3 Connect Virtual Disks."

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 "6.4.3 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.

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 GUI of ISM, 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 one of the following collecting mode, and then select the [Run] button.

   - Full: Collection of ISM RAS Logs, ISM-VA Operating System Logs, and database information together
   - Partial: Collection of ISM RAS Logs only

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 maintenance data capacity" 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 GUI of ISM, 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 GUI of ISM, 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 GUI of ISM, 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 GUI of ISM 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 5 weeks after collected.

- vc-support log is collected from vCenter as maintenance documentation for the Virtual Resources Management. For details, refer to "To collect ESX/ESXi and vCenter Server diagnostic data" from the following URL.

  https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2032892

  In Step 6 of the log collection procedure in the URL above, for the ESXi host log collection target, select all the vSAN cluster ESXi hosts where an error has occurred.

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

   - Collection of ISM RAS Logs only

   ```
   # ismadm system snap -dir /Administrator/ftp
   snap start
   Your snap has been generated and saved in:
     /Administrator/ftp/ismsnap-20160618175323.tar.gz
   ```

   - Batch collection of ISM RAS Logs, ISM-VA Operating System Logs, and database information

   ```
   # ismadm system snap -dir /Administrator/ftp -full
   snap start
   Your snap has been generated and saved in:
    /Administrator/ftp/ismsnap-20160618175808.tar.gz
   ```

   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.

   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 maintenance data capacity" in "User's Guide."

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.

- vc-support log is collected from vCenter as maintenance documentation for the Virtual Resources Management. For details, refer to "To collect ESX/ESXi and vCenter Server diagnostic data" from the following URL.

  https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2032892

  In Step 6 of the log collection procedure in the URL above, for the ESXi host log collection target, select all the vSAN cluster ESXi hosts where an error has occurred.

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 to ISM-VA

When you apply patches to ISM-VA, execute the following procedure.

This section describes the procedure to transfer the patch file (ISM240x_S20190901-01.tar.gz) to "/Administrator/ftp" of the ISM-VA and to apply the patch.

Note

- When applying patches, stop the ISM service temporarily.
- After applying the patch, reboot ISM-VA.
- Before applying the patch, back up ISM-VA.

  For information on the procedure to back up ISM-VA, refer to "2.1.2 Export ISM-VA."

1. Connect with FTP as an administrator to transfer the patch file to the ISM-VA.

   Access "ftp://<ISM administrator><password>@<ISM-VA IP address>/Administrator/ftp" to store the patch file.

   Note

   - Patch files (tar.gz format) are included in the published files (zip format).
     Decompress the published files to obtain the patch files.
   - When you transfer the patch files with FTP, transfer them in binary mode.

2. Log in to the ISM-VA as an administrator to connect with SSH.
3. In order to apply patches, stop the ISM service temporarily.

   ```
   # ismadm service stop ism
   ```

4. Execute the command for applying patches.

   Execute the following command, specifying the patch file.

   ```
   # ismadm system patch-add -file <Patch file>
   ```

   Example of command execution

   ```
   # ismadm system patch-add -file /Administrator/ftp/ISM240x_S20190901-01.tar.gz
   ```

   If the following is displayed, patch application is complete.

   ```
   Complete!
   ======================================
            Update finished successfully.
            Please restart ISM-VA.
   ======================================
   ```

5. Confirm that the patches are applied.

   ```
   # ismadm system show
   ```

   Confirm that the [ISM Version] of the command results output is the version of the applied patch.

   Example:

```
ISM Version     : 2.4.0.x (S20190901-01)
```

6. After applying the patch, restart ISM-VA.

```
# ismadm power restart
```

This finishes the procedure for applying the patches to ISM-VA.

9.2 Upgrade ISM-VA

If you need to upgrade ISM, contact your local Fujitsu customer service partner.

Note

- If you want to upgrade from V1.0 - V1.5 to V2.4, contact your local Fujitsu customer service partner.
- Before upgrade, back up ISM-VA.

  For information on the procedure to back up ISM-VA, refer to "2.1.2 Export ISM-VA."

After obtaining the upgrade file, execute upgrade according to the following procedure.

1. Transfer the upgrade files to ISM-VA with FTP.

   Access "ftp://<ISM-VA IP address at restoration destination>/Administrator/ftp" with FTP to store the upgrade file.

   For the upgrade file name, refer to "readme.txt" or "readme_en.txt" stored in the upgrade program.

   For information on the procedure to transfer with FTP, refer to "2.1.2 FTP Access" in "User's Guide."

2. From the Console as an administrator, log in to ISM-VA.

3. In order to execute upgrade, stop the ISM service temporarily.

```
# ismadm service stop ism
```

4. Execute the upgrade command.

   Execute the following command, specifying the upgrade file name.

```
# ismadm system upgrade -file <Upgrade file name>
```

   Example of command execution

```
# ismadm system upgrade -file /Administrator/ftp/ISM240_S2019xxxx-0X.tar.gz
```

5. After executing the upgrade, restart ISM-VA.

```
# ismadm power restart
```