

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

## **User's Guide**

CA92344-2707-01  
February 2019

# Preface

## Purpose

This manual describes the installation procedure and the general functions 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")



"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 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 and 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.  In this manual, it is referred to as "ISM for PRIMEFLEX Parameter List."
FUJITSU Software Infrastructure Manager V2.4	This document defines the terms that you need to understand in order to use this product.  In this manual, it is referred to as "Glossary."

Manual Name	Description
Infrastructure Manager for PRIMEFLEX V2.4 Glossary	
FUJITSU Software Infrastructure Manager V2.4 Infrastructure Manager for PRIMEFLEX V2.4 Plug-in and Management Pack Setup Guide	<p>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.</p> <ul style="list-style-type: none"> <li>- Infrastructure Manager Plug-in for Microsoft System Center Operations Manager</li> <li>- Infrastructure Manager Plug-in for Microsoft System Center Virtual Machine Manager</li> <li>- Infrastructure Manager Plug-in for VMware vCenter Server</li> <li>- Infrastructure Manager Plug-in for VMware vCenter Server Appliance</li> <li>- Infrastructure Manager Management Pack for VMware vRealize Operations</li> </ul> <p>In this manual, it is referred to as "ISM Plug-in/MP Setup Guide."</p>

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 system administrators, network administrators, facility administrators, and service technicians who have sufficient knowledge of hardware 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.



.....  
Describes the content of an important point.  
.....



.....  
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 7.6 (for Intel64)	RHEL 7.6	Red Hat Enterprise Linux Or Linux
Red Hat Enterprise Linux 7.5 (for Intel64)	RHEL 7.5	
Red Hat Enterprise Linux 7.4 (for Intel64)	RHEL 7.4	
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)	

Official name	Abbreviation		
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 (for AMD64 & Intel64)	SUSE 15(AMD64) SUSE 15(Intel64) or SLES 15(AMD64) SLES 15(Intel64)	SUSE Linux Enterprise Server  Or Linux	
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)		
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	-	-

# Contents

---

Chapter 1 Overview of Infrastructure Manager.....	1
1.1 Overview.....	1
1.1.1 Configuration of Functions.....	2
1.1.2 Product System and Licenses.....	3
1.2 Overview of Main Functions.....	4
1.2.1 Overview of Node Management.....	4
1.2.2 Overview of Monitoring.....	4
1.2.3 Overview of Profile Management.....	4
1.2.4 Overview of Log Management.....	4
1.2.5 Overview of Firmware Management.....	5
1.2.6 Overview of Network Management.....	5
1.2.7 Overview of Virtual Resource Management.....	5
1.2.8 Overview of Packet Analysis of Virtual Network.....	6
1.2.9 Overview of ISM for PRIMEFLEX.....	6
1.3 ISM Functions and Infrastructure Operation Management Scenarios.....	7
1.3.1 ISM Function Image for Each Infrastructure Operation Management Scene.....	7
1.4 Configuration.....	10
1.5 System Requirements.....	12
1.5.1 System Requirements for ISM-VA (Virtual Machines).....	12
1.5.2 System Requirements for Management Terminals.....	13
1.5.3 Service Requirements for ISM Operations.....	14
1.5.4 Operation Requirements for ISM for PRIMEFLEX.....	15
1.6 ISM Maintenance and Updates.....	16
Chapter 2 Functions of ISM.....	17
2.1 User Interface.....	17
2.1.1 GUI.....	17
2.1.2 FTP Access.....	20
2.1.3 Console Access.....	22
2.1.4 REST API.....	22
2.2 Node Management.....	22
2.2.1 Registration of Datacenters/Floors/Racks/Nodes.....	22
2.2.1.1 Registration of datacenters/floors/racks.....	23
2.2.1.2 Registration of nodes.....	23
2.2.1.3 Management of node information.....	25
2.2.1.4 Management of information on node mounting positions in racks.....	25
2.2.1.5 Registration of node OS information.....	26
2.2.1.6 Discovery of nodes.....	26
2.2.1.7 Adding tags to nodes.....	33
2.2.2 Confirmation of Datacenters/Floors/Racks/Nodes.....	34
2.2.3 Editing of Datacenters/Floors/Racks/Nodes.....	35
2.2.4 Deletion of Datacenters/Floors/Racks/Nodes.....	36
2.3 Monitoring.....	36
2.3.1 Setting of Monitoring Items and Threshold Values.....	37
2.3.2 Monitoring of Network Statistics Information.....	38
2.3.3 Action Settings.....	38
2.3.4 Registration of Alarm Settings.....	42
2.3.5 Graph Display of Monitoring History.....	45
2.4 Profile Management.....	45
2.4.1 Profile Usage.....	46
2.4.2 Profiles and Policies.....	47
2.4.2.1 Creation of policy groups/policies.....	49
2.4.2.2 Creation of profile groups/profiles.....	49
2.4.2.3 Assignment of profiles.....	50
2.4.2.4 Editing and reassigning profiles.....	50



2.4.2.5 Releasing and deleting profiles.....	51
2.4.2.6 Exporting and importing profiles.....	52
2.4.2.7 Editing/deleting profile groups.....	53
2.4.2.8 Editing/deleting policy groups.....	53
2.4.2.9 Specifying behavior when assigning profiles.....	53
2.4.3 OS Installation Settings.....	54
2.4.4 Virtual IO Management.....	55
2.4.5 Pool Management.....	57
2.4.6 Confirmation of Boot Information.....	58
2.5 Log Management.....	59
2.5.1 Types of Collectable Logs.....	60
2.5.2 Setting Log Retention Periods.....	62
2.5.3 Setting Log Collection Targets, Dates and Times.....	63
2.5.4 Operations for Log Collection.....	64
2.5.5 Searching Node Logs.....	66
2.5.6 Downloading Node Logs.....	67
2.5.7 Downloading Archived Logs.....	68
2.5.8 Deleting Node Logs.....	69
2.5.9 Deleting Archived Logs.....	70
2.6 Firmware Management.....	71
2.6.1 Confirmation of Firmware Versions of Nodes.....	71
2.6.2 Firmware Updates.....	72
2.6.2.1 How to update firmware.....	72
2.6.2.2 Behavior during updates.....	73
2.6.2.3 Execution of firmware updates.....	74
2.6.3 Confirmation of Documentation that is supplied with Firmware Data.....	76
2.6.4 Job Management.....	78
2.6.5 Firmware Baseline.....	78
2.6.5.1 Creating Firmware Baseline definitions.....	79
2.6.5.2 Assigning Firmware Baseline definitions.....	79
2.6.5.3 Releasing Firmware Baseline definition assignments.....	80
2.6.5.4 Firmware update using Firmware Baseline definitions.....	80
2.6.5.5 Editing Firmware Baseline definitions.....	80
2.6.5.6 Deleting Firmware Baseline definitions.....	81
2.7 Network Management.....	81
2.7.1 Display of Network Connection Information.....	82
2.7.2 Updates of Network Management Information.....	84
2.7.3 Confirmation of Information on Changes in Network Connections.....	84
2.7.4 Setting of Reference Information for Changes in Network Connections.....	85
2.7.5 Display of Network Statistics Information.....	86
2.7.6 Confirmation of VLAN and Link Aggregation Settings.....	86
2.7.7 Change of VLAN Settings.....	87
2.7.8 Change of Link Aggregation Settings.....	88
2.7.9 Manual Setting of Network Connection Information.....	88
2.8 Power Capping.....	89
2.8.1 Adding/Editing Power Capping Settings.....	89
2.8.2 Enabling/Disabling Power Capping.....	90
2.9 Virtual Resource Management.....	90
2.9.1 Supported Virtual Resources.....	91
2.9.2 GUI for Virtual Resource Management.....	92
2.9.3 Operation of Virtual Resource Management.....	93
2.9.3.1 Monitoring of the utilization status of storage pools.....	94
2.9.3.2 Identification of the errors in storage pools.....	97
2.9.3.3 Updates of virtual resources.....	101
2.10 Backup/Restore Hardware Settings.....	102
2.10.1 Backup of the File of Backup Hardware Settings.....	103
2.10.2 Export of the File of Backup Hardware Settings.....	103

2.10.3 Addition of Profiles from the File of Backup Hardware Settings.....	103
2.10.4 Addition of Policies from the File of Backup Hardware Settings.....	104
2.10.5 Import of the File of Backup Hardware Settings.....	104
2.10.6 Restoration of the File of Backup Hardware Settings.....	105
2.10.7 Deletion of the File of Backup Hardware Settings.....	105
2.11 Packet Analysis of Virtual Network.....	106
2.11.1 Support Targets.....	106
2.11.2 Check of Analysis VM.....	106
2.11.3 Display Item of Packet Analysis of Virtual Network.....	107
2.11.4 Function difference of Packet Analysis of Virtual Network.....	107
2.11.5 Operation of Packet Analysis of Virtual Network.....	108
2.12 Functions of ISM for PRIMEFLEX.....	108
2.12.1 Cluster Management.....	109
2.12.1.1 Cluster Management GUI.....	109
2.12.1.2 Environments supported by Cluster Management.....	118
2.12.1.3 Refreshing cluster information.....	119
2.12.1.4 Management and monitoring of clusters.....	120
2.12.1.5 Virtual disk monitoring for PRIMEFLEX for Microsoft Storage Spaces Direct.....	122
2.12.2 Cluster Creation.....	123
2.12.2.1 Automatic setting item.....	124
2.12.2.2 Link with Profile Management.....	127
2.12.2.3 Cluster Definition Parameters.....	128
2.12.2.4 Task list.....	128
2.12.3 Cluster Expansion.....	129
2.12.3.1 Automatic setting item.....	130
2.12.3.2 Link with Profile Management.....	132
2.12.3.3 Cluster Definition Parameters.....	133
2.12.3.4 Task list.....	134
2.12.4 Firmware Rolling Update.....	134
2.12.4.1 Operation in link with Firmware Management.....	135
2.12.4.2 Task list.....	136
2.13 Functions of ISM Operating Platform.....	137
2.13.1 User Management.....	137
2.13.2 Repository Management.....	144
2.13.2.1 Storing and deleting firmware data.....	144
2.13.2.2 Storing and deleting OS installation files.....	149
2.13.2.3 Storing and deleting ServerView Suite DVD.....	150
2.13.3 Installation of Emulex OneCommand Manager CLI and Qlogic QConvergeConsole CLI.....	151
2.13.4 Task Management.....	151
2.13.5 ISM-VA Management.....	152
2.13.5.1 List of commands in ISM-VA Management.....	153
2.13.6 Management of Cloud Management Software.....	156
2.13.6.1 Registering cloud management software.....	156
2.13.6.2 Retrieving information from cloud management software.....	157
2.13.6.3 Editing cloud management software.....	158
2.13.6.4 Deleting cloud management software.....	159
2.13.7 Shared Directory Management.....	159
2.13.7.1 Adding shared directories.....	159
2.13.7.2 Editing shared directories.....	160
2.13.7.3 Deleting shared directories.....	160
2.13.7.4 Mounting shared directories.....	161
2.13.7.5 Unmounting shared directories.....	161
2.13.8 Link with ISM.....	161
2.13.8.1 Link display for other ISM status information.....	161
2.13.8.2 Certificate management for other ISM links.....	162
2.13.9 Linking with Other Software.....	163
2.13.9.1 Preparations in advance for Deep Security Link.....	164

2.13.9.2 Procedure to link with Deep Security.....	166
2.14 Operations When Deleting Nodes and When Modifying Groups.....	168
<b>Chapter 3 Installation of ISM.....</b>	<b>170</b>
3.1 Workflow for Installing ISM.....	170
3.2 Installation Design for ISM.....	171
3.2.1 Disk Resource Estimation.....	171
3.2.1.1 Estimation of log storage capacity.....	173
3.2.1.2 Estimation of required capacities for repositories.....	173
3.2.1.3 Estimation of node management data capacity.....	174
3.2.1.4 Estimation of ISM RAS log capacity.....	174
3.2.1.5 Estimation of maintenance data capacity.....	174
3.2.1.6 Estimation of required capacities for ISM backup/restoration.....	175
3.2.2 Network Design.....	175
3.2.3 Node Name Setup.....	175
3.2.4 User Design.....	176
3.3 Installation of ISM-VA.....	176
3.3.1 Installation on Microsoft Windows Server Hyper-V.....	176
3.3.2 Installation on VMware vSphere Hypervisor.....	177
3.3.3 Installation on KVM.....	177
3.4 Environment Settings for ISM-VA.....	178
3.4.1 First Start of ISM-VA.....	178
3.4.1.1 For ISM-VA running on Microsoft Windows Server Hyper-V (First Time).....	179
3.4.1.2 For ISM-VA running on VMware vSphere Hypervisor (First Time).....	179
3.4.1.3 For ISM-VA running on KVM (First Time).....	182
3.4.2 Initial Setup of ISM-VA.....	182
3.4.2.1 Initial setup using the Basic Setting Menu.....	182
3.4.2.2 Initial setup using the ismadm command.....	183
3.5 Registration of Licenses.....	186
3.6 Registration of Users.....	188
3.7 Allocation of Virtual Disks.....	188
3.7.1 Allocation of Virtual Disks to Entire ISM-VA.....	188
3.7.2 Allocation of Virtual Disks to User Groups.....	189
3.8 Pre-Settings for Virtual Resource Management.....	190
3.9 Pre-Settings for Cluster Management.....	191
3.9.1 Pre-Settings for vSAN.....	191
3.9.2 Pre-settings for Microsoft Storage Spaces Direct.....	194
3.9.3 Pre-settings for ISM.....	195
<b>Chapter 4 Operation of ISM.....</b>	<b>197</b>
4.1 Start and Stop of ISM.....	197
4.1.1 Start of ISM-VA.....	197
4.1.1.1 For ISM-VA running on Microsoft Windows Server Hyper-V (after installation).....	197
4.1.1.2 For ISM-VA running on VMware vSphere Hypervisor (after installation).....	198
4.1.1.3 For ISM-VA running on KVM (after installation).....	201
4.1.2 Stop of ISM-VA.....	201
4.1.3 Restart of ISM-VA.....	202
4.1.4 Start and Stop of ISM Service.....	202
4.2 ISM-VA Basic Settings Menu.....	203
4.3 Modification of Destination Port Number.....	205
4.4 Backup and Restoration of ISM-VA.....	205
4.4.1 Backup/restoration of ISM-VA with the Hypervisor.....	206
4.4.2 Backup/restoration of ISM with the ISM-VA Management Command.....	206
4.4.2.1 Backup of ISM.....	210
4.4.2.2 Restoration of ISM.....	211
4.4.2.3 Display of backup file list.....	211
4.5 Collection of Maintenance Data.....	212
4.5.1 ISM/ISM-VA Maintenance Data.....	212

4.5.1.1	Switching the ISM RAS Log mode.....	213
4.5.1.2	Switching the ISM RAS Log level.....	213
4.5.1.3	Specification of core file collection directory.....	214
4.5.1.4	How to collect ISM maintenance data.....	215
4.5.2	ISM for PRIMEFLEX Maintenance Data.....	215
4.5.2.1	Logs for Cluster Creation.....	215
4.5.2.2	Logs for Cluster Expansion.....	215
4.5.2.3	Logs for Cluster Management.....	216
4.5.2.4	Logs for Firmware Rolling Update.....	216
4.6	Management of Virtual Disks.....	216
4.6.1	Cancellation of Virtual Disk Allocations.....	216
4.6.2	Allocation of Additional Virtual Disks to Entire ISM-VA.....	217
4.6.3	Allocation of Additional Virtual Disks to User Groups.....	218
4.7	Certificate Activation.....	219
4.7.1	Deployment of SSL Server Certificates.....	219
4.7.2	Display of SSL Server Certificates.....	219
4.7.3	Export of SSL Server Certificates.....	219
4.7.4	Creation of Self-signed SSL Server Certificates.....	220
4.7.5	Download of CA Certificates.....	220
4.8	License Settings.....	220
4.9	Network Settings.....	221
4.10	Alarm Notification Settings.....	222
4.11	ISM-VA Service Control.....	222
4.12	Display of System Information.....	223
4.13	Modification of Host Names.....	224
4.14	Operation of Plug-in.....	224
4.14.1	Application of Plug-in.....	224
4.14.2	Display of Plug-in.....	225
4.14.3	Deletion of Plug-in.....	225
4.15	ISM-VA Internal DHCP Server.....	226
4.15.1	Settings for ISM-VA Internal DHCP Server.....	226
4.15.2	Operation of ISM-VA Internal DHCP Service.....	227
4.15.3	Confirmation of ISM-VA Internal DHCP Server Information.....	228
4.15.4	Switch of DHCP Servers.....	228
4.16	MIB File Settings.....	228
4.17	Application of Patches.....	229
4.18	Upgrade of ISM-VA.....	230
4.19	ISM-VA Statistics Information Display.....	230
4.19.1	Overview of Statistics Information Display.....	230
4.19.2	Network Statistics Information Display.....	231
4.19.3	Real Time Information Display.....	232
4.19.4	Output Statistics Information File.....	232
4.20	Change of the SSL/TLS Protocol Version.....	233
4.21	Settings for Links with Other Software.....	233
4.22	File Upload Using the GUI.....	234
<b>Chapter 5</b>	<b>Maintenance of Nodes.....</b>	<b>235</b>
5.1	Maintenance Mode.....	235
5.2	Investigation of Errors.....	236
<b>Appendix A</b>	<b>Instructions for Manage and Operate Nodes.....</b>	<b>237</b>
A.1	ISM Environmental Settings.....	237
A.1.1	DHCP/PXE Settings in Using Profile Management/Firmware Management.....	237
A.1.2	Pre-settings for Virtual Resource Management.....	238
A.1.3	Notes on MIB File Import.....	241
A.2	Details of Managed Nodes Settings.....	243
A.2.1	List of Available Port Numbers.....	243
A.2.2	Details of Node Settings.....	245

A.3 Details of Other Settings.....	248
A.3.1 ETERNUS DX/AF Drive Enclosure Display.....	248
A.3.2 General Standards for Firmware Update Time.....	249
A.3.3 General Standards for Disk Usage in Using Log Management.....	250
Appendix B Uninstallation of ISM-VA.....	254
Appendix C Successor Cluster Expansion.....	257
C.1 Successor Cluster Expansion Requirements.....	257
C.1.1 Addable Successor Servers.....	257
C.1.2 Network Configuration.....	257
C.1.3 Hardware Requirements.....	259
C.1.4 Software Requirements.....	262
C.2 Successor Cluster Expansion.....	263
C.2.1 Preparations.....	264
C.2.2 Cluster Expansion with ISM for PRIMEFLEX.....	265
Appendix D Troubleshooting.....	266

# Chapter 1 Overview of Infrastructure Manager

This chapter describes an overview of Infrastructure Manager and Infrastructure Manager for PRIMEFLEX.

## 1.1 Overview

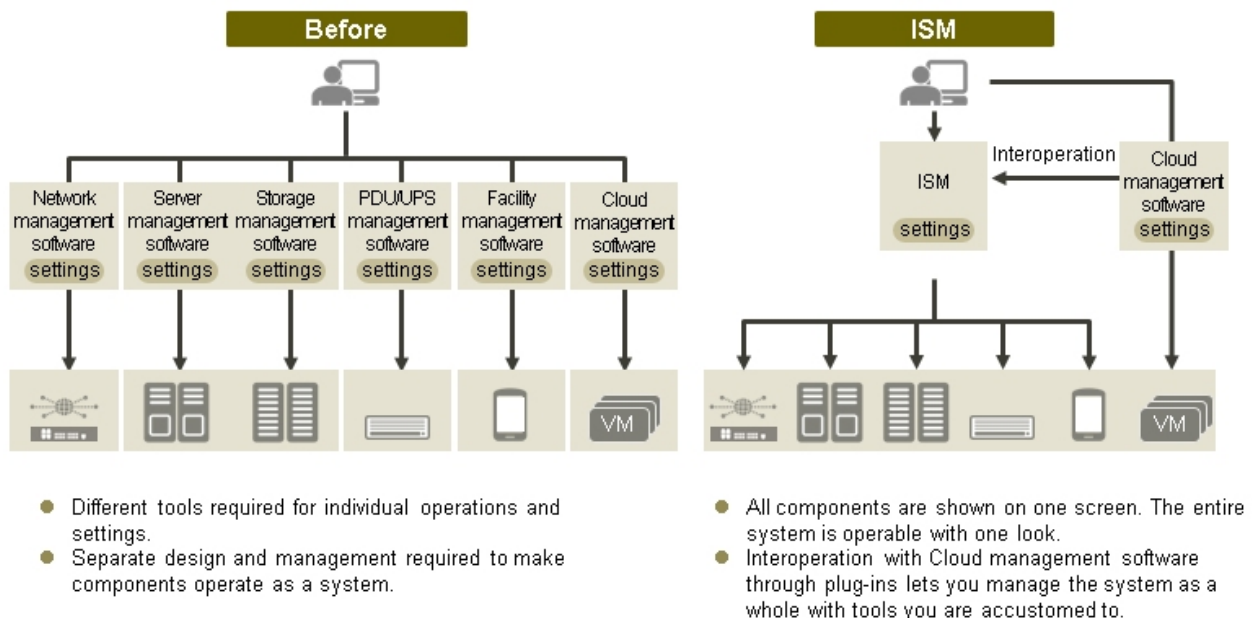
By installing Infrastructure Manager or Infrastructure Manager for PRIMEFLEX, multiple and various types of ICT devices can be managed in an integrated way. With this software, you can monitor the status of all the ICT devices in a datacenter or a machine room. You can also execute batch firmware updates for multiple devices and configure servers automatically. It can reduce operating costs and increase the operation quality for the operation manager.

Hereafter, when a description applies to both Infrastructure Manager and Infrastructure Manager for PRIMEFLEX, both will collectively be referred to as "Infrastructure Manager" or "ISM."

When description is given only for Infrastructure Manager for PRIMEFLEX, it is referred to as "ISM for PRIMEFLEX."

ICT and facility devices that are operated and managed in an ISM environment are called "nodes."

Figure 1.1 Integrated operation and management through installation of ISM

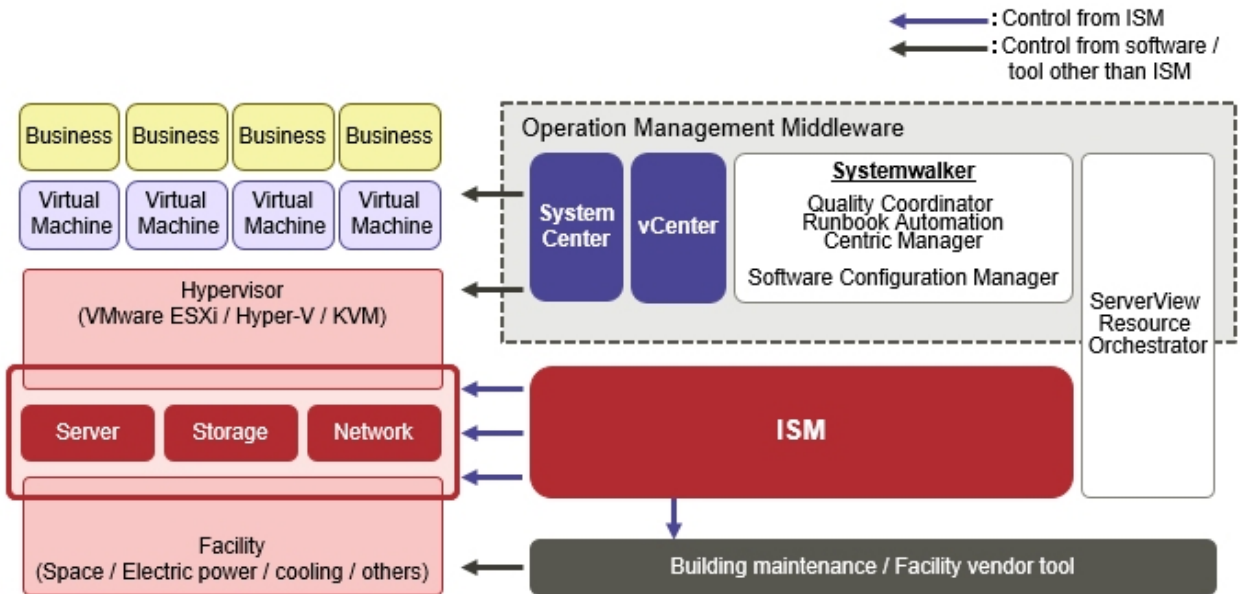


- Optimize large-scale collective operations at the physical layer, spanning servers, storages, and networks
  - Hardware management, collection and management of configuration information
  - Integration of the management screen
  - Integrated firmware/BIOS update operations for servers, storages, and switches

ISM primarily handles the management and operations of servers, storages, networks, and other hardware. It can link with operation management middleware that manages virtualized datacenter resources. UPS/PDU and other facilities supported by ISM can be controlled from ISM.

By linking ISM with operation management middleware, seamless operation management of physical resources and virtual resources becomes possible.

Figure 1.2 Working in links with other products



For the latest information on managed devices and supported functions, contact your local Fujitsu customer service partner.

### 1.1.1 Configuration of Functions

ISM is software that manages and operates the ICT devices already installed as well as new ICT devices.

ISM for PRIMEFLEX is software that manages and operates the devices configured for the vertically integrated Virtualized Platform PRIMEFLEX HS or PRIMEFLEX for VMware vSAN and PRIMEFLEX for Microsoft Storage Spaces Direct. It contains the ISM features and both ICT devices that are already installed and new ones can be managed and operated.

#### Point

ISM for PRIMEFLEX is ISM with the Virtualized Platform Expansion function added.

For detail information on the Virtualized Platform Expansion function, refer to "[1.2.9 Overview of ISM for PRIMEFLEX.](#)"

The functions supported by ISM and ISM for PRIMEFLEX are as follows.

Note: Y = Supported, N = Not supported

Function	Product	
	ISM	ISM for PRIMEFLEX
Node Management	Y	Y
Monitoring	Y	Y
Profile Management	Y	Y
Log Management	Y	Y
Firmware Management	Y	Y
Network Management	Y	Y
Power Capping	Y	N
Virtual Resource Management	Y	Y
Backup/Restore Hardware Settings	Y	Y
Packet Analysis of Virtual Network	Y	Y

Function		Product	
		ISM	ISM for PRIMEFLEX
Virtualized Platform Expansion function	Cluster Management	N	Y
	Cluster Creation	N	Y
	Cluster Expansion	N	Y
	Firmware Rolling Update	N	Y

For details of each function, refer to "[Chapter 2 Functions of ISM.](#)"

## 1.1.2 Product System and Licenses

The ISM products comprise media packs, server licenses, and node licenses.

ISM product	ISM	ISM for PRIMEFLEX
Media packs	<ul style="list-style-type: none"> <li>- Infrastructure Manager for Red Hat Enterprise Linux KVM Media Pack V2</li> <li>- Infrastructure Manager for vSphere Media Pack V2</li> <li>- Infrastructure Manager for Windows Server Hyper-V Media Pack V2</li> </ul>	<ul style="list-style-type: none"> <li>- Infrastructure Manager for PRIMEFLEX Media Pack (ESXi) V2</li> <li>- Infrastructure Manager for PRIMEFLEX Media Pack (Hyper-V) V2</li> </ul>
Server licenses	Infrastructure Manager Advanced Edition Server License V2	Infrastructure Manager Advanced Edition for PRIMEFLEX Server License V2
Node licenses	Infrastructure Manager Node License V2 [Note 1]	Infrastructure Manager for PRIMEFLEX Node License V2 [Note 1]

[Note 1]: The product name differs depending on the number of nodes that can be used.

### Media packs

The ISM installation media. ISM is provided as packaged virtual appliance into which the software serving as the operating platform for virtual machines. You must select the media pack according to the hypervisor operating ISM (virtual appliance).

### Server licenses

License permitting the use of ISM. A server license is required to operate ISM.

### Node licenses

A license granting permission for the maximum number of nodes that can be managed in ISM. A node license is required to monitor/operate nodes in ISM. It is possible to add licenses as required.



### Note

- The name of this product has changed to "Infrastructure Manager" since ISM 2.3.0. The "ServerView Infrastructure Manager" license can be used also for the upgrade to ISM 2.4.
- Use media packs and server licenses/node licenses for the same product. When using an ISM media pack, server licenses/node licenses for ISM for PRIMEFLEX cannot be used. The reverse is also true.
- For the procedure for estimating the node licenses and the official product names for the server licenses and node licenses you are purchasing, contact your local Fujitsu customer service partner.

For the installation procedure using a media pack, refer to "[3.3 Installation of ISM-VA.](#)"

ISM requires the registration of both server licenses and node licenses. For the procedure for registering server licenses and node licenses, refer to "[3.5 Registration of Licenses.](#)"



Also, for the procedure to check the license type, refer to "[4.8 License Settings](#)."

To install ISM, preparations and environment settings are required. When installing, refer to "[Chapter 3 Installation of ISM](#)."

## 1.2 Overview of Main Functions

---

This section describes an overview of the ISM functions.

### 1.2.1 Overview of Node Management

---

Node Management is a function that executes the following actions.

- Device information management  
Manages device information such as model names, serial numbers, and IP addresses.
- Device registration  
Registers nodes to be managed by ISM.

With this function, you can discover and register the nodes that are connected to your network, making your node registration work more efficient. Moreover, you can manage rack locations on datacenter floors, node positions within racks, as well as configurations and current statuses of nodes. By using the function of visualizing the nodes in the racks (Rack View) or location on the floors (Floor View), you can execute Node Management intuitively.

For details on Node Management, refer to "[2.2 Node Management](#)."

### 1.2.2 Overview of Monitoring

---

Monitoring is a function you can use to monitor for the following events.

- SNMP Traps sent from nodes
- Changes in the "Normal" and "Error" statuses indicated by nodes
- Whether the values for Air Inlet Temperature, CPU Usage, and Power Consumption obtained from each node are within the normal ranges you have set in ISM

For these events, you can set up actions such as executing a user-created script or sending an e-mail. You can also monitor nodes according to each user's operating procedure.

For details on Monitoring, refer to "[2.3 Monitoring](#)."

### 1.2.3 Overview of Profile Management

---

Profile Management is a function that creates, stores, and assigns profiles which are the setting information for the managed nodes.

- Execute hardware settings for the managed nodes
- Install OS on the managed nodes (servers)
- Execute assignment of virtual MAC address/virtual WWN and boot settings to managed nodes (servers)
- Creates RAID/Hot spare on managed nodes (storages)

Profile Management realizes batched processing of multiple managed nodes settings and makes it easy to execute settings to the new managed nodes.

For details on Profile Management, refer to "[2.4 Profile Management](#)."

### 1.2.4 Overview of Log Management

---

Log Management is a function that operates log collection of various kinds of logs (Hardware logs, Operating System logs, and ServerView Suite logs) for multiple managed nodes together and executes integrated management of collected logs.

- Automate collection of various kinds of logs

- Automate log management by setting their retention period/generation
- Increase efficiency of error investigation by detecting conditions of messages included in logs

You can operate error monitoring/investigation for the managed nodes effectively by using Log Management.

For details on Log Management, refer to "[2.5 Log Management](#)."

## 1.2.5 Overview of Firmware Management

---

Firmware Management is a function that operates firmware updates for multiple managed nodes together and manages versions of the firmware in an integrated manner.

- Automate firmware updates
- Integrate management of the firmware version of the managed nodes

Firmware Management can decrease your time and efforts for the maintenance of managed nodes.

For details on Firmware Management, refer to "[2.6 Firmware Management](#)."

## 1.2.6 Overview of Network Management

---

Network Management is a function that manages the status of physical connection between managed nodes and the status of virtual connection between virtual machines, virtual switches, and virtual routers.

Network Map that displays wiring of the network and its connection status enables the following operations.

- Grasp the extent of the impact of the network error visually
- Monitor change of the network connection status
- Grasp network performance (traffic) by using a graph
- Change the network switch settings (VLAN settings, link aggregation settings) easily

Network Management helps you monitor and investigate network errors between managed nodes.

For details on Network Management, refer to "[2.7 Network Management](#)."

## 1.2.7 Overview of Virtual Resource Management

---

Virtual resources means a virtual storage (storage pool) configured with multiple storages.

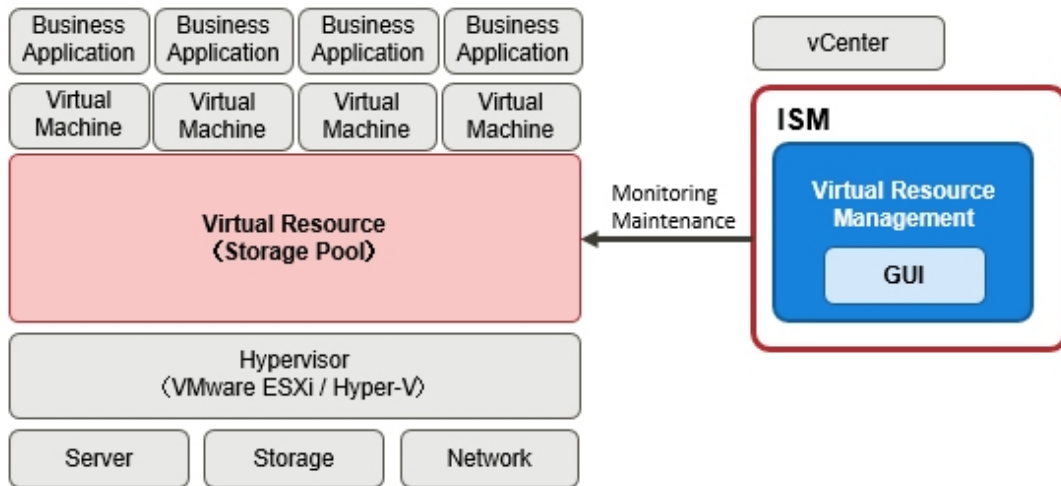
Virtual Resource Management is a function that manages storage pools by displaying status and usage rate of the storage pools.

- Monitor the usage and status of the storage pool in connection with the status of the configuring hardware devices (nodes)
- Enable smooth maintenance operation by an integrated management of storage pools on the display
- Supports re-deployment and addition (provisioning) of resources by an integrated management of storage pools to visualize the usage rate of resources and predicting the timing for additions

Virtual Resource Management supports your monitoring of errors and maintenance operation by making it easy to check relations of managed nodes and resource pools.

For details on Virtual Resource Management, refer to "[2.9 Virtual Resource Management](#)."

Figure 1.3 Overview of Virtual Resource Management



## 1.2.8 Overview of Packet Analysis of Virtual Network

Packet Analysis of Virtual Network is a function that displays the trends of the traffic volume and the status of the traffic quality by port, by network, or by host based on the collected packet information.

- Grasping the traffic status visually
- Support for the identification of the causes for degradations in performance

Packet Analysis of Virtual Network helps you grasp network trends and identify any trouble smoothly by yourselves.

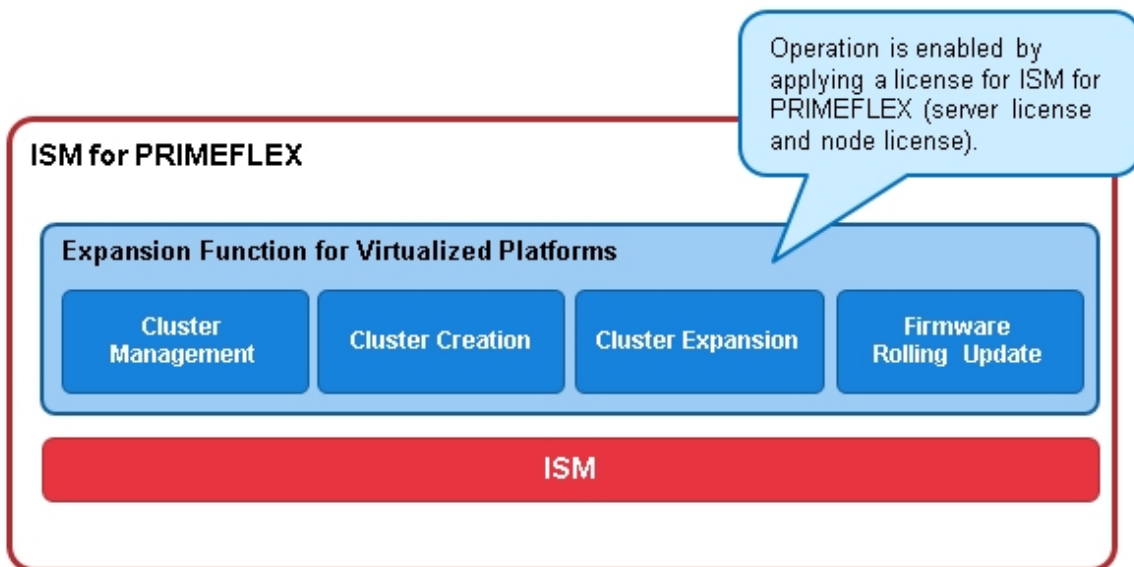
For details on Packet Analysis of Virtual Network, refer to "2.11 Packet Analysis of Virtual Network."

## 1.2.9 Overview of ISM for PRIMEFLEX

ISM for PRIMEFLEX is ISM with the Virtualized Platform Expansion function added. In addition to the ISM functions, functions for Cluster Management, Cluster Creation, Cluster Expansion, and Firmware Rolling Update are provided.

ISM for PRIMEFLEX is infrastructure management software that is installed in the vertically integrated virtual platform environments for PRIMEFLEX HS, PRIMEFLEX for VMware vSAN, and PRIMEFLEX for Microsoft Storage Spaces Direct.

Figure 1.4 Overview of ISM for PRIMEFLEX



The following is an overview of the Virtualized Platform Expansion function provided by ISM for PRIMEFLEX.

Virtualized Platform Expansion function	Overview of Function
Cluster Management	Displays the cluster information and various types of information for the related physical resources and virtual resources.
Cluster Creation	Automates the operation of creating second and later clusters, which differ from the existing one.
Cluster Expansion	Automates the operation of adding servers to expand a cluster when the cluster resources are being depleted.
Firmware Rolling Update	For a series of servers configuring the virtualized platform, firmware update can be executed without stopping the operations.

For details on the functions of ISM for PRIMEFLEX, refer to "2.12 Functions of ISM for PRIMEFLEX."

### Point

- Cluster Management can manage resources on a cluster basis.
- Cluster Creation uses the "Create Cluster" wizard added in ISM for PRIMEFLEX V2.3 to create clusters.
- Cluster Expansion uses the "Expand Cluster" wizard to expand clusters.
- Firmware Rolling Update uses the "FW Rolling Update" wizard added in ISM for PRIMEFLEX V2.4 to update firmware.

### Note

Power Capping cannot be used in ISM for PRIMEFLEX.

## 1.3 ISM Functions and Infrastructure Operation Management Scenarios

This section describes the major functions of ISM, separately for each usage.

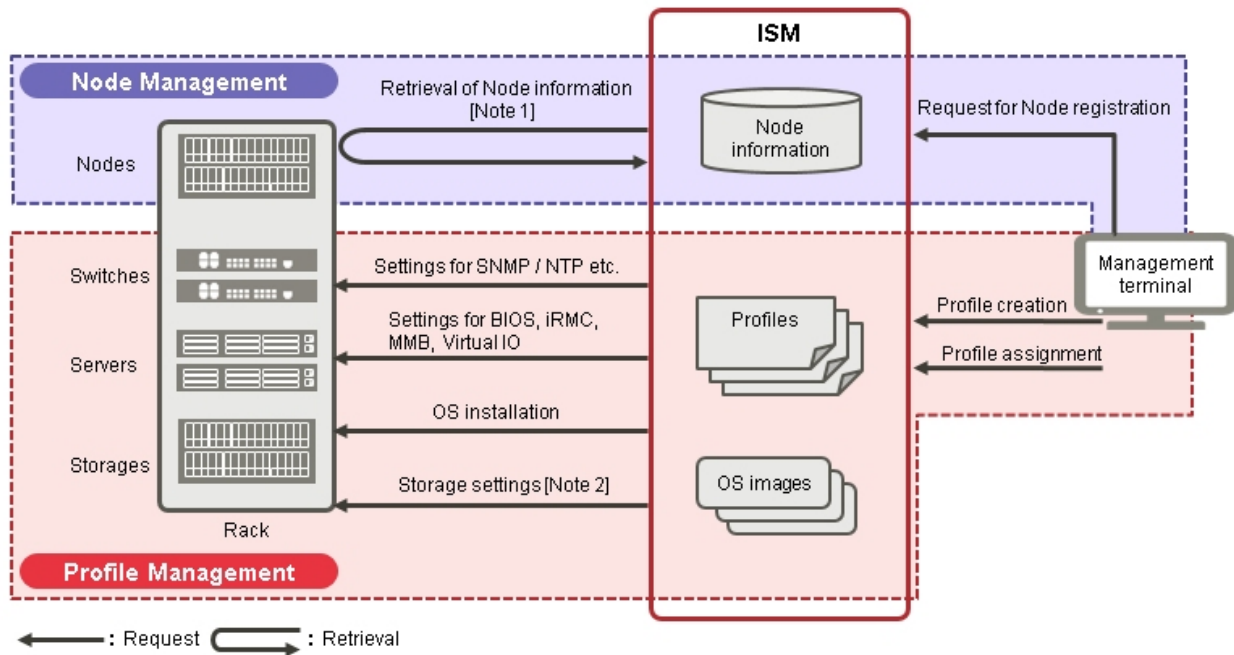
Functions of ISM	Operation Management Type		
	System Configuration	Monitoring operations for managed nodes	Maintenance of managed nodes
Node Management	Y	Y	-
Monitoring	-	Y	-
Profile Management	Y	-	-
Log Management	-	Y	Y
Firmware Management	-	-	Y
Network Management	-	-	Y
Power Capping	-	Y	-
Virtual Resource Management	-	Y	-

### 1.3.1 ISM Function Image for Each Infrastructure Operation Management Scene

## (1) System configuration

When you are initially installing ICT devices or adding new ICT devices, you can configure systems by effectively using Node Management and Profile Management.

Figure 1.5 Image of functions: system configuration



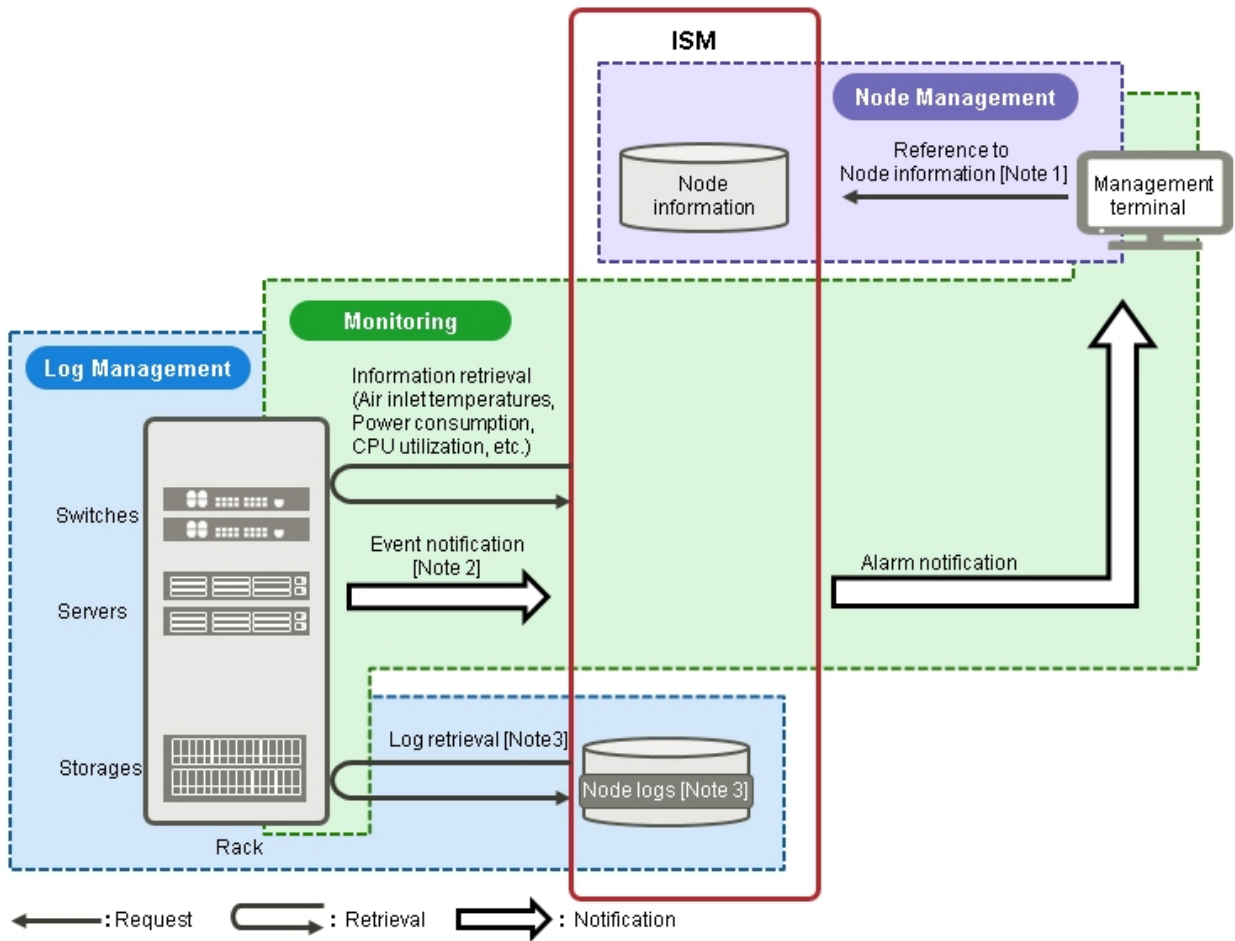
[Note 1]: Model names, serial numbers, IP addresses, and similar hardware information

[Note 2]: RAID group, volume, hot spare, and Affinity settings

## (2) Monitoring operations for managed nodes

When you are monitoring managed nodes, you can execute monitoring operations for managed nodes by effectively using Node Management, Monitoring and Log Management.

Figure 1.6 Image of functions: monitoring operations for managed nodes



[Note 1]: Model names, serial numbers, IP addresses, mounting positions in racks, and similar hardware information

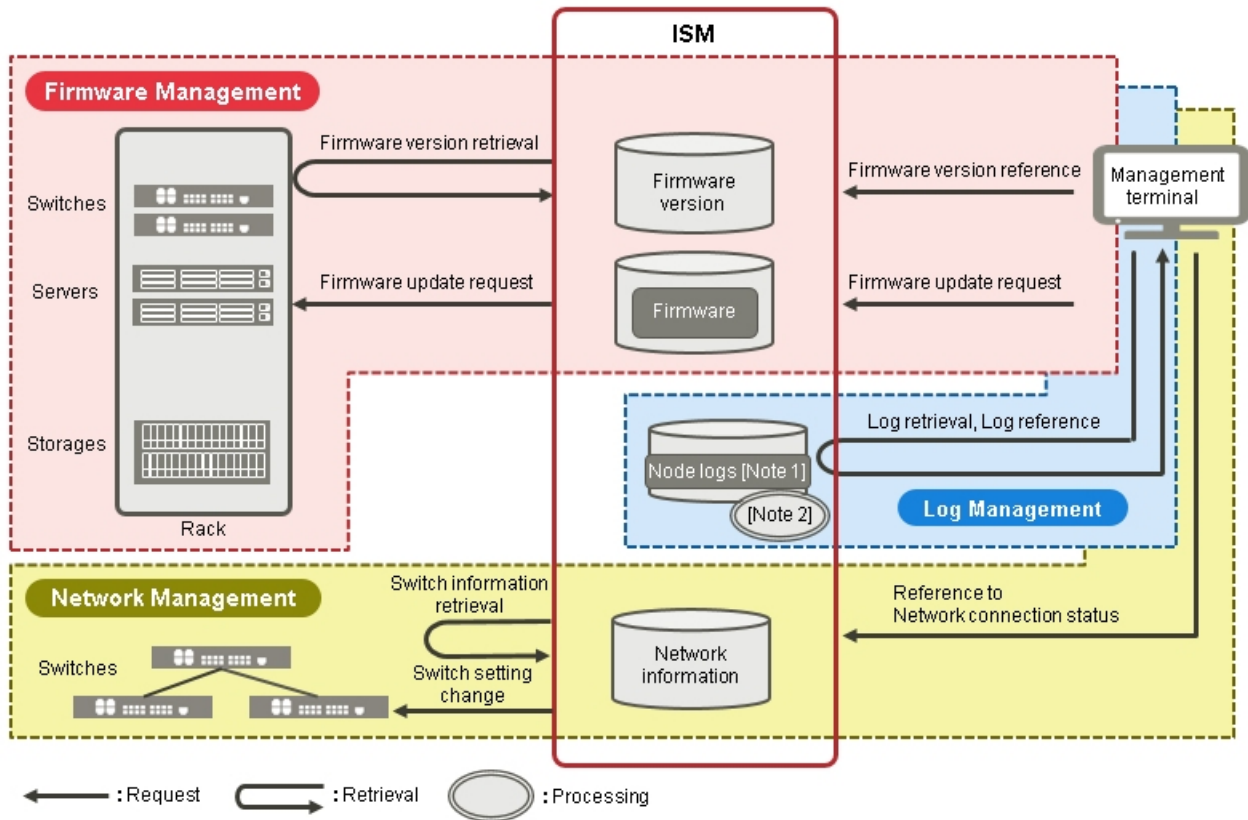
[Note 2]: SNMP traps

[Note 3]: Hardware logs and operating system logs

### (3) Maintenance of managed nodes

When you perform maintenance on managed nodes, you can execute the maintenance of managed nodes by using Log Management, Firmware Management, and Network Management.

Figure 1.7 Image of functions: maintenance of managed nodes



[Note 1]: Hardware logs and operating system logs

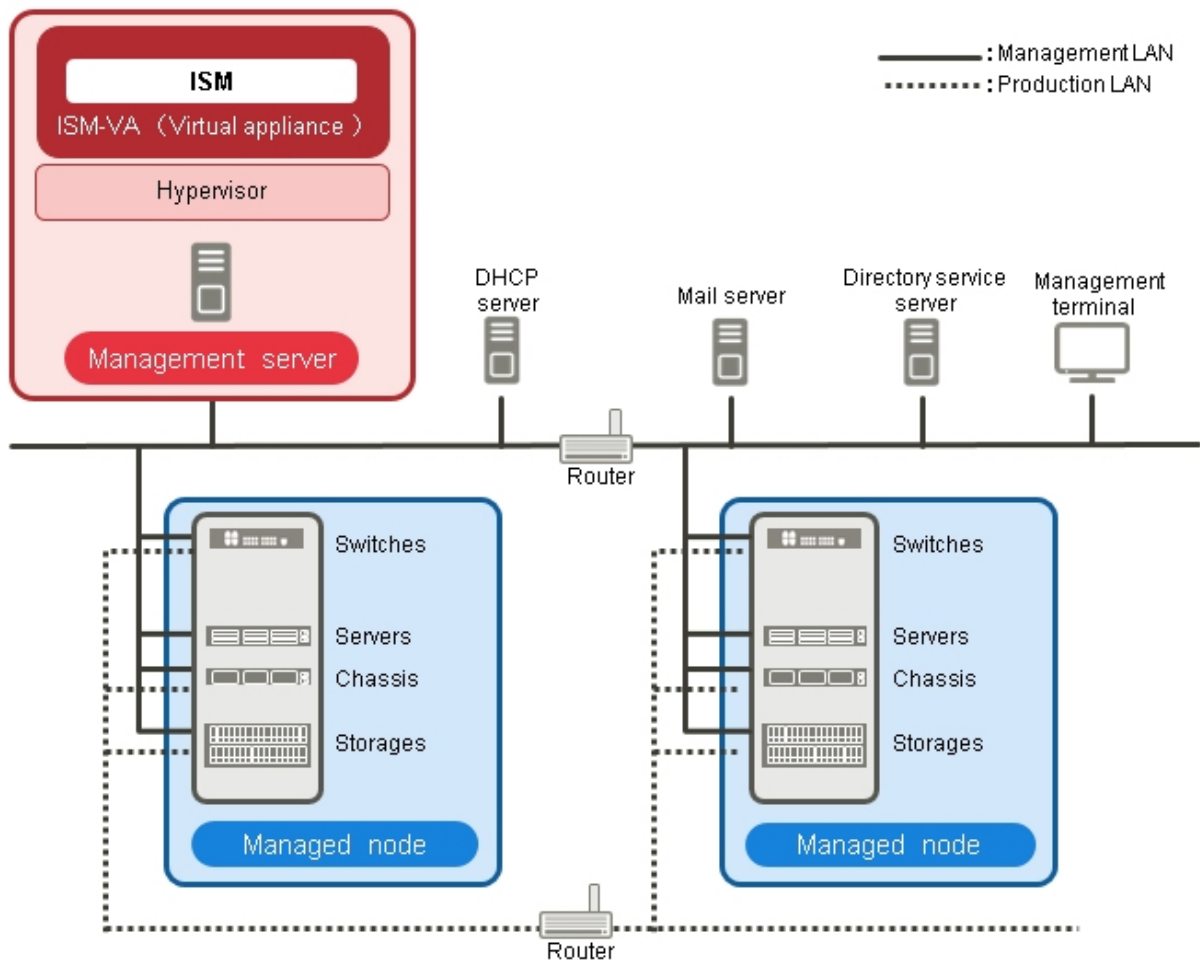
[Note 2]: Processing of log searches

## 1.4 Configuration

In principle, ISM runs on a server that is separate from the servers to be managed. This manual refers to devices that are being managed as "nodes" (or "managed nodes"), and to servers on which ISM is running as "management servers." The management server and nodes are connected via LAN.

You can define only one network interface for ISM. If you are going to configure multiple networks, configure the router to enable communication between the networks.

Figure 1.8 Network configuration



 Note

For details on the servers and services shown in "Figure 1.8 Network configuration" that are external to ISM, refer to "1.5.3 Service Requirements for ISM Operations."

Device and function		Description
Network	Management LAN	LAN used for communicating with the managed nodes so ISM can monitor and control these nodes and transfer data. To ensure security, an isolated connection environment is recommended.
	Production LAN	LAN used for transferring service data between servers and clients. This network does not connect to management servers.
Management server	Infrastructure Manager (ISM)	The software that is the operating platform of this product. ISM is provided as packaged virtual appliances into virtual machine.  The virtual appliances, which are packaged ISM, will hereafter be referred to as ISM-VA.  After installing ISM-VA on a hypervisor, you can control ISM-VA with a hypervisor console or an SSH client.
Management terminal		PC or tablet that is used for operating ISM through the management LAN.
Managed nodes	Switches	A node whose status is monitored and controlled by ISM.



Device and function		Description
	Storage	
	Server (Managed Server)	A node whose status is monitored and controlled by ISM. BMC (iRMC) have to be connected to the management LAN. To use all the functions in ISM, the onboard LAN and LAN card also connects to the management LAN.
	Chassis	A node whose status is monitored and controlled by ISM. Connects MMB to the management LAN.

For information on designing network configurations and further detailed information, refer to "[A.1.1 DHCP/PXE Settings in Using Profile Management/Firmware Management.](#)"

## 1.5 System Requirements

This section describes the system requirements for ISM-VA (virtual machines) and management terminals that serve as the operating environment for ISM. This section also describes the external services required for a variety of ISM operations.

### 1.5.1 System Requirements for ISM-VA (Virtual Machines)

The system requirements for virtual machines to run ISM-VA are as follows.

Item	Description
Number of CPU cores	2 cores or more [Note 1] [Note 5]
Memory capacity	8 GB or more [Note 1] [Note 5]
Free disk space	35 GB or more [Note 2] [Note 3] [Note 4] [Note 5]
Network	1 Gbps or higher
Hypervisor	Windows Server 2012/2012 R2/2016/2019 with the Hyper-V role included VMware ESXi 5.5/6.0/6.5/6.7 Red Hat Enterprise Linux 7.2/7.3/7.4/7.5/7.6 with KVM installed SUSE Linux Enterprise Server 12 SP3/15 with KVM installed

[Note 1]: The required number of cores and memory capacity depend on the number of nodes to be managed.

Number of nodes	Number of CPU cores	Memory capacity
1 to 100	2	8 GB
101 to 400	4	8 GB
401 to 1000	8	12 GB

[Note 2]: This is the minimum disk capacity required for monitoring approximately 100 nodes. The disk capacity must be estimated based on the number of nodes to be managed and the ISM functions to be used. For details on how to estimate the disk capacity, refer to "[3.2.1 Disk Resource Estimation.](#)"

[Note 3]: To back up ISM-VA, a management server must have free disk space equivalent to or larger than that of ISM-VA.

[Note 4]: The disk space must be statically allocated upon installation of ISM-VA.

[Note 5]: To use Packet Analysis of Virtual Network, the following resources are additionally required.

Target	Additional number of CPU cores	Additional memory capacity	Additional disk capacity
ISM-VA	2 cores or more	8 GB or more	60 GB or more
Host Operated by Analysis VM	2 cores or more	4 GB or more	20 GB or more

## 1.5.2 System Requirements for Management Terminals

### System requirements for GUI (browser)

The system requirements for management terminals to run the GUI of ISM are as follows.

Item	Description
Device	PC, server, Windows 10 tablet, Android tablet, iPad
Display	<ul style="list-style-type: none"> <li>- PC, server, and Windows 10 tablet: 1280 x 768 pixels or more</li> </ul> <p>The window size of your browser for displaying the GUI of ISM must be at least 1280 x 768 pixels.</p> <ul style="list-style-type: none"> <li>- Tablet: built-in display of the devices stated above</li> </ul>
Network	100 Mbps or higher
Web browser	<ul style="list-style-type: none"> <li>- PC, server, Windows 10 tablet: <ul style="list-style-type: none"> <li>- Internet Explorer 11 or later</li> <li>In order to display the "3D View" screen, version 11.0.15 or later must be applied.</li> <li>- Microsoft Edge 25 or later</li> <li>- Mozilla Firefox 38 or later</li> <li>- Google Chrome 43 or later</li> </ul> </li> <li>- Android tablet: Google Chrome 43 or later</li> <li>- iPad: Safari 8 or later</li> </ul>
Related software	Acrobat Reader (to display manuals)

The following devices and web browsers are supported.

Note: Y = Supported, N = Not supported

Web browser	Device			
	PC or server	Windows 10 tablet	Android tablet	iPad
Microsoft Internet Explorer	Y [Note 1][Note 4]	Y [Note 1][Note 2][Note 4]	N	N
Microsoft Edge	Y [Note 4]	Y [Note 2][Note 4]	N	N
Mozilla Firefox	Y [Note 4]	Y [Note 2][Note 4]	N	N
Google Chrome	Y [Note 4]	Y [Note 4]	Y [Note 4]	N
Safari	N	N	N	Y [Note 3][Note 4]

[Note 1]: If pop-up blocking is enabled, the GUI help will not be displayed. If the help does not appear, add the URL for displaying the GUI to [Internet Options] - [Privacy] - [Pop-up block] - [Settings] - [Addresses of trusted web sites].

[Note 2]: On the "3d View" screen, you cannot rotate, move in parallel, or zoom in and out using touch operations.

[Note 3]: Files cannot be saved because of device restrictions. Therefore, you cannot export monitoring data to CSV format, download the node logs or archived logs, or export profiles.

[Note 4]: Pop-up blocking must be disabled to open the iRMC screen from the ISM GUI. Allow pop-ups for the URL of ISM in the browser you use.



## System requirements for management terminals for file transfer




The system requirements for the management terminal that transfers the files to ISM-VA, such as data required to set up managed nodes and ISM logs, are as follows.

Item	Description
Device	PC or server
Free disk space	8 GB or more
Network	100 Mbps or higher
Required software	FTP client software
Related software	SSH client software

## 1.5.3 Service Requirements for ISM Operations

This section describes the external services required for a variety of ISM operations.

Item	Description
Mail server (SMTP server)	<p>An email server is required when sending notification mails for errors and changes in the statuses of managed nodes.</p> <p>Set up with [Events] - [Alarms] - [SMTP Server].</p> <p> <b>Note</b></p> <p>.....</p> <p>In ISM, only one mail server can be registered.</p> <p>.....</p>
Directory server	<p>A directory server is required for the following use case.</p> <ul style="list-style-type: none"> <li>- For User Management in ISM</li> </ul> <p>You can use the following two directory services.</p> <ul style="list-style-type: none"> <li>- OpenLDAP</li> <li>- Microsoft Active Directory</li> </ul> <p>Register the configured directory server in [Settings] - [Users] - [LDAP Server Setting].</p> <p> <b>Note</b></p> <p>.....</p> <ul style="list-style-type: none"> <li>- In ISM, two LDAP servers can be registered, one primary and one secondary.</li> <li>- When a managed node uses a directory service, ISM does not work with the directory service which a managed node belongs to. Individually set up the account capable of accessing the managed node.</li> </ul> <p>.....</p>
DHCP server	<p>A DHCP server is required in the following cases.</p> <ul style="list-style-type: none"> <li>- When OS installation is executed using Profile Management</li> <li>- When Offline Update of Firmware Management is used</li> </ul> <p>To enable PXE boot on a managed node (server), configure the DHCP server so that an appropriate IPv4 address can be leased to the node.</p>

Item	Description
	<p> <b>Point</b></p> <p>.....</p> <p>The ISM-VA internal DHCP server function can be used instead of preparing a separate DHCP server.</p> <p>For details on how to use the ISM-VA internal DHCP function, refer to "<a href="#">4.15 ISM-VA Internal DHCP Server.</a>"</p> <p>.....</p>
DNS server	<p>A DNS server is required for the following use cases.</p> <ul style="list-style-type: none"> <li>- Accessing ISM by hostname</li> <li>- Using an FQDN for a variety of sever settings of ISM, such as integration with an LDAP server</li> </ul> <p>For the procedure for setting up a DNS server, refer to "Add DNS server" in "<a href="#">4.9 Network Settings.</a>"</p> <p> <b>Point</b></p> <p>.....</p> <ul style="list-style-type: none"> <li>- Manually setting a hostname for ISM-VA if you want to access ISM with a hostname without using a DNS server. For details on how to set up the hostname manually, refer to "<a href="#">4.13 Modification of Host Names.</a>"</li> <li>- Settings for ISM servers such as LDAP integration with IP addresses if you are not using a DNS server.</li> </ul> <p>.....</p>
NTP server	<p>An NTP server is required when time synchronization is required between ISM and managed nodes and managed clients.</p> <p>Use the ismadm command or the ismsetup command when you are setting the NTP server for ISM.</p> <p>For details on how to set it up, refer to "Enable/Disable NTP synchronization" and "Add/Remove NTP server" in "<a href="#">3.4.2 Initial Setup of ISM-VA.</a>"</p>
Proxy server	<p>A proxy server is required when accessing ISM from a management client via a proxy server.</p> <p> <b>Note</b></p> <p>.....</p> <p>Monitored nodes and ISM cannot be connected via a proxy server.</p> <p>.....</p>
Router	<p>You can define only one network interface for ISM.</p> <p>If you are using ISM in an environment with multiple networks, you must set up a router to allow communication between the networks.</p> <p>If you are setting a gateway in ISM, use the ismadm command or the ismsetup command.</p> <p>For details on how to set it up, refer to "Modification of network settings" in "<a href="#">4.9 Network Settings.</a>"</p>

For information on designing network configurations and further detailed information, refer to "[A.1.1 DHCP/PXE Settings in Using Profile Management/Firmware Management.](#)"

## 1.5.4 Operation Requirements for ISM for PRIMEFLEX

### Operation requirements for the ISM for PRIMEFLEX Virtualized Platform Expansion function

The operation requirements are as follows.

- The following licenses must be registered after the installation of ISM for PRIMEFLEX
  - Infrastructure Manager Advanced Edition for PRIMEFLEX HS Server License V2
  - Infrastructure Manager for PRIMEFLEX HS Node License V2

For the procedure to register licenses, refer to "[3.5 Registration of Licenses](#)."

### **Requirements for using Cluster Management**

Refer to the following:

- Requirements for the Cluster Management Environment: "[2.12.1.2 Environments supported by Cluster Management](#)"
- Pre-setting requirements: "[3.9 Pre-Settings for Cluster Management](#)"

### **Requirements for using Cluster Creation**

Refer to the following:

- Requirements for PRIMEFLEX HS, PRIMEFLEX for VMware vSAN: "6.7.2.1 Operation requirements for Cluster Creation" in "Operating Procedures"
- Requirements for PRIMEFLEX for Microsoft Storage Spaces Direct: "6.8.2.1 Operation requirements for Cluster Creation" in "Operating Procedures"

### **Requirements for using Cluster Expansion**

Refer to the following:

- Requirements for PRIMEFLEX HS, PRIMEFLEX for VMware vSAN: "6.9.2.1 Operation requirements for Cluster Expansion" in "Operating Procedures"
- Requirements for PRIMEFLEX for Microsoft Storage Spaces Direct: "6.10.2.1 Operation requirements for Cluster Expansion" in "Operating Procedures"

### **Requirements for using Firmware Rolling Update**

Refer to the following:

- Precautions and prerequisites: "6.6.2.1 Operation requirements for Firmware Rolling Update" in "Operating Procedures"

### **Products supported by ISM for PRIMEFLEX V2.4**

For the latest information on products supported by ISM for PRIMEFLEX V2.4, contact your local Fujitsu customer service partner.

## **1.6 ISM Maintenance and Updates**

---

If you need MIB files, correction patches or upgrades for ISM, contact your local Fujitsu customer service partner.

# Chapter 2 Functions of ISM

This chapter describes the functions of ISM.

## Point

In order to allow users to use the various ISM functions, you must assign privileges (user roles) for the registered user groups to the appropriate users. For details on users and privileges (User Role), refer to "2.13.1 User Management."

The icons shown in below table indicate the combinations of User Groups and User Roles and whether they can execute operations.

User Group to which user belongs	User Role held by user	Can execute	Cannot execute
Administrator group	Administrator role	<b>Admin</b>	
	Operator role	<b>Operator</b>	Operator
	Monitor role	<b>Monitor</b>	Monitor
Other than Administrator group	Administrator role	<b>Admin</b>	Admin
	Operator role	<b>Operator</b>	Operator
	Monitor role	<b>Monitor</b>	Monitor

In the following descriptions, the groups and users that have privileges to execute an operation are indicated.

Example:



- When the display is as shown above, users with the following user attributes can execute operations:
  - Users who belong to an Administrator group and have an Administrator role or Operator role
  - Users who belong to a group other than an Administrator group and have an Administrator role or Operator role
- Users with a Monitor role indicated by the gray icon cannot execute the respective functions.

## 2.1 User Interface

This section describes the ISM user interface.

ISM provides the following user interfaces:

- GUI: graphical user interface for operating ISM
- FTP: file transfer interface between an FTP client and ISM-VA
- Console: command line interface for operating ISM-VA
- REST API: interface to link with application software created by users

### 2.1.1 GUI

ISM provides a GUI that can be operated with web browsers.



- In your browser, you must enable cookies and JavaScript.
- If you are using Firefox, settings to register the server certificate in the browser are required.
  1. Open Firefox and, from the menu, select [Options].
  2. Select [Advanced], and then select [Certificates].
  3. Select [View Certificates].
  4. On the [Servers] tab, select [Add Exception].
  5. Enter "https://<IP address of ISM server> or <FQDN name of ISM server>:25566/" in [URL], and then select [Get Certificate].
  6. Confirm that the [Permanently store this exception] checkbox is checked, and then select [Confirm Security Exception].
- If you are using Internet Explorer, the following settings are required.
  1. Open Internet Explorer and, from the menu, select [Tools] - [Internet options].
  2. On the [Security] tab, select the [Custom level] button and select [Enable] for the following items before you select the [OK] button.
    - [Run ActiveX controls and plug-ins] under [ActiveX controls and plug-ins]
    - [Run ActiveX controls and plug-ins] under [Script ActiveX controls marked safe for scripting]
    - [File download] under [Downloads]
    - [Font download] under [Downloads]
  3. On the [Advanced] tab, under [Multimedia], select the "Play animations in web pages" checkbox and select the [OK] button.
- In order to display the "3D View" screen in Internet Explorer 11, Microsoft's technical support information (hereafter referred to as "KB") 2991001 must be applied. The "3D View" screen is a GUI that displays floors, racks, and device positions within racks as three-dimensional images.

<https://support.microsoft.com/en-us/kb/2991001>

If the "3D View" screen does not display the racks, apply Microsoft's security update MS14-051, which also includes KB 2991001. For details, refer to the following website:

<https://technet.microsoft.com/en-us/library/security/ms14-051>
- If you are using Google Chrome, depending on the hardware capabilities of your terminal and your graphics driver, the WebGL function (for displaying 3D graphics in browsers) may be disabled. If the WebGL function is disabled, you cannot display the "3D View" screen.

You can use the following procedure to check whether the WebGL function is enabled or disabled.

  1. Open Google Chrome and enter "chrome://gpu" into the address bar.
  2. If, under [Graphics Feature Status], [Hardware accelerated] is displayed for [WebGL], the WebGL function is enabled. Otherwise the WebGL function is disabled.
- Do not save the ISM user name and password in the Web browser. If you saved them, delete the ISM user name and password.

The procedure for starting up the ISM GUI is as follows.

1. Start a browser and enter the following URL:

`https://<IP address of ISM server> or <FQDN name of ISM server>:25566/`

2. When the login screen is displayed, enter your user name and password, and then select the [Login] button.

If a warning for the security certificate is displayed, refer to "[4.7 Certificate Activation](#)" and execute the authentication settings.

When the first time you log in, the "Fujitsu End User Software License Agreement" screen is displayed.

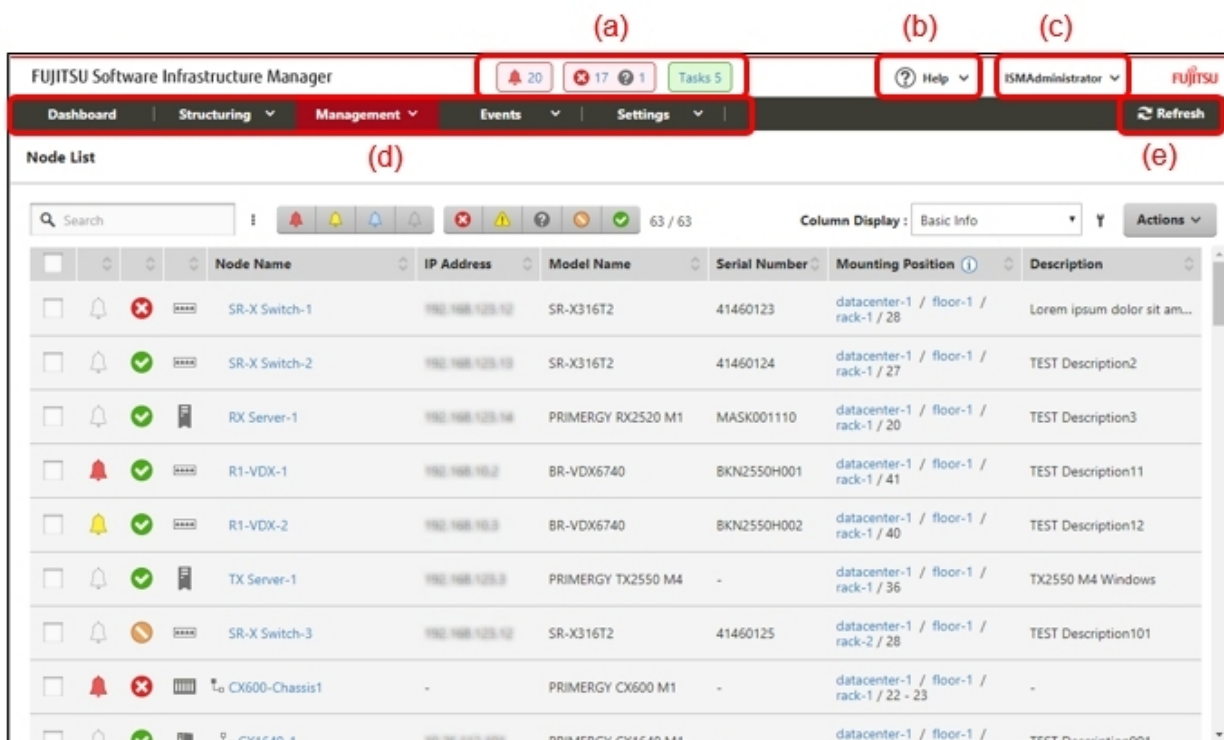
3. Check the contents, and then check [Above contents are correct.].
4. Select the [Agree] button.

### Point

When you log in for the first time, use the following user name and password. After logging in with this user name, change the password for the default user and create new users before you continue operations.

- User Name: administrator
- Password: admin

The structure of ISM's GUI screen is as follows.



(a) Alarm status, status, task icon

Alarm status:

The number of nodes with Error alarm status is displayed. When there are no nodes with Error alarm status, the Warning alarm status icon and the number of nodes with Warning alarm status is displayed.

When there are no nodes with Error or Warning alarm status, this will not be displayed.

Status:

The number of nodes with Error status, the Unknown status icon, and the number of nodes with Unknown status are displayed.

When there are no nodes with Error status, the Warning status icon, and the number of nodes with Warning status are displayed.

When there are no nodes with Error, Warning, or Unknown status, this will not be displayed.

Task:

Displays the number of currently running tasks.

(b) Help

Displays help and guidance.



(c) User name

You can view the user name with which you are logged in.

In order to log out from ISM, move the mouse pointer over the user name and select [Log out].

Select [Language] when you change the settings for the displayed Language, Date Format and Time Zone on the GUI.

(d) Global Navigation Menu

This menu serves to access the various screens of ISM.

(e) Refresh button

Selecting this button refreshes the entire screen.

The GUI screens of ISM are not updated automatically as long as you stay on the same screen. (However, when you move to another screen, the latest information is retrieved again from the server).

Therefore, to confirm the latest information, you have to select the [Refresh] button to update the screen.

If the following screens are set up, the screens are refreshed automatically.

- "Dashboard" screen
- "Node Registration" screen
- "Tasks" screen
- "Jobs" screen

## 2.1.2 FTP Access

---

You can use an FTP client to access the file transfer area.

Specify the IP address that you set in "3.4.2 Initial Setup of ISM-VA" to make the connection.

For security reasons, no files or directories are displayed immediately after login; move to the directory with the group name to which the login user belongs and access the file transfer area from there.

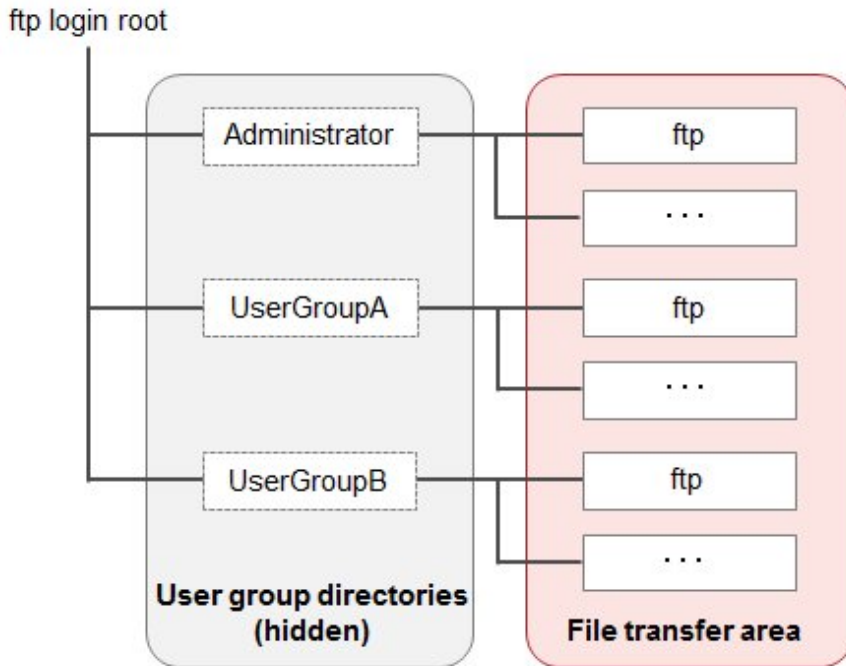
As shown in [Figure 2.1](#), files that are sent or received via FTP are stored under "/<User group name>/ftp."



### Note

- Directory names to be specified as user group names must be either User group names created with User Group Management in ISM or Administrator. For details of User Group Settings, refer to "2.7.2 Manage User Groups" in "Operating Procedures."
- Whenever you transfer files via FTP, be sure to use the "ftp" subdirectory in the <User group name> directory.
- Do not modify or delete any existing directories.
- When transfer patch files and other binary data, transfer it in binary mode.
- When accessing via FTP with a user that is linked with Microsoft Active Directory or LDAP, use the password registered in ISM and not the linked password.

Figure 2.1 Directory configuration in the file transfer area



### Example of FTP access

The example below shows access by an administrator user who belongs to an Administrator group.

```
# ftp 192.168.1.50
Connected to 192.168.1.50 (192.168.1.50).
220 (vsFTPD 3.0.2)
Name (192.168.1.50:root): administrator
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.

ftp> ls
227 Entering Passive Mode (192,168,1,50,156,64).
150 Here comes the directory listing.
226 Transfer done (but failed to open directory).
      *Nothing is displayed directly after log in.

ftp> cd Administrator
250 Directory successfully changed.
      *Move to the directory of the group name the logged in user belongs to.

ftp> ls
227 Entering Passive Mode (192,168,1,50,156,64). 150 Here comes the directory listing.
drwxr-sr-x  2 0      1001      33 Jun 16 20:36 bin
drwxrws---  3 992    989      26 Jun 16 21:54 elasticsearch
drwxrws---  3 0      1001      21 Jun 16 23:20 ftp
drwxrws---  2 0      0         6 Jun 16 20:36 imported-fw
drwxrws---  2 0      0         6 Jun 16 20:36 imported-os
drwxrws---  2 0      0         6 Jun 16 20:36 ismlog
drwxrws---  2 0      0         6 Jun 16 20:36 logarc
drwxrws---  8 0      0        75 Jun 17 14:03 profile
drwxrws---  2 0      0         6 Jun 16 20:36 tmp
drwxrws---  2 0      1001      6 Jun 16 20:36 transfer
```

226 Directory send OK.

\*It is possible to access the file transfer area.

## 2.1.3 Console Access

---

You can execute management commands with a hypervisor console or an SSH client.

If you connect with an SSH client, specify the IP address that you set in "[3.4.2 Initial Setup of ISM-VA](#)" to make the connection.

As described in "[2.13.1 User Management](#)," it can only be used by users with the Administrator role.

For the commands that can be used, refer to "[2.13.5.1 List of commands in ISM-VA Management](#)."



### Note

Automatic completion of command parameters by using the [Tab] key is not supported.

## 2.1.4 REST API

---

ISM is equipped with REST API. By using this, ISM functions can be called from external programs. For details, refer to "REST API Reference Manual."

## 2.2 Node Management

---

Node Management manages nodes in four levels structure: datacenters, floors, racks, and nodes. Each layer is defined as follows.

- Datacenter: a building that accommodates datacenter facilities
- Floor: a machine room within a datacenter facility
- Rack: a rack that is located on a floor
- Node: a managed device that is mounted in a rack

The following functions are available.

- [2.2.1 Registration of Datacenters/Floors/Racks/Nodes](#)
- [2.2.2 Confirmation of Datacenters/Floors/Racks/Nodes](#)
- [2.2.3 Editing of Datacenters/Floors/Racks/Nodes](#)
- [2.2.4 Deletion of Datacenters/Floors/Racks/Nodes](#)

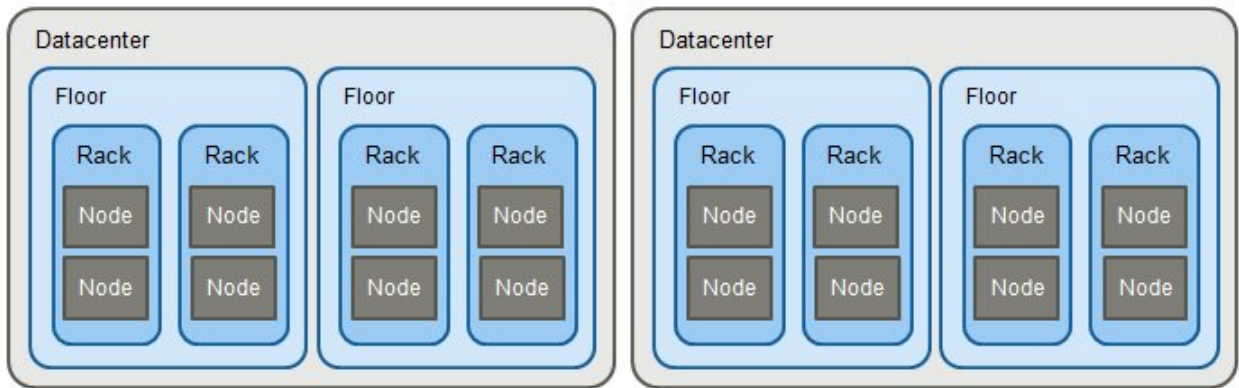
### 2.2.1 Registration of Datacenters/Floors/Racks/Nodes

---

With ISM, you can manage the physical location information on nodes. The location information is uniquely specified within the level structure "Datacenter > Floor > Rack > Node mounting position in the rack (Slot number/Partition number)."

With ISM, you can set up and manage the individual information on each datacenter, floor, rack, and node as well as their mutual level structures.

Figure 2.2 Relationships between datacenters, floors, racks, and nodes



You can execute the following operations:

- [2.2.1.1 Registration of datacenters/floors/racks](#)
- [2.2.1.2 Registration of nodes](#)
- [2.2.1.3 Management of node information](#)
- [2.2.1.4 Management of information on node mounting positions in racks](#)
- [2.2.1.5 Registration of node OS information](#)
- [2.2.1.6 Discovery of nodes](#)
- [2.2.1.7 Adding tags to nodes](#)

### 2.2.1.1 Registration of datacenters/floors/racks



You can additionally register information on datacenters, floors, and racks in ISM. The datacenter, floor, and rack names to be registered must be set to unique names in ISM.

If you have registered a floor, you can display it on the "Floor View" and "3D View" screens of the GUI.

If you have registered a rack, you can display it on the "Rack View" screen of the GUI.

### 2.2.1.2 Registration of nodes



To manage nodes in ISM, nodes must first be registered with ISM.

When you register a node, enter all the required information. The following are the conditions for the information to be registered.

- Node names must be set to unique names in ISM.  
You cannot register a node with the same IP address or serial number as for a node that is already registered in ISM.
- To access a node, the required account information must be set in the node information.

In ISM, the specified account information is used for data communication with nodes in order to retrieve node information and for processing monitoring, profile assignment, firmware updates, log collection, and so on.

For the account information that is required to communicate with each type of target node and for the settings that are required before node registration, refer to "[A.2.2 Details of Node Settings](#)."

There are two procedures for registration as follows:

- Setting the required information and then registering manually.
- Discovering and then registering nodes with the discovery function of ISM.

The following is a sample operation for manual registration in ISM. For the registration procedure that uses the discovery function, refer to "[2.2.1.6 Discovery of nodes](#)." To register nodes, you must confirm information such as the model names and the IP addresses set for the nodes to be registered in advance.

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Node Registration].
2. From the [Actions] button, select [Manually register nodes].
3. Follow the "Node Manual Registration" wizard and enter the setting items.
  - Node Name  
Set a name that is unique across the entire ISM system.
  - Node Type  
Select the type of node to be registered.
  - Model Name  
Select the model name of the node. To register a type of device that is not supported, enter the model name manually.
  - IP Address  
Set the IP address of the node.
  - Web i/f URL  
Set the URL for accessing the web management screen for the node.
  - Description  
Freely enter a description of the node (comment) as required.
4. Enter the account information for each node.
5. Enter the information for mounting position of each node in the racks.
6. Select the node groups to which each node is going to belong.  
If you do not specify a node group, the node is handled as not allocated to a node group. Nodes that are not allocated can be managed only by a user belonging to an Administrator group.
7. Specify the tag information to be set for the node.
8. Execute Register.

## Point

---

- It is not recommended to monitor the same node with multiple instances of ISM or multiple monitoring software. Monitoring may not operate correctly, as, depending on each node, there are only a limited number of sessions that can access a node simultaneously.
  - It is recommended that you set a static IP address for the nodes registered in ISM. The node cannot be managed if its IP address is changed.
  - When you use SNMPv3 to execute trap reception from nodes, you have to set the SNMP trap reception settings. For details, refer to "[2.3 Monitoring](#)"-"[Trap reception setting](#)."
-

### 2.2.1.3 Management of node information



On the "Node List" screen, you can select a [Node] and confirm the node information.

The account information that is set in each node in ISM is used to automatically collect information from the node in 24-hour intervals. If you want to retrieve the latest information from the node, you can also retrieve it manually.

Immediately after node registration, retrieval of the node information is executed automatically.

The following is a sample operation for retrieving the node information.

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes] to display the "Node List" screen.
2. Select the node name of the target node to display the Details of Node screen.
3. From the [Actions] button, select [Get Node Information].

As soon as retrieval of the node information is completed, a log with the Message ID "10020303" is exported to the [Events] - [Events] - [Operation Log].

4. Select the [Refresh] button to update the Details of Node screen.



#### Note

If executing node information retrieval directly after powering on the PRIMERGY BX chassis (MMB), the BX server blade and connection blade may not be displayed in Rack view.

Wait for a while and then retrieve the node information again.

### 2.2.1.4 Management of information on node mounting positions in racks



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

#### Setting of information on mounting positions in racks

You can set the information of the node mounting positions in a rack when you register a node. Alternatively, you can also execute the settings after node registration.

The following is a sample operation for setting the information for node mounting positions in racks after node registration.

Before you can set the information for node mounting positions in a rack, the rack must be registered.

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes] to display the "Node List" screen.
2. Select the applicable node, and then select the [Actions] button - [Set Node Position].
3. Select the rack in which the node is mounted.
4. Select and then apply the positions of the node.

## 2.2.1.5 Registration of node OS information



If an OS is already installed on the server that is registered in ISM, register the OS information.

The OS information includes information such as the OS type, IP addresses, and the account information that is required for connecting to the OS.

When you monitor a server using a domain user ID, enter the FQDN of the realm name of Active Directory in the domain name field, and enter the user name without the realm name in the user name field.

In ISM, the registered OS information is used for retrieving information that is managed by the OS on a node.

For the latest information on supported devices and OS versions, contact your local Fujitsu customer service partner.

### Note

- In order to make a server OS the monitoring target from ISM, a separate installation procedure is required for each OS.  
When you register a domain name in the account information and a domain user in the account, you must add settings to allow monitoring by a domain user in the OS that will be monitored.  
For the information on installation procedures, refer to the following document. For details, contact your local Fujitsu customer service partner.  
"Settings for Monitoring Target OS and Cloud Management Software"
- When you monitor the OS by using the domain user, you are required to set up DNS settings and domain environment settings.  
For details on how to set it, refer to "[3.4.2 Initial Setup of ISM-VA.](#)"
- If no OS information is registered or the respective OS has been shut down, a portion of the node information cannot be retrieved. Also, the information that is managed by the OS on a node cannot be retrieved.
- Enter the domain name with uppercase letters when you register OS information.

The following is a sample operation.

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes] to display the "Node List" screen.
2. Select the node name of the applicable node and select the [OS] tab.
3. From the [OS Actions] button, select [Edit OS Information].
4. Enter and then apply the required information.
5. From the [Actions] button, select [Get Node Information].  
As soon as retrieval of the node information is completed, a log with the Message ID "10020303" is exported to the [Events] - [Events] - [Operation Log].
6. Select the [Refresh] button to refresh the display on the [OS] tab.

## 2.2.1.6 Discovery of nodes



With ISM, you can discover the nodes that are connected to a network. The discovery function can automatically retrieve some of the required information for registering the discovered nodes and makes node registration easier.

The following types of node discovery functions are available:

- [Manual Discovery](#)
- [Auto Discovery](#)

Before you execute discovery, you must set the demanded account information for connecting to the nodes you want to discover.

The protocol used for discovery varies with the type of node to be discovered.

For the latest information on supported devices and OS versions, contact your local Fujitsu customer service partner.

### Point

If the IP address of the DNS server is set in ISM-VA, the DNS name of the discovered node will be retrieved.

If the DNS name was retrieved, it will be entered as the default node name when registering the discovered node.

For the settings for the IP address of the DNS server, refer to "[4.2 ISM-VA Basic Settings Menu.](#)"

### Note

When retrieving the DNS name of the IP address of the discovered node, if reverse lookup zone is not set for the DNS, discovery will take longer time compared with if it is set.

In this case, set reverse lookup zone for the DNS.

## Manual Discovery

Node discovery is executed manually. You can execute the following operations:

- Execute Manual Discovery
  - Enter the discovery settings and execute Manual Discovery
  - Upload a CSV file and execute Manual Discovery
- Confirmation of results of Manual Discovery
- Registering discovered nodes

Enter the discovery settings and execute Manual Discovery

Set the required information for Manual Discovery. Node discovery is executed for the range of IP addresses that you specify. Also, some of the required node information for registration can be retrieved using the account information that was set.

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Node Registration] to display the "Node Registration" screen.
2. From the [Actions] button, select [Discover nodes].
3. Enter the required information for discovery.

Item	Description
Discovery IP address range	Set the target range of IP addresses for discovery.
Discovery target	Select discovery target.
Communication method	Enter the account information according to the communication method of the discovery target. If you specify the discovery target, the input field to enter the communication method is displayed.

4. Execute Discovery.



## Upload a CSV file and execute Manual Discovery

Upload a CSV file with the required information for the Manual Discovery. Node discovery is executed for the information entered in the CSV file. Also, some of the required node information for registration can be retrieved using the account information that was set.

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Node Registration] to display the "Node Registration" screen.
2. From the [Actions] button, select [Discover nodes].
3. Select "CSV upload" in [Discovery method].
4. Enter the required information for discovery.

Item	Description
File selection method	Select a specification method for CSV files.
File Path	Select a CSV file to use for discovery.
Password encryption	Select a password encryption method for the CSV file.
Behavior after execution of discovery	Specify behavior after execution of discovery. It is displayed if you select "FTP" for the file selection method.

5. Execute Discovery.

### Point

- If you select "FTP" in [File selection method], the CSV file is required to be transferred via FTP to under the "/Administrator/ftp" directory in advance.

For FTP connection and how to transfer FTP, refer to "[2.1.2 FTP Access.](#)"

- For the [Password encryption] setting, if you use encryption for the password in the account information in the CSV file, select "Encrypted," and if you are not using encryption, select "Unencrypted."
- When you select "FTP" in [File selection method], if you check [Delete source file] in [Action after execute], the CSV file is deleted after discovery has been executed.

### CSV File

Download the CSV file template from the GUI of ISM.

In the downloaded file, the first row is the item name and the options for the selected item is in the second row.

Add the information of the nodes to be discovered into this CSV file.

The procedure to download the CSV file template is as follows.

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Node Registration] to display the "Node Registration" screen.
2. From the [Actions] button, select [Discover nodes].
3. Select "CSV upload" in [Discovery method].
4. Specify the device type in [Template], and then select the [Download] button to start the download.

It is possible to specify multiple device types.

### Note

Delete the second row (the row with the options) of the downloaded CSV file until before uploading.

The setting items for the CSV file are described below.

Item Name	Description
IpAddress	IP address of the discovery target node (IPv4 or IPv6)
IpmiAccount	User name of iRMC/BMC (IPMI)
IpmiPassword	Password of iRMC/BMC (IPMI)
IpmiPort	Port number of iRMC/BMC (IPMI) If there is no setting, 623 (default port number) is used
SshAccount	User name for SSH
SshPassword	Password for SSH
SshPort	Port Number for SSH If there is no setting, 22 (default port number) is used
HttpsAccount	User name for HTTPS
HttpsPassword	Password for HTTPS
HttpsPort	Port Number for HTTPS If there is no setting, 443 (default port number) is used
SnmpType	SNMP Version Setting value: One of SnmpV1, SnmpV2, or SnmpV3 If you are using SNMPv2c, specify SnmpV2
SnmpPort	Port Number for SNMP If there is no setting, 161 (default port number) is used
Community	Community Name Required if either SnmpV1 or SnmpV2 is set for SnmpType
V3Account	User name for SNMPv3
V3SecLevel	SNMPv3 Security Level Setting value: Either authPriv, authNoPriv, or noAuthNoPriv
V3AuthProtocol	Authentication Protocol for SNMPv3 Setting value: Either MD5 or SHA
V3AuthPassword	Authentication Password for SNMPv3
V3PrivProtocol	Privacy Protocol Setting value: Either DES or AES
V3PrivPassword	Privacy Password for SNMPv3
V3EngineId	Engine ID for SNMPv3
V3ContextName	Context name for SNMPv3

The specific setting items for each account type are described below.

Note: R = Required, Y = Can be omitted, - = Not required

Item Name	Account type					
	IPMI	SSH	HTTPS	SNMP		
				V1	V2	V3
IpAddress	R	R	R	R	R	R
IpmiAccount	R	-	-	-	-	-

Item Name	Account type					
	IPMI	SSH	HTTPS	SNMP		
				V1	V2	V3
IpmiPassword	R	-	-	-	-	-
IpmiPort	Y	-	-	-	-	-
SshAccount	-	R	-	-	-	-
SshPassword	-	Y	-	-	-	-
SshPort	-	Y	-	-	-	-
HttpsAccount	-	-	R	-	-	-
HttpsPassword	-	-	R	-	-	-
HttpsPort	-	-	Y	-	-	-
SnmpType	-	-	-	R	R	R
SnmpPort	-	-	-	Y	Y	Y
Community	-	-	-	R	R	-
V3Account	-	-	-	-	-	R
V3SecLevel	-	-	-	-	-	R
V3AuthProtocol	-	-	-	-	-	Y [Note 1]
V3AuthPassword	-	-	-	-	-	Y [Note 1]
V3PrivProtocol	-	-	-	-	-	Y [Note 2]
V3PrivPassword	-	-	-	-	-	Y [Note 2]
V3EngineId	-	-	-	-	-	Y
V3ContextName	-	-	-	-	-	Y

[Note 1]: Required if V3SecLevel is authPriv or authNoPriv.

[Note 2]: Required if V3SecLevel is authPriv.

The procedure to write to the CSV file is as follows.

- Create the CSV file with an arbitrary name.
- The item names are written in the first row.
- Write down the target node information in the second row and following rows.
  - Enter the settings values so that they match with the position of the item names in the first row.
  - You must enter the IpAddress.
  - Omit setting values that are not required for the discovery of the target nodes.
  - The entire item name row can be deleted for items that are not required for any of the nodes to be discovered.
  - It is recommended to set an encrypted password for each password (IpmiPassword, V3AuthPassword, V3PrivPassword, SshPassword, HttpsPassword).

Unencrypted passwords can also be set.

For the password encryption procedure, refer to "REST API Reference Manual."

## Note

Encrypted passwords and unencrypted passwords cannot be mixed in the CSV file. You must make all the same.

An example of the contents of the CSV file is displayed below.

```
"IpAddress", "IpmiAccount", "IpmiPassword", "SnmpType", "Community", "SshAccount", "SshPassword"
"192.168.10.11", "admin1", "*****", "", "", "", ""
"192.168.10.12", "admin2", "*****", "", "", "", ""
"192.168.10.21", "", "", "SnmpV1", "comm1", "user1", "*****"
```

### Confirmation of results of Manual Discovery

Refresh the "Node Registration" screen and wait for the discovery process displayed in [Discovery Progress] to finish. After completion, confirm the discovered nodes.

If node discovery using the set account information is successful, the status becomes successful and the discovered nodes can be checked.

## Note

- The discovered node information is only enabled during the same session.
- Devices that are not supported may be displayed in the discovery results. Do not register devices that are not supported.
- For a VDX switch, the target for node registration and node discovery becomes VCS Fabric (Brocade VCS Fabric). Specify the virtual IP address set in the fabric and execute node discovery and node registration. The physical switches will be discovered and registered automatically with Get Node Information after the fabric is registered as a node. If discovering a physical switch during node discovery, result becomes "Only automatic registration."
- If you operate a CFX switch or PRIMERGY BX Ethernet Switch/IBP 10Gbit/s 18/8+2 SBAX3 in fabric mode, the target for the node discovery and node registration is the virtual IP address set in the fabric. The physical switches will be discovered and registered automatically with Get Node Information after the fabric is registered as a node.

### Registering discovered nodes

The following is a sample operation for registering discovered nodes using the Manual Discovery.

1. Confirm the discovered nodes.
2. From the discovered nodes, select the ones you want to register, then from the [Actions] button, select [Register discovered nodes].
3. Enter the information that is required for node registration, such as node name, chassis name, Web i/f URL, description.  
If you are changing the IP address set to the device, select the version of the IP address, and then select [Edit] button and set it. If you set it, the IP address setting operation will be executed for the device when registering nodes.
4. Set the information for the node's mounting position in a rack.
5. Set the node group information.
6. Execute registration.

The account information that was used to successfully access the node during Node Discovery is registered as the account information for the node. The account to be registered is displayed in the [Discovered Node List] - [Succeeded methods] column.

## Note

- The IP address set for the device can be changed only for PRIMERGY servers and PRIMEQUEST 3000B with DHCP settings.
- If you change the IP address, check that the IP address set it from a range that can be accessed from ISM. If you set an IP address that cannot be accessed from ISM, you may not be able to connect to the device.

- If you are using the "Log Collection" or "Firmware Update" functions of Cisco Catalyst switches, after register nodes, set the password for raising the SSH privilege on the node edit screen.

## Auto Discovery

Node discovery is executed automatically. In Auto Discovery, automatic node discovery is executed with UPnP/Redfish.

The following are the nodes based upon Auto Discovery Type of nodes.

Auto Discovery Type	Target Node
UPnP	PSWITCH 2048 T PSWITCH 2048 P PSWITCH 4032 P
Redfish	PRIMERGY M4 series PRIMEQUEST 3000B

In Auto Discovery you can execute the following operations:

- Executing Auto Discovery
- Confirming the results of Auto Discovery
- Registering discovered nodes

### Executing Auto Discovery

Auto Discovery is executed automatically. There are no items for which the settings need to be changed.



The following requirements must be met in order to execute Auto Discovery with UPnP/Redfish.

- The Auto Discovery is on at the target device side
- A network configuration where multi-cast transmission packets sent from the target device can be received with ISM

### Confirming the results of Auto Discovery

When a device is discovered, it is displayed in [Discovered Node List] on the "Node Registration" screen.

### Registering discovered nodes

The following shows an example of when registering a node discovered with Auto Discovery.

1. Confirm the discovered nodes.
2. From the discovered nodes, select the ones you want to register, then from the [Actions] button, select [Register discovered nodes].
3. Enter the information that is required for node registration, such as node name, chassis name, Web i/f URL and description. Also specify the IP address to register in ISM.

In Auto Discovery, both IPv4 and IPv6 addresses may be discovered for devices where both have been set. Specify the IP address to be registered in ISM.

To change the node IP address, select the version of setting IP address (IPv4 /IPv6), select the [Edit] button to set. If you set it, an IP address will be set for the device when registering the node.

4. Set a communication method.

Nodes discovered with Auto Discovery are displayed. Set a communication method for each node. When changing the IP address of a device, you must set a communication method.

5. Set the information for the node's mounting position in a rack.

6. Set the node group information and tag information.
7. Execute Register.

### Note

- The devices cannot be managed with IPv6 link local address. If the automatically discovered IP address is only IPv6 link local address, IP address setting is required.
- The IP address set for the device can be changed only in the following cases.

Device	Description
PRIMERGY server PRIMEQUEST 3000B	Can only be changed if the device is using a DHCP setting. If a fixed IP address is set to the device, execute the registration without changing the IP address.
PSWITCH 2048 T PSWITCH 2048 P PSWITCH 4032 P	Can only be changed if the device is using a fixed IP address setting. Set the right IP address to the device and execute the registration.

- If you change the IP address, check that the IP address set it from a range that can be accessed from ISM. If you set an IP address that cannot be accessed from ISM, you may not be able to connect to the device.

## 2.2.1.7 Adding tags to nodes



In ISM tags can freely be added to nodes. Tag is a function that adds information to allow the user to freely group nodes. For grouping nodes, there is a node group function, but it controls the access rights of the user. On the other hand, tags can be set without coordinating with access rights. It is possible to set multiple tags for a node.

For example, by setting tags for a group of nodes with the same purpose, nodes with the same tag can be displayed in the node list and managed by using filtering.

Tags can be added to nodes during node registration. Settings can also be executed after node registration.

### Adding tags after node registration

The following displays a sample operation for when adding tags after node registration.

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes].
2. Select the target node name to display the [Properties] tab.
3. From the [Actions] button, select [Edit].
4. Edit the tag information.
5. Select [Apply] to make the changed contents effective.

### Executing bulk edit to tags of multiple nodes

You can edit the tags for multiple nodes together. The following is a sample operation for editing the tags of multiple nodes.

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes].
2. Select the nodes you want to edit tags for, then, select [Edit Tag] from the [Actions] button.

3. Edit the tag information.
  - For adding tags  
Input new tag(s) in the [Add tag(s) to multiple nodes] field, or select existing tags and select [Add].
  - For deleting multiple tags together  
Select tags from the [Delete tag(s) from multiple nodes] field, and select [Delete].
  - For deleting tags individually  
Select [x] displayed on the [Tag] field in [Target Nodes].
4. Select [Apply] to make the changed contents effective.

### Specifying tags to execute filtering



The following is a sample operation for settings tags to filter nodes.

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes].
2. In the search box on the top left of the screen, enter the tag name that you want to filter. If you enter a character string in the search box, candidates will be displayed and you can select "Tag:."  
Or select the [ ] button on the right of the search box and enter the tag that you want to filter on the displayed screen and then, select the [Filter] button.
3. Filtering is executed and nodes with the specified tag set are displayed on the "Node List" screen.

#### Point

Select the nodes among the filtering results and execute [Assign Profile] or [Update Firmware]. For profile assignment and firmware update, refer to "2.4 Profile Management" and "2.6 Firmware Management."

## 2.2.2 Confirmation of Datacenters/Floors/Racks/Nodes



Here, you can confirm the information that is registered in ISM.

### Confirming datacenters, floors and racks

From the Global Navigation Menu on the GUI of ISM, select [Management] - [Datacenters] to display the "Datacenter List" screen. On the "Datacenter List" screen, select the applicable datacenter, and then confirm the display on the right side of the screen.

### Confirming nodes

Confirm the nodes that are registered in ISM.

From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes] to display the "Node List" screen. By selecting the node name of an applicable node and opening the [Properties] tab, you can confirm the information.

#### Point

With the settings below, log in from the login screen (iRMC) becomes unnecessary, and the Web screen can be displayed by selecting the Web URL of the nodes (PRIMERGY server).

- User management settings using Microsoft Active Directory
- Central Authentication Service (CAS) settings

For details, refer to "3.6 Use CAS to Log In to the Web Screen of the Server" in "Operating Procedures."

There are two conditions that the settings need to meet.

- That the user belongs to the user group that manages all nodes
- That the user has a user role exceeding the roles specified in the CAS settings



### Confirming node OS information

If the OS account information is registered on the node, you can confirm the network, disk, and card information from the OS.

Enter the FQDN of the realm name of Active Directory in the domain ID field, and enter the user name without the realm name but as the user name for when you monitor cloud management software by using a domain user ID.

In this case, only the information items that can be retrieved with the domain user's access rights are displayed on the GUI.

For the setup procedures for the monitoring target OS, refer to the following document. For details, contact your local Fujitsu customer service partner.

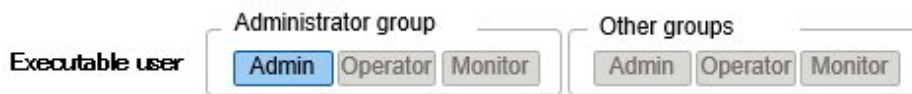
"Settings for Monitoring Target OS and Cloud Management Software"

## 2.2.3 Editing of Datacenters/Floors/Racks/Nodes

---

Edit the information that is registered in ISM.

### Editing datacenters, floors, and racks



The following is the operation procedure for editing datacenter, floor, and rack information.

1. From the Global Navigation Menu on the GUI, select [Management] - [Datacenters], and then select the datacenter, floor, or rack to be edited on the displayed "Datacenter List" screen.
2. From the [Actions] button, select [Edit Datacenter], [Edit Floor], or [Edit Rack] accordingly.
3. Edit the information.
4. Execute [Apply] to make the contents of the information effective.

### Editing nodes



The following is the operation procedure for editing node information.

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes] to display the "Node List" screen.
2. Select the node name of the applicable node to display the [Properties] tab.
3. From the [Actions] button, select [Edit].
4. Edit the information about the node.
5. Execute [Apply] to make the contents of the node information effective.



## 2.2.4 Deletion of Datacenters/Floors/Racks/Nodes

---



Delete any information that is registered in ISM.

### Deletion of datacenters

If you are going to delete a datacenter, you cannot delete it if any floors are registered in that datacenter. Delete or move any floors before you delete the datacenter.

### Deletion of floors

If you are going to delete a floor, you cannot delete it if any racks are registered on that floor. Delete or move any racks before you delete the floor.

### Deletion of racks

If you are going to delete a rack, you cannot delete it if any nodes are registered in that rack. Delete or move any nodes before you delete the rack.

### Deletion of nodes

This operation deletes the monitoring information, log information, and other information for the applicable nodes.



#### Note

.....

An error message such as "The object does not exist" or "The object is already deleted" may appear if you are logged in from multiple terminals and have deleted any datacenters, floors, racks, and /or nodes. In such a case, refresh the screen contents by one of the following procedures before you resume operation.

- For screens other than Network Map  
Select the Refresh button.
  - For Network Map  
From the [Actions] button, execute [Update network information].
- .....



#### Point

.....

You cannot delete any datacenters with registered floors, floors with registered racks, or racks with registered nodes. However, when you delete a chassis in which nodes are registered, both the chassis and the nodes are deleted at the same time.

.....

## 2.3 Monitoring

---

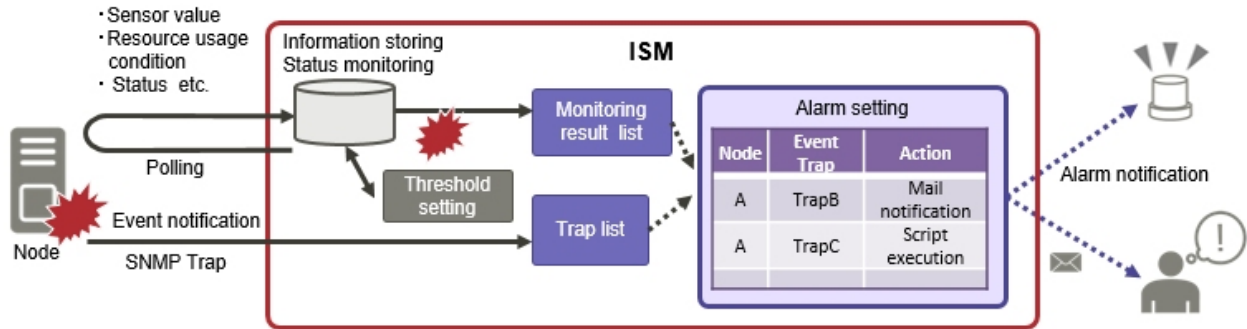
Monitoring is a function you can use for the following purposes.

- It polls statuses of resource utilization, such as for sensor values of node temperature or CPU utilization rate, and accumulates the information.
- It monitors the comparison between the threshold value set in advance and the polling result, as well as status changes.
- It receives incoming event notifications (SNMP Trap) from the nodes.
- It issues external alarm notifications on monitoring results and incoming event notifications from the nodes.

Specify the alarm notification method as an action of alarm settings in advance.

The following shows the operation overview of Monitoring.

Figure 2.3 Image of Monitoring



The following settings are related to Monitoring.

- [2.3.1 Setting of Monitoring Items and Threshold Values](#)
- [2.3.2 Monitoring of Network Statistics Information](#)
- [2.3.3 Action Settings](#)
- [2.3.4 Registration of Alarm Settings](#)
- [2.3.5 Graph Display of Monitoring History](#)

## 2.3.1 Setting of Monitoring Items and Threshold Values



Set the monitoring items (items for which to retrieve values) and the threshold values.

The following items are registered as monitoring items by default during node registration. (The item details that can actually be managed, however, vary with each device model.)

Default monitoring item	Description
Overall status	The overall status of each managed node itself as a whole system is monitored.
Power consumption	The power consumption of each managed device as a whole system as well as of individual parts are monitored.
Temperature information	The temperatures inside the racks, at air inlets and other positions are monitored.
Statuses of the various LEDs	Power LEDs, CSS LEDs, Identify LEDs, and Error LEDs are monitored. This is only applicable for PRIMERGY.

The following items can be additionally specified to be monitored.

Additional monitoring item	Description
Various types of resource information	CPU utilization rate, memory utilization rate, and other resource statuses are monitored.
Fan speed	The speeds of the various fans in managed devices are monitored.
Average power consumption/Average Intake Temperature	Power consumption and intake temperature are monitored at 3-minute intervals. When Power Capping is enabled and the nodes with Power Capping that are set as targets can be monitored.

### Procedure for adding monitoring items and threshold values

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes] to display the "Node List" screen.
2. Select the node name of the applicable node.
3. Select the [Monitoring] tab.
4. From the [Monitoring Actions] button, select [Add] to add monitoring items.

### 2.3.2 Monitoring of Network Statistics Information



Regarding the network switch, each type of statistic information (traffic and so on) can be retrieved on a port basis and threshold monitoring can be set up.

#### Setup procedure for monitoring of network statistics information/threshold monitoring

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes] to display the "Node List" screen.
2. Select the node name of the applicable node.
3. Select the [Network statistics] tab.
4. From the [Network statistics Actions] button, select [Edit] and enable monitoring of network statistics information.



#### Note

If you are using monitoring of network statistics information, use v2c or v3 for the SNMP account of the target node.

### 2.3.3 Action Settings



When ISM discovers an event, or when a trap is received from a node, an alarm can be sent for notification.

The following types of notification method (actions) are available.

Type of notification method	Description
Execute Remote Script	Execute an arbitrary script saved on an external host on the external host.
Send E-Mail	Sends e-mails with any user-defined contents.
Send/Forward Trap	Forward the received SNMP trap to an external SNMP manager, or forward an event discovered in ISM as an SNMP trap. When forwarding, the following forwarding types can be selected. <ul style="list-style-type: none"> <li>- ISM forwards the trap as a sender. The send SNMP trap is processed as if it was sent straight from ISM. Apart from information on the sender, the trap information is sent as it is.</li> <li>- The received trap is forwarded as-is. The received trap is forwarded to the SNMP manager as it is.</li> </ul>
Forward Syslog	Forward events/trap messages to an external Syslog server.

If you are using Forward Syslog, you must set the external Syslog servers so that they can receive Syslog forwarded from ISM. For details on how to set it, refer to "2.6 Set an Alarm (ISM internal events)" in "Operating Procedures."

## Macro

The macro (automatic variable) functions displayed below can be used in the title and text body of a sent email as well as to specify parameters when executing scripts. These macros are automatically replaced with the information of the node or event.

In addition, macros that can be used differ depending on the applicable type you selected when creating the alarm setting.

The list of macros and the correspondence between the macros and the applicable types are as follows.

Note: Y = Can be used, N = Cannot be used

Method of notation of macro	Overview	Applicable type	
		Node	System
\$_ISM	ISM host Name	Y	Y
\$_TRGID	Node ID of target for event (Node)	Y	N
\$_TRGTYPE	Target for event (System or Node)	Y	Y
\$_TRG	Target name for event (Node name)	Y	N
\$_IPA	IP address of the node	Y	N
\$_IDN	Serial number of the node	Y	N
\$_MDL	Model name of the node	Y	N
\$_DC	Name of the datacenter where the node in the rack is located	Y	N
\$_FLR	Name of the floor where the node in the rack is located	Y	N
\$_RACK	Name of the rack where the node is located	Y	N
\$_POS	Mounting position of the node in the rack The display format is different depending on the device. <ul style="list-style-type: none"> <li>- When 1U server is mounted in 2U : 2U</li> <li>- When CX400 chassis (2U) is mounted in 2U, and the target server exists in its slot 2 : 2-3U slot#2</li> <li>- When BX900 chassis (10U) is mounted in 2U, and the target connection blade exists in its back slot 2 : 2-11U CB#2</li> <li>- When PDU is mounted : PDU2</li> <li>- When Rack CDU is mounted : Not displayed</li> </ul>	Y	N
\$_MIB	MIB file name of the SNMP trap	Y	N
\$_SPC	Specific Trap Code of SNMP trap Last digit of the OID of the SNMP trap	Y	N
\$_TRP	Character string defining the TYPE of MIB of the SNMP trap	Y	N
\$_SEV	Severity of the event	Y	Y

Method of notation of macro	Overview	Applicable type	
		Node	System
\$_EVT	Message ID	Y	Y
\$_MSG	Description	Y	Y
\$_TIM	Time when the event occurred UTC time is displayed in RFC3339 format. (Example: 2018-01-01T00:00:00.000Z)	Y	Y
\$_TIM2	Time when the event occurred Displayed in local time format. (Example: 2018-01-01-00.00.00)	Y	Y

### Point

When the macro cannot be used (when [N] is shown in the table above), or when the value to be replaced does not exist, (none) is output.

### Procedure for adding actions

1. From the Global Navigation Menu on the GUI of ISM, select [Events] - [Alarms].
2. Select [Actions] from the menu on the left side of the screen to display the "Action List" screen.
3. From the [Actions] button on the right side of the screen, select [Add] to add an action.

### Required preparations before using each action

#### Execute Remote Script

Any script files to be executed is required to be saved on an external host.

The following are the OS for the external host and script files that can be used.

OS	Script file (Extension)
Windows	Batch file (bat)
Red Hat Enterprise Linux	Shell script (sh)
SUSE Linux Enterprise Server	Shell script (sh)

1. Prepare the script file to be used in the action setting.
2. Deploy the script file in an arbitrary directory in the OS on the external server.  
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 settings is required to access an external host from ISM and execute a script file.

For the setting procedures, refer to the following document. For details, contact your local Fujitsu customer service partner.

"Settings for Monitoring Target OS and Cloud Management Software"

### Note

For Execute Remote Script, a maximum execution time (default: 300 seconds) is set.

If script execution is not completed within the set time, script execution is forcibly terminated.

Set a time in which the script can complete successfully.

## E-Mail Sending

In order to send e-mails, you have to register the SMTP server information in advance.

1. From the Global Navigation Menu on the GUI of ISM, select [Events] - [Alarms].
2. Select [SMTP Server] from the menu on the left side of the screen to display the "SMTP Server Settings" screen.
3. From the [Actions] button on the right side of the screen, and then select [Edit] to register SMTP server information.

Also note that message encryption with S-MIME is available for sending e-mails. The user certificates to be used for encryption must be imported into ISM-VA in advance.

1. Prepare the personal certificates to be used in the action setting.
2. Transfer the certificate files to ISM-VA.

These certificates must be in PEM encoding format.

3. In ISM-VA Management, execute the command for registering certificates.

For details, refer to "[Registration of certificates for alarm notification mails.](#)"

## Send/Forward Trap

When sending or forwarding an SNMP trap, you must register the SNMP manager to send or forward it to.

1. From the Global Navigation Menu on the GUI of ISM, select [Events] - [Alarms].
2. Select [SNMP Manager] from the menu on the left side of the screen to display the "SNMP Manager List" screen.
3. From the [Actions] button on the right side of the screen, select [Add] to register SNMP manager information.

## Procedure for test execution for action

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

The "Action test" screen is displayed.

5. Select the [Test] button on the right side of the screen and execute a test.

When executing a test, the macro set for the action will be replaced with the following character string.

Macro	Character string after replacement
\$_ISM	TEST_ISM
\$_TRGID	TEST_TRGID
\$_TRGTYPE	TEST_TRGTYPE
\$_TRG	TEST_TRG
\$_IPA	TEST_IPA
\$_IDN	TEST_IDN
\$_MDL	TEST_MDL
\$_DC	TEST_DC
\$_FLR	TEST_FLR
\$_RACK	TEST_RACK
\$_POS	TEST_POS

Macro	Character string after replacement
\$_MIB	TEST_MIB
\$_SPC	TEST_SPC
\$_TRP	TEST_TRP
\$_SEV	TEST_SEV
\$_EVT	TEST_EVT
\$_MSG	TEST_MSG
\$_TIM	TEST_TIM
\$_TIM2	TEST_TIM2

### 2.3.4 Registration of Alarm Settings



Alarm settings sets the action to be executed when an event is discovered in ISM, or when a trap is received from a node, in advance.

#### Procedure for adding alarms

1. From the Global Navigation Menu on the GUI of ISM, select [Events] - [Alarms].
2. Select [Alarms] from the menu on the left side of the screen to display the "Alarm List" screen.
3. From the [Actions] button on the right side of the screen, select [Add] to add an alarm.

For events within ISM itself (for example, completion of DVD import), select "System" under [Applicable Type].

#### Event type

There are the following types of events.





Event Type	Description
Event	<p>Various events that are discovered internally in ISM.</p> <p>Events that alarms occur for are specified either according to their degree of severity or individually (Multiple can be specified).</p>
Trap	<p>SNMP traps sent from devices to be monitored.</p> <p>Based on the MIB information registered within ISM-VA, a list of receivable traps is displayed.</p> <p>Traps that alarms occur for are specified according to their degree of severity or individual traps are specified.</p> <p>It will not be displayed if "System" was selected under [Applicable Type].</p>



If the event type is Trap, the traps that become targets for generating alarms are only SNMP traps sent from monitored hardware.

#### Alarm status

Each node has one value for its alarm status, and this value changes when any kind of ISM event or SNMP trap relating to the node is discovered. Alarm statuses can take on the following values.

Alarm Status	Priority	Displayed by icons in the ISM GUI	Description
Error	High	 Red bell icon	This icon changes when any of the following events are discovered: - ISM event at Error level - SNMP trap at CRITICAL level
Warning	Medium	 Yellow bell icon	This icon changes when any of the following events are discovered: - ISM event at Warning level - SNMP trap at MAJOR or MINOR level
Info	Low	 Blue bell icon	This icon changes when any of the following events are discovered: - ISM event at Info level - SNMP trap at INFORMATIONAL level
None	-	 White bell icon	This is the status when no event is discovered.

An alarm status value of "Info" or higher means that an event corresponding to each level was discovered. Select [Events] - [Events] and when the "Event List" screen is displayed, select each tab and check the contents of the discovered event.

When you have completed confirming and recovering from the discovered event, execute the following procedure to clear the alarm status.

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes] to display the "Node List" screen.
2. Select the node name of the applicable node.
3. From the [Actions] button, select [Clear Alarm].

## Point

- Alarm statuses are not cleared automatically. However, if a status with a higher priority is discovered, it is displayed instead.
- When maintaining the node, you may systematically need to turn off the node. ISM has a "Maintenance Mode" function that temporarily interrupts its monitoring function so that ISM does not detect alarms that may occur during maintenance, such as a power-off alarm.

As alarm detection and background processing in ISM is restricted for nodes that are switched into Maintenance Mode, this prevents alarms from being issued repeatedly for the node.

For information on the Maintenance Mode, refer to ["5.1 Maintenance Mode."](#)

## Trap reception setting

Executable user

Administrator group	Other groups
<input checked="" type="checkbox"/> Admin <input type="checkbox"/> Operator <input type="checkbox"/> Monitor	<input type="checkbox"/> Admin <input type="checkbox"/> Operator <input type="checkbox"/> Monitor

v1, v2c, and v3 are supported as SNMP trap reception protocols.

Process for adding SNMP trap reception settings

1. From the Global Navigation Menu on the GUI of ISM, select [Settings] - [General].
2. Select [Trap Reception] from the menu on the left side of the screen to display the "Trap Reception Setting List" screen.
3. From the [Actions] button on the right side of the screen, and select [Add] to add trap reception settings.



4. Select the SNMP Version to be set, enter the required information.

When executing SNMPv3 trap reception setting, select applicable reception node and set "Engine ID."

### Point

By retrieving node information, the latest "Engine ID" is displayed on the Trap Reception Settings screen.

### Note

- When you add, edit, or delete trap reception settings, the changes are applied immediately. During the period between when a request is received and reflected, temporarily no SNMP traps will be received. When editing the trap reception settings, make sure that this behavior will not cause errors.
- When executing SNMPv3 trap reception, SNMP trap reception setting is required for each node. After node registration, execute SNMP trap reception settings.
- If you changed the "Engine ID" set to the node, retrieve the node information, and then re-set the retrieved, latest "Engine ID."
- Depending on the device, "Engine ID" cannot be retrieved when retrieving node information. For details on the node settings or details on retrieving the "Engine ID" by retrieving node information, refer to "[A.2.2 Details of Node Settings](#)."

## MIB file

MIB is public information regarding the status of the network devices managed with SNMP, and is standardized as MIB-II, which was published as RFC 1213. The MIB file is text-based file that defines this public information. To send and receive SNMP traps, the receiving side is required to save the MIB file provided by the device side.

Add/update the MIB file in the following cases.

- If you want to add a new MIB file to receive SNMP traps from non Fujitsu devices.
- If you want to update an MIB file already registered in ISM to execute firmware update.

### Note

- Registered MIB files can be deleted, however if the SNMP trap that was defined in the deleted MIB files is received, it is processed as an unknown trap.
- Do not register multiple MIB files for which the same trap is defined. If you have registered multiple MIB files with the same trap defined, this is handled as if the multiple of the same traps were received.
- To manage the severity of traps with ISM, MIB files to be imported are required to be written in specific format. If MIB files written in a format out of the specified format are imported, the behavior could differ from the definition. Check that there are no errors in the format before MIB files import.

For details of the format for MIB files, refer to "[A.1.3 Notes on MIB File Import](#)."

## Registering MIB

You can add a new MIB file that has not yet been registered on ISM.

1. Prepare an MIB file. Note that all the files that have a dependency relationship to MIB are required.
2. Transfer the MIB file to ISM-VA.
3. Execute the MIB registration command from ISM-VA Management.

For details, refer to "[4.16 MIB File Settings](#)."

## Point

You can update an MIB file by registering a file having the same name as the MIB file already registered on ISM.

### Confirming MIB files

You can confirm the names of MIB files registered on ISM using a list. To confirm the list of MIB file names, execute the MIB reference command of ISM-VA Management.

For details, refer to "4.16 MIB File Settings."

### Deleting MIB files

To release the registration of MIB files registered in ISM, delete the corresponding MIB file. To delete the MIB files, execute the MIB file deletion command of ISM-VA Management.

For details, refer to "4.16 MIB File Settings."

## Point

Whenever you delete an MIB file, you should pay attention to its dependency relationship. If you have deleted an MIB file having a dependency relationships, this could result in that the traps is not received.

## 2.3.5 Graph Display of Monitoring History

The history of the monitoring items accumulated in Monitoring can be displayed in a graph on the ISM GUI. The graph display allows the user to easily grasp changes and tendencies in the history of the monitored items. There is the method to display a graph for each node, and the method to display the graph for multiple nodes in a dashboard widget.

For details, refer to "4.5 Display Monitoring History in a Graph" in "Operating Procedures."

## 2.4 Profile Management

Profile Management is a function that is mainly used for installation and construction of the system.

You can set up servers, network switches, and storages to be managed nodes.

The Profile Management target nodes for each type of node and the items that can be set are displayed below.

Table 2.1 Target nodes and available setting items of Profile Management

Node type	Target node (example)	Available setting items
Server	PRIMERGY RX PRIMERGY TX PRIMERGY BX PRIMERGY CX	- BIOS setup - iRMC setup - OS installation - Virtual IO setup
	PRIMEQUEST 2000-Partition	- MMB setup - OS installation
	PRIMEQUEST 3000E-Partition	- MMB setup - OS installation - Virtual IO setup (physical partition only)
	PRIMEQUEST 3000B	- BIOS setup - iRMC setup - OS installation

Node type	Target node (example)	Available setting items
Network switch	SR-X	- Setting of administrator passwords - SNMP, NTP, and STP settings
	VDX PSWITCH 2048 T PSWITCH 2048 P PSWITCH 4032 P	- Setting of administrator passwords - SNMP and NTP settings
	CFX	- Administrator passwords and AAA settings - SNMP, Interface, and NTP settings
Storage	ETERNUS DX	- Creation of RAID groups/volumes - Creation of global hot spares - Host Affinity settings
	ETERNUS NR (NetApp)	- SNMP and NTP settings

Here, the following points are described:

- [2.4.1 Profile Usage](#)
- [2.4.2 Profiles and Policies](#)
- [2.4.3 OS Installation Settings](#)
- [2.4.4 Virtual IO Management](#)
- [2.4.5 Pool Management](#)
- [2.4.6 Confirmation of Boot Information](#)

## 2.4.1 Profile Usage

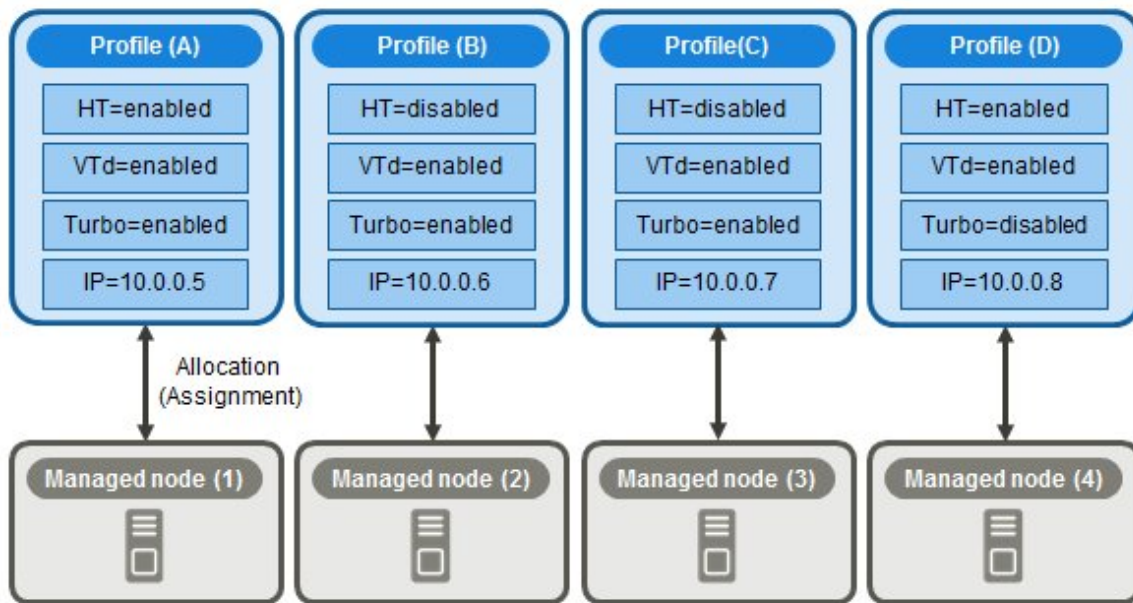
---

Before you can use Profile Management to execute node settings, as a preparatory task, you have to record the hardware settings (configuration) of each node and the settings at the time of OS installation in a set of definitions called "profile."

By allocating (Assignment) this profile to nodes, the settings become effective for those nodes.

Profiles are assigned to managed nodes one-on-one. This means you require one profile for each node to be managed by a profile.

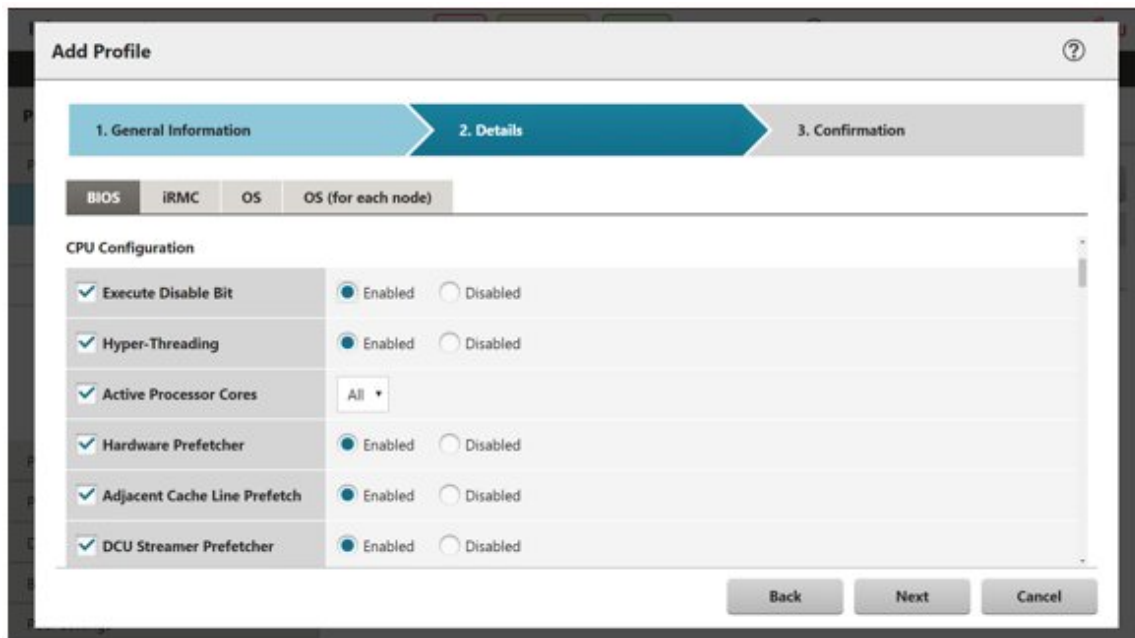
Figure 2.4 Relationships between profiles and managed nodes



Note

When you assign a profile containing OS-related settings to a node, the OS will be installed anew according to the profile contents. This means that, if there already is an OS installed, the profile does not merely change the settings but deletes the existing OS and data before newly installing the OS.

Figure 2.5 "Creation of Profile" screen sample (GUI)



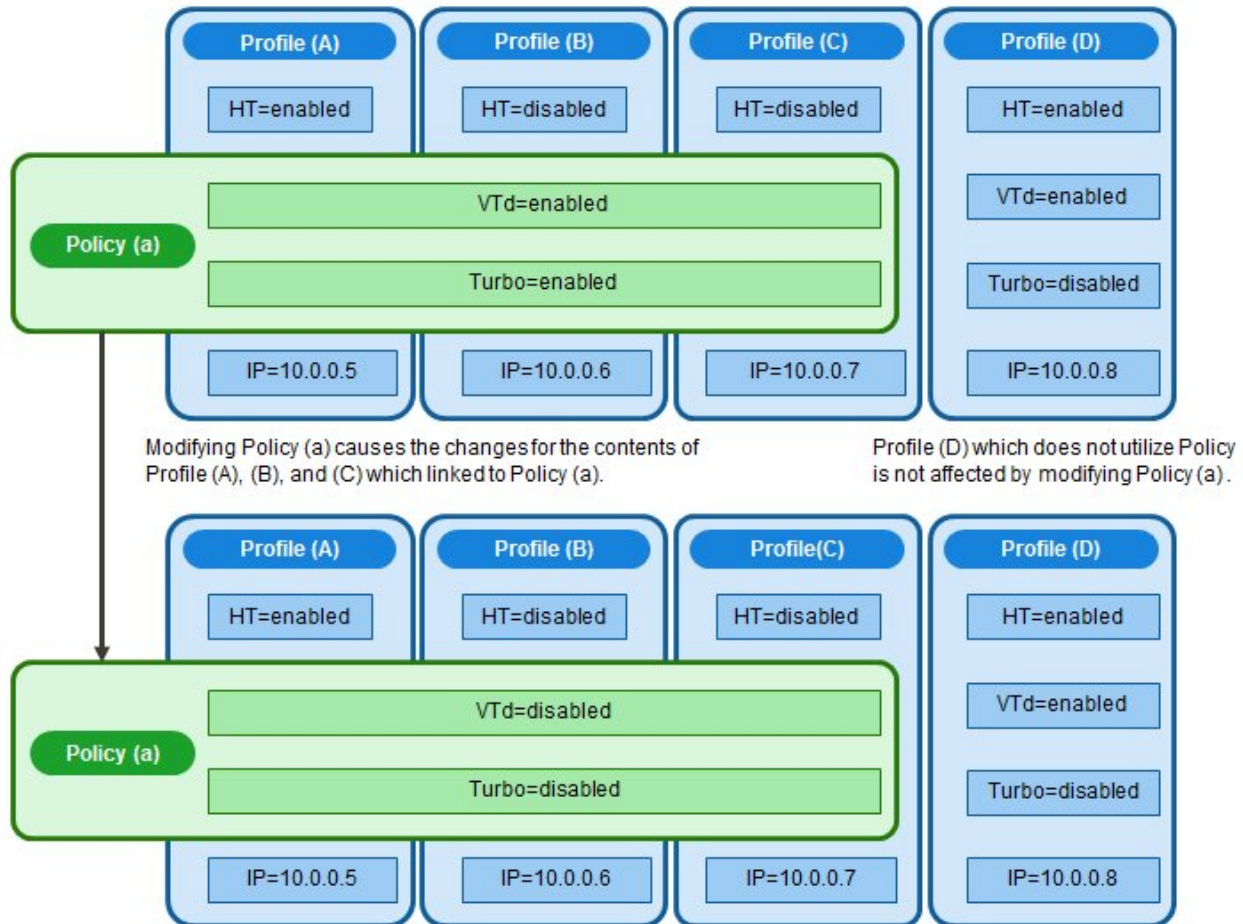
## 2.4.2 Profiles and Policies

Policies are structures that extract those setting contents that are the same across multiple profiles to allow for batch settings. The settings in a policy are written in the same way as in a profile, but, instead of assigning a policy directly to nodes, a profile looks up the contents of the policy to assign the settings to the nodes indirectly. The contents of a single policy can be looked up by multiple profiles.

One profile is required for each node. For example, in order to set the same contents for the hardware configuration of multiple nodes, you have to prepare the same number of profiles as you have nodes for which to execute the same settings. After creating the first profile, you can use the "Reference Create" function to edit duplicates of that profile for creating the same number of profiles as you have nodes. This procedure, however, requires that you repeat modifying all profiles, even when you want to change the same setting contents on all nodes.

If you assume such circumstances, you can use the policy function to create the profiles in advance, which will allow you to easily change the multiple settings together.

Figure 2.6 Relationships between profiles and policies



### Note

- Profiles and policies contain general setting items that are supported on the target nodes. However, there are also some setting items that are not supported, depending on the model and firmware version of the target node. Therefore, in the profiles and policies, do not execute any settings for items that are not supported on the nodes to which they are assigned.
- When you install an OS, you cannot install any OS that is not supported by the target node and the ServerView Suite DVD you are using.

### Point

- If you are going to use a policy, create the policy before you create the profiles.
- You can use policies for the OS settings, BIOS settings, iRMC settings, or MMB settings on servers.

## Profile groups and policy groups

Profiles and policies can be managed group wise. You can freely create groups as required (for example, by operating purpose or by time of installation) and include any profiles or policies to facilitate management.

You can include profiles in profile groups, and policies in policy groups.

### 2.4.2.1 Creation of policy groups/policies



#### Creating policy groups

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Profiles] and then select [Policy Settings] from the menu on the left side of the screen.
2. With the location where you want to create a policy group selected in the tree on the left side of the screen, select the [Actions] button and select [Add Group].

#### Creating policies

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Profiles], and then select [Policy Settings] from the menu on the left side of the screen.
2. With the location where you want to create a policy selected in the tree on the left side of the screen, select the [Actions] button and select [Add Policy].
3. Enter the setting items according to the "Add Policy" wizard.

From the policy setting items, select those setting values that you want to be reflected in the profile by selecting the corresponding checkboxes under [2.Details] in the "Add Policy" wizard. Policy setting items for which the checkbox is not selected will not take effect in the profile.

### 2.4.2.2 Creation of profile groups/profiles



#### Creating profile groups

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Profiles].
2. With the location where you want to create a profile group selected in the tree on the left side of the screen, select the [Actions] button and select [Add Group].

#### Creating profiles

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Profiles].
2. With the location where you want to create a profile selected in the tree on the left side of the screen, select the [Actions] button and select [Add Profile].
3. Enter the setting items according to the "Add Profile" wizard.

From the profile setting items, select those setting values that you want to be reflected in the profile by selecting the corresponding checkboxes under [2.Details] in the "Add Profile" wizard. Profile setting items for which the checkbox is not selected will not take effect in the profile.

### 2.4.2.3 Assignment of profiles



#### Note

- Executing a profile assignment while logged in to the target node with a web operating screen or SSH may sometimes result in a profile assignment error.
- If you are going to install an OS, you must prepare the required settings and files in advance. Refer to the following:

["Required preparations before OS installation"](#)

1. If the target node of profile assignment is a server, power off the server before you assign the profile. For nodes other than servers, switch the power on.
2. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes].
3. In the [Column Display] field on the "Node List" screen, select [Profile].
4. Select the checkbox for the node to which you want to assign the profile, then select the [Actions] button and select [Assign/Reassign Profile].

#### Point

Depending on the profile contents, profile assignment may require a long time to complete (for example, more than an hour). You can confirm the current progress of profile assignment on the "Tasks" screen. For details, refer to ["2.13.4 Task Management."](#)

### 2.4.2.4 Editing and reassigning profiles



You can modify node settings by editing a profile that is assigned to the node and assigning the profile to the node again.

You can edit the contents of a profile while it is assigned to a node. At that time, however, editions of the profile do not immediately carry over into changed node settings. For the time being, ISM handles this status as a mismatch between content of the profile and the node.

Reassign the edited profile to the node whenever suits you best. As soon as reassignment is complete, the node settings change, so the status can return to normal again, with matching profile and node settings.

#### Reassigning profiles

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Profiles].
2. In the tree on the left side of the screen, select the location of the profile to be edited, and then select the profile in the list on the right.
3. From the [Actions] button, select [Edit] to edit profiles.
4. If the target node of profile assignment is a server, power off the server before you assign the profile. For nodes other than servers, switch the power on.
5. From the Global Navigation Menu, select [Management] - [Nodes].
6. In the [Column Display] field on the "Node List" screen, select [Profile].
7. Select the applicable node, then select the [Actions] button and select [Assign/Reassign Profile].

## Confirming whether node settings match profiles

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes].
2. In the [Column Display] field on the "Node List" screen, select [Profile].

For nodes whose settings do not match the profile, [Reassignment] is displayed under [Status].

For nodes whose settings match the profile, [Assigned] is displayed under [Status].

For nodes where only the nodes settings and the profile of server OS settings do not match, [Assigned (Differences)] is displayed under [Status].

### Note

- Modifying any settings directly on a node without using Profile Management causes a mismatch between the contents of the applied profile that are displayed on the ISM screen and the actual node status.
- When [Status] is [Assigned (Differences)], you cannot perform normal re-assignment.

In this case, in the "Profile Assignment" screen, check the [Enable Advanced Settings] checkbox and use "Handle profile as assigned in ISM without actually assigning it to the node."

## 2.4.2.5 Releasing and deleting profiles



In the following cases, you have to release any assigned profiles in advance:

- When you are going to delete an assigned profile
- When you are going to delete a node to which a profile is assigned from ISM
- When you are going to remove a node to which a profile is assigned from its node group, or going to modify the node group

### Point

For details on node groups, refer to "2.13.1 User Management."

## Releasing profiles

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes].
2. In the [Column Display] field on the "Node List" screen, select [Profile].
3. Select the checkbox for the node to which the profile is assigned, then select the [Actions] button and select [Release Profile].

## Deleting profiles

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Profiles].
2. In the tree on the left side of the screen, select the location of the profile to be deleted, and then select the profile in the list on the right.
3. From the [Actions] button, select [Delete].

You can only delete profiles whose status is [Not assigned].



## 2.4.2.6 Exporting and importing profiles



You can export and import the profiles as text files written in JSON format, for example, if you want to reuse profiles in another ISM system or store assigned profiles in the Management terminal.

### Point

Also, you can export and import policies.

### Exporting profiles

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Profiles].
2. Select the profiles to be exported.
3. From the [Actions] button, select [Export].
4. Set up an encryption password key (required), and then execute the export by the [Export] button.

### Importing profiles

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Profiles].
2. Select the location where the profile is stored in the tree on the left side of the screen, select the [Actions] button - [Import].
3. Select from the options in [File selection method].
  - Local  
Import a profile stored locally.
  - FTP  
Import a profile from the FTP server of ISM-VA.  
You must transfer the profile to the "/<User group name>/ftp" directory of ISM-VA in advance.  
For FTP connection and how to transfer FTP, refer to "2.1.2 FTP Access."
4. Specify the profile to be imported in [File Path].
5. Select [Profile Type].
6. Enter [Profile Group Name].
7. Enter the decryption password key you set up in [Decryption Password Key] when exporting the profiles (required), and then execute the import by the [Import] button.

### Point

- The files you deployed on the FTP server of ISM-VA are no longer required after the import has finished. Use an FTP command to delete them.
- Since profiles contain passwords and other security information, you must set up a freely specifiable encryption key when you export profiles.

### 2.4.2.7 Editing/deleting profile groups



#### Editing profile groups

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Profiles].
2. In the tree on the left side of the screen, select the location of the profile group to be edited, and then select the profile group in the list on the right.
3. From the [Actions] button, select [Edit] to edit profile groups.

#### Deleting profile groups

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Profiles].
2. In the tree on the left side of the screen, select the location of the profile group to be deleted, and then select the profile group in the list on the right.
3. From the [Actions] button, select [Delete].

### 2.4.2.8 Editing/deleting policy groups



#### Editing policy groups

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Profiles] and then select [Policy Settings] from the menu on the left side of the screen.
2. In the tree on the left side of the screen, select the location of the policy group to be edited, and then select the policy group in the list on the right.
3. From the [Actions] button, select [Edit] to edit policy groups.

#### Deleting policy groups

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Profiles] and then select [Policy Settings] from the menu on the left side of the screen.
2. In the tree on the left side of the screen, select the location of the policy group to be deleted, and then select the policy group in the list on the right.
3. From the [Actions] button, select [Delete].

### 2.4.2.9 Specifying behavior when assigning profiles

Normally, you either newly assign a profile to a node or reassign an already assigned profile after changing it, but, during the assignment/reassignment operation on the GUI, you can select the [Enable Advanced Settings] checkbox on the "Profile Assignment" screen to change the behavior conditions (Assignment mode) when assigning profiles. Moreover, for servers, you can specify the scope to which to assign a profile separately for each function group (BIOS, iRMC, MMB, OS, and Virtual IO).

The behavior conditions (Assignment mode) you can specify are as follows.

- "Assign profile also to unchanged portions"

With a profile being assigned, the node settings are overwritten even if the node and profile contents are matching.

Note, however, that you cannot reassign an OS part of the profile.

- "Hot Profile Assignment (with node power remaining on)"

When you assign a profile to a server, it is usually required to assign the profile while the power of the target node is switched off. Selecting this operation allows you to assign the profile while the power of the target node remains on.

Note the following points.

- Some parts of BIOS settings, iRMC settings, and MMB settings are not made effective until the server is rebooted.

After completion of the profile assignment, reboot the server at any timing.

- You cannot select this mode when OS settings or virtual IO settings are the target of your profile assignment.
- For servers where iRMC S5 is installed, profiles for BIOS settings cannot be assigned in this mode.
- If the iRMC firmware version of the server where iRMC S4 is installed is 9.xxF or later, profiles for BIOS settings cannot be assigned in this mode. If you want to assign profiles for BIOS settings in this mode, use iRMC firmware version 8.xxF.

- "Handle profile as assigned in ISM without actually assigning it to the node"

Profile assignment is completed only internally within ISM management, without actually executing any changes on the node. Therefore, after an assignment, differences between node statuses and ISM Management statuses may occur.

## 2.4.3 OS Installation Settings

---

### Required preparations before OS installation

- The OS installation media and the ServerView Suite DVD require to be copied to the repository area on ISM-VA in advance. This task is called "import."

If you are going to import an ISO image of the OS installation media, allocate a virtual disk to the user group.

For details, refer to "[3.7.2 Allocation of Virtual Disks to User Groups](#)."

Import the ServerView Suite DVD as an ISM administrator (user of Administrator group). Since it is shared with all user groups, it is not required to import it with respect to each user group.

For details, refer to "[2.13.2 Repository Management](#)."

- Use the PXE boot function on the target node. Complete the network connections and the BIOS settings of the target server in advance, so as to enable PXE booting from the management LAN. Moreover, a separate DHCP server is required within the network. Set the DHCP server so as to allow the target nodes to lease appropriate IPv4 addresses during the PXE boot.

For details, refer to "[A.1.1 DHCP/PXE Settings in Using Profile Management/Firmware Management](#)."

### Precautions on OS installation

If there are errors in the network environment settings or the BIOS settings of the target servers, it may occur that the PXE boot fails and the OS that was already installed on the respective server starts up. In such a case, the server on which to install the OS cannot be shut down from ISM. When the timeout time for processing the profile assignment (Task) elapses, processing ends with an error.

In order to forcibly abort processing for a profile assignment before it ends with a timeout error, cancel the task.

### Procedure for specifying scripts to be executed after OS installation

To execute any specified scripts after installing an OS, you must transfer the script files to the ISM-VA in advance.

1. Prepare the scripts you want to execute after OS installation.
2. Connect to ISM-VA via FTP and transfer the script files.

In the "ftp" directory, create a freely named subdirectory for the scripts and transfer them into that subdirectory.

For FTP connection and how to transfer FTP, refer to "[2.1.2 FTP Access](#)."

3. Add or edit a profile to specify the directory names where you stored the script files and the names of the script files to be executed under the item of [Execute Script after Installation].

## 2.4.4 Virtual IO Management

---

Virtual IO Management is a function that virtualizes the LAN, FC (Fibre Channel) I/O parameters (MAC and WWN).

- A virtual MAC address can be used instead of the MAC address of the LAN controller.
- A virtual WWN can be used instead of the WWN of the FC controller.
- Virtual MAC address, virtual WWN, network channel allocation, and I/O parameters for network boot can be saved in a profile.

### Point

.....

The virtual MAC address and virtual WWN must be unique across all nodes managed with ISM, or in the node group. Because of this, profiles where virtual IO such as virtual MAC address and virtual WWN has been set cannot be assigned to multiple nodes.

.....

### Note

- .....
- When the software that manages virtual IO such as ServerView Virtual-IO Manager (VIOM) is running, be careful not to be in conflict with ISM.
  - To avoid conflict when VIOM is running, make sure that ISM and VIOM do not manage the same node.
  - The parameter setting for the UEFI boot mode of the virtual IO is reflected in the CSM Configuration settings of the BIOS. For details on each setting of UEFI boot mode, refer to "4.2 Port Setting" in "Items for Profile Settings (for Profile Management)."
  - For the PRIMERGY BX series, do not reset the virtual IO settings from MMB.
  - For PRIMEQUEST 3000E partitions, expansion partitions are not supported. Only physical partitions can be set up.
  - For PRIMEQUEST 3000E partitions, you must set the IP address and a user account for the iRMC partition. For setting procedures, refer to the following site.

<http://manuals.ts.fujitsu.com/>

How to display the "Manuals" page:

1. From the "Manuals" menu on the left side of the screen, select [x86 Servers] - [PRIMEQUEST Servers].
2. From the pull-down menu for "SELECT" in the middle of the screen, select [PRIMEQUEST 3000 Series] - [Enterprise Model].

- Setting an iRMC IP address

"FUJITSU Server PRIMEQUEST 3000 Series Enterprise Model Tool Reference (MMB)" - "2.4.3.1 [IPv4 Console Redirection Setup] window"

- Setting an iRMC user account

"FUJITSU Server PRIMEQUEST 3000 Series Enterprise Model Tool Reference (MMB)" - "3.2.78 set irmc user"

In addition, set the iRMC information in "Edit Node" of the partition.

- For PRIMEQUEST 3000E partitions, disable the CSM settings of the BIOS.
  - For PRIMEQUEST 3000E partitions, use UEFI. For the method to set UEFI, refer to "4.2 Port Setting" in "Items for Profile Settings (for Profile Management)."
  - For PRIMERGY or PRIMEQUEST 3000E partitions, you must set the boot number of the port of the LAN card to more than one in the virtual MAC address settings.
- .....

### MAC address and WWN virtualization

By managing the virtual IO settings (virtual MAC address, virtual WWN and so on) of servers as profiles, Virtual IO Management can be used by assigning these profiles. When replacing managed servers or PCI cards, this reduces the workload for changing the settings of peripheral devices and makes it easy to re-set network information.

For replacing managed servers or PCI cards that used Virtual IO Management, it is assumed to be executed according to the following procedure.

Figure 2.7 Replacing a managed server that used Virtual IO Management

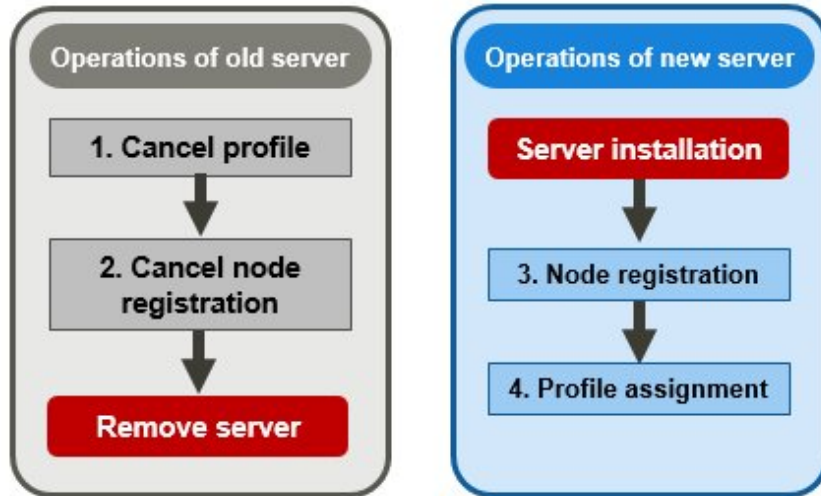
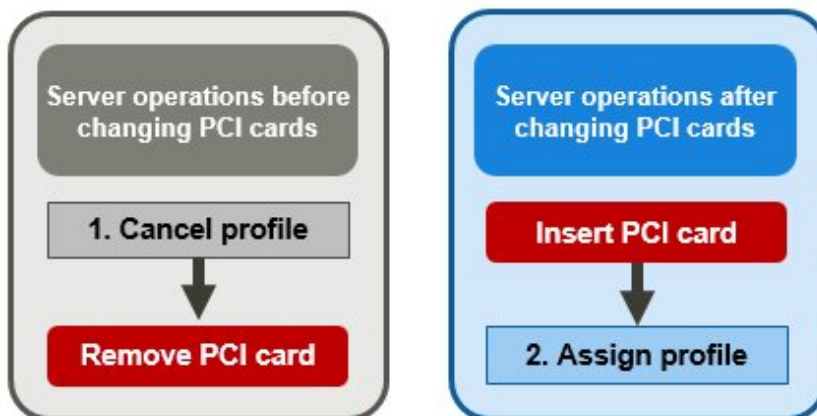


Figure 2.8 Replacing a PCI card that used Virtual IO Management



### iRMC AC power OFF recovery for virtual IO

If iRMC loses all power (all electric cable connections are broken, or the data center loses power), iRMC loses the virtual IO settings. Apply the virtual IO settings again when the AC power is restored and iRMC has been booted again.

Required preparations for iRMC AC power OFF recovery for virtual IO

You must set the IP address of ISM as the SNMP trap destination to the server in advance.

#### Note

- For operating this process, it must be possible to access ISM and iRMC.
- iRMC AC power OFF recovery for virtual IO is enabled only in PRIMERGY.

For PRIMEQUEST 3000E partitions, set the iRMC account of the partition on the device side again, and then re-assign the profile manually.

## Point

For the time it takes until the reassign of the virtual IO settings has been completed, iRMC will regularly send an SNMP trap to ISM, encouraging the reassign of the virtual IO settings. This process can be stopped by disabling the virtual IO management status from the iRMC user interface or the BIOS interface.

An error message may be displayed even if the virtual IO was successfully reassigned. Confirm that the virtual IO was reassigned.

Re-assign the profile if re-assigning is not executed using the recovery function.

## 2.4.5 Pool Management

The Pool Management function is a function that manages address resources by arranging them into pools. The following main functions are available.

- Set the address range a user can use as a pool
- Allocate values from the pool as required.
- Return the value that is no longer required to the pool

### Target resources of the pool

The target resources of the pool are the following virtual addresses.

- Virtual MAC Address
- Virtual WWN

The Pool Management function is used when using the Virtual IO Management function to set the virtual addresses above.

When setting the virtual addresses above during the creation of profiles, values can automatically be allocated from the pool range without having to enter the values of the virtual address. You can select the values allocated from the set pool.

If you delete the profile that the above virtual addresses have been set for, the virtual address is returned to the pool as an unnecessary value.

Here, the following operations are described:

- [Register pool settings](#)
- [Confirm pool settings](#)
- [Edit pool settings](#)
- [Delete pool settings](#)

### Register pool settings



1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Profiles] - [Pool Settings].
2. From the [Actions] button, select [Register].
3. In the "Register Pool" screen, set the required information and select [Register].
  - Pool Type  
Select the type of pool to set.
  - Start Address and End Address  
Set the start address and the finish address of the pool range to be set.

- Authorized user group

Select a user group that can allocate values from the pool range to be set.

If you selected [All user groups], any user group can allocate values from the pool range set here.

### Confirm pool settings

Executable user

Administrator group	Other groups
<input checked="" type="checkbox"/> Admin <input type="checkbox"/> Operator <input type="checkbox"/> Monitor	<input checked="" type="checkbox"/> Admin <input checked="" type="checkbox"/> Operator <input checked="" type="checkbox"/> Monitor

From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Profiles] - [Pool Settings] to display the "Pool List" screen.

The pool settings that the user can use are displayed on the "Pool List" screen. You can also confirm the number of addresses that are available and the number of allocated addresses.

If the number of available addresses is 0, addresses cannot be allocated from the range of this pool. Execute "[Register pool settings](#)" or "[Edit pool settings](#)" to add pool range.

### Edit pool settings

Executable user

Administrator group	Other groups
<input checked="" type="checkbox"/> Admin <input type="checkbox"/> Operator <input type="checkbox"/> Monitor	<input type="checkbox"/> Admin <input type="checkbox"/> Operator <input type="checkbox"/> Monitor

When editing the settings of a pool, only the Start Address and End Address can be edited.

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Profiles] - [Pool Settings].
2. Select the pool you want to edit and select [Edit] from the [Actions] button.
3. Set the required information in the "Edit Pool" screen, and select [Register].

### Note

If there are allocated addresses, the allocated addresses cannot be set outside of the range of the pool. Confirm the allocated addresses when editing.

### Delete pool settings

Executable user

Administrator group	Other groups
<input type="checkbox"/> Admin <input type="checkbox"/> Operator <input type="checkbox"/> Monitor	<input type="checkbox"/> Admin <input type="checkbox"/> Operator <input type="checkbox"/> Monitor

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Profiles] - [Pool Settings].
2. Select the pool setting to be deleted and select [Delete] from the [Actions] menu.
3. Confirm the item to be deleted and select [Delete].

## 2.4.6 Confirmation of Boot Information

Executable user

Administrator group	Other groups
<input checked="" type="checkbox"/> Admin <input checked="" type="checkbox"/> Operator <input checked="" type="checkbox"/> Monitor	<input checked="" type="checkbox"/> Admin <input checked="" type="checkbox"/> Operator <input checked="" type="checkbox"/> Monitor

You can confirm the boot information of the node set with Virtual IO Management.

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

2. From [Column Display] on the "Node List" screen, select [Boot Info].

## 2.5 Log Management

Log Management is a function that is mainly used for the following purposes:

- Collecting Node Logs periodically, according to a specified schedule
- Collecting Node Logs at any suitable time
- Downloading and using collected logs
- Referring and searching with key words on the GUI screen

In ISM, you can set the "Type of log to be collected" and the "Collection schedule" separately for each node.

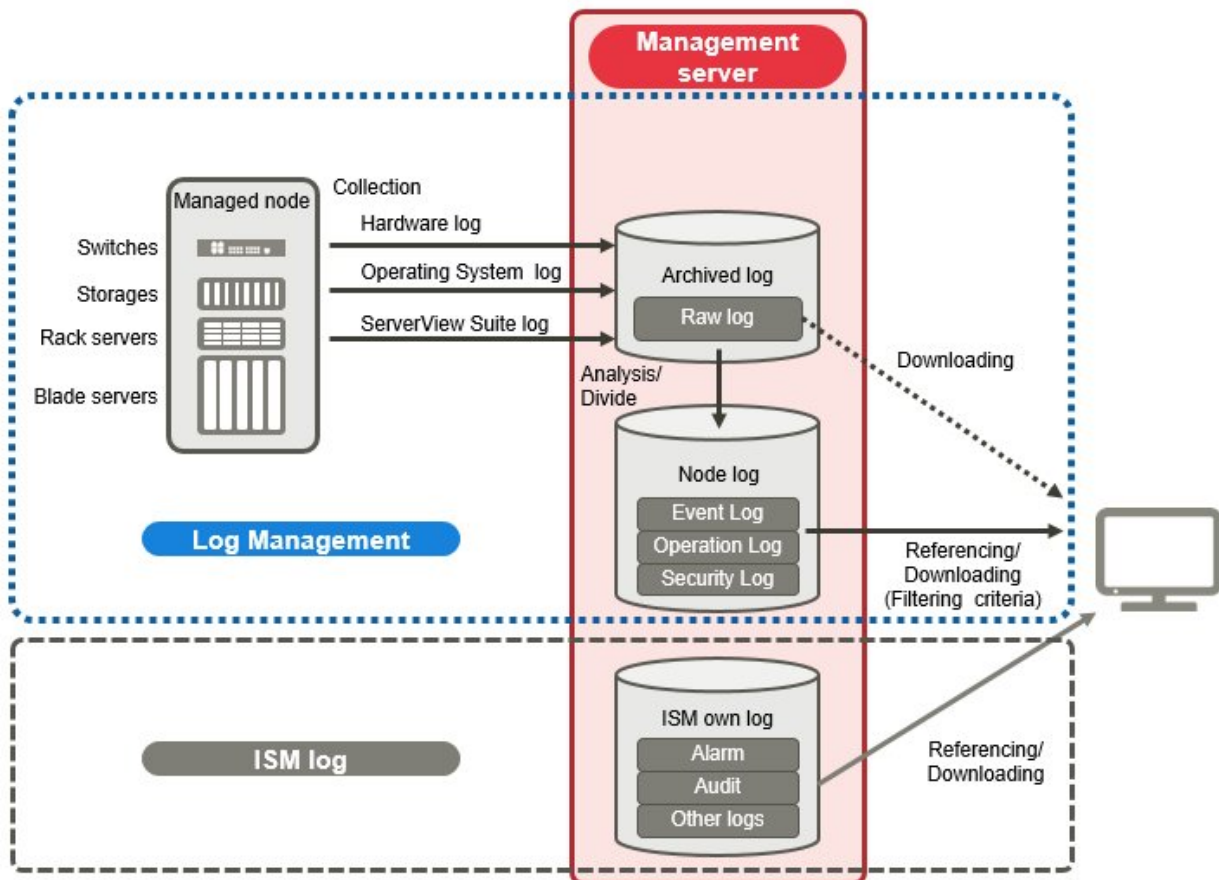
The bulk of log data that are collected from nodes according to these settings are called "Archived Logs."

Archived Logs are stored on the management server without any changes to the data format of the log files collected from each node. By operations on the GUI of ISM at an arbitrary timing, you can download the Archived Logs converted into zip files to the management terminal.

Any of the log files from Archived Logs can be classified as "Event Logs," "Operation Logs," and "Security Logs" according to ISM standards. On the management server, the "Data for log search" (for list or search display on the GUI) and the "Data for download" are accumulated separately. In ISM, logs with these statuses are collectively called "Node Logs."

These "Node Logs" are displayed as a list on the GUI, and the display contents can be filtered by factors such as their classification into "Event Logs," "Operation Logs," and "Security Logs" as well as the date and time of occurrence. Moreover, you can view a list of the filtered logs and download them, converted into CSV or zip files, to the management terminal.

Figure 2.9 Image of Log Management







ISM analyzes the formats of Archived Logs to classify them into "Event Logs," "Operation Logs," and "Security Logs." Therefore, do not change the OS defaults of the log message formats of each node.

If, for example, the log message format for a Linux operating system log is changed in the OS system log settings, ISM can no longer recognize the log and, consequently, generate no correct Node Log.

Here, the following points are described:

- [2.5.1 Types of Collectable Logs](#)
- [2.5.2 Setting Log Retention Periods](#)
- [2.5.3 Setting Log Collection Targets, Dates and Times](#)
- [2.5.4 Operations for Log Collection](#)
- [2.5.5 Searching Node Logs](#)
- [2.5.6 Downloading Node Logs](#)
- [2.5.7 Downloading Archived Logs](#)
- [2.5.8 Deleting Node Logs](#)
- [2.5.9 Deleting Archived Logs](#)

## 2.5.1 Types of Collectable Logs

Log Management can collect three types of log: hardware logs, operating system logs, and ServerView Suite logs. For supported hardware, OSes, and other details, contact your local Fujitsu customer service partner.

### Hardware logs

Log Management collects device logs from each managed node.

Type	Node from which to collect log	Type of Archived Log to be collected	Type of Node Log to be analyzed and accumulated
Server	PRIMERGY (Except CX1430 M1)	SEL System Report (Server with iRMC S4 and later)	SEL
	PRIMEQUEST 3000B		
	IPCOM VX2		
	PRIMERGY CX1430 M1	SEL (binary)	None
Chassis	PRIMERGY BX	Exported results of "show Log/ MgmtBlade LogMgmtBladeAll" command Exported results of "set SystemInfo/ Dump Started=true" command	Exported results for "show Log/MgmtBlade LogMgmtBladeAll" command
	PRIMEQUEST 3000E	SEL Exported results for "opelogview" command Exported results for "selview" command Exported results for "configview" command	SEL
Storage	ETERNUS DX/AF	Exported results for "export log" command	Exported results for "show events" command

Type	Node from which to collect log	Type of Archived Log to be collected	Type of Node Log to be analyzed and accumulated
		Exported results for "show events" command	
	ETERNUS NR (NetApp)	Exported result for "event log show" command Each file type under the /mroot/etc/log directory	Exported result for "event log show" command
Connection Blade	Ethernet Switch	Exported results for "show tech-support" command	Exported results for "show logging persistent" or "show logging syslog" command (Included in exported results for "show tech-support" command)
	Fibre Channel Switch	Exported result for "supportshow" command Each type of file created with the "supportsave" command	Exported result for "supportshow" command
Switches	SR-X	Exported results for "show tech-support" command	Exported results for "show logging syslog" command (Included in exported results for "show tech-support" command)
	CFX		
	PSWITCH 2048 T PSWITCH 2048 P PSWITCH 4032 P	Exported results for "show tech-support" command	Exported results for "show logging persistent" command (Included in exported results for "show tech-support" command)
	VDX	Various files created with the "copy support" command	Exported results for the "show logging raslog" command Exported results for the "show logging audit" command (Included in "<Arbitrary text string as required>.INFRA_USER.txt.gz" file created with the "copy support" command)
	Cisco Catalyst	Exported results for "show tech-support" command	Exported results for "show logging" command (Included in exported results for "show tech-support" command)

## Operating system logs

Log Management retrieves logs for the OSEs that are running on the managed servers.

OS for which to retrieve logs	Type of log to be collected	
	Name in OS	Classification in ISM
Windows	Event Log (system log or application log)	Operating system log (Event Log)
	Event Log (security log)	Operating system log (Security Log)
Linux	System log (/var/log/messages)	Operating system log (Event Log)
	System log (/var/log/secure)	Operating system log (Security Log)
VMware ESXi	System log (syslog.log)	Operating system log (Event Log)
IPCOM OS	System log (/var/log/messages)	Operating system log (Event Log)
	System log (/var/log/secure)	Operating system log (Security Log)

OS for which to retrieve logs	Type of log to be collected	
	Name in OS	Classification in ISM
	Technical support information	-

### Note

Logs for OSES running on virtual machines are exempt from retrieval.

## ServerView Suite logs

Log Management retrieves logs for the software (ServerView Suite products) that is running on the managed servers.

Software for which to retrieve logs	Type of Node Log to be collected
ServerView Agents	Exported results for "PrimeCollect" command
ServerView Agentless Service	Exported results for "PrimeCollect" command
ServerView RAID Manager	Operation Logs (RAIDLog.xml and snapshot.xml)

### Note

- Logs for ServerView Suite products running on virtual machines are exempt from retrieval.
- ServerView Suite logs are exempt from Node Log creation.

## 2.5.2 Setting Log Retention Periods



You can set the log retention periods separately for logs classified into "Event Logs," "Operation Logs," and "Security Logs." Also, you can set different numbers of retained generations for unclassified "Archived Logs."

You can freely set arbitrary values for the log retention periods as required.

Each of the retention periods for logs classified into "Event Logs," "Operation Logs," and "Security Logs" are specified by the number of days. Logs with a time stamp older than the specified number of days are deleted. With the default settings, logs are retained for the past 30 days. The available setting range is 1 - 1830 days (approx. 5 years).

For "Archived Logs" you have to set the number of generations of past log collections to be retained, counting each collection as "1" regardless of whether it was automatic (scheduled) or manual (any time). "Archived Logs" that are older than the specified number of generations are deleted. With the default settings, logs are retained for the past 7 generations. The available setting range is 1 - 366 generations.

### Point

- The retention periods and the numbers of retained generations for logs classified into "Event Logs," "Operation Logs," "Security Logs," and "Archived Logs" have no effect on each other.

For example, if the retention period for "Event Logs," "Operation Logs," and "Security Logs" is set to 30 days for each and the logs for the past one year have accumulated on the respective node, executing a log collection will result in the "Archived Log" retaining all records for that year. In contrast, the "Event Log," "Operation Log," and "Security Log" do not store any logs that are older than 30 days.

- Be sure to confirm that the retention periods are set to optimum values for operation before you execute a log collection for the first time.

By default, the retention periods for "Event Logs," "Operation Logs," and "Security Logs" are each set to 30 days.

When you retrieve an "Archived Log" from a node in your first log collection, any logs that are older than 30 days are deleted without accumulating them as "Event Logs," "Operation Logs," and "Security Logs."

Even if you modify the retention period to be longer than 30 days before the second and subsequent log collections, Node Logs older than 30 days are not accumulated.

If you want to accumulate logs from before the past 30 days, modify the settings for the log retention periods to any value larger than "30 days" before you execute a log collection for the first time.

---

## 2.5.3 Setting Log Collection Targets, Dates and Times

---



Logs cannot be appropriately collected from a node by merely registering a node in ISM.

When you execute log collections from nodes, you have to set the following contents on each node in advance.

- Log Collection Target

As log types to be collected, you can specify any combination out of "Hardware Log," "Operating System Log," and "ServerView Suite Log."

For log collection target nodes other than servers, you can only specify "Hardware Log."

If you select none at all, log collection will not be executed.

- Retention Period (required for all items)

Event Log: Set the maximum number of days for log retention.

Operation Log: Set the maximum number of days for log retention.

Security Log: Set the maximum number of days for log retention.

Archived Log: Set the maximum number of generations for log retention.

For collecting logs from nodes, the following 2 execution procedures can be used:

- Manual execution at any suitable time
- Automatic execution according to a schedule

To execute log retrievals periodically and automatically according to a schedule, you have to set an execution schedule separately for each node.



After retrieving and confirming information from the nodes, ISM judges whether these nodes are enabled targets for collecting the three types of log: "Hardware Log," "Operating System Log," and "ServerView Suite Log."

If the Log Collection Target settings do not allow for executing "Hardware Log," "Operating System Log," and "ServerView Suite Log" settings, which should originally be available, information retrieval from that node may not have completed normally.

- If the settings for "Hardware Log" cannot be executed, confirm the network connections between management servers and nodes and the node property settings (especially network-related items) again, and then execute [Get Node Information] again.
- If the settings for "Operating System Log" and "ServerView Suite Log" cannot be executed, confirm again that the contents of node OS information are correctly registered, and then execute [Get Node Information] again.
- Settings for "ServerView Suite Log" are available only if the OS permits installation of ServerView Suite products (ServerView Agents, ServerView Agentless Service, and ServerView RAID Manager) that support log collection.

To have log collections executed periodically, you have to set a schedule.

With a schedule set separately for each node, you can collect specific types of logs at specific times and store them in a designated area in ISM-VA.

There are two types of specifying the collection schedule as follows.

- Specify by Day of the Week

Here, you can specify the time of log retrieval separately for each day of the week. Specify the day of the week and the time of log retrieval in the format "Every x-day at hh:mm." Alternatively, you can also specify in the format "Every n-th x-day of the month at hh:mm."

Example 1: Log retrieval every Sunday at 23:00

Example 2: Log retrieval every first Monday of a month at 12:10

Example 3: Log retrieval every Wednesday at 11:00, and every Friday at 18:00

- Specify by Date

Here, you can specify the time of log retrieval separately for a specific day or the last day of every month.

Example 1: Log retrieval on every 10th at 11:00, and on every 20th at 18:00

Example 2: Log retrieval on the last day of every month at 23:50

The following is a sample setting operation using the GUI.

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 for which to execute the settings. By selecting the checkboxes for multiple nodes, you can set the same contents to the multiple nodes.
4. From the [Actions] button, select [Edit Log Collection Settings].

### Point

The operations to edit the log collection settings can be executed using the same operations for the screens described in the following procedure.

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes].
2. Execute one 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 select the [Log Collection Settings] tab.

### Note

Set the time set in the [Edit Log Collection Settings] schedule in the time zone of the ISM-VA.

If you set the time of the time zone of the ISM GUI, regular log collection may not be executed at the expected schedule time.

After setting the schedule, confirm that the expected schedule time has been set in [Next Execution Date].

For the time zone of ISM-VA, check with your ISM administrator.

## 2.5.4 Operations for Log Collection



## Periodical log collection

Periodical log collection collects and accumulates Node Logs periodically, according to a specified schedule.

To have log collections executed periodically, you have to set a log collection schedule.

Logs are collected automatically at the times that you set in the schedule.

### Note

- With periodical log collection, if a node is in a status that does not allow for log collection at the scheduled starting time, that collection is skipped and executed at the next scheduled date and time.

Examples for statuses that do not allow for log collection are as follows:

- Log collection from the node cannot be normally executed (power is off, no network communication available etc.)
- A different operation has been executed with ISM for the node
- The node is in Maintenance Mode (manual retrieval is possible)
- ISM is stopped

Whenever log collection fails, this is recorded as an error event (logs starting with message ID "5014") under [Events] - [Events] - [Operation Log] in ISM.

- Depending on the type of node, log collection may take some time to complete. This may cause large differences between the scheduled times for log collection and the time stamps of retained logs.
- After starting periodical log collection, you cannot cancel it in the middle of the process. Therefore, if maintenance such as firmware update, profile assignment and etc. to target nodes is planning and it overlaps the periodical log collection execution time, Maintenance can be failed. It is recommended to either disable the periodical log collection or change the setting of schedule.
- There is an upper limit for the number of nodes from which logs can be collected simultaneously. If the maximum number of log collections is in progress, any log collection you start after that will not be executed immediately but only after the preceding log collections have finished.
- 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.

## Manual log collection

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

For details on how to operate it, refer to "5.3 Collect Logs of Managed Nodes" in "Operating Procedures."

## Monitoring for disk capacities of log storage locations

Log files are stored in the log storage area of the user group to which the node belongs.

This function serves to monitor the capacities of the log storage areas in the user groups.

The upper limit for the total size (for example, Size restriction) of various log files (for example, Archived Log, Node Log (for download data), and Node Log (for log search data)) stored in ISM and the specified value for monitoring the disk capacity (Threshold monitoring) are set in Edit User Group Settings. For details of User Group Settings, refer to "2.7.2 Manage User Groups" in "Operating Procedures."

If the total size of each of the various log files approaches this capacity setting value its specified value, this is recorded as a warning event under [Events] - [Events] - [Operation Log] tab in the Global Navigation Menu. When the preset value is exceeded (when an error event was registered), new logs are no longer stored.

To allow for retrieving new logs after an error event was registered, you can either manually delete any obsolete logs for the node on which the event occurred or another node belonging to the same user group, or wait until the free area increases due to automatic deletion of logs for which the storage period has expired.

Condition	Behavior
<p>The total size of log files exceeds the size of the specified value for monitoring the disk capacity:</p> <p>Example:</p> <p>When the specified upper limit value is 10 GB and the specified value for monitoring the disk capacity is 80%, if the total size of the log files exceeds 8 GB, the operation described on the right is executed.</p>	<ul style="list-style-type: none"> <li>- Log collection is executed.</li> <li>- A warning event is exported under [Events] - [Operation Log].</li> </ul> <p>The contents of the displayed messages are as follows.</p> <ul style="list-style-type: none"> <li>- For Archived Logs: <ul style="list-style-type: none"> <li>During log collection for node (&lt;node name&gt;) Archived Log for the user group (&lt;User group name&gt;) became (xxMB) and exceeded the capacity (xxMB) threshold (xx%) set for log retention.</li> <li>Refer to "<a href="#">2.5.9 Deleting Archived Logs.</a>"</li> </ul> </li> <li>- For Node Logs (data for download): <ul style="list-style-type: none"> <li>During log collection for node (&lt;node name&gt;) the Node Log (download data) for the user group (&lt;User group name&gt;) became (xxMB) and exceeded the capacity (xxMB) threshold (xx%) set for log retention.</li> <li>Refer to "<a href="#">2.5.8 Deleting Node Logs.</a>"</li> </ul> </li> <li>- For Node Logs (data for log searches): <ul style="list-style-type: none"> <li>During log collection for node (&lt;node name&gt;) the Node Log (data for log search) became (xxMB) and exceeded the capacity (xxMB) threshold (xx%) set for log retention.</li> <li>Refer to "<a href="#">2.5.8 Deleting Node Logs.</a>"</li> </ul> </li> </ul>
<p>The total size of log files exceeds the upper limit specified value:</p> <p>Example:</p> <p>When the specified upper limit value is 10 GB the operation described on the right is executed.</p>	<ul style="list-style-type: none"> <li>- Log collection is not executed.</li> <li>- An error event is exported under [Events] - [Operation Log].</li> </ul> <p>The contents of the displayed messages are as follows.</p> <ul style="list-style-type: none"> <li>- For Archived Logs: <ul style="list-style-type: none"> <li>During log collection for node (&lt;node name&gt;) Archived Log for the user group (User group name&gt;) exceeded the capacity (xxMB) set for log retention.</li> <li>Refer to "<a href="#">2.5.9 Deleting Archived Logs.</a>"</li> </ul> </li> <li>- For Node Logs (data for download): <ul style="list-style-type: none"> <li>During log collection for node (&lt;node name&gt;) the Node Log (download data) for the user group (&lt;User group name&gt;) exceeded the capacity (xxMB) set for log retention.</li> <li>Refer to "<a href="#">2.5.8 Deleting Node Logs.</a>"</li> </ul> </li> <li>- For Node Logs (data for log searches): <ul style="list-style-type: none"> <li>During log collection for node (&lt;node name&gt;) the Node Log (log discovery data) exceeded the capacity (xxMB) set for log retention.</li> <li>Refer to "<a href="#">2.5.8 Deleting Node Logs.</a>"</li> </ul> </li> </ul>

## 2.5.5 Searching Node Logs



You can search the "Node Logs" you accumulated for logs that contain specific keywords and then display these logs.

The first display after opening the "Node Logs" screen shows a list of "Node Logs" in blocks for each node where they were accumulated.

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

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Log Collection].
2. From the [Log Collection] menu, select [Node Log Search].
3. Enter a keyword into the search text box on the GUI.

The logs that contain the keyword you entered are displayed.

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

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Log Collection].
2. From the [Log Collection] menu, select [Node Log Search].
3. Select the [Filter] button.
4. Enter the parameters on the "Filter" screen, and select the [Filter] button.

The logs that match the condition you entered are displayed.

### Point

As a simple function for downloading logs, you can export the contents currently display on the GUI screen to a CSV file. You can export data in CSV format by selecting the [Actions] button and selecting [Export in CSV Format].

## 2.5.6 Downloading Node Logs

---



You can download accumulated Node Logs by specified periods and types. The period is set to the date of the time zone of the ISM-VA.

You can also download logs of multiple nodes collectively.

The downloaded files are compressed into a single zip file.

Moreover, you can also set a password for such a zip file.

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

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Log Collection].
2. From the [Log Collection] menu, select the [Log Management] - [Node Log] tab.
3. Select the checkboxes for the target nodes.
4. From the [Actions] button, select [Create Download Files], and follow the instructions on the screen to create a download file.

The "Result" screen is displayed. Take a memo of the detailed task number that is displayed on this screen.

5. Wait until creation of the download files finishes.

The creation status can be checked in the download file item at the top of the screen.

From the top of the Global Navigation Menu, select [Tasks] and check the processing status.

Under Task Type, [Creating Node Log download file] is displayed.

For the Task ID, confirm the detailed task number of which you took a memo on the "Result" screen.

6. After the creation of the download file has been completed, select the [Download] button.



## Point

- The node download procedure can be executed using the same operations as for the screens displayed in the following procedure.
  1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes].
  2. Execute one 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 select the [Log Collection Settings] tab.
- The download files can be packaged as one zip file even when selecting multiple nodes.

## Note

- For the date of the period specified in the creation of the download file for the Node Log, specify the date of the ISM-VA time zone. If you specified the date of the time zone of the ISM GUI, the Node Log from the expected date may not be downloaded. For the time zone of ISM-VA, check with your ISM administrator.
- ISM can retain only one download file at a time. Therefore, if you execute multiple download operations for logs successively, the previously created download files are deleted.
- You cannot create a download file for the node that is executing log collection. Create a download file after the log collection is completed.

The downloaded logs are saved with the following file name.

- Name of download file

```
NodeLog_<specified download period>.zip
```

The format of <Specified download period> is <Specified Start Date>-<Specified End Date>, with each date displayed as "YYYYMMDD" (year, month, and day).

Example: If you specified the period from November 1, 2017 through November 7, 2017

```
NodeLog_20171101-20171107.zip
```

The folder structure after decompressing the zip file is as follows.

- Folder structure

```
<node name>_<node ID>\<category>\<log type>
```

The format of <category> is "hardware/os."

The format of <log type> is "event/operation/security."

## 2.5.7 Downloading Archived Logs



Archived Logs can be downloaded. You can also download logs of multiple generations from the same node or logs of multiple nodes collectively. The downloaded files are compressed into a single zip file. Moreover, you can also set a password for such a zip file.

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

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Log Collection].
2. From the [Log Collection] menu, select the [Log Management] - [Archived Log] tab.

3. Select the checkboxes for the Archived Logs to be downloaded.
4. From the [Actions] button, select [Create Download Files], and follow the instructions on the screen to create a download file.  
The "Result" screen is displayed. Take a memo of the detailed task number that is displayed on this screen.  
Download can also be executed from the screen displayed if you select [Show Archived Log Files] from the [Actions] menu. In this case, check the files to be downloaded.
5. Wait until creation of the download files finishes.  
The creation status can be checked in the download file item at the top of the screen.  
From the top of the Global Navigation Menu, select [Tasks] and check the processing status.  
Under Task Type, [Creating Archive Log download file] is displayed.  
For the Task ID, confirm the detailed task number of which you took a memo on the "Result" screen.
6. After the creation of the download file has been completed, select the [Download] button.

### Point

- The download of Archived Log can be executed using the same operations as for the screens displayed in the following procedure.
  1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes].
  2. Execute one 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 select the [Log Collection Settings] tab.
- Download files can be packaged into a single zip file even if multiple nodes are selected or if multiple Archived Logs are selected.

### Note

- ISM can retain only one download file at a time. Therefore, if you execute multiple download operations for logs successively, the previously created download files are deleted.
- You cannot create a download file for the node that is executing log collection. Create a download file after the log collection is completed.

The downloaded logs are saved with the following file name.

- Name of download file

```
ArchivedLog_<date when download file was created>.zip
```

The folder structure after decompressing the zip file is as follows.

- Folder structure

```
<node name>_<node ID>\<date and time>_<node name>_<node ID>\<category>
```

<Date and time> is displayed in the format "YYYYMMDDhhmmss" (year, month, day, hours, minutes, and seconds).

The format of <Category> is "hardware/software."

## 2.5.8 Deleting Node Logs



Node Logs (data for download and data for log search) for which the retention period you set has expired are deleted automatically, but you can also individually delete any Node Logs manually. In that case, use the node name, the retention period or the log type as filtering conditions, and then use the search results to delete the relevant log.

Data for download and data for log search are deleted simultaneously if these data are for the same target.

The following is a sample operation using the GUI for deleting Node Logs.

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Log Collection].
2. From the [Log Collection] menu, select the [Log Management] - [Node Log] tab.
3. Select the checkboxes for the target nodes.  
Multiple nodes can be selected.
4. From the [Actions] button, select [Delete Node Log Files] to execute log deletion according to the instructions on the screen.  
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, [Deleting Log files] is displayed.  
For the Task ID, confirm the detailed task number of which you took a memo on the "Result" screen.

### Note

- Deleting Node Logs may take some time to complete. Therefore, the information of a Node Log that you set to be deleted may be displayed on the GUI until deletion processing for Node Logs is completed. In such a case, under the corresponding task on the "Tasks" screen, confirm that processing for Node Log deletion is completed, and then open this screen again.
- If you are deleting a large number of Node Logs, deletion may take several minutes or even hours. However, if it is OK to delete all logs for a selected node, you can select all log types under [Type] in the conditions for deletion and specify the current date of the day of deletion under [Period] in order to complete the deletion in a short time.
- For log deletion executed for nodes where Node Logs are currently being collected, it will be suspended until log collection has been completed, then after log collection has been completed it will be executed.

## 2.5.9 Deleting Archived Logs

---



Archived Logs for which the retention count you set is exceeded are deleted automatically, but you can also manually delete accumulated Archived Logs individually by specifying any Archived Log and its retention generation.

The following is a sample operation using the GUI for deleting Archived Logs.

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Log Collection].
2. From the [Log Collection] menu, select the [Log Management] - [Archived Log] tab.
3. Select the checkboxes for the target nodes.  
Multiple nodes can be selected.
4. From the [Actions] button, select [Delete Archived Log Files] to execute deletion according to the instructions on the screen.  
The "Result" screen is displayed. Take a memo of the detailed task number that is displayed on this screen.  
Deletion can also be executed from the screen displayed if you select [Actions] button and select [Show Archived Log Files].  
In this case, select the checkboxes for the files to be deleted. By selecting the checkboxes for multiple files, you can delete them together.

5. From the top of the Global Navigation Menu, select [Tasks], and check the processing status.

Under Task Type, [Deleting Log files] is displayed.

For the Task ID, confirm the detailed task number of which you took a memo on the "Result" screen.

### Note

- Deleting Archived Logs may take some time to complete. Therefore, the information of an Archived Log that you set to be deleted may be displayed on the GUI until deletion processing for Node Logs is completed. In such a case, confirm under the corresponding task on the "Tasks" screen that processing for Archived Log deletion is completed, and then open this screen again.
- For log deletion executed for nodes where logs are currently being collected, it will be suspended until log collection has been completed, then after log collection has been completed it will be executed.

## 2.6 Firmware Management

---

Firmware Management is a function that is mainly used for the following purposes:

- Displaying the firmware versions that are currently running on managed nodes on the GUI of ISM
- Updating the firmware on managed nodes
- Confirming the documentation that is supplied with the firmware data

Firmware Management is available for the following nodes:

- Servers and any mounted PCI cards
- Storage devices
- Switches

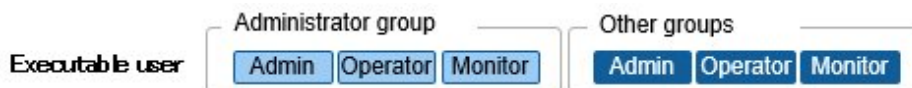
For details on the target nodes, contact your local Fujitsu customer service partner.

Here, the following points are described:

- [2.6.1 Confirmation of Firmware Versions of Nodes](#)
- [2.6.2 Firmware Updates](#)
- [2.6.3 Confirmation of Documentation that is supplied with Firmware Data](#)
- [2.6.4 Job Management](#)
- [2.6.5 Firmware Baseline](#)

### 2.6.1 Confirmation of Firmware Versions of Nodes

---



The following is a sample operation using the GUI.

1. Retrieve the current node information from the applicable node.

For details on retrieving detailed node information, refer to "[2.2.1.3 Management of node information.](#)"

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

3. In the [Column Display] field, select [Firmware].

4. Confirm the [Current Version] field.

The [Current Version] field displays the currently running firmware version.

## 2.6.2 Firmware Updates

Here, the following points are described:

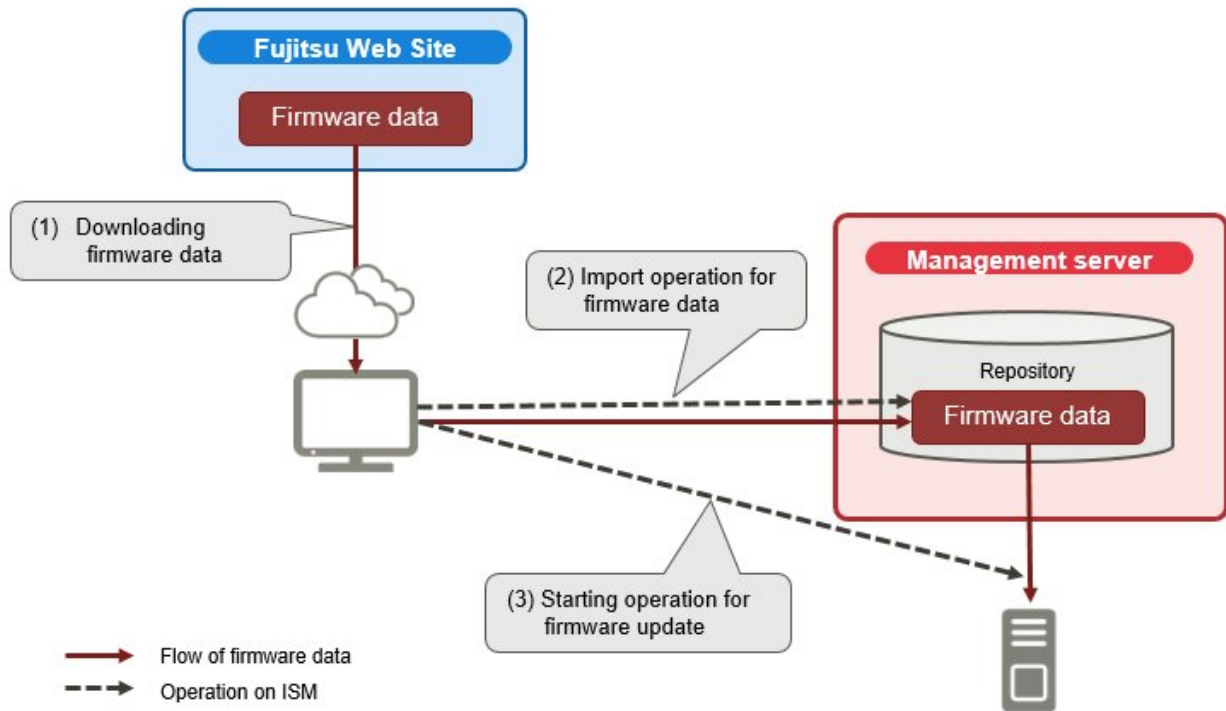
- [2.6.2.1 How to update firmware](#)
- [2.6.2.2 Behavior during updates](#)
- [2.6.2.3 Execution of firmware updates](#)

For updating the firmware, you have to import the firmware data into ISM in advance.

Download the firmware data from FUJITSU or another website ((1) in the diagram below), and transfer these data to the repository on ISM-VA ((2) in the diagram below). ISM uses the firmware data that is deployed in the repository to update the target nodes ((3) in the diagram below).

For details on operations to transfer firmware data to the repository, refer to "[2.13.2 Repository Management](#)."

Figure 2.10 Image of Firmware Management



### 2.6.2.1 How to update firmware

When using Update Firmware, two kinds of firmware update, "Online Update" and "Offline Update," can be used.

#### Online Update

Update procedure for when the power of the target device is turned on. When the target of firmware update is a server (BIOS/iRMC), online update can be executed even if the power is turned off.

This procedure can be used when the target of firmware update is a server (BIOS/iRMC/with PCI card mounted), switches, storage or PRIMERGY BX Chassis (MMB).

#### Offline Update

Update procedure for when the power of the target device is turned off.

This procedure can be used when the target of firmware update is a server (BIOS/iRMC/with PCI card mounted).

When executing Offline Update, switch off the power of the server in advance.

#### Required preparations before using Offline Update

- The ServerView Suite DVD and the ServerView Suite Update DVD require to be copied to the repository area on ISM-VA in advance. This task is called "import."

If you are going to import an ISO image of the ServerView Suite Update DVD, extend the size of the LVM volume for the user group.

If you are going to import an ISO image of the ServerView Suite DVD, extend the size of the LVM volume for the system. Once you imported the ServerView Suite DVD into ISM, there is no required to import it again. (It is not required to import it separately for each user group.)

For details, refer to "[2.13.2 Repository Management](#)."

- Use the PXE boot function on the target node.

The management LAN used for PXE boot can be set from the [Firmware] tab in the Details of Node screen. Moreover, you can execute the setting on the "Node List" screen displayed when selecting target nodes on the "Firmware" screen. If it is not set, the first port of the on board LAN will be used.

Complete the network connections and the BIOS settings of the target server in advance, so as to enable PXE booting from the management LAN. Moreover, a separate DHCP server is required within the network. Set the DHCP server so as to allow the target nodes to lease appropriate IPv4 addresses during the PXE boot.

For details, refer to "[A.1.1 DHCP/PXE Settings in Using Profile Management/Firmware Management](#)."



#### Note

The required firmware data may differ between "Online Update" and "Offline Update." Also, the support scope varies depending on the PCI card mounted. For details, contact your local Fujitsu customer service partner.

## 2.6.2.2 Behavior during updates

Depending on the type of target node on which the firmware is updated, the behavior during and after the update differs.

Execute any updates according to the tables shown below.

Table 2.2 Online Update

Type	Behavior during and after updates
Server (iRMC)	Updates can be executed regardless of whether the server power is on or off.
Server (BIOS)	<p>Updates can be executed regardless of whether the server power is on or off.</p> <ul style="list-style-type: none"> <li>- If you execute an update with the power remaining on           <p>You must reboot the server and turn the power on again in order to switch to the new firmware (BIOS). You can execute the reboot whenever suits you best. The firmware is automatically applied when you reboot, and then the power of the server turns off.</p> <p>After the power has turned off, you can switch to the new firmware by turning the power on the Details of Node screen in ISM and so on.</p> <p>After that, check the following.</p> <ul style="list-style-type: none"> <li>- The BIOS version of the server is updated</li> <li>- In the iRMC system event log, no errors have occurred during the update</li> </ul> </li> <li>- If you execute an update with the power turned off           <p>You must turn the server power on again in order to switch to the new firmware (BIOS). As soon as the firmware update completes, the server power switches on automatically, and then switches off.</p> </li> </ul>

Type	Behavior during and after updates
	<p>After the power has turned off, you can switch to the new firmware by turning the power on the Details of Node screen in ISM and so on.</p> <p>After that, check the following.</p> <ul style="list-style-type: none"> <li>- The BIOS version of the server is updated</li> <li>- In the iRMC system event log, no errors have occurred during the update</li> </ul>
Server (Firmware of the server)	Updates can be executed when the server power is on.
Server (with mounted PCI card)	Updates can be executed on the server if a supported OS is running. The new firmware will run only after a reboot. You can execute the reboot whenever suits you best.
Switch (except CFX, PY CB Eth Switch 10/40Gb 18/8+2) Storage	Execute the firmware update with the node power remaining on. After the firmware update, the node may be rebooted.
Switch (CFX, PY CB Eth Switch 10/40Gb 18/8+2)	Execute the firmware update with the node power remaining on. You must reboot the node in order to switch to the new firmware. You can execute the reboot whenever suits you best. Depending on the system configuration, the connection may be broken when rebooting. Take your system configuration into account when rebooting.
PRIMERGY BX Chassis MMB	Execute the firmware update with the node power remaining on. After the firmware update, you may have to reboot the node.

Table 2.3 Offline Update

Type	Behavior during and after updates
Server (iRMC)	Updates can be executed with the server power off.
Server (BIOS)	<p>During firmware update the server is powered on or restarted, the power is turned off after the firmware update has been completed. If you select "Turn on the nodes after updating firmware" on the Update Settings screen, the power will be turned on after the completion of the updates.</p> <p>After the firmware update has been completed, it will automatically be switched over to the new firmware.</p>
Server (with mounted PCI card)	

### 2.6.2.3 Execution of firmware updates



#### Note

- While an update is in progress, observe the following notes.
    - Do not turn the target node on or off.
    - Do not reboot nor reset the target node.
    - Do not interrupt the network connection between ISM and the target node.
    - Do not reboot the management server. Do not power off the management server.
    - Do not delete any import data or firmware data from the repository.
  - Before you start any firmware update, confirm the precautions in the documentation that is supplied with the firmware data.
  - Firmware data that can be applied on target nodes must be saved in advance, before any update operation.
- For details on how to save the firmware data, refer to "[2.13.2 Repository Management](#)."

- As network switches other than CFX are reset after updating them, data communication is temporarily interrupted. If you are using a redundant network, you should update the sections in the redundancy configuration one after another.
- For a VDX switch, you cannot execute firmware updates specifying VCS Fabric (Brocade VCS Fabric). Execute firmware update to each VDX fabric switch under it.
- When you execute a firmware update on ETERNUS DX/AF, account information with a Maintainer role must already be registered in ISM.
- When you execute a firmware update of a PCI card, the OS information of the server on which the PCI card is mounted must already be registered in ISM.

For information on registration of the OS information of the node, refer to "[2.2.1.5 Registration of node OS information](#)". Also note that firmware updates of PCI cards are supported only for the following OS types:

- Red Hat Enterprise Linux
  - SUSE Linux Enterprise Server
- Firmware updates for PCI cards mounted on servers are executed for all mounted cards of the same type.

If there are multiple cards of the same type, you cannot specify different firmware versions for each card or update only some of the cards. Even if you specify only some cards to be updated, or if you specify different firmware versions for different cards on the ISM screen, the firmware update is executed for all cards of the same type, so all these cards are updated to the same latest firmware version.

- For executing a firmware update for PCI cards (FC/CNA/LAN cards) on Linux, the Qlogic QConvergeConsole CLI must be installed on the OS of the servers on which these PCI cards are mounted.

For details on the installation of Emulex OneCommand Manager CLI or QlogicQConvergeConsole CLI, refer to "[2.13.3 Installation of Emulex OneCommand Manager CLI and Qlogic QConvergeConsole CLI](#)".

- For certain nodes and PCI cards, the format of the version number in the current version column and latest version column may be different.

For applicable nodes and PCI cards, and for how they are displayed, contact your local Fujitsu customer service partner.

- Cisco switch (Catalyst, Nexus) does not compare the current version and the latest version.

If the values of the current version and the latest version are different, it becomes the update target.

- For certain nodes, you must execute firmware update in stages. Refer to the document attached to each firmware update.
- After using Online Update to update the server BIOS and the PCI card mounted on a server, the old firmware will continue to run even after update processing has finished in ISM. In order to switch operation to the new firmware, execute the following procedure.
  - If you update the PCI card mounted on a server, you must reboot the server in order to switch to the new firmware. You can execute the reboot whenever suits you best.
  - If you execute an update of the server BIOS with the power remaining on, you must reboot the server and turn the power on again in order to switch to the new firmware (BIOS). You can execute the reboot whenever suits you best. The firmware is automatically applied when you reboot, and then the power of the server turns off. After the power has turned off, you can switch to the new firmware by turning the power on the Details of Node screen in ISM and so on.
  - If you execute an update of the server BIOS with the power turned off, you must turn the server power on again in order to switch to the new firmware (BIOS). As soon as the firmware update completes, the server power switches on automatically, and then switches off. After the power has turned off, you can switch to the new firmware by turning the power on the Details of Node screen in ISM and so on.

- If processing for the firmware update cannot start normally, or if an update fails, ISM's update processing usually ends with an error. In some cases, however, such as when a target node stops to respond while an update is in progress, timeout errors are not discovered.

If processing does not finish for much longer than the presumed time for the task, confirm the status of the target node directly. If there is any error, cancel the firmware update task in ISM.

For information on approximate processing times for firmware updates, refer to the information published on the web.

- There is an upper limit for the number of nodes that firmware update can be executed simultaneously. This upper limit is 50 for the entire ISM-VA. If firmware update is executed on a specified number of nodes exceeding the upper limit, the firmware update is first executed



on the set maximum number of nodes, and after the preceding firmware update is completed, the update will be executed on the remaining nodes.

If firmware update is executed while the maximum number of firmware updates is already running, it will be executed after the first firmware updates have been finished.



1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Firmware].
2. Set the Maintenance Mode to a node to be updated.
3. Confirm the "Current Version" and the "Latest Version" on the node on which you are going to execute the update.
4. Select the checkbox for the node to be updated, then select the [Actions] button - [Update Firmware].
5. Execute the operations according to the instructions on the screen.

- If specifying a date and time for firmware updates

Select [Update firmware at the specified time] and specify the date and time for execution. Check the operation status on the "Jobs" screen since it is registered as an ISM job. The job ID is displayed in the "List of Jobs" field in the result confirmation dialog box displayed after execution. When selecting [Structuring] - [Jobs] on the GUI of ISM, a list of jobs is displayed. Identify the job based on its job ID.

- If you selected [Update firmware immediately] and executed.

Since, after starting the update, the task is registered as a "Task" in ISM, confirm its current status on the "Tasks" screen. After executing, the "Task Details" field in the dialog box for confirmation of the result displays the task ID.

The following tasks types are registered under Firmware Update tasks.

- Online Update: Updating firmware
- Offline Update: Updating firmware (Offline mode)

When selecting [Tasks] from the top of the Global Navigation Menu on the GUI of ISM, the Task List is displayed. Identify the applicable task by its task ID and task type.

6. After confirming that the relevant task has completed, release the Maintenance Mode on the target node.

## Point



- The firmware update can be executed using the same operations also for the screens displayed in the following procedure.
  1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes].
  2. Execute one of the following.
    - From the [Column Display] field in the node list, select [Firmware].
    - From the node list, select the target [Node Name] and select the [Firmware] tab.
- If specifying a date and time for firmware updates, you must enable the Workflow service in advance. Refer to "[4.11 ISM-VA Service Control](#)" and execute "Enable internal service individually" and "Start of internal service individually."
- If you selected "Switch to the 'Maintenance Mode' when updating firmware." on the update settings screen, Maintenance Mode will be set just before the firmware update, and Maintenance Mode will be released just after the update has been completed. Use when you specify a date and time for firmware updates.



## **2.6.3 Confirmation of Documentation that is supplied with Firmware Data**

Use one of the following procedures to confirm the documentation that is supplied with the firmware.

## Point

- The update procedures in ISM are different from those described in the documentation that is supplied with the firmware data.
- The procedure of Online Update for iRMC/BIOS of servers differs from the "Online Update" of the documents attached to the firmware data and the processing corresponding to "Remote update" is executed. The firmware data is transferred from the FTP server in ISM-VA by using the iRMC Web interface of the target server.

### **If selecting the node registered in ISM to check the documentation**

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Firmware].
2. From the menu on the left side of the screen, select [Update].
3. Select the "Current Version" field or the "Latest Version" field of the node that you want to confirm the documentation of.  
The firmware document list screen is displayed.
4. In the [Document] field, select the document and confirm the documentation.

## Point

The operations can be executed using the same operations for the screens displayed in the following procedure.

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes].
2. From the node list, select the target [Node Name] and select the [Firmware] tab.  
The following procedure is the same as the above.

### **If selecting the imported firmware data to check the documentation**

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Firmware].
2. From the menu on the left side of the screen, select [Import], and then select [Firmware Data].
3. Select the "Version" field of the node that you want to confirm the documentation of.  
The firmware document list screen is displayed.
4. In the [Document] field, select the document and confirm the documentation.

### **If confirming the documentation during update of the firmware.**

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Firmware].
2. Select the checkbox for the node to be updated, then select the [Actions] button - [Update Firmware].
3. From the pull-down menu, select the update version and import data, and then select the [Next] button.
4. In the [Document] field, select the document and confirm the documentation.

## Point

The operations can be executed using the same operations for the screens displayed in the following procedure.

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes].
2. Execute one of the following.
  - From the [Column Display] field in the node list, select [Firmware].
  - From the node list, select the target [Node Name] and select the [Firmware] tab.

3. From the [Actions] button, select [Update Firmware].

The following procedure is the same as the above.

---

## 2.6.4 Job Management

---

If Update Firmware is executed by specifying date and time, the process is managed as a job.

The status of each job is displayed on list in the "Job" screen, not in the operating screen.

If canceling the executing process, deleting the process before execution, or deleting the executed process, either case is operated in the "Jobs" screen.



The number of jobs has an upper limit. A total of 100 or more jobs cannot be registered in ISM-VA. Delete unnecessary jobs in order not to exceed the upper limit.

---

## 2.6.5 Firmware Baseline

---

Firmware Baseline is a function that compares the firmware versions between the managed node and the assigned firmware. This function displays whether the node is operating with the intended firmware version in comparison to the firmware version that is assigned by the user. This supports users to integrate the operation environment as intended.

Firmware Baseline definitions are the definitions of the firmware version that should be applied to the nodes. Firmware Baseline compares this definition to the firmware version of the managed nodes and determines if the firmware is compatible, incompatible, or non-comparable to the definition. You can select incompatible nodes and perform batch firmware updates to the defined version for multiple nodes.

### Status of Firmware Baseline

The comparison results between the components and component versions defined in the Firmware Baseline definition and the components and component versions of managed nodes are shown as follows.

#### Compatible

Firmware versions of all components match

#### Incompatible

Firmware versions of some components or all components do not match

#### Non-comparable (N/A)

One of the following statuses:

- Some or all of the components defined in the Firmware Baseline definition do not exist in the managed nodes
- The firmware version of some or all of the components of the managed nodes is missing

In this case, check the target component and the Firmware Baseline definition. If the firmware version of the target components cannot be retrieved, delete the definitions of the target components in the Firmware Baseline definition.

If there are "Incompatible" components and "Non-comparable" components in the node, the node status is displayed as "Incompatible."

For information on the devices (components) that can be managed with Firmware Baseline, contact your local Fujitsu customer service partner.

Here, the following points are described:

- [2.6.5.1 Creating Firmware Baseline definitions](#)
- [2.6.5.2 Assigning Firmware Baseline definitions](#)
- [2.6.5.3 Releasing Firmware Baseline definition assignments](#)

- [2.6.5.4 Firmware update using Firmware Baseline definitions](#)
- [2.6.5.5 Editing Firmware Baseline definitions](#)
- [2.6.5.6 Deleting Firmware Baseline definitions](#)

## 2.6.5.1 Creating Firmware Baseline definitions



To integrate the firmware versions applied to the managed nodes, create definitions of the firmware version for each model with Firmware Baseline.

There are two procedures to create a Firmware Baseline definition.

- Create a Firmware Baseline definition manually using the firmware managed in the repository
- Automatically created when importing firmware data from the ServerView Suite DVD

The following shows an example of using the firmware managed in the repository create a Firmware Baseline definition manually.

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Firmware].
2. From the menu on the left side of the screen, select [Baseline].
3. From the [Actions] button, select [Create].
4. Execute the operations according to the instructions on the screen.

### Point

- All firmware versions for the components defined in the Firmware Baseline definition are targets for comparison. If there are unnecessary definitions, the node will not become compatible. Correct the Firmware Baseline definitions as necessary.
- It is recommended that you use ServerView Suite Update DVD to create Firmware Baseline definitions. If you are managing firmware for models that are not included on the ServerView Suite Update DVD, create the Firmware Baseline definition manually, or edit it.
- If you create a Firmware Baseline definition manually, register the firmware in the repository in advance. For details, refer to "[2.13.2.1 Storing and deleting firmware data.](#)"

## 2.6.5.2 Assigning Firmware Baseline definitions



Assign the created Firmware Baseline definitions to the nodes. By selecting a Firmware Baseline definition and assigning it to the target node, you can compare the firmware versions of the target node and the version defined in the Firmware Baseline definition.

The following shows an example of Firmware Baseline definition assignment.

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Firmware].
2. From the menu on the left side of the screen, select [Baseline].
3. Select the target baseline from the Baseline List.
4. From the [Actions] button, select [Assign to Nodes].
5. Execute the operations according to the instructions on the screen.

## Note

- When using the ServerView Suite Update DVD to automatically create Firmware Baseline definition, select whether to assign Firmware Baseline definitions for managed nodes during import automatically. If a Firmware Baseline definition already has been assigned, this Firmware Baseline definition will be overwritten.
- When assigning Firmware Baseline definitions for nodes registered with Auto Discovery of Nodes, it fails to assign if the model name of the registered node is different from the model name defined in the Firmware Baseline. Change the model name of the node to the model name of the Firmware Baseline definition.

### 2.6.5.3 Releasing Firmware Baseline definition assignments



When you assign a Firmware Baseline definition to a node that has already been assigned a different Firmware Baseline definition, you must release the assignment first. Then you can assign a different Firmware Baseline definition to the node whose assignment has been released.

The following shows an example of the release of Firmware Baseline definition assignment.

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Firmware].
2. From the menu on the left side of the screen, select [Baseline].
3. Select the target baseline from the Baseline List.
4. From the [Actions] button, select [Release from Nodes].
5. Execute the operations according to the instructions on the screen.

### 2.6.5.4 Firmware update using Firmware Baseline definitions



For nodes that has been determined to be incompatible, use Firmware Baseline to update the firmware version to match the version defined in the Firmware Baseline definition.

The following shows an example of firmware update using the Firmware Baseline definition.

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Firmware].
2. From the menu on the left side of the screen, select [Baseline].
3. Select the target baseline from the Baseline List.
4. From the [Actions] button, select [Update Firmware].
5. Execute the operations according to the instructions on the screen.

### 2.6.5.5 Editing Firmware Baseline definitions



When adding or deleting models from the created Firmware Baseline definition, or changing the defined firmware version, edit the Firmware Baseline definition.

The following shows an example of editing Firmware Baseline definitions.

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Firmware].
2. From the menu on the left side of the screen, select [Baseline].
3. Select the target baseline from the Baseline List.
4. From the [Actions] button, select [Edit].
5. Execute the operations according to the instructions on the screen.

### Point

The Firmware Baseline definition can be changed also when it has been assigned to a target node. After the change has been applied, Firmware Baseline can compare the firmware versions.

## 2.6.5.6 Deleting Firmware Baseline definitions



The following shows an example of deleting Firmware Baseline definitions.

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Firmware].
2. From the menu on the left side of the screen, select [Baseline].
3. Select the target baseline from the Baseline List.
4. From the [Actions] button, select [Delete].
5. Execute the operations according to the instructions on the screen.

### Point

When deleting Firmware Baseline definitions, Firmware Baseline definition assignment is released at the same time.

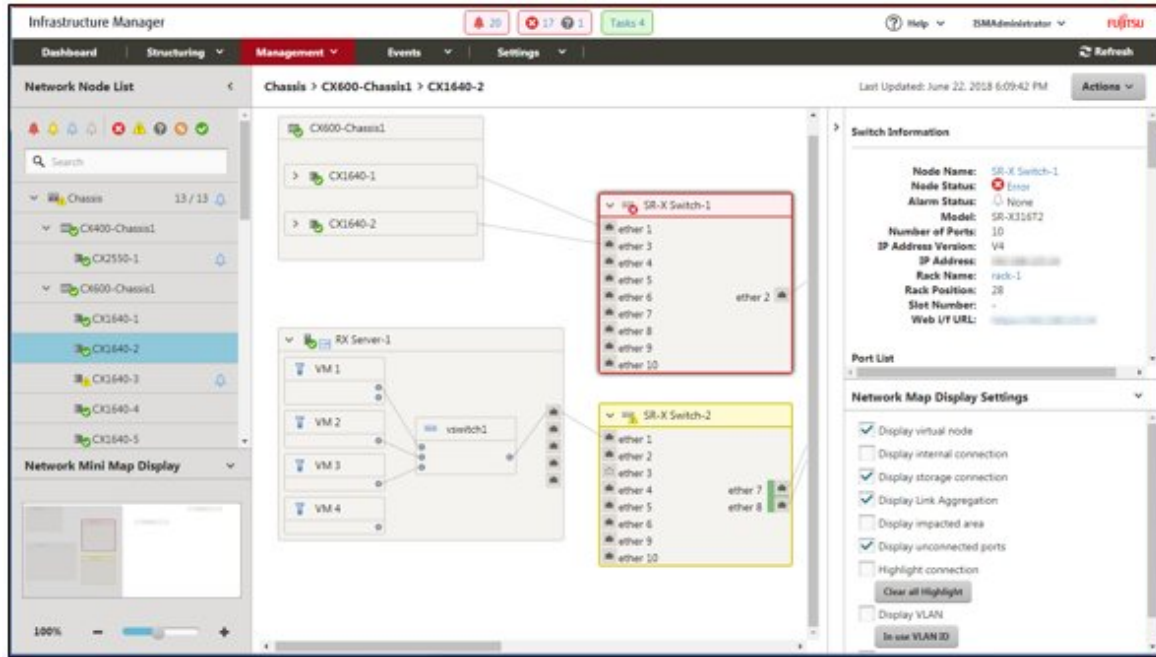
## 2.7 Network Management

---

Network Management is a function that is mainly used for the following purposes:

- Confirming information on physical network connections and port information between managed nodes on the Network Map
- Confirming the changes in the information on network connections between managed nodes
- Confirming the virtual connections on the Network Map between the physical ports of the managed nodes and the virtual machines, virtual switches, and virtual routers of the managed node
- Confirming the statistical information of the network of the managed node is possible in the Network Map
- Confirming the VLAN and Link Aggregation settings for network switches and changing these settings

Figure 2.11 Network Map



Here, the following points are described:

- 2.7.1 Display of Network Connection Information
- 2.7.2 Updates of Network Management Information
- 2.7.3 Confirmation of Information on Changes in Network Connections
- 2.7.4 Setting of Reference Information for Changes in Network Connections
- 2.7.5 Display of Network Statistics Information
- 2.7.6 Confirmation of VLAN and Link Aggregation Settings
- 2.7.7 Change of VLAN Settings
- 2.7.8 Change of Link Aggregation Settings
- 2.7.9 Manual Setting of Network Connection Information

## 2.7.1 Display of Network Connection Information



You can graphically confirm the connections on networks between managed nodes in the Network Map. Easy operations allow you to display detailed information for each managed node, including the current statuses of their ports. Also, you can confirm the connection relationships between servers, network switches, and storage on a single screen.

Also, you can also confirm the virtual connection relationships between the physical ports of the managed node and the virtual ports of the virtual components (virtual switches, virtual machines, and virtual routers) of the managed nodes.

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

A list of the nodes that are displayed on the Network Map is displayed as a tree structure in the Network Node List on the left side of the screen.

By selecting the [<] icon, you can hide away the Network Node List at the left edge of the screen.

- From the Network Node List, select the nodes that are the network connection points you want to confirm.

When opening the network map, the node at the top of the Network Node List is selected.

The Network Map is displayed at the center of the screen.

## Switch the Network Map display

The information displayed on the Network Map can be switched using the Network Map Display Settings panel.

Display Setting Name	Description
Display virtual node	Switch the display of virtual nodes (virtual machines, virtual switches, virtual routers, and CNA ports) displayed on the Network Map ON and OFF.
Display internal connection	Switch the display of internal connections (fabric internal switches, BX chassis internal connections) on the Network Map ON and OFF.
Display storage connection	Switch the display of the ports and connections used for the connection with the storage on the Network Map ON and OFF.
Display Link Aggregation	Switch the display of Link Aggregation settings on the Network Map ON and OFF.
Display impacted area	Switch the display the impacted area of an error on the Network Map ON and OFF. For connection with a node where an error or fault has occurred, the edge of the next node connected to as well as the port connected to are displayed in yellow. If virtual networks are constructed on the node connected to, the affected virtual networks will also be displayed in yellow.
Display unconnected ports	Switch the display of the link down port on the Network Map ON and OFF.
Highlight connection	Switch the display highlights function on the Network Map ON and OFF. If you select a managed node or its ports with the highlight connection function on, its connections are highlighted. If you select [Clear all Highlight], all the displayed highlights are cleared.
Display VLAN	Switch the display of the VLAN highlight display on the Network Map ON and OFF. The node or port that the VLAN ID entered in the text box is set for is highlighted in green. From the [In use VLAN ID] button you can display a list of and confirm the VLAN IDs set to the nodes displayed on the Network Map.
Display network statistics	Switch the display of the network statistics display on the Network Map ON and OFF. Detected ports or connections with a value exceeding the threshold value are displayed in orange (critical threshold value exceeded) or yellow (warning threshold value exceeded).  When changing the monitoring item to display, it can be selected from the list in the selection box displayed when you check this item.

### Point

The Network Map displays the nodes that have a connection relationship with the nodes you selected in the Network Node List. By selecting the node name of a node on the Network Map, the extended display of the ports within the node is displayed.

### Note

- LLDP (Link Layer Discovery Protocol) is used for retrieving information on physical network connections. If your nodes do not support LLDP or if LLDP is disabled, the information for actually existing connections cannot be retrieved. For information on whether a node supports LLDP and on how to confirm whether the LLDP settings of the node are enabled or disabled, confirm the technical specifications of each respective node.
- The displayed Network Map shows either the status retrieved when you last executed [Update network information] or the status at the point of the periodical update of network management information once a day with ISM. In order to confirm the most recent status after registering nodes, modifying any connections, or after an error, select the [Actions] button and execute [Update network information]. Also, whenever the hardware configuration of a node was changed, on the Details of Node screen for the respective node, execute [Get



Node Information] and then [Update network information]. The periodical update of network management information starts at 4:00 AM local time.

- To display the connection relationships between the virtual switches and the virtual machines, you must register the OS information of the cloud management software and of the managed target nodes to ISM. Regarding cloud management software registration, refer to "2.13.6 Management of Cloud Management Software," and regarding OS information registration, refer to "2.2.1 Registration of Datacenters/Floors/Racks/Nodes."
- For managed nodes, the display of the link status of the port, and of the connection relationship between ports with teaming (bonding) set up and virtual switches are supported.

---

## 2.7.2 Updates of Network Management Information

---



The network connection information is updated periodically to the latest information. You can also update it at any suitable time. The following operating procedure shows how to update the network management information.

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Network Map].
2. From the [Actions] button, select [Update network information].
3. Select the [Update Network Information] button.

### Note

You cannot retrieve network connection information or set this information for any node while a network management information update is in progress. Execute the operation again when processing for the information update is complete.

### Point

- Update the node information for each managed node before updating the network management information. For retrieving node information, refer to "2.2.1.3 Management of node information."
- Depending on the number of managed nodes, updating the network management information may take some time to complete.
  - To confirm that the information update is complete, confirm the event in the Operation Log under Tasks that indicates completion of the information update.
  - The latest update time of the network management information is displayed on the upper right part of the Network Map. The time displayed here is the time when the last information update processing was completed.
- A periodical update of the network management information is executed once a day at 4:00 AM local time.
- You can maintain updates of the latest network management information by executing the command after updating the information for each node.

---

## 2.7.3 Confirmation of Information on Changes in Network Connections

---



On the Network Map, you can confirm for any status changes in network connections that occurred after a set reference point in time. The available types of status change are "Added" and "Deleted."

- Added

"Added" is displayed for connections that were recently added and other newly discovered connections. "Added" connections are displayed as bold lines, on the Network Map.

- Deleted

"Deleted" is displayed for disconnections and previously discovered connections that were removed in the meantime. "Deleted" connections are displayed, as bold dashed lines, on the Network Map.

Using this function, you can easily grasp any changes in network connections, discover at an early stage when any positions in the network are disconnected and identify these positions.

You can also use the following operating procedure for confirming information on changes in network connections in list format.

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Network Map].  
A list of the nodes that are displayed on the Network Map is displayed as a tree structure in the Network Node List on the left side of the screen.
2. From the Network Node List, select the nodes that are the network connection points you want to confirm.  
When opening the network map, the node at the top of the Network Node List is selected.  
The Network Map is displayed at the center of the screen.
3. From the [Actions] button, select [Confirm connection status change].  
You can confirm "Added" and "Deleted" connection information separately.

### Point

The currently set "Reference Point" can be confirmed in the date and time in [Last Update] in the "Connection status change List" screen.

### Note

Selecting the [Refresh] button under the "Connection status change List" screen, updates the reference point and deletes the information on changes.

## 2.7.4 Setting of Reference Information for Changes in Network Connections



The displayed information on changes in network connections is based on the changes ("Added" and "Deleted") after a given reference point. You can modify the reference point. The reference point is set when the configuration of network connections is changed etc. As soon as you modify the reference point in time and refresh the display, it shows only the changes in the network connection information ("Added" and "Deleted") that were made after that point in time.

You can use the following operating procedure for modifying the reference point in time.

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Network Map].  
A list of the nodes that are displayed on the Network Map is displayed as a tree structure in the Network Node List on the left side of the screen.
2. From the Network Node List, select the nodes that are the network connection points you want to confirm.  
When opening the network map, the node at the top of the Network Node List is selected.  
The Network Map is displayed at the center of the screen.

- From the [Actions] button, select [Confirm connection status change]. The date and time of the latest refresh is the reference point in time that is currently set.
- Select the [Refresh] button.  
A confirmation screen is displayed.
- Confirm the contents and select the [Yes] button.  
The reference point is updated to the time when you executed the operation.

## 2.7.5 Display of Network Statistics Information



Each type of statistic information (traffic, and so on) for the port of the network switch can be checked visually on the Network Map.

- From the Global Navigation Menu on the GUI of ISM, select [Management] - [Network Map].  
A list of the nodes that are displayed on the Network Map is displayed as a tree structure in the Network Node List on the left side of the screen.
- From the Network Node List, select the nodes that are the network connection points you want to confirm.  
When opening the network map, the node at the top of the Network Node List is selected.  
The Network Map is displayed at the center of the screen.
- Check [Display network statistics] in the Network Map Display Settings panel and select the monitoring items of the network statistics information that you want to check.  
For each monitoring item of the network statistics information, the ports or connections that exceed the threshold value are displayed in orange (critical threshold value exceeded) or yellow (warning threshold value exceeded).

### Point

If you want to check each past type of statistic information (traffic, and so on), you can check the [Graph] of traffic information in "Port Information," which is displayed when selecting the port of the network switch.

## 2.7.6 Confirmation of VLAN and Link Aggregation Settings



You can visually confirm the current settings of VLANs and Link Aggregations on the Network Map.

- From the Global Navigation Menu on the GUI of ISM, select [Management] - [Network Map].  
A list of the nodes that are displayed on the Network Map is displayed as a tree structure in the Network Node List on the left side of the screen.
- From the Network Node List, select the nodes that are the network connection points you want to confirm.  
When opening the network map, the node at the top of the Network Node List is selected.  
The Network Map is displayed at the center of the screen.
- Execute the following procedure for the item you want to confirm.
  - VLAN  
Check [Display VLAN] on the Network Map Display Settings panel, then enter the VLAN ID you want to display in the VLAN ID text box.

The ports assigned to the VLAN ID as well as its connections are shown in green on the Network Map.

- Link Aggregation

Select the node name of a node on the Network Map.

The ports in the node are extended and displayed, and the Link Aggregation settings are displayed.

 **Point**

- Selecting [In use VLAN ID] on the Network Map Display Settings panel allows you to check the VLAN information that is already used.
- Use the [Display Link Aggregation] on the Network Map Display Settings panel to switch the display of the link aggregation settings on the Network Map ON and OFF.
- Depending on the network switch, other names than Link Aggregation (EtherChannel, etc.) may be used. Link Aggregation is used as the general term for this in ISM.

## 2.7.7 Change of VLAN Settings



You can change the VLAN settings of a network switch.

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Network Map].
2. From the Network Node List, select the node, serving as the point of the network connection that you want to set up.  
When opening the network map, the node at the top of the Network Node List is selected.  
The Network Map is displayed at the center of the screen.
3. From the [Actions] button, select [Set Multiple VLANs].
4. Check to select the respective ports for which you want to set the same VLAN ID, and select the [Setting] button on the top right side.
5. Enter the VLAN ID you set and edit the contents, and then select the [Confirm] button.
6. Confirm the changed contents of the setting, and then select the [Register] button.

The VLAN settings are changed.

 **Point**

VLAN settings can be changed also on a node basis. From the [Actions] button, select [Set VLAN].

 **Note**

- Depending on the VLAN settings contents, VLAN settings assignment may take some time to complete. Refresh the screen after you have completed VLAN settings. You can confirm the current progress of VLAN settings assignment on the "Tasks" screen. For details, refer to "[2.13.4 Task Management](#)."
- VLAN settings have their own specifications and therefore may differ depending on the models of network switches. Execute settings after confirming the device specifications.
- The number of VLAN IDs that can be set for a port is up to one hundred (100).
- There exists a reserved VLAN IDs depending on the models of network switches. You cannot change the settings of reserved VLAN ID. Check the specifications of respective nodes.

## 2.7.8 Change of Link Aggregation Settings

---



You can change the settings of Link Aggregation of a network switch.

The following is an example operation of adding link aggregation settings.

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Network Map].
2. From the Network Node List, select the node, serving as the point of the network connection that you want to set up.  
When opening the network map, the node at the top of the Network Node List is selected.  
The Network Map is displayed at the center of the screen.
3. From [Actions] button, select [Set Link Aggregation].
4. Select the name of the target node for which you set up a Link Aggregation and select the [Add] button of Link Aggregation Setting.
5. Enter the LAG Name and Mode, confirm the port for which you set the Link Aggregation, and then select the [Confirm] button.
6. Confirm the setting contents of the Link Aggregation and select the [Register] button.

### Note

- Link Aggregation settings have their own specifications and therefore may differ depending on the models of network switches. Execute settings after confirming the device specifications.
- The LAG Name that can be set differs depending on the models of networks switches. For the scope of the LAG Name that can be set, check the specifications of respective nodes.
- You cannot set up a Link Aggregation between the ports having different VLAN IDs. Be sure to confirm that these ports have the same VLAN settings to change the Link Aggregation settings.
- When you set up a Multi-Chassis Link Aggregation between different nodes, you must change Link Aggregation settings for respective switches. To set Multi-Chassis Link Aggregation, you must execute the settings for the peer link connection between nodes and the settings for the managed nodes in advance.
- The name of Multi-Chassis Link Aggregation (MLAG, vPC, etc.) as well as pre-settings will differ depending on the type of the network switch. Execute settings after confirming the device specifications.

## 2.7.9 Manual Setting of Network Connection Information

---



Whenever you cannot retrieve the connection information on physical networks automatically, you can set this information manually. The following operating procedure shows how to set the connection information manually.

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Network Map].  
A list of the nodes that are displayed on the Network Map is displayed as a tree structure in the Network Node List on the left side of the screen.
2. From the Network Node List, select the nodes that are the network connection points you want to confirm.  
When opening the network map, the node at the top of the Network Node List is selected.  
The Network Map is displayed at the center of the screen.
3. From the [Actions] button, select [Edit Connection].

4. Select the ports at both ends for which you want to execute the settings, and then select the [Add] button.

### Note

After selecting the [Add] button and if you want to cancel the settings you executed manually, select the [Clear] button.

5. After adding all the connection information you want to set, select the [Save] button.
6. Confirm that the edited contents are correct and then select the [Save] button.

## 2.8 Power Capping

---

For the devices mounted in racks, Power Capping is used to keep it from exceeding the set upper limit value for power consumption.

Beforehand, register the control information and power capping policy for each node in the rack and start power capping operations by enabling the power capping policy.

### Point

There are the following four types of power capping policies.

- Custom 1, Custom 2

Power capping policy for normal operations. Two types can be operated and switched between.

- Schedule

Policy that is only enabled on the specified day/time.

- Minimum

Control where power consumption is kept to a minimum.

### Note

Power Capping cannot be used in ISM for PRIMEFLEX.

### 2.8.1 Adding/Editing Power Capping Settings

---



#### Node power settings

Set the power information and operation priority for each node.

Power Capping is executed from a node with low operation priority.

The current power consumption value can be confirmed if it is a device that power consumption value can be retrieved for, and if the power capping status is [Stopped Power Capping] or [Power Capping].

If the node cannot execute Power Capping, maximum power consumption value is alternated as a fixed value.

#### Power capping policy

Set the upper limit value for power consumption for each policy.

Set operation schedule for schedule policy.

## 2.8.2 Enabling/Disabling Power Capping

---

Executable user

Administrator group	Other groups
<input checked="" type="checkbox"/> Admin <input type="checkbox"/> Operator <input type="checkbox"/> Monitor	<input type="checkbox"/> Admin <input type="checkbox"/> Operator <input type="checkbox"/> Monitor

Switch the power capping policy between enabled and disabled.

### Point

Each power capping policy can be enabled independently but if minimum is set, minimum is prioritized and used. If multiple policies other than minimum are enabled, the policy with the lowest upper limit value for power consumption is used.

### Note

- For racks with an already executed power capping policy, you must change the power capping settings if a node was added. If the settings are not changed, the power consumption per rack will be greater than the set upper limit value.  
It is recommended that you review the upper limit value in the rack power capping settings even for nodes that have been deleted.  
When migrating nodes, you must take measures accordingly to each rack before and after migration.
- The upper limit value is the power capping target value. Normally the upper limit is set with some margin so that the actual power consumption is below, but if the upper limit value is set low the power consumption may exceed it.
- If using the PRIMERGY RX/TX S7 series, set a numerical value higher than the sum total of the minimum power consumption value of the PRIMERGY RX/TX S7 series.  
The minimum power consumption value of the devices can be checked in the [Power Capping] - [Current Power Consumption] - [Current Total Power Consumption] column in the iRMC Web interface.
- If changing the date and time of ISM-VA to past dates or times, the power consumption value displayed in [Rack Information] in the [Rack Details] screen and the average power consumption value and average intake air temperature value in the [Monitoring] tab in the Details of Node screen will not be displayed correctly.  
When the date and time set in ISM-VA passes, it will be displayed correctly again.

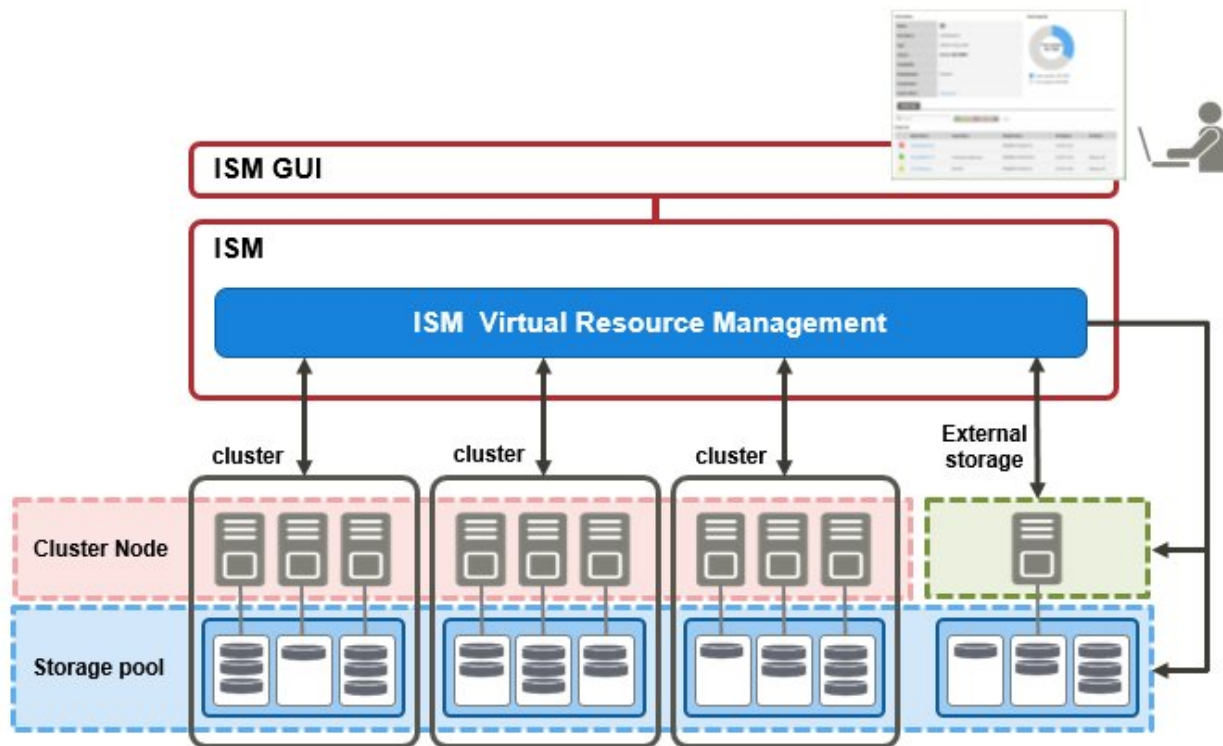
## 2.9 Virtual Resource Management

---

Virtual Resource Management is a function to manage and monitor the items managed as virtual resource.

The following is the environment configuration operating this function.

Figure 2.12 Configuration of the operating environment for Virtual Resource Management



**Note**

For pre-settings for Virtual Resource Management, refer to "A.1.2 Pre-settings for Virtual Resource Management."

### 2.9.1 Supported Virtual Resources

The following is the virtual resource to be supported by this function.

**Software environment**

Software environments that can be operated by Virtual Resource Management depends on the type of SDS (Software Defined Storage) and its version. Also, the hypervisor and cloud management software differs depending on the type of SDS.

The following are the software environments supported by Virtual Resources Management.

Note: Y = Supported, N = Not supported

Software environment (SDS)		Hypervisor	Cloud management software	Supported/Not supported	
VMware vSAN	5.x	VMware ESXi 5.x	vCenter Server Appliance 5.x	N	
	6.x	6.2	VMware ESXi 6.0 Update2	vCenter Server Appliance 6.0 Update2	Y
		6.5	VMware ESXi 6.5	vCenter Server Appliance v6.5	Y
		6.6	VMware ESXi 6.5 [Note 1]	vCenter Server Appliance 6.5 [Note 1]	Y
		6.6.1	VMware ESXi 6.5 Update1	vCenter Server Appliance 6.5 Update1	Y
		6.6.1 U2	VMware ESXi 6.5 Update2	vCenter Server Appliance 6.5 Update2	Y
		6.7	VMware ESXi 6.7	vCenter Server Appliance 6.7	Y
		Except the above			



Software environment (SDS)	Hypervisor	Cloud management software	Supported/Not supported
Microsoft Storage Spaces	Windows Server 2012 Hyper-V	Microsoft Failover Cluster	N
		Microsoft System Center 2012	N
Microsoft Storage Spaces Direct	Windows Server 2016 Hyper-V	Microsoft Failover Cluster	Y
		Microsoft System Center 2016	N
	Windows Server 2019 Hyper-V	Microsoft Failover Cluster	Y
		Microsoft System Center 2019	N

[Note 1]: For VMware vSAN 6.6, VMware ESXi 6.5d or later and vCenter Server Appliance 6.5d or later are required.

### Note

You must enable CredSSP authentication in advance. For pre-settings for Virtual Resource Management, refer to "[A.1.2 Pre-settings for Virtual Resource Management](#)."

## ETERNUS Storage

ISM GUI attribute information, status and other information regarding ETERNUS Storage are displayed.

For information on the devices supported by Virtual Resources Management, contact your local Fujitsu customer service partner.

### Note

The display of thin provisioning pool for ETERNUS is not supported.

The volume used by thin provisioning pool is not reflected even when RAID group is built into thin provisioning pool.

For reference and management of thin provisioning pool, use ETERNUS Web GUI.

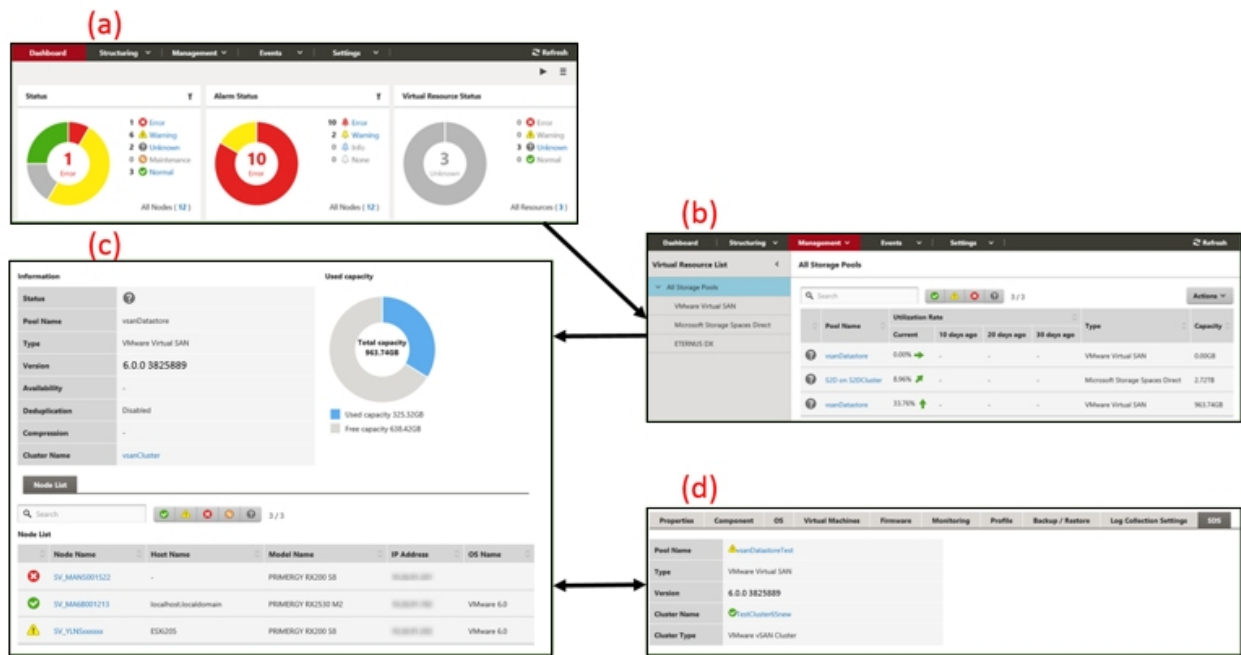
## 2.9.2 GUI for Virtual Resource Management

---

Virtual Resource Management is equipped with the management GUI.

The following displays the functions of each GUI screen and the mutual display relationships.

Figure 2.13 GUI for Virtual Resource Management



(a) Display of Virtual resources widget

The status of the virtual resources is displayed in a widget on the ISM dashboard.

(b) Display of Virtual resources list

Displays a list for the statuses of the virtual resources.

The resource utilization status is also displayed by the color and direction of the arrows.

(c) Display of Virtual resources detailed information

Detailed information, such as virtual resource settings information and utilization rate, is displayed.

The physical nodes configuring the virtual resources are displayed and related screens can be displayed.

For vSAN, the ESXi version and build number is displayed in "Version." From this version and build number, the vSAN version can be checked from the following website.

<https://kb.vmware.com/s/article/2150753>

(d) Display of Virtual resource information on node information ([SDS] tab)

The [SDS] tab that displays virtual resource information on the Details of Node screen is displayed.

If you select the [SDS] tab, the virtual resource information related to nodes on vSAN or Microsoft Storage Spaces Direct is displayed.

For vSAN, the ESXi version and build number is displayed in "Version." From this version and build number, the vSAN version can be checked from the following website.

<https://kb.vmware.com/s/article/2150753>

## 2.9.3 Operation of Virtual Resource Management

The following describes how to operate Virtual Resource Management.

- 2.9.3.1 Monitoring of the utilization status of storage pools
- 2.9.3.2 Identification of the errors in storage pools
- 2.9.3.3 Updates of virtual resources

## Point

Before monitoring with ISM, you must register virtual resource environment to ISM. It is executed with the following procedures.

1. Confirm that nodes configuring the storage pool (cluster) are already registered in ISM.  
For details on how to register nodes and to confirm the information, refer to "[2.2 Node Management](#)."
2. Confirm that cloud management software is already registered in ISM.  
For details on how to register cloud management software and to confirm the information, refer to "[2.13.6 Management of Cloud Management Software](#)."
3. Refresh the virtual resource information.  
For details on how to update, refer to "[2.9.3.3 Updates of virtual resources](#)."  
The storage pool information is displayed on the virtual resource GUI.

### 2.9.3.1 Monitoring of the utilization status of storage pools








Here the procedure for monitoring utilization status of storage pools is described.

1. From the Global Navigation Menu on the GUI of ISM, select [Dashboard] to display the virtual resource widget "Virtual Resource List."

For the widget addition method, refer to the ISM online help.











- Refer to "Utilization Rate" for the current utilization rate of the storage pools.

Status	Pool Name	Type	Capacity	Utilization Rate
	vSANDatastore-1	VMware Virtual SAN	22.01TB	57.32%
	vSANDatastore-2	VMware Virtual SAN	13.96TB	21.92%
	StoragePool-1	Microsoft Storage Spaces Direct	11.23TB	19.87%
	vSANDatastore-3	VMware Virtual SAN	2.82TB	91.92%
	raidgrp-1	ETERNUS DX	27.38TB	71.31%

- More detailed utilization rate status can be checked on the screen of the Virtual Resources List display.

The current utilization rate can be determined from the direction and color of the arrows.

From the Global Navigation Menu on the GUI of ISM, select [Management] - [Virtual Resource]. The list of virtual resources that can be managed with ISM displays the various types of resources in a tree and list form.

All Storage Pool							
Search		5 / 5				Actions	
Pool Name	Utilization Rate				Type	Capacity	
	Current	10 days ago	20 days ago	30 days ago			
 vSANDatastore-1	57.32% 	55.02%	50.01%	49.02%	VMware Virtual SAN	22.01TB	
 vSANDatastore-2	21.92% 	15.11%	11.23%	9.83%	VMware Virtual SAN	13.96TB	
 StoragePool-1	19.87% 	16.02%	8.02%	-	Microsoft Storage Spaces Direct	11.23TB	
 vSANDatastore-3	91.92% 	-	-	-	VMware Virtual SAN	2.82TB	
 raidgrp-1	71.31% 	63.31%	58.99%	56.00%	ETERNUS DX	27.38TB	

The utilization rate is interpreted in the following way.

- Color of the arrow

Displays the current total utilization rate.

Green: Less than 70% is utilized.

Yellow: Between 70% and 90% is utilized

Red: More than 90% is utilized

- Direction of the arrow

The utilization rate displays an increase rate compared to the utilization rate 10 days earlier.

Sideways: The utilization rate is moving sideways, is increasing slightly (The utilization rate is increasing with less than 5%) or is decreasing

Diagonal upwards: The utilization rate is increasing (The utilization rate is increasing with between 5% - 15%)

Upwards: The utilization rate is increasing sharply (The utilization rate is increasing with more than 15%)

- If you want to check detailed information, selecting a pool name displays the Detailed Information screen, where you can check the currently used capacity and available capacity in [Used capacity].

For Microsoft Storage Spaces Direct, in addition to the capacity information of the storage pools you can also check the capacity information of the virtual disks created on the storage pools.

The screenshot shows the 'StoragePool-1' detailed information page. It includes a table of pool information, a donut chart for capacity usage, and a table of virtual disks.

Information	Value
Status	✓
Pool Name	StoragePool-1
Type	Microsoft Storage Spaces Direct
Version	Windows Server 2016
Availability	Mirror
Deduplication	Enabled
Compression	-
Cluster Name	MSFC-1

**Used capacity**

Total capacity: 2.45TB

- Used capacity: 0.20TB
- Free capacity: 1.15TB
- Not allocated: 1.10TB

**Virtual Disk List**

Virtual Disk Name	Utilization Rate	Total capacity	Used capacity	Free capacity	Type
vdisk01	16.68%	180.00GB	30.03GB	149.97GB	ReFS
vdisk02	48.33%	80.00GB	38.66GB	41.34GB	ReFS
vdisk03	0.00%	200.00GB	0.00GB	200.00GB	ReFS

The classification of the capacity information displayed in the circle diagram of the utilization rate status for Storage Spaces Direct is described below.

- Used capacity: Displays the total used capacity of the virtual disks created on the storage pool.
- Free capacity: Displays the total free capacity of the virtual disks created on the storage pool.
- Not allocated: Displays the capacity that has not been allocated to a storage pool or where virtual disks have not been created.

Also, if you select the [Virtual Disk] tab, a list of the disks that exist on the storage pools and their used capacity and other information is displayed.

For details on the displayed contents, refer to the ISM online help.

## Point

The redundancy set up for the virtual disks is reflected in the capacity information in the [Virtual Disk] tab.

The capacity value displayed in the [Used capacity] circle diagram takes the redundancy of the capacity of each virtual disk into account.

3. Execute the following procedure if there is not sufficient capacity available.

- Add storage.

The nodes configuring the storage pool are displayed in the node list. If there is not sufficient available capacity, there is a risk this limits the available space in the storage made up by the nodes.

The insufficient available capacity can be mitigated by adding nodes to the disk, or by adding new nodes.

- Execute the required maintenance operations if an error is found in the nodes.

If the statuses shown in then node list show any errors, the storage capacity of this node cannot be used and capacity may become insufficient.

Check the incident for the node in Event Log and take appropriate measures.

### 2.9.3.2 Identification of the errors in storage pools



The following describes the procedure for discovering error and identifying cause in storage pools.

#### Step 1

Refresh the information of the virtual resources.

From the [Actions] menu, select [Refresh Virtual Resource Information]. For details, refer to "2.9.3.3 Updates of virtual resources."

The virtual resource information on the GUI is refreshed to the latest. If an error occurs, the displayed status will change.

#### Step 2

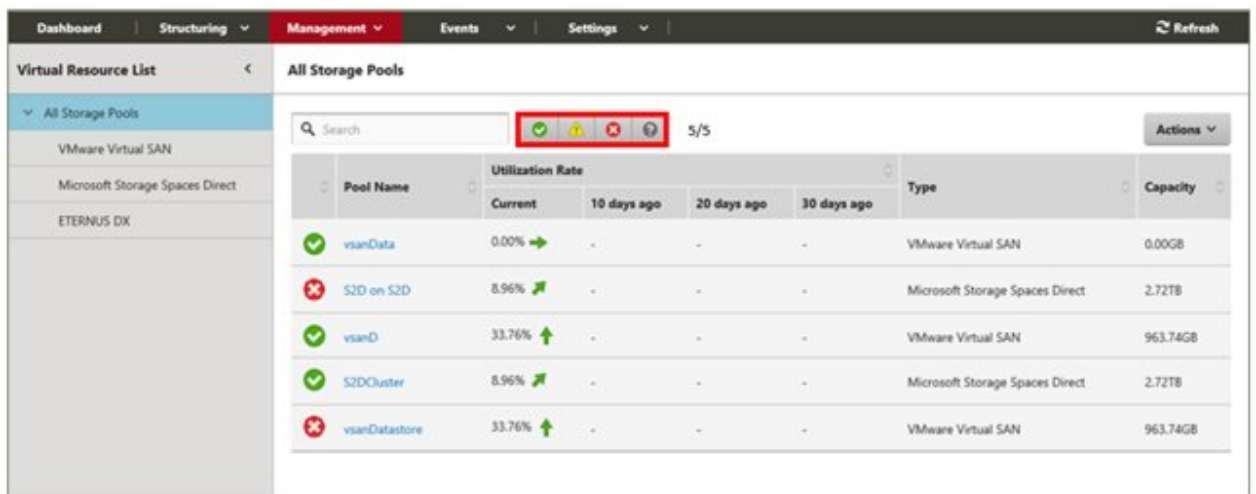
Discover and identify errors.

Resource errors can be checked from the screen of the Virtual Resources List display. If displaying the "Virtual Resource Status" widget on the dashboard, any resource errors are displayed in the widget.

(1) When identifying the place of an error from the screen of the Virtual Resources List display

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

The screen of the Virtual Resources List display is displayed.



Virtual resources with the selected status can be filtered out from the status filter icon at the top of the screen.

2. Select the pool name.

When the virtual resources detailed information screen is displayed, check the node names that error is displayed for in the "Node List."

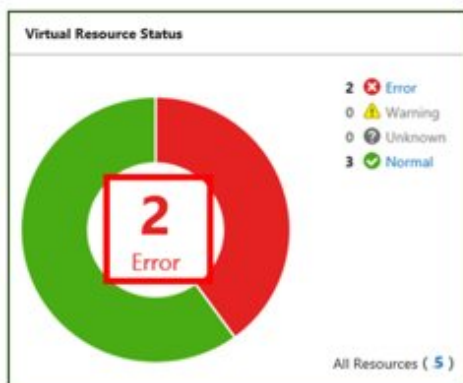
The screenshot displays the VMware vSphere interface for the 'vsanDatastore' configuration page. The left sidebar shows the 'Virtual Resource List' with 'VMware Virtual SAN' selected. The main content area includes an 'Information' section with details such as Status (Warning), Pool Name (vsanDatastore), Type (VMware Virtual SAN), Version (6.0.0 3825889), Availability (-), Deduplication (Disabled), Compression (-), and Cluster Name (vsanCluster). A 'Used capacity' donut chart shows a total capacity of 963.74GB, with 325.32GB used and 638.42GB free. Below the information is a 'Node List' table with a search bar and status icons. The table lists three nodes, with the first one, 'SV\_MANS001522', highlighted with a red border and a red error icon.

Node Name	Host Name	Model Name	IP Address	OS Name
SV_MANS001522	-	PRIMERGY RX200 S8	192.168.1.101	
SV_MA68001213	localhost.localdomain	PRIMERGY RX2530 M2	192.168.1.101	VMware 6.0
SV_YLNSxxxxx	ESX-205	PRIMERGY RX200 S8	192.168.1.101	VMware 6.0

(2) When identifying the place of an error from the dashboard

1. Select the numbers displayed in the middle of the "Virtual Resource Status" widget on the ISM dashboard.

A list of the error status resources will be displayed.



Pool Name	Utilization Rate				Type	Capacity
	Current	10 days ago	20 days ago	30 days ago		
vsanData	0.00%	-	-	-	VMware Virtual SAN	0.00GB
S2D on S2D	8.96%	-	-	-	Microsoft Storage Spaces Direct	2.72TB
vsanD	33.76%	-	-	-	VMware Virtual SAN	963.74GB
S2DCluster	8.96%	-	-	-	Microsoft Storage Spaces Direct	2.72TB
vsanDatastore	33.76%	-	-	-	VMware Virtual SAN	963.74GB

2. Select the pool name.

When the virtual resources detailed information screen is displayed, check the device names that error is displayed for in the "Node List."

### Step 3

Check the details of the error that occurred.

(1) If an error is displayed for the virtual resource





If the storage pool status displays an error, the following situations are probable.

Layer where error status occurred	Status
Physical layer	<p>An error occurred in the storage pool because of a problem with a physical component (HDD, SSD, and node).</p> <p>Depending on the type of SDS, it will be one of the following states.</p> <ul style="list-style-type: none"> <li>- If it is a vSAN, errors occur in the health of vSAN</li> <li>- If it is Microsoft Storage Spaces Direct, errors occur on the nodes or physical disks configuring the storage pool</li> <li>- If it is ETERNUS, errors occur on RAID groups, physical disks, or ETERNUS devices</li> </ul>



Layer where error status occurred	Status
Virtual layer	An error has occurred in the virtual resource layer (data store).

The following are statuses of storage pools according to each status.

Status	Displayed by icons in the ISM GUI	Status
Error		An error has occurred in the storage pool and it is not possible to continue to use.
Warning		An error has occurred in the storage pool but it is possible to continue to use.
Unknown		An error has occurred in the storage pool and its status cannot be confirmed.
Normal		The storage pool is in a normal status.

### Point

.....

If the capacity of the storage pool is reduced by an error in the physical or virtualized layer, whether it can continue to be used as a storage pool can be determined by the "Error" status.

.....

The error details and place where it occurred are checked in the following way.

### Point

.....

For details on how to identify detailed error location and its corrective actions, or to restore the error, execute procedures according to each storage pool manuals.

.....

For vSAN

The status of the storage view vSAN datastore and the "Health" of the vSAN are checked on either the ISM GUI or in the VMware vCenter Web Client.

1. From the virtual resources list on the ISM GUI or from the details screen, check "Pool Name" and "Cluster Name."
2. Sign in to VMware vCenter Server Web Client and in the [Storage Views] tab, check the status of the displayed pool name previously checked in step 1.

If it is operating normally there is no mark, and any errors are marked in red.

3. In "Hosts and Clusters," select the node name checked in step 1.
4. From the [Monitor] tab, select [Virtual SAN] - [Health].

Refer to the "Test result" of the vSAN health and identify the error contents.

Execute the following after recovering from an error.

1. Sign in to the VMware vCenter Server Web Client and select the cluster name in "Hosts and Clusters."
2. From the [Monitor] tab - [Virtual SAN] - [Health], select [Retest] in the displayed Virtual SAN health screen and then check that the test result that was "Failed" now has changed to "Passed."
3. Select the [Storage Views] tab and from the displayed datastore list, check that the status of the vSAN datastore is normal.
4. From the Virtual Resource list screen on the ISM GUI, select the [Actions] button - [Refresh Virtual Resource Information] and check that the status has returned to normal.

## Microsoft Storage Spaces Direct

From the ISM GUI or the server manager on the management server, check the status of the storage pool and the status of the physical disk.

1. From the virtual resources list or the details screen on the ISM GUI, check the "pool name."
2. Open the server manager on the management server, select [File and Storage Services] - [Storage Pool], and check the status of the storage pool name checked in step 1. Check the physical disks displaying errors from "Physical Disks."

Execute the following after recovering from an error.

1. Open the server manager on the management server, select [File and Storage Services] - [Storage Pool], and check that the storage pool and the physical disk are operating normally.

Since the displayed information may be old, select the [Refresh] button on the screen, and check after refreshing the information.

2. From the Virtual Resource list screen on the ISM GUI, select the [Actions] button - [Refresh Virtual Resource Information] and check that the status has returned to normal.

## ETERNUS Storage

Open ETERNUS Web GUI with web browser, check the statuses of RAID groups and physical disks.

For URL of ETERNUS Web GUI, move to "Node Lists" on the details of the virtual resource screen, then you can confirm it by the node information when selecting the device name of ETERNUS.

After recovering the error, from the Virtual Resource list screen on the ISM GUI, select [Refresh Virtual Resource Information] from the [Actions] button and check that the status has returned to normal.

### (2) If the node error is displayed in the "Node list"

Check the details of the error in the ISM Event Log.

1. From the Global Navigation Menu on the GUI of ISM, select [Events] - [Events].  
The "Event List" screen is displayed.
2. Check the error contents by entering "Node name" into the search box and search for events for the entered node.

## 2.9.3.3 Updates of virtual resources



From the virtual resources list screen, execute [Refresh Virtual Resource Information] from the [Actions] button.



### Point

- Since the information displayed on the GUI may be old, make sure to refresh it when checking the status of the virtual resources.  
The refresh process is registered in ISM tasks.

If the displayed information remains old, check if the task of task type of "Refresh Virtual Resource" on the "Tasks" screen on ISM GUI is "Completed."

Status	Progress	Result	Task ID	Task Type	Operator	Start Time	Completion Time
Completed	1 / 1	Success	1	Refresh Virtual Resource	administrator	May 9, 2017 1:32:46 AM	May 9, 2017 1:32:50 AM

- The virtual resource information is periodically and automatically refreshed as follows (Tasks are not displayed).
  - All virtual resource information is automatically refreshed every day at AM 0:00 of local time.
  - The virtual resource statuses are automatically refreshed every three minutes.

## 2.10 Backup/Restore Hardware Settings

This function collects the hardware settings, saves them as files, and can then export the saved files. The target hardware settings are the following.

- BIOS/iRMC settings of PRIMERGY and PRIMEQUEST3000B
- Storage settings of ETERNUS NR (NetApp)
- Switch settings of VDX

This function can import the exported files to a separate ISM and reflect the imported BIOS/iRMC settings file to PRIMERGY or PRIMEQUEST 3000B, and the switch settings file to VDX.

Figure 2.14 "Backup/Restore Hardware Settings" screen sample (GUI)

Status	Node Name	IP Address	Model Name	Last Backup		
				Type	Saved time	Description
Backup completed	RX_180	10.10.10.10	PRIMERGY RQ200 S8	Server (BIOS)	2018/05/21 10:06:57	
				Server (iRMC)	2018/05/21 10:07:14	
Backup completed	RX_182	10.10.10.10	PRIMERGY RQ2530 M1	Server (BIOS)	2018/05/21 10:05:48	
				Server (iRMC)	2018/05/21 10:06:50	
Backup canceled	RX_184	10.10.10.10	PRIMERGY RQ2530 M1	Server (BIOS)	2018/05/21 10:07:09	
				Server (iRMC)	-	-
Backup error	VDX_188	10.10.10.10	BR-VDX6740	Switch	-	-
Backup not saved	NR_191	10.10.10.10	NetAppCluster	Storage	-	-

### Point

- The files of hardware settings are saved separately for BIOS and iRMC.
- When backing up the BIOS hardware settings, switch off the power of the server in advance.
- When backing up the storage settings and the switch settings, switch on the power of the hardware in advance.

## 2.10.1 Backup of the File of Backup Hardware Settings

---



Retrieve the hardware settings backup from the specified node.

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, then select [Backup Hardware Settings] from the [Actions] button.

The "Backup Hardware Settings" screen is 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 returned to "Off."
5. Select the checkboxes for the [Server (BIOS)], [Server (iRMC)], [Storage] or [Switch] to which the settings will be backed up, and then select the [Execute] button.

### Point

.....  
You can select multiple nodes and hardware settings, and back them up collectively.  
.....

## 2.10.2 Export of the File of Backup Hardware Settings

---



Export the specified, already registered backup file.

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, then select [Export (Backup file)] from the [Actions] button.
4. Following the on-screen instructions, select the file, and then select the [Execute] button.

### Point

.....  
You can select multiple nodes and hardware settings, and export them collectively.  
.....

## 2.10.3 Addition of Profiles from the File of Backup Hardware Settings

---



Convert the specified, already registered backup to a profile and add it.

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, then select [Add Profile From Backup] from the [Actions] button.
4. Following the "Add Profile From Backup" wizard and enter the setting items.

## Point

- You can select multiple nodes, and add profiles collectively.
- It can only be used for PRIMERGY/PRIMEQUEST 3000B server backups.

### 2.10.4 Addition of Policies from the File of Backup Hardware Settings

---



Convert the specified, already registered backup to a policy and add it.

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, then select [Add Policy From Backup] from the [Actions] button.
4. Following the "Add Policy From Backup" wizard and enter the setting items.

## Point

- You can select multiple nodes, and add policies collectively.
- It can only be used for PRIMERGY/PRIMEQUEST 3000B server backups.

### 2.10.5 Import of the File of Backup Hardware Settings

---



Import the exported backup file.

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 the node, then select [Import] from the [Actions] button.
4. Select from the options in [File selection method].
  - Local  
Import a backup file stored locally.
  - FTP  
Import a backup file from the FTP server of ISM-VA.  
You must transfer the backup file to the "/<User group name>/ftp" directory of ISM-VA in advance.  
For FTP connection and how to transfer FTP, refer to "2.1.2 FTP Access."
5. Specify the backup file to be imported in [File] and then start import with the [Execute] button.

## Point

- The files you deployed on the FTP server of ISM-VA are no longer required after the import has finished. Use an FTP command to delete them.

- You can select multiple nodes, and import collectively.

### Note

ETERNUS NR (NetApp) backup files cannot be imported.

## 2.10.6 Restoration of the File of Backup Hardware Settings

	Administrator group	Other groups
Executable user	Admin Operator Monitor	Admin Operator Monitor

Reflect the hardware settings of the specified, already registered back up on the node.

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, then select [Restore Hardware Settings] from the [Actions] button.
5. Following the on-screen instructions, select the file, and then select the [Execute] button.

### Point

Multiple nodes can be selected and restored.

### Note

- ETERNUS NR (NetApp) backup files cannot be restored.
- When you restore the VDX, execute restoring after initializing setting items. If the setting items are not initialized before restoring, 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 restoring and execute settings if required.

## 2.10.7 Deletion of the File of Backup Hardware Settings

	Administrator group	Other groups
Executable user	Admin Operator Monitor	Admin Operator Monitor

Delete the specified, already registered backup.

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 the link in the [Last Backup] field of the node you want to delete.
4. Select the hardware settings to be deleted, then select [Delete] from the [Actions] button.

### Point

You can select multiple hardware settings backup files and delete them collectively.

## 2.11 Packet Analysis of Virtual Network

This function visualizes the traffic status of the virtual network.

Based on the retrieved information, tendencies in the communication volume can be checked for each port, each network and each host. Also, by checking the communication quality, it becomes easier to find locations with errors and communication quality can be improved.

### 2.11.1 Support Targets

The following is the hypervisors and cloud management software supported by this function.

Item		Hypervisor	Cloud management software
VMware	5.x	VMware ESXi 5.5	vCenter Server 5.5
			vCenter Server Appliance 5.5
	6.x	VMware ESXi 6.0	vCenter Server 6.0
			vCenter Server Appliance 6.0
		VMware ESXi 6.5	vCenter Server 6.5
			vCenter Server Appliance 6.5
VMware ESXi 6.7	vCenter Server 6.7		
	vCenter Server Appliance 6.7		
Redhat	7.x	Redhat Enterprise Linux 7.2 (KVM)	OpenStack
		Redhat Enterprise Linux 7.3 (KVM)	
		Redhat Enterprise Linux 7.4 (KVM)	
		Redhat Enterprise Linux 7.5 (KVM)	
		Redhat Enterprise Linux 7.6 (KVM)	

### Note

- To monitor virtual network adapters, some settings may be required for hypervisor or cloud management software to be used in advance.
- For operational performance using OpenStack, contact your local Fujitsu customer service partner.

### 2.11.2 Check of Analysis VM

This function supports the following ISM version and Analysis VM versions.

ISM version	Infrastructure Manager Analysis VM for KVM	Infrastructure Manager Analysis VM for VMware
ISM 2.4.0	V1.1.0	V1.1.1

### 2.11.3 Display Item of Packet Analysis of Virtual Network

This function visualizes the following information of the virtual network. The data retention period is one month or less.

Table 2.4 Information of performance statistics retrieved from the monitored host

Display item	Description
CPU usage	Displays the utilization rate of the physical CPU on the target host.
CPU usage of VM vCPU	Displays the utilization rate of the virtual CPUs for each virtual machine operating on the target host.
CPU usage of virtual network adapter [Note 1]	Displays the CPU utilization rate in virtual network adapter units.
Traffic information of virtual network adapter [Note 1]	Displays the volume of the sent and received packets, the number of error packets, and the number of dropped packets for each virtual network adapter.

[Note 1]: The upper limit of the number of virtual adapters that can be monitored by the function is 1000.

Table 2.5 Packet analysis results showing information on details and quality of communication

Monitoring targets of Analysis VM	Description
Port traffic information	Displays the sent and received packet information for each TCP/UDP port.
Network traffic information	Displays the sent and received packet information for each subnet.
Host traffic information	Displays the sent and received packet information for each host.
Host quality information	Displays the communication quality of the TCP (number of losses, delay time, etc.) for each host.

### 2.11.4 Function difference of Packet Analysis of Virtual Network

The following are the function difference between Packet Analysis of Virtual Network for VMware and for KVM.

Functions supported	Display item	VMware	KVM
Information of performance statistics retrieved from the monitored host	CPU usage	Y [Note 1]	Y
	CPU usage of VM vCPU	Y	Y
	CPU usage of virtual network adapter	Y [Note 2]	Y
	Traffic information of virtual network adapter	Y [Note 3]	Y
Packet analysis results showing information on details and quality of communication	Port traffic information	Y	Y
	Network traffic information	Y	Y
	Host traffic information	Y	Y
	Host quality information	Y	Y

[Note 1]: Information of process CPU utilization cannot be displayed.

[Note 2]: Information of CPU scheduler cannot be displayed.

[Note 3]: Only the number of dropped packets can be displayed.



Xen cannot be used.

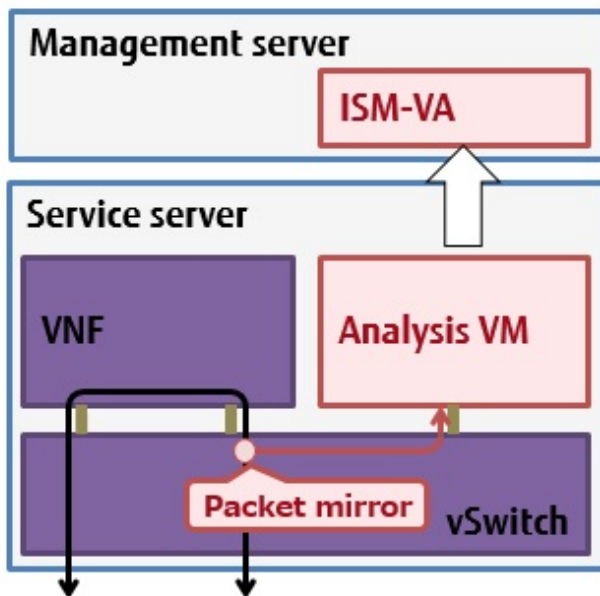


## 2.11.5 Operation of Packet Analysis of Virtual Network

By deploying Analysis VM manually to the hypervisor on which is decreased communication performance, Packet Analysis of Virtual Network retrieves information required when Analysis VM analyzes actual packets on the virtual switch in order to specify the cause of a decrease in the communication performance. The following items are the targets for retrieval.

- Performance information by port number (TCP/UDP), by terminal (VM), or by session.
- Quality degradation information such as traffic volume, the number of packet loss, or the volume of traffic delay.

Figure 2.15 Image of operation of Packet Analysis of virtual network



### Point

- Analysis VM only analyzes the captured header information of the packet (L2, L3, L4 headers).
- After analyzing the header information, the captured header information is discarded without being saved, meaning that no information is saved.

## 2.12 Functions of ISM for PRIMEFLEX

The ISM for PRIMEFLEX function is the ISM with the Virtualized Platform Expansion function added. Included in the functions of ISM, the following functions are provided.

- [2.12.1 Cluster Management](#)
- [2.12.2 Cluster Creation](#)
- [2.12.3 Cluster Expansion](#)
- [2.12.4 Firmware Rolling Update](#)

### Note

ISM Power Capping cannot be used in ISM for PRIMEFLEX.

## 2.12.1 Cluster Management

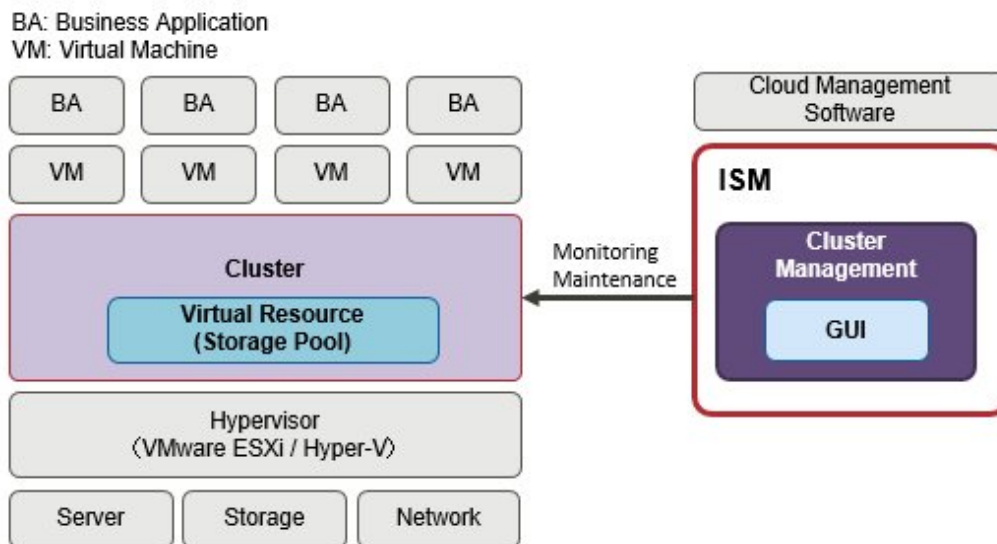
This function can be used only with the license for ISM for PRIMEFLEX.

Cluster Management provides functions to manage clusters in link with ISM.

By allowing for monitoring in link with the statuses of the hardware (nodes) in a cluster and for monitoring storage pools and other virtual storage environments (Software Defined Storage, hereafter referred to as "SDS"), these functions can be used to efficiently determine smooth cluster maintenance and addition (provisioning) of resources.

For the types of cluster that can be managed and their requirements, refer to "2.12.1.2 Environments supported by Cluster Management."

Figure 2.16 Overview of Cluster Management



Cluster Management provides various GUIs that are linked with the ISM GUI for Cluster Management and features the following functions:

- List of clusters and summary display including cluster statuses
- Displays the detailed cluster information

For the cluster configuration information, information such as the following is displayed.

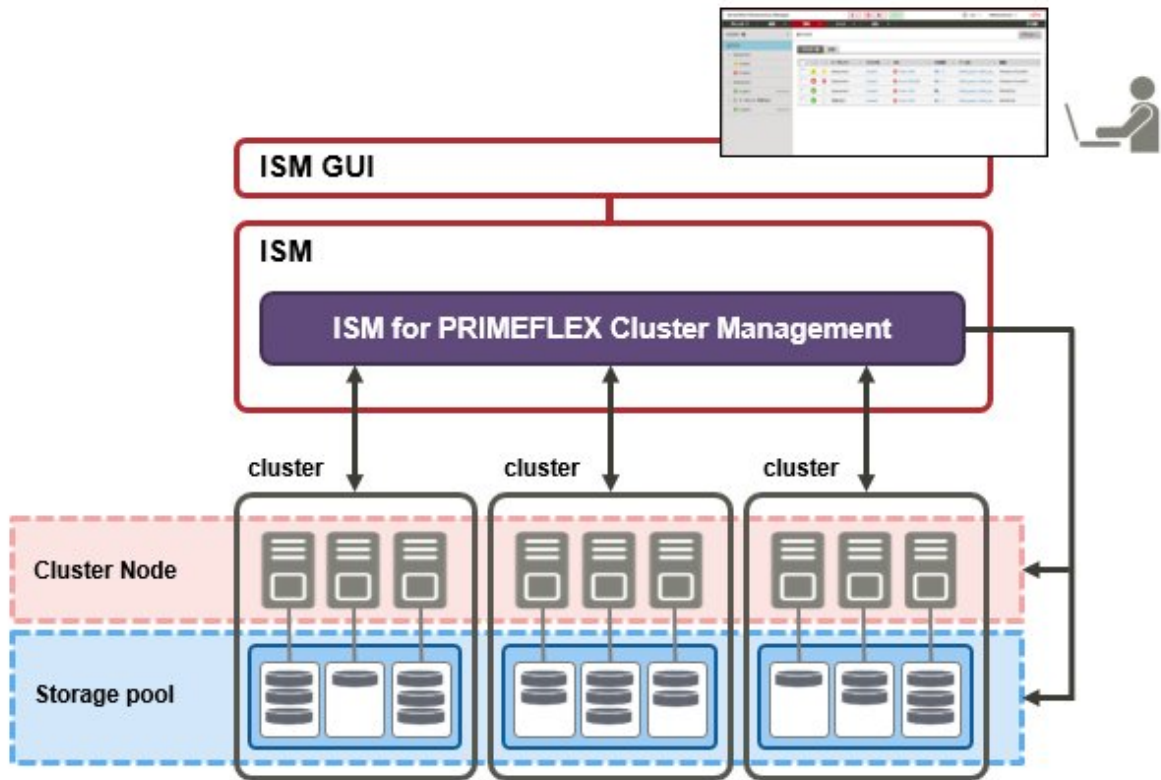
- Information of the nodes configuring the cluster
- Information of the virtual resources in the cluster
- Parameter settings information of Cluster Creation and Cluster Expansion
- Widget that makes cluster monitoring possible from the dashboard

### 2.12.1.1 Cluster Management GUI

Cluster monitoring and management can be used from the ISM GUI.

The following is the environment configuration operating Cluster Management.

Figure 2.17 Configuration of the operating environment for Cluster Management



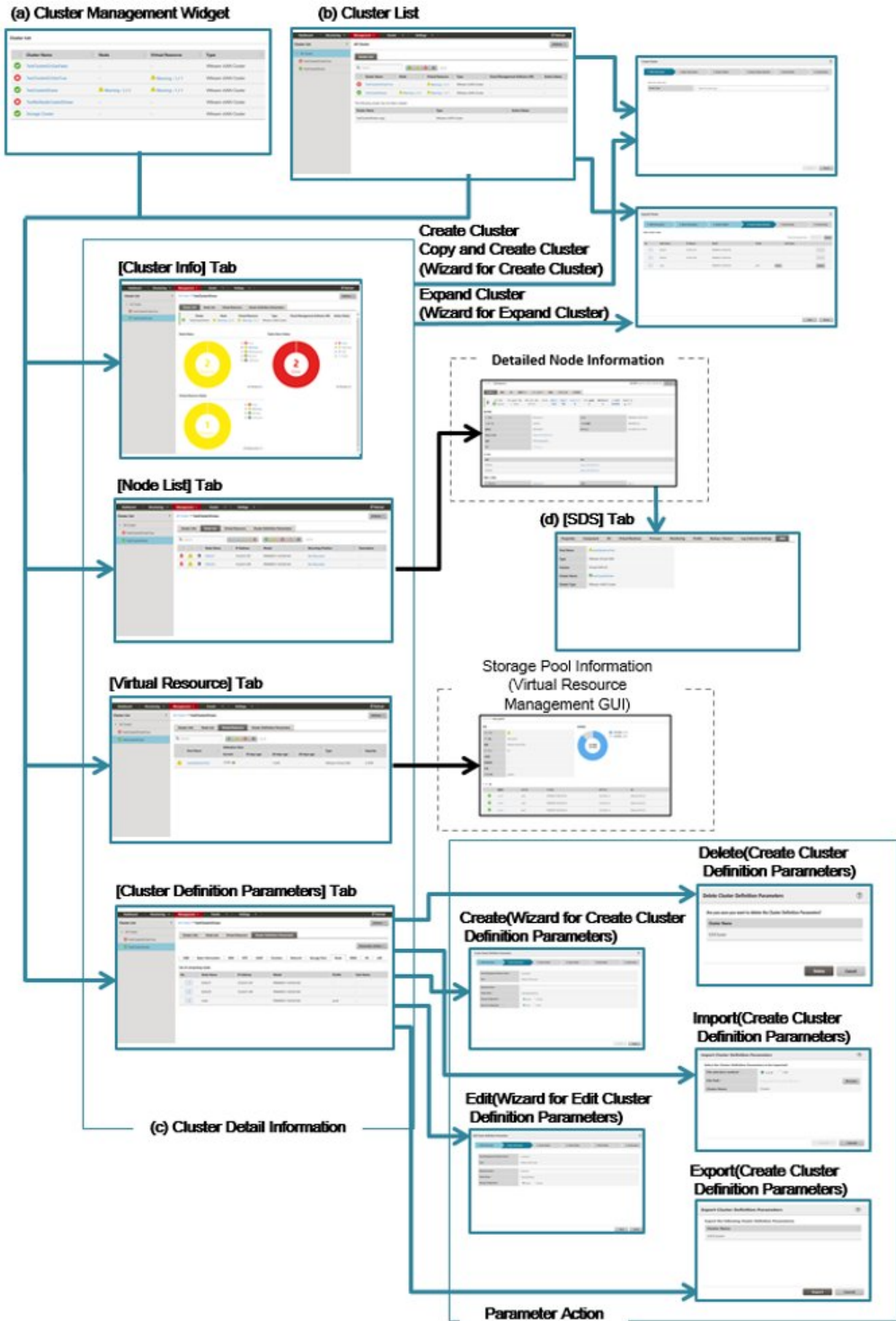
The following displays the functions of each screen and the mutual display relationships.

The Cluster Management GUI ((a) - (d) in the [Figure 2.18 Cluster Management GUI](#)) displays various kinds of information on the clusters. More detailed information can be checked, linked with node information (the "Node List" screen) and virtual resource information (virtual resource GUI).

For more information on the node list and the GUI for Virtual Resource Management, refer to "[2.9.2 GUI for Virtual Resource Management](#)."

For descriptions of the GUI display items, refer to the ISM online help.

Figure 2.18 Cluster Management GUI



(a) Cluster Management Widget

On the ISM Dashboard, Cluster Management Widget is displayed.

It is possible to check cluster information and states monitored on ISM from the widget.

For details, refer to "[Operation in link with Dashboard.](#)"

(b) Cluster List

A list of the clusters is displayed.

When you select a cluster name, the management screen of "(c) Cluster Detail Information" is displayed.

(c) Cluster Detail information

Information for the cluster and the components that configure the cluster is displayed by switching tabs.

For details on the screens displayed as tabs, refer to "[Details of Cluster screen \(tab display screen\).](#)"

(d) Cluster information on node information ([SDS] tab)

The [SDS] tab that displays virtual resource information on the Details of Node screen is displayed.

When you select the [SDS] tab, the nodes and the related information are displayed. For details, refer to "[Operation in link with node information \(\[SDS\] tab\).](#)"

The following describes the contents of Cluster Management GUI.

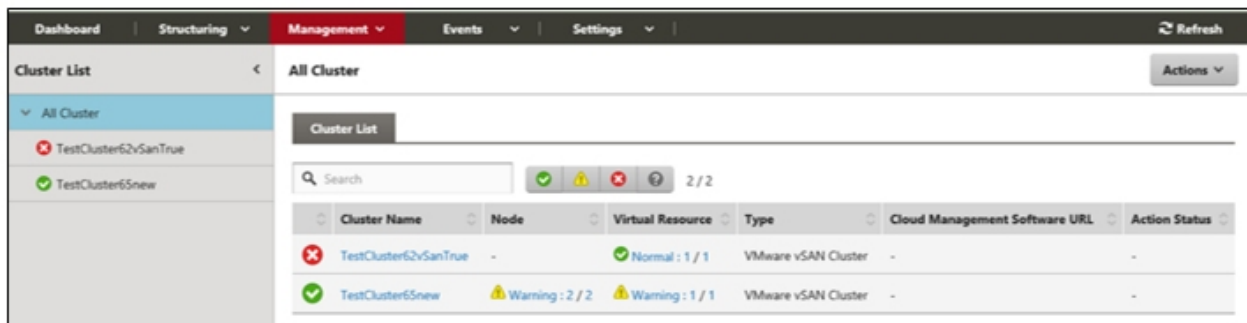
**Cluster List screen**

From the Global Navigation Menu on the ISM GUI, select [Management] - [Cluster] to display the cluster list screen.

A list of the clusters that can be managed by ISM is displayed.

The list shows the status of each cluster and the components that configure the cluster.

Figure 2.19 Cluster List screen



**Details of Cluster screen (tab display screen)**

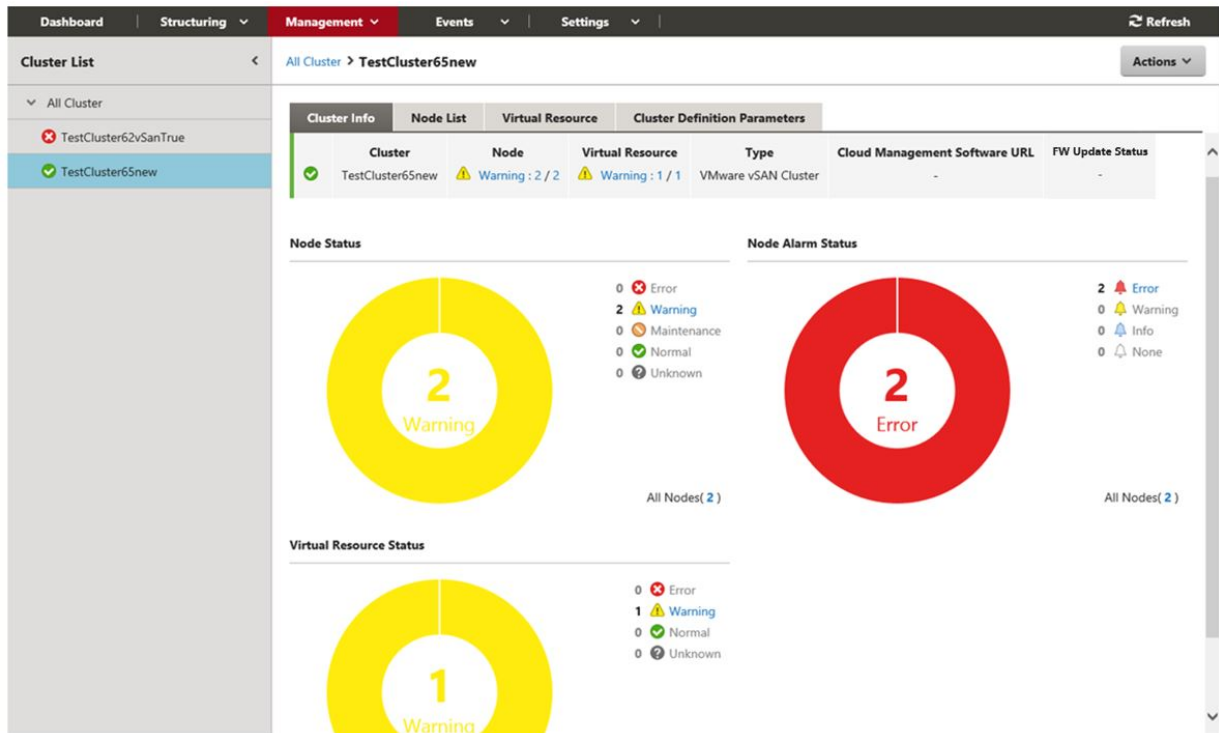
Selecting a cluster name on the cluster list screen opens the Details of Cluster screen for the selected cluster, allowing you to check the information on the nodes and the components that configure the cluster.

This screen displays the resource settings, utilization statuses, lists of nodes that configure the resources, and other cluster management information.

[Cluster Info] tab

Displays summary information on the clusters and the components that configure each cluster.

Displays cluster information (cluster names), node statuses (statuses, alarms) and statuses of virtual resources.



[Node List] tab

A list of the information of the nodes configuring the cluster is displayed. The status of the node, its position and other information is displayed.

If you select the node, you move to the Details of Node screen, where you can check the hardware information, detailed node status information, and configuration information.

For description of the Details of Node screen, refer to the ISM online help.

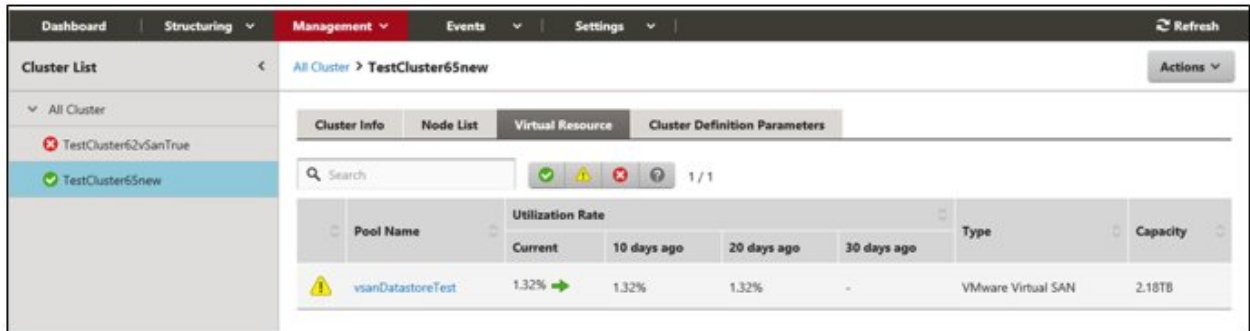


[Virtual Resource] tab

A list of the information of the SDS storage pools created in the cluster is displayed.

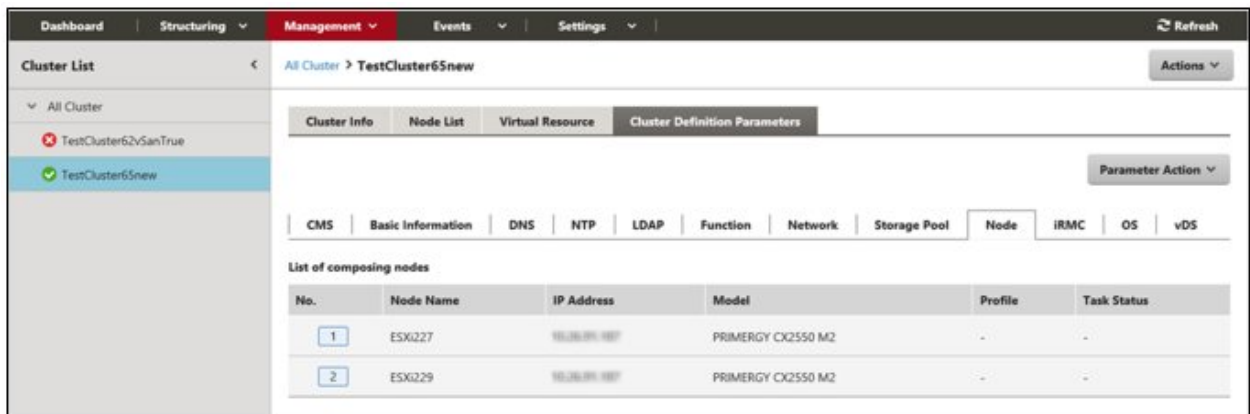
Selecting a storage pool name displays the storage pool information screen of the GUI for Virtual Resource Management.

For descriptions of the GUI for virtual Resource Management, refer to "2.9.2 GUI for Virtual Resource Management" or to the ISM online help.



[Cluster Definition Parameters] tab

Displays parameters referred to when creating clusters and when adding servers to clusters.



The parameter information can be referred to by switching between the following tabs.

For information on the displayed information, refer to "ISM for PRIMEFLEX Parameter List" or refer to the ISM online help.

Tab name	Description
CMS	The information of the cloud management software is displayed.
Basic information	The cluster name and other basic information of the cluster is displayed.
DNS	The DNS information of the cluster is displayed.
NTP	The NTP information of the cluster is displayed. [Note 1]
LDAP	The LDP information of the cluster is displayed.
Function	The setting information of vSAN and vSphere is displayed. [Note 1]
Network	The network information of the cluster is displayed. [Note 2]
Storage pool	The storage pool information of the cluster is displayed.
Node	The information of the nodes configuring the cluster is displayed.
iRMC	The setting information of the user of iRMC is displayed.
OS	The setting information of the local user of the OS is displayed.
vDS	The setting information of the virtual distributed switch (vDS: virtual Distributed Switch). [Note 1]
Virtual switch	The setting information of the virtual switch is displayed. [Note 3]

[Note 1]: Displayed if the cluster type is "VMware vSAN Cluster."

[Note 2]: Unique information is displayed if the cluster type is "VMware vSAN Cluster" and "Microsoft Failover Cluster."

[Note 3]: Displayed if the cluster type is "Microsoft Failover Cluster."

The following parameter operations can be executed from the [Parameter Action] button.

Select the [Parameter Action] button, select from the menu and follow the wizard or screen that is displayed to enter the setting values.

For the setting items in the wizard, refer to "ISM for PRIMEFLEX Parameter List." In addition, for detailed information on setting procedures, refer to the ISM online help.

- Create

The "Create Cluster Definition Parameters" wizard is displayed and you can create new parameters.

- Edit

The "Edit Cluster Definition Parameters" wizard is displayed and you can edit the parameters.

- Delete

"Delete Cluster Definition Parameters" screen is displayed and parameters can be deleted.

- Import

"Import Cluster Definition Parameters" screen is displayed and parameters can be imported.

- Export

"Export Cluster Definition Parameters" screen is displayed and parameters can be exported.

## Actions menu

Selecting the [Actions] button on the top right side of the screen displays the following menu and allows you to execute operations for the cluster.

- Refresh Cluster Information

When selecting this menu, the cluster information is retrieved and the information is refreshed.

Refer to "[2.12.1.3 Refreshing cluster information](#)" for details on how to execute the operations.

- Create Cluster

Selecting this menu opens the "Create Cluster" wizard. Follow the wizard to create a cluster.

For details, refer to "[2.12.2 Cluster Creation](#)." For the procedure, refer to "Operating Procedures."

- Copy and Create Cluster

Selecting this menu opens the "Create Cluster" wizard. Follow the wizard to create a cluster reference.

For details, refer to "[2.12.2 Cluster Creation](#)." For the procedure, refer to "Operating Procedures."

- Expand Cluster

Selecting this menu opens the "Expand Cluster" wizard. Follow the wizard to add servers to the cluster.

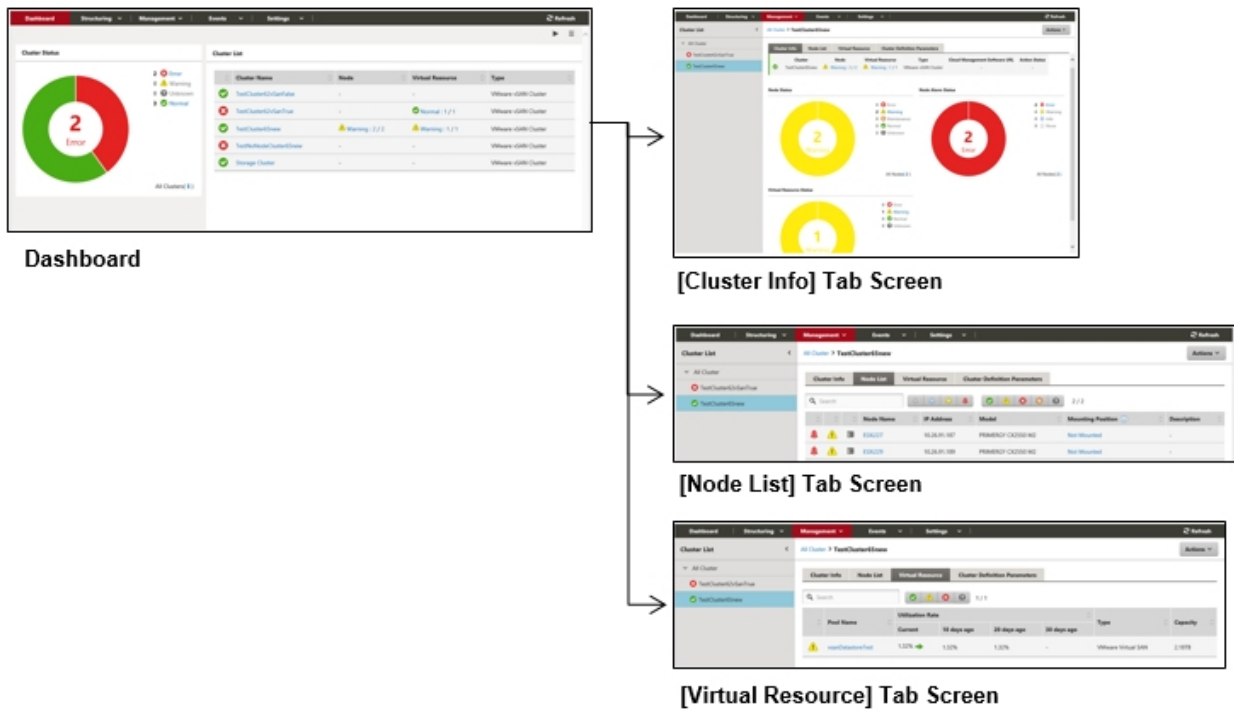
For details, refer to "[2.12.3 Cluster Expansion](#)." For the procedure, refer to "Operating Procedures."

## Operation in link with Dashboard

By adding the information display screen (widget) related to Cluster Management on ISM dashboard, you can, with just one click on the Dashboard, display the information on clusters and components that configure each cluster (nodes and storage pools) for which you want to check the details.

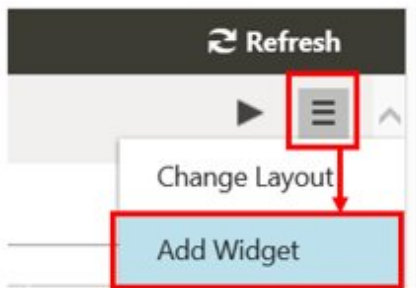


Figure 2.20 Operation in link with Dashboard



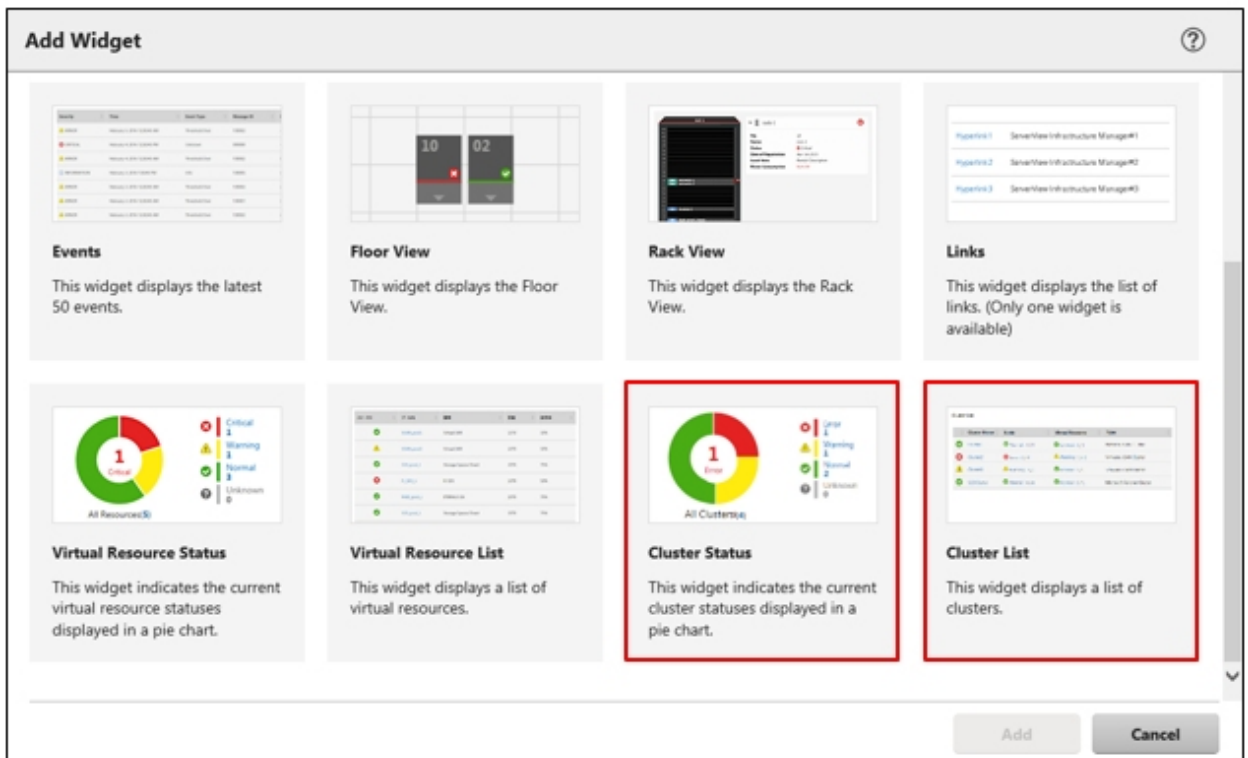
The procedure for adding widgets to the ISM Dashboard is as follows:

1. From the [☰] at the top of the screen, select [Add Widget].

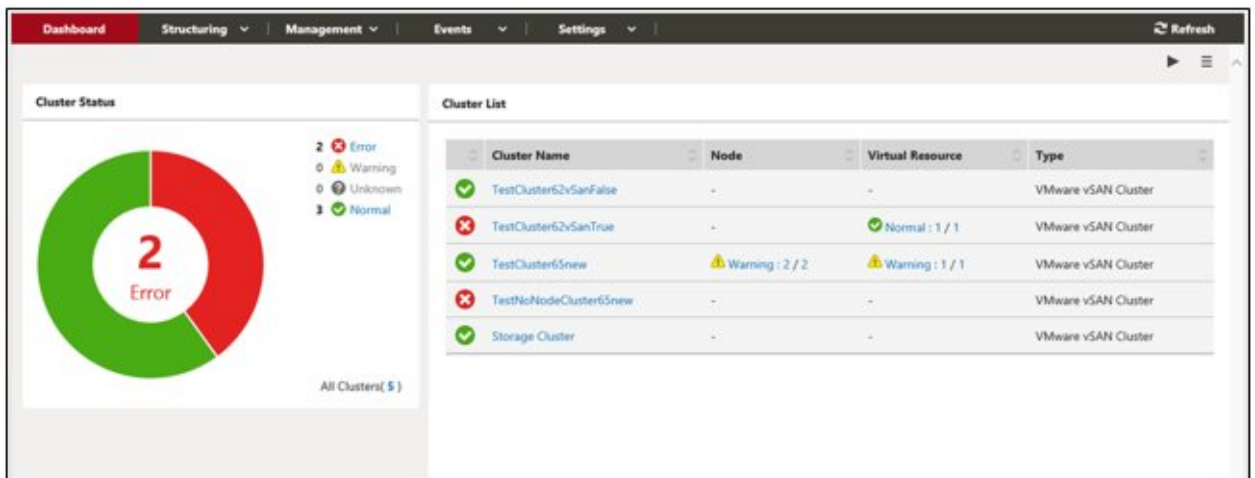


A menu for adding widgets is displayed.

- "Cluster Status" and "Cluster List" are widgets for displaying clusters. Select either one and select the [Add] button.



The widget you selected is displayed on the Dashboard.



### Operation in link with node information ([SDS] tab)

You can embed Virtual Resource Management information into the Details of Node screen in order to link these types of information to each other.

- From the Global Navigation menu on the GUI of ISM, select [Management] - [Nodes], and then select a node name on the "Node List" screen.

On the Details of Node screen, the [SDS] tab is displayed.

The [SDS] tab is displayed only for nodes that are configured by SDS (not for nodes that are not configured by SDS).

- Select the [SDS] tab.

The SDS information related to each node is displayed.

The storage pool name and the cluster name that configure the SDS are displayed.



Selecting the cluster name displays the cluster information screen.

Selecting the pool name displays the screen with the detailed information on the storage pool.

For a description of the screen, refer to "2.9.2 GUI for Virtual Resource Management."

## 2.12.1.2 Environments supported by Cluster Management

Cluster Management supports the following environments.

- VMware Virtual SAN Cluster
- Microsoft Failover Cluster

### VMware Virtual SAN Cluster

VMware Virtual SAN cluster (hereafter referred to as "vSAN cluster") is a system configured with multiple servers that have VMware ESXi installed as a hypervisor.

vCenter Server Appliance (hereafter referred to as "vCenter Server") is used as the management software, and Cluster Management collects cluster information from vCenter Server to display it on the ISM GUI.

In the vSAN cluster, the storage mounted on each server is aggregated to configure the "vSAN Storage Pool" virtual storage. The vSAN storage pool can be monitored from ISM.

The following are the requirements for vSAN cluster environments.

Item	Requirement
Hypervisor	<ul style="list-style-type: none"> <li>- VMware ESXi 6.0 Update 2</li> <li>- VMware ESXi 6.5</li> <li>- VMware ESXi 6.5 Update 1</li> <li>- VMware ESXi 6.7</li> </ul>
Cloud management software	<ul style="list-style-type: none"> <li>- vCenter Server Appliance 6.0 Update 2</li> <li>- vCenter Server Appliance 6.5</li> <li>- vCenter Server Appliance 6.7</li> </ul>
SDS	<ul style="list-style-type: none"> <li>- VMware Virtual SAN 6.2</li> <li>- VMware Virtual SAN 6.5</li> <li>- VMware Virtual SAN 6.6</li> <li>- VMware Virtual SAN 6.6.1</li> </ul>

### Microsoft Failover Cluster

Microsoft Failover Cluster is a system configured with multiple servers that have Windows Server installed.

Cluster Management collects cluster information from the Windows Server OS to display it on the ISM GUI.

In each cluster, the "Storage Pool" virtual storage of Storage Spaces Direct is configured by aggregating the physical storages mounted on each server. The storage pool can be monitored from ISM.

The following are the requirements for Microsoft Failover Cluster environments.

Item	Requirement
OS	<ul style="list-style-type: none"> <li>- Windows Server 2016</li> <li>- Windows Server 2019</li> </ul>
Role and function	<p>The following roles and functions must be installed on the nodes configuring the cluster.</p> <ul style="list-style-type: none"> <li>- Hyper-V</li> <li>- Microsoft Failover Cluster</li> </ul>
Hypervisor	Hyper-V
SDS	Microsoft Storage Spaces Direct
Other	<ul style="list-style-type: none"> <li>- It must be possible to monitor OSEs and clusters from ISM</li> <li>- CredSSP authentication must be enabled on the nodes configuring the cluster</li> </ul>



### Note

The following is required for Microsoft Failover Cluster.

- Pre-settings to enable OS monitoring from ISM for each node
- Pre-settings to enable failover cluster monitoring from ISM.
- CredSSP authentication must be enabled on every node.

For details on how to set it, refer to "[3.9.2 Pre-settings for Microsoft Storage Spaces Direct.](#)"

For the setup procedures for the monitoring target OS, refer to the following document. For details, contact your local Fujitsu customer service partner.

"Settings for Monitoring Target OS and Cloud Management Software"

- "2.1. Setting Procedure for Windows"
- "3.2. Setting Procedure for Microsoft Failover Cluster"

## 2.12.1.3 Refreshing cluster information

If you are retrieving the virtualized platform on the ISM GUI or refreshing the displayed contents, you must refresh the information from the ISM GUI.

If you are checking the virtual resources from the Cluster Management GUI, refresh the displayed contents.

From the [Actions] button, execute [Refresh Cluster Information].

The cluster information is displayed on the ISM GUI. For the displayed information, refer to "[2.12.1.1 Cluster Management GUI.](#)"



### Point

- Since the information displayed on the GUI may be old, make sure to refresh it when checking the status of the clusters.

- The refreshed cluster information is registered in the ISM tasks.

At the top of the Global Navigation Menu on the GUI of ISM, select [Tasks], and check the tasks whose type is "Refresh Virtual Resource."

Status	Progress	Result	Task ID	Task Type	Operator	Start Time	Completion Time
Completed	1 / 1	Success	1	Refresh Virtual Resource	administrator	May 9, 2017 1:32:46 AM	May 9, 2017 1:32:50 AM

Until the status of the task becomes "Completed" the refreshing of the display has not been completed.

After checking that the status has become "Completed," refresh the ISM GUI screen (select the refresh button in the upper left part of the screen).

- The information on the GUI is automatically refreshed every day at AM 0:00 of local time.
- The statuses of the clusters displayed on the GUI are refreshed every three minutes.

## 2.12.1.4 Management and monitoring of clusters



Monitoring and operation of cluster can be executed by using Cluster Management.

The following types of monitoring can be executed using Cluster Management.

- Cluster monitoring
- Monitoring of the nodes configuring the cluster
- Monitoring of virtual resource on cluster

### Cluster monitoring

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

The list of clusters managed by ISM is displayed.

In addition to cluster statuses, the statuses of the nodes configure the cluster and storage pool configured in the cluster can be checked.

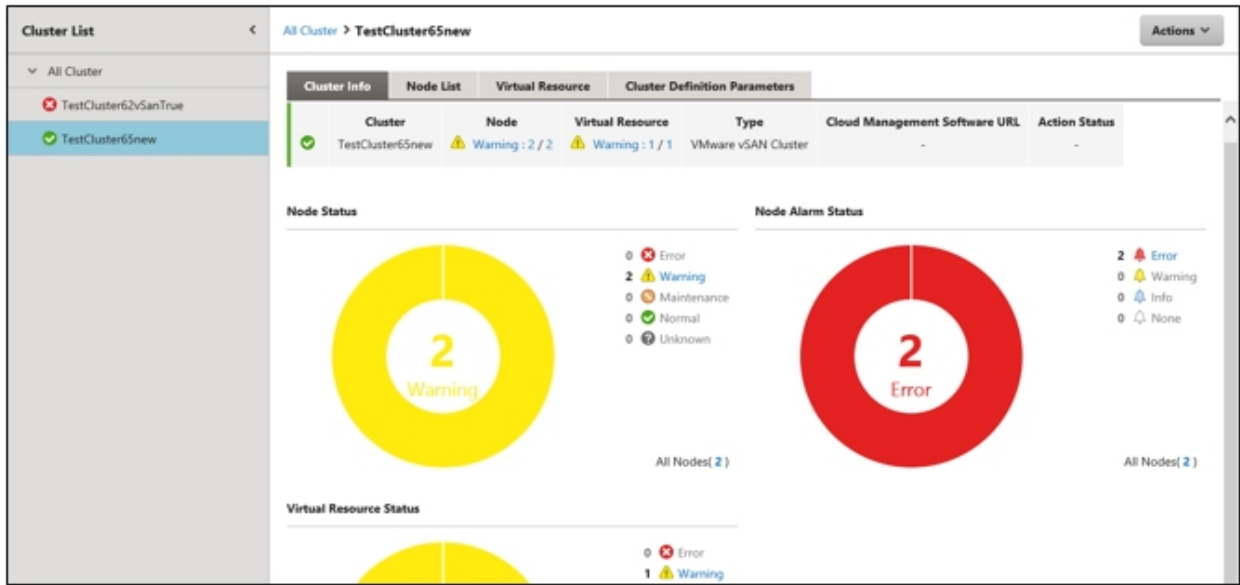
Cluster Name	Node	Virtual Resource	Type	Cloud Management Software URL	Action Status
TestCluster62vSanTrue	-	Normal : 1 / 1	VMware vSAN Cluster	-	-
TestCluster65new	Warning : 2 / 2	Warning : 1 / 1	VMware vSAN Cluster	-	-

When you select a cluster name, the display moves to the details of cluster screen.

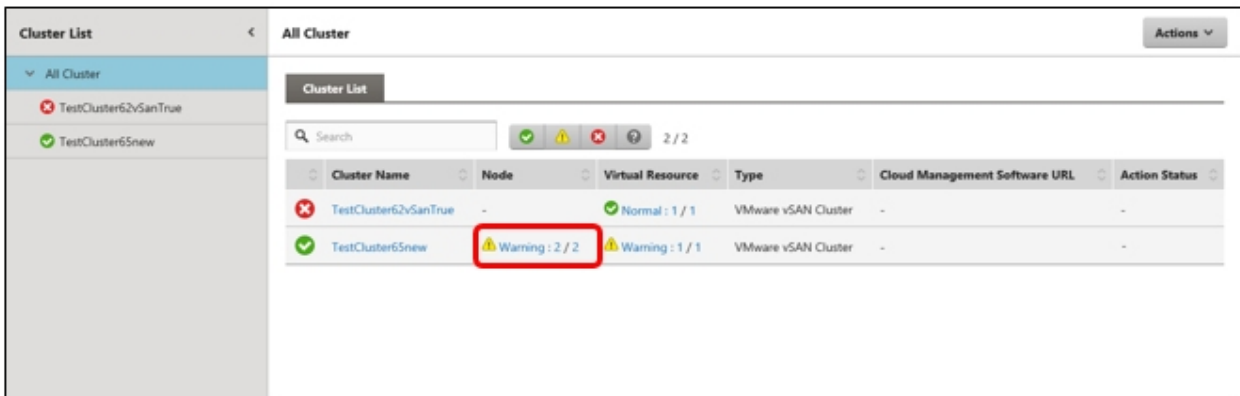
In the detailed screen, information such as summary related to the cluster ([Cluster Info] tab screen), nodes configuring the cluster, virtual resources, and Cluster Definition Parameters is displayed.

For nodes configuring the cluster, you can check the information on the [Node List] tab screen.

Moreover, storage pool configured in the cluster can be checked on the [Virtual Resource] tab screen.



In the cluster list screen, the number of errors for the nodes and virtual resources is displayed.



The number displaying the errors is displayed in the following format.

[Number of managed targets in error statuses] / [Total number of managed targets]

[Number of managed targets in error statuses] displays the number of targets in the most severe status.

The following shows the severity of error statuses.

Status	Displayed Icon	Severity	Description
Error		High	Fatal errors are occurring in the monitoring targets. This is displayed for the highest priority of all statuses.
Warning		Medium	Errors occur in the monitoring targets. This is displayed with priority if there are no "Error" targets.
Unknown		Low	The status of the monitoring targets is unknown. This is displayed with priority if there are no "Error" or "Caution" targets.
Normal		-	This is the normal state with no errors in the monitoring targets. In the "Cluster List" screen, it is displayed as "-."

When you select a number for the Nodes or the managed Virtual Resources on the Cluster List screen, you move to the tab screen display in the Cluster Details screen.

The targets in error states are filtered and displayed.

By grasping the overview of the components that configure the cluster, the error display makes it easy to determine whether cluster operation can be handled.

In addition, monitoring from Cluster Management Widget in the ISM Dashboard can be executed.

For Cluster Management Widget, refer to "[2.12.1.1 Cluster Management GUI](#)" - "[Operation in link with Dashboard](#)."

### Monitoring of the nodes configuring the cluster

When selecting the [Node List] tab, a list of the nodes that configure the cluster is displayed.

For the contents of the screen, refer to "[2.12.1.1 Cluster Management GUI](#)" - "[Node List] tab." In addition, for detailed information on displayed information, refer to the ISM online help.

For detailed information on nodes, use the node list information of ISM.

When selecting a node name, you move to the detailed screen of the node list and can check the detailed information about hardware configurations and their states. For information on the node list, refer to the ISM online help.

### Monitoring of virtual resource on cluster

When selecting the [Virtual Resource] tab, SDS storage pool configured in the cluster is displayed.

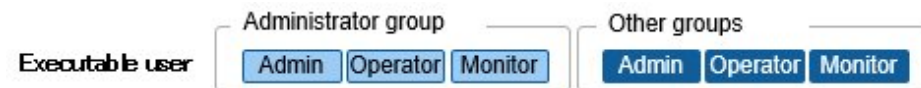
Information such as storage pool states, storage utilization and so on is displayed.

For the contents of the screen, refer to "[2.12.1.1 Cluster Management GUI](#)" - "[Virtual Resource] tab." In addition, for detailed information on displayed information, refer to the ISM online help.

When selecting a storage pool name, you move to the detailed screen of the virtual resource GUI and can check the detailed information about the storage pool.

For virtual resource monitoring, refer to "[2.9 Virtual Resource Management](#)."

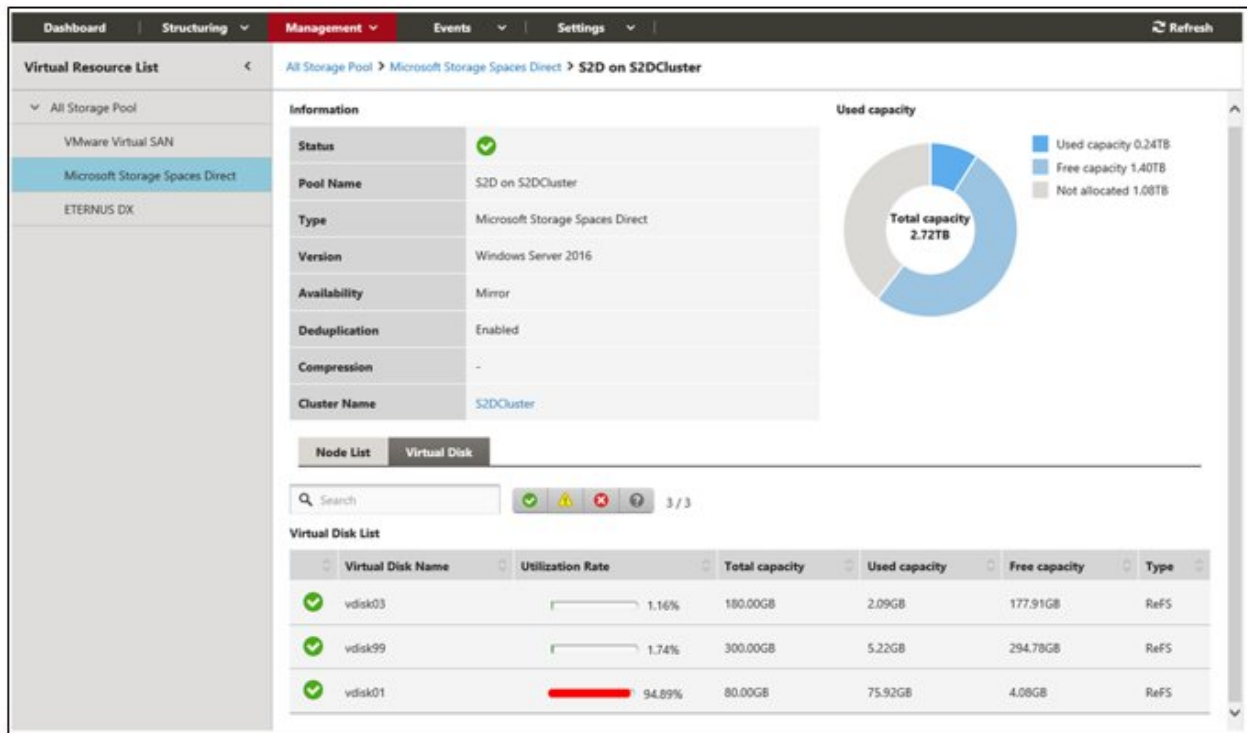
### 2.12.1.5 Virtual disk monitoring for PRIMEFLEX for Microsoft Storage Spaces Direct



Selecting a pool name on the Virtual Resources Management GUI displays the Detailed Information screen, where you can check the currently used capacity and available capacity in [Used capacity].

For details on how to use the Virtual Resources Management GUI, refer to "[2.9 Virtual Resource Management](#)."

For PRIMEFLEX for Microsoft Storage Spaces Direct, in addition to the capacity information of the storage pools you can also check the capacity information of the virtual disks created on the storage pools.



The meaning of the capacity information displayed in the Storage Spaces Direct utilization status circle diagram is described below.

- Used capacity: Displays the total used capacity of the virtual disks created on the storage pool.
- Free capacity: Displays the total free capacity of the virtual disks created on the storage pool.
- Not allocated: Displays the capacity that has not been allocated to a storage pool or where virtual disks have not been created.

Also, if you select the [Virtual Disk] tab, a list of the disks that exist on the storage pools and their used capacity and other information is displayed.

For details on the displayed contents, refer to the ISM online help.

## Point

The redundancy set up for the virtual disks is reflected in the capacity information in the [Virtual Disk] tab.

The capacity value displayed in the Used capacity circle diagram takes the redundancy of the capacity of each virtual disk into account.

## 2.12.2 Cluster Creation

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

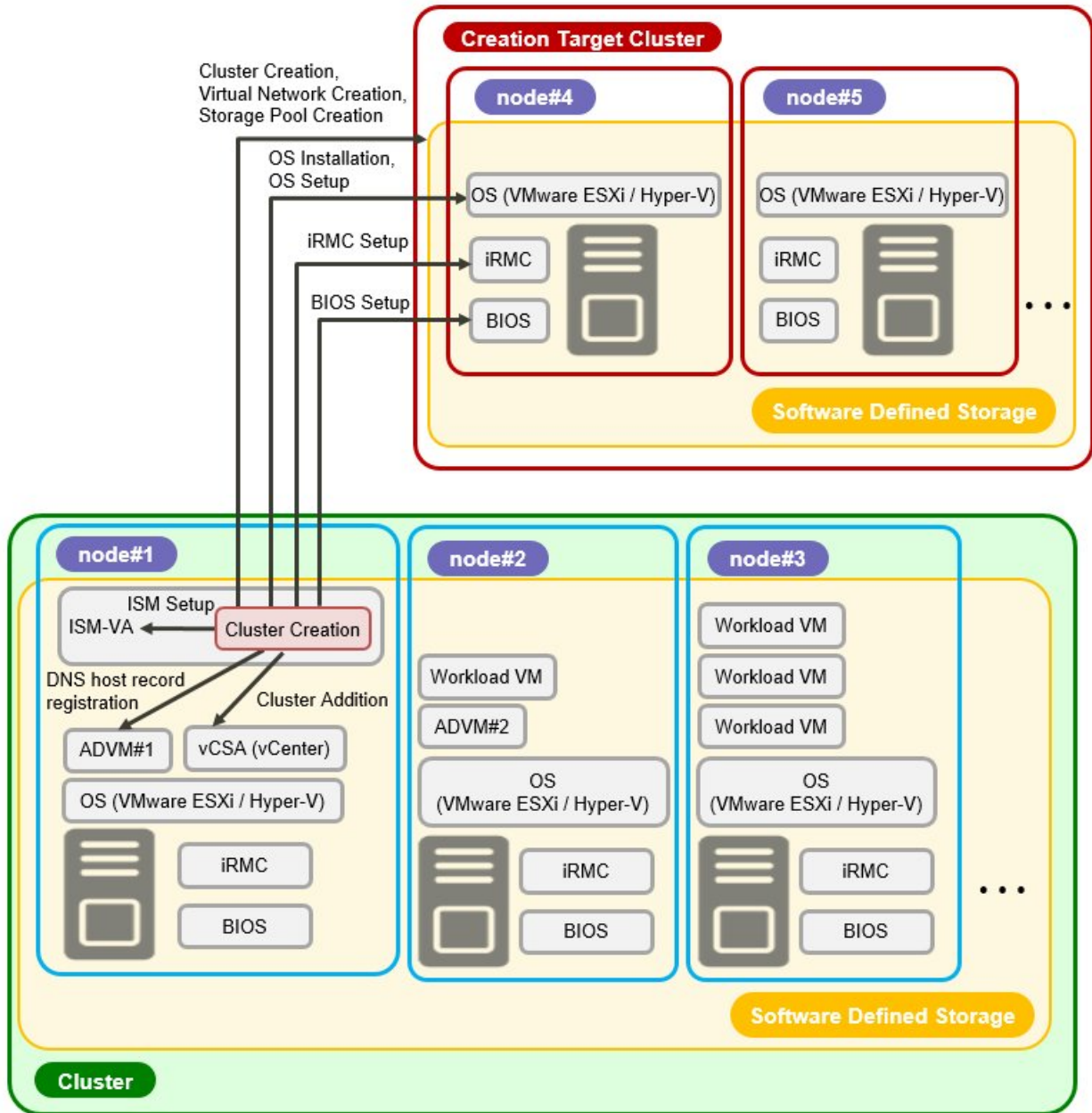
Cluster Creation is a function that creates new clusters to expand the resources of the virtual platform environments of the PRIMEFLEX HS/PRIMEFLEX for VMware vSAN and PRIMEFLEX for Microsoft Storage Spaces Direct. This function links with Profile Management of ISM and reduces the workload of the user by automatizing the operations from the cluster creation and installing an OS on the target server and adding it to the cluster.

Cluster Creation is a function that is mainly used for the following purposes:

- Creation of new clusters
- Creation of virtual networks for the new clusters
- Creation of storage pools for the new clusters
- Installation and setup of the OS of the servers for creating new clusters
- Addition of servers for creating a new cluster to the new clusters



Figure 2.21 Overview of Cluster Creation



### 2.12.2.1 Automatic setting item

By using Cluster Creation, the following items are set automatically.

Table 2.6 PRIMEFLEX for VMware vSAN automatic setting item list

Automatic setting item	Description
OS installation	<ul style="list-style-type: none"> <li>- Install the OS of the servers for creating a new cluster</li> <li>- Execute the system date and time settings for the servers for creating a new cluster</li> <li>- Apply VMware SMIS Provider file to the servers for creating a new cluster</li> <li>- Apply the OS patches for the servers for creating a new cluster</li> </ul>
DNS host record registration	<ul style="list-style-type: none"> <li>- Register DNS for the ESXi servers for creating a new cluster (Do not register when using a configuration that does not use the ADVM of the PRIMEFLEX configuration)</li> </ul>
OS settings	<ul style="list-style-type: none"> <li>- Enable and start ESXi shell</li> </ul>

Automatic setting item	Description
	<ul style="list-style-type: none"> <li>- Enable and start SSH service</li> <li>- Apply VMware SMIS Provider (Only set for PRIMERGY M4 series and VMware ESXi 6.5)</li> <li>- Enable ixgben driver (Only set for PRIMERGY M4 series, VMware ESXi 6.5 and VMware ESXi 6.5 Update 1)</li> <li>- Add local administrator users</li> <li>- Set host name to FQDN</li> <li>- Enable SSL v3</li> <li>- Disable IPv6</li> <li>- Set IP address for secondary DNS servers</li> <li>- Set DNS suffix</li> <li>- Set IP address for NTP server</li> <li>- Set firewall for NTP client</li> <li>- Execute NTP client service</li> <li>- Set the power management settings of the host to high performance</li> <li>- Restart OS</li> <li>- Add adapter to virtual distributed switch (virtual distributed switch for workload/virtual distributed switch for management)</li> <li>- Set NIC to virtual distributed switch (virtual distributed switch for workload/virtual distributed switch for management)</li> <li>- Set NIC to Management Network</li> <li>- Set Active Directory authentication settings for ESXi of the servers for creating a new cluster (Do not set if you are not using PRIMEFLEX configuration ADVN or AD link using AD server in your environment)</li> <li>- Disable and stop ESXi shell</li> <li>- Disable and stop SSH service</li> </ul>
iRMC Settings	<ul style="list-style-type: none"> <li>- Create local users (pflocaladmin)</li> <li>- Change admin user password</li> <li>- Set Active Directory authentication settings for iRMC of the servers for creating a new cluster (Do not set if you are not using PRIMEFLEX configuration ADVN or AD link using AD server in your environment)</li> <li>- Reset the iRMC for the servers for creating a new cluster</li> </ul>
Add servers to the cluster	<ul style="list-style-type: none"> <li>- Register the servers for creating a new cluster to the virtual distributed switch for management</li> <li>- Register the servers for creating a new cluster to the virtual distributed switch for workload</li> <li>- Execute the settings for the virtual distributed switch</li> <li>- Set up the capacity device of SSD (When using an All Flash environment)</li> <li>- Add the servers for creating a new cluster to the cluster</li> </ul>
ISM settings	<ul style="list-style-type: none"> <li>- Change the password of the admin user of iRMC registered in ISM</li> <li>- Change the Web interface URL of iRMC registered in ISM</li> <li>- Set the collection targets and collection date and time for ISM Log Management</li> </ul>

Automatic setting item	Description
Cluster Creation	- Create a cluster
Virtual Network creation	<ul style="list-style-type: none"> <li>- Create virtual distributed switch (virtual distributed switch for workload/virtual distributed switch for management)</li> <li>- Enable NIOC</li> <li>- Create and set port groups</li> <li>- Set up NIOC of the virtual distributed switch (virtual distributed switch for workload/virtual distributed switch for management)</li> </ul>
Storage pool creation	<ul style="list-style-type: none"> <li>- Enable vSAN</li> <li>- Set deduplication and compression</li> </ul>
Refresh Virtual Resource	- Refresh Cluster Information

Table 2.7 PRIMEFLEX for Microsoft Storage Spaces Direct automatic setting items list

Automatic setting item	Description
OS installation	- Install the OS of the servers for creating a new cluster
OS settings	<ul style="list-style-type: none"> <li>- Enable the remote connection function</li> <li>- Enable Basic authentication</li> <li>- Enable CredSSP authentication</li> <li>- Register root certificates (cer file), personal certificate (pfx file) prepared in advance</li> <li>- Set https listeners</li> <li>- Open port for https listeners</li> <li>- Create local user (pflocaladmin)</li> <li>- Execute the settings for the servers for creating a new cluster <ul style="list-style-type: none"> <li>- Install Hyper-V</li> <li>- Set MAC address range</li> <li>- Install Windows Server back up</li> <li>- Install a failover cluster</li> <li>- Create virtual switches</li> <li>- Create VM network adapter</li> <li>- Set VLAN for the VM network adapter</li> <li>- Switch over the network adapter of management LAN</li> <li>- Disable IPv6</li> <li>- Set Prioritized DNS server</li> <li>- Set Alternative DNS server</li> <li>- Disable SR/IOV for the Intel, Mellanox LAN driver</li> <li>- Enable VMQ for the Intel, Mellanox LAN driver</li> <li>- Set VMQ for the management LAN port</li> <li>- Set VMQ for the production LAN port</li> <li>- Disable QoS for the Intel, Mellanox LAN driver</li> </ul> </li> </ul>
iRMC settings	- Create local users (pflocaladmin)

Automatic setting item	Description
	<ul style="list-style-type: none"> <li>- Change the admin user password</li> <li>- Set Active Directory authentication of iRMC for the servers creating a new cluster.</li> <li>- Reset the iRMC for the servers for creating a new cluster</li> </ul>
Add servers to the cluster	<ul style="list-style-type: none"> <li>- Add the servers for creating a new cluster to the failover cluster</li> </ul>
ISM settings	<ul style="list-style-type: none"> <li>- Change the password of the admin user of iRMC registered in ISM</li> <li>- Change the Web interface URL of iRMC registered in ISM</li> <li>- Change the account of the OS registered in ISM.</li> <li>- Set the collection targets and collection date and time for ISM Log Management</li> </ul>
Cluster Creation	<ul style="list-style-type: none"> <li>- Verify a cluster</li> <li>- Create a cluster</li> </ul>
Virtual Network creation	<ul style="list-style-type: none"> <li>- Execute cluster network settings</li> </ul>
Kerberos delegation configuration	<ul style="list-style-type: none"> <li>- Add SPN to the Active Directory</li> <li>- Configure Kerberos delegation to the Active Directory</li> </ul>
Storage pool creation	<ul style="list-style-type: none"> <li>- Enable Storage Spaces Direct</li> <li>- Execute Journal Settings for the virtual disk</li> <li>- Execute the Storage Tier Settings</li> </ul>
Refresh Virtual Resource	<ul style="list-style-type: none"> <li>- Add CMS information</li> </ul>

## 2.12.2.2 Link with Profile Management

Profile Management in ISM executes the hardware settings (BIOS, iRMC) and OS installation settings for the server.

Cluster Creation links with Profile Management and automates the cluster creation process.

By selecting profile created in advance from the "Create Cluster" wizard, profiles can be assigned and hardware settings and OS installation can be done when executing Cluster Creation.

After profile assignment has been completed, the OS setup script is executed by the "Executing Script after Installation," which is a function of Profile Management. Afterward, execute the server registration process of the servers for creating a new cluster.



### Point

The OS setup script is a script that executes the settings required to connect to the OS of the servers for creating a new cluster during the Cluster Creation processing.

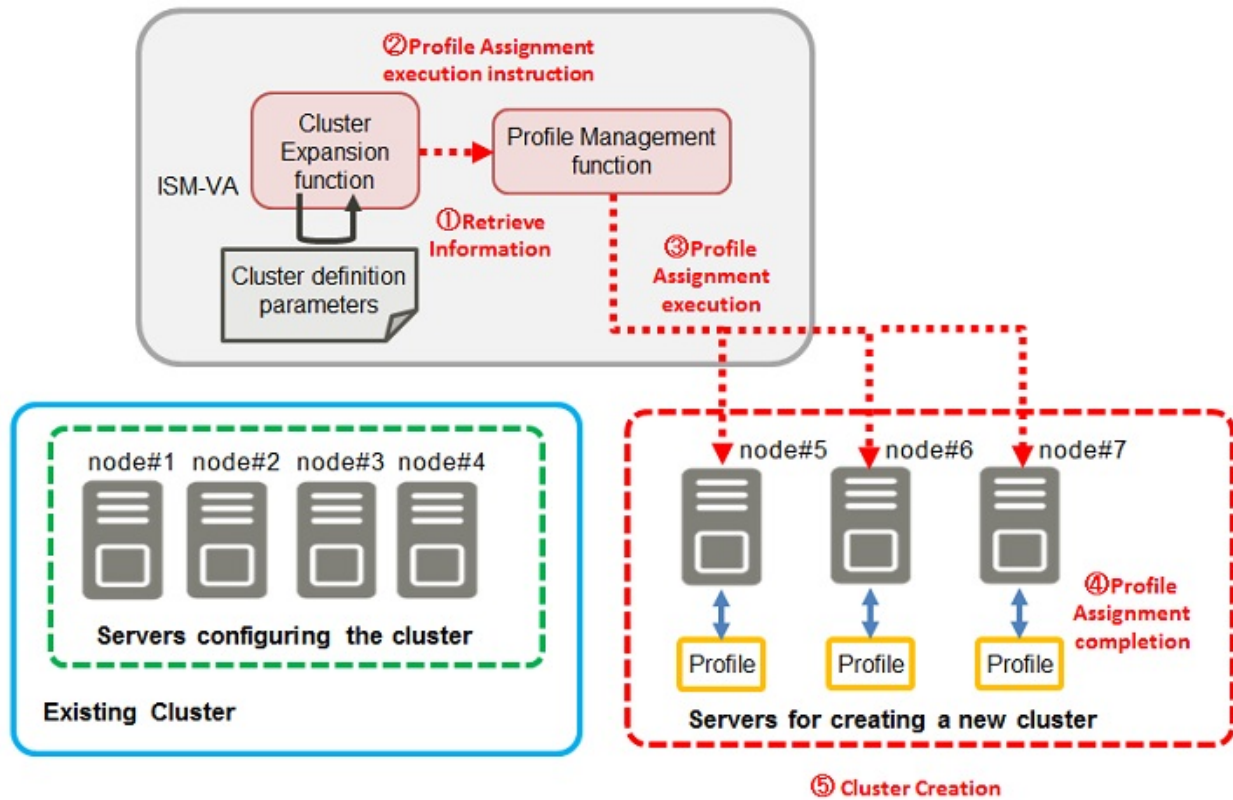


### Note

- Before executing Cluster Creation, create profiles in advance.
- The OS setup script used by Execute Script after Installation is automatically specified when executing Cluster Creation. During profile creation, do not specify anything in "Executing Script after Installation." If it is specified, it will be overwritten by the OS setup script when executing Cluster Creation.

A relation diagram of Cluster Creation and Profile Management is shown below.

Figure 2.22 Operation in link with Cluster Creation and Profile Management



### 2.12.2.3 Cluster Definition Parameters

The Cluster Definition Parameters are the parameters used when executing Cluster Creation. The setting information for the new clusters or nodes configuring clusters can be retained. When creating clusters, enter the parameters for the part of the new cluster and execute.

If you want to store Cluster Definition Parameters in a device external to ISM (Management terminal), for example, you can export/import Cluster Definition Parameters as a text file written in JSON format. For detailed procedures, refer to "6.11 Export/Import/Delete Cluster Definition Parameters" in "Operating Procedures."

#### Note

If you import and use Cluster Definition Parameters, you need to edit them.

For details of the Cluster Definition Parameters, refer to "ISM for PRIMEFLEX Parameter List."

### 2.12.2.4 Task list

Cluster Creation is executed from the "Create Cluster" wizard. The processing of the cluster creation is registered as an ISM task. Confirm the current status of the task on the "Tasks" screen.

From the top of the Global Navigation Menu on the ISM GUI, select [Tasks] and Task List will be displayed in the "Tasks" screen. The task name of Cluster Creation is "Cluster Creation." From the task list when selecting the [Task ID] whose task type is "Cluster Creation," then the task information and subtask list are displayed in the "Tasks" screen. The subtask lists are displayed for each server configuring a new cluster.

Each processing name displayed in the message column of the subtask list in the following format and its implemented contents are shown below.

```
<Processing name>:<Setting item name>
```

Table 2.8 PRIMEFLEX for VMware vSAN subtask processing list

Processing name	Implemented contents
Prep Check	Check the execution requirements for creating a new cluster.
OS Installation	Install the OS of the server for creating a new cluster.
DNS Settings	Register the DNS host record of the server for creating a new cluster.
iRMC Settings	Execute the iRMC settings and the ISM settings for the server for creating a new cluster.
OS Settings	Execute the OS settings for the server for creating a new cluster.
Cluster Settings	Execute the cluster settings (first half settings) for the server for creating a new cluster.
Ism Settings	Execute the ISM settings for the server for creating a new cluster.
Cluster Creation	Create a new cluster.
Virtual Network Creation	Create a virtual network of the new cluster.
Storage Pool Creation	Create a storage pool of the new cluster.
Cluster Settings	Execute the cluster settings (second half settings) for the servers for creating a new cluster.
Cluster Post Settings	Execute the cluster settings (post-settings) for the servers for creating a new cluster.
ResourceList Registration	Refresh the new cluster Information
ESXi Host Post Settings	Execute the OS settings (post-settings) for the server for creating a new cluster.

Refer to "[Table 2.6 PRIMEFLEX for VMware vSAN automatic setting item list](#)" for the implemented contents.

Table 2.9 PRIMEFLEX for Microsoft Storage Spaces Direct subtask processing list

Processing name	Implemented contents
Prep Check	Check the execution requirements for creating a new cluster.
OS Installation	Install the OS of the server for creating a new cluster.
iRMC Settings	Execute the iRMC settings and the ISM settings for the server for creating a new cluster.
OS Settings	Execute the OS settings for the server for creating a new cluster.
Cluster Settings	Execute the cluster settings for the server for creating a new cluster.
Ism Settings	Execute the ISM settings for the server for creating a new cluster.
Cluster Creation	Create a new cluster.
Virtual Network Creation	Create a virtual network for the new cluster.
Kerberos Delegation	Configure the Kerberos delegation for the new cluster.
Storage Pool Creation	Create a storage pool of the new cluster.
ResourceList Registration	Refresh the new cluster Information

Refer to "[Table 2.7 PRIMEFLEX for Microsoft Storage Spaces Direct automatic setting items list](#)" for the implemented contents.

## 2.12.3 Cluster Expansion

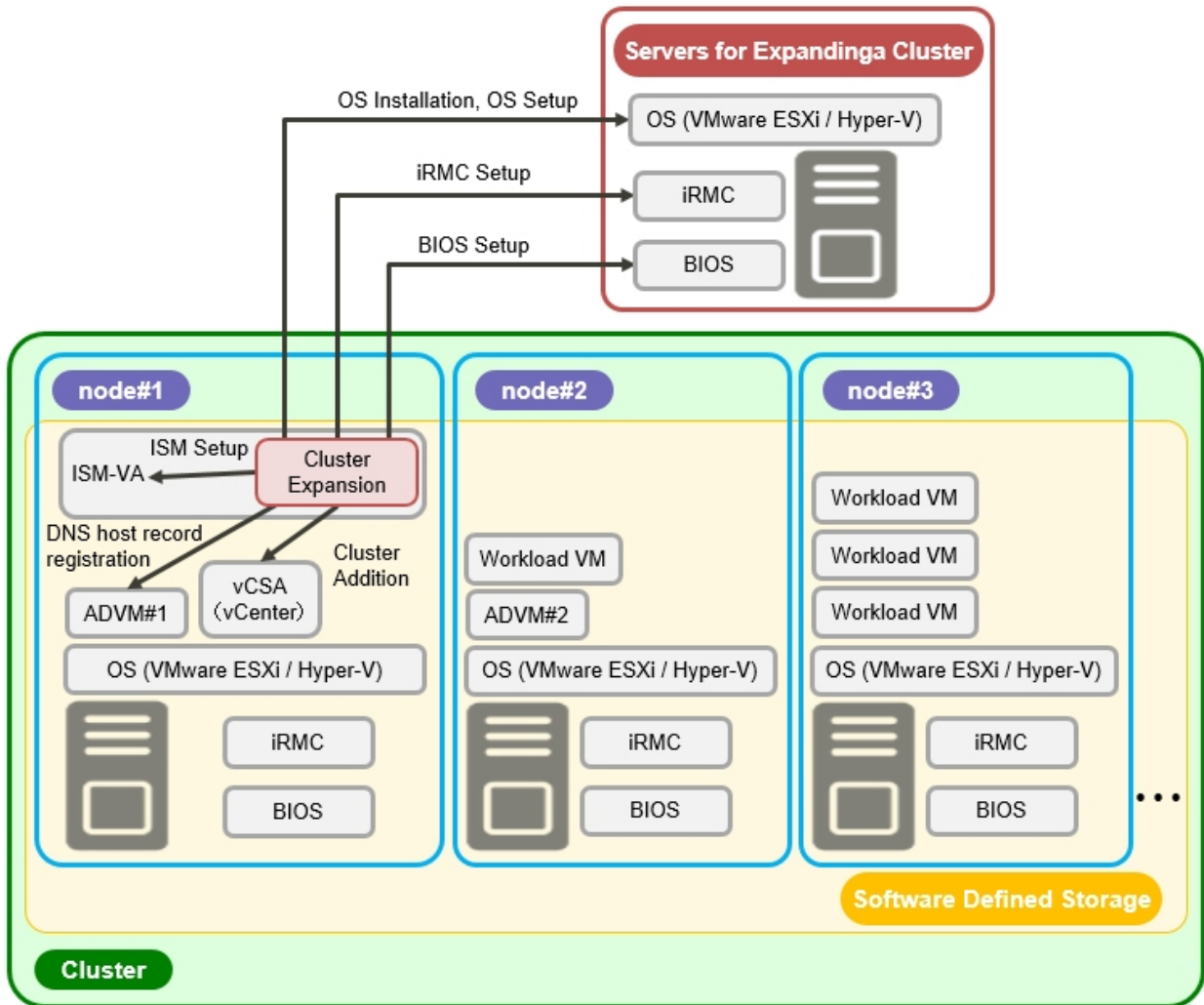
This function can be used only with the license for ISM for PRIMEFLEX.

Cluster Expansion is a function that increases the resources by adding new servers to the PRIMEFLEX HS/PRIMEFLEX for VMware vSAN or PRIMEFLEX for Microsoft Storage Spaces Direct virtual platforms when the storage resources of VMware vSAN or Microsoft Storage Spaces Direct are being depleted. This function links with Profile Management of ISM and reduces the workload of the user by automatizing the operations from installing an OS on the target server to adding it to the cluster.

Cluster Expansion is a function that is mainly used for the following purposes:

- Installing and setting up OS on the server for expanding a cluster.
- Adding the servers for expanding a cluster to the existing cluster

Figure 2.23 Overview of Cluster Expansion



### 2.12.3.1 Automatic setting item

By using Cluster Expansion, the following items are set automatically.

Table 2.10 PRIMEFLEX HS/PRIMEFLEX for VMware vSAN automatic setting items list

Automatic setting item	Description
OS installation	<ul style="list-style-type: none"> <li>- Install OS on the servers for expanding a cluster</li> <li>- Execute the system date and time settings for the servers for expanding a cluster</li> <li>- Apply the OS patches for the servers for expanding a cluster</li> </ul>
DNS host record registration	<ul style="list-style-type: none"> <li>- Register DNS for the ESXi servers for expanding a cluster (Do not register if the configuration does not use ADVM of PRIMEFLEX configuration)</li> </ul>
OS settings	<ul style="list-style-type: none"> <li>- Enable and start ESXi shell</li> <li>- Enable and start SSH service</li> <li>- Apply VMware SMIS Provider (Only set for PRIMERGY M4 series and VMware ESXi 6.5)</li> <li>- Enable ixgben driver (Only set for PRIMERGY M4 series, VMware ESXi 6.5 and VMware ESXi 6.5 Update 1)</li> <li>- Add local administrator users</li> </ul>

Automatic setting item	Description
	<ul style="list-style-type: none"> <li>- Set host name to FQDN</li> <li>- Enable SSL v3</li> <li>- Disable IPv6</li> <li>- Set IP address for secondary DNS servers</li> <li>- Set DNS suffix</li> <li>- Set IP address for NTP server</li> <li>- Set firewall for NTP client</li> <li>- Execute NTP client service</li> <li>- Set the power management settings of the host to high performance</li> <li>- Restart OS</li> <li>- Add adapter to virtual distributed switch (virtual distributed switch for workload/virtual distributed switch for management)</li> <li>- Set NIC to virtual distributed switch (virtual distributed switch for workload/virtual distributed switch for management)</li> <li>- Set NIC to Management Network</li> <li>- Set Active Directory authentication settings for ESXi of the servers for expanding a cluster (Do not set if you are not using PRIMEFLEX configuration ADVN or AD link using AD server in your environment)</li> </ul>
iRMC Settings	<ul style="list-style-type: none"> <li>- Create local users (pfllocaladmin)</li> <li>- Change admin user password</li> <li>- Set Active Directory authentication settings for iRMC of the servers for expanding a cluster (Do not set if you are not using PRIMEFLEX configuration ADVN or AD link using AD server in your environment)</li> <li>- Reset the iRMC settings of the servers for expanding a cluster</li> </ul>
Add servers to the cluster	<ul style="list-style-type: none"> <li>- Register the servers for expanding a cluster to the virtual distributed switch for management</li> <li>- Register the servers for expanding a cluster to the virtual distributed switch for workload</li> <li>- Execute the settings for the virtual distributed switch</li> <li>- Set capacity device of SSD (when using an All Flash environment)</li> <li>- Add the servers for expanding a cluster to the cluster</li> </ul>
ISM settings	<ul style="list-style-type: none"> <li>- Change the password of the admin user of iRMC registered in ISM</li> <li>- Change the Web interface URL of iRMC registered in ISM</li> <li>- Set the collection targets and collection date and time for ISM Log Management</li> </ul>

Table 2.11 PRIMEFLEX for Microsoft Storage Spaces Direct automatic setting item list

Automatic setting item	Description
OS installation	<ul style="list-style-type: none"> <li>- Install OS on the servers for expanding a cluster.</li> </ul>
OS settings	<ul style="list-style-type: none"> <li>- Enable the remote connection function</li> <li>- Enable Basic authentication</li> <li>- Enable CredSSP authentication</li> </ul>



Automatic setting item	Description
	<ul style="list-style-type: none"> <li>- Register root certificates (cer file), personal certificate (pfx file) prepared in advance</li> <li>- Set https listeners</li> <li>- Open port for https listeners</li> <li>- Create local user (pflocaladmin)</li> <li>- Execute the settings for the servers for expanding a cluster               <ul style="list-style-type: none"> <li>- Install Hyper-V</li> <li>- Set MAC address scope</li> <li>- Install Windows Server back up</li> <li>- Install failover cluster</li> <li>- Create virtual switches</li> <li>- Create VM network adapter</li> <li>- Set VLAN for the VM network adapter</li> <li>- Switch over the network adapter of management LAN</li> <li>- Disable IPv6</li> <li>- Set Prioritized DNS server</li> <li>- Set Alternative DNS server</li> <li>- Enable VMQ for the Intel, Mellanox LAN driver</li> <li>- Disable SR/IOV for the Intel, Mellanox LAN driver</li> <li>- Set VMQ for the management LAN port</li> <li>- Set VMQ for the production LAN port</li> <li>- Disable QoS for the Intel, Mellanox LAN driver</li> </ul> </li> </ul>
iRMC settings	<ul style="list-style-type: none"> <li>- Create local user (pflocaladmin)</li> <li>- Change admin user password</li> <li>- Set Active Directory authentication of iRMC for the servers for expanding a cluster.</li> </ul>
Add servers to the cluster	<ul style="list-style-type: none"> <li>- Add the servers for expanding a cluster to the failover cluster</li> </ul>
ISM settings	<ul style="list-style-type: none"> <li>- Change the password of the admin user of iRMC registered in ISM</li> <li>- Change the Web interface URL of iRMC registered in ISM</li> <li>- Change the account of the OS registered in ISM.</li> <li>- Set the collection targets and collection date and time for ISM Log Management</li> </ul>

### 2.12.3.2 Link with Profile Management

Cluster Expansion links with Profile Management and automatizes the expansion process.

By selecting profile created in advance from the "Expand Cluster" wizard, profiles can be assigned and hardware settings and OS installation can be executed when executing Cluster Expansion.

After profile assignment has been completed, the OS setup script is executed by the "Executing Script after Installation," which is a Profile Management function. Afterward, execute the registration process of the servers for expanding a cluster for the target cluster.

## Point

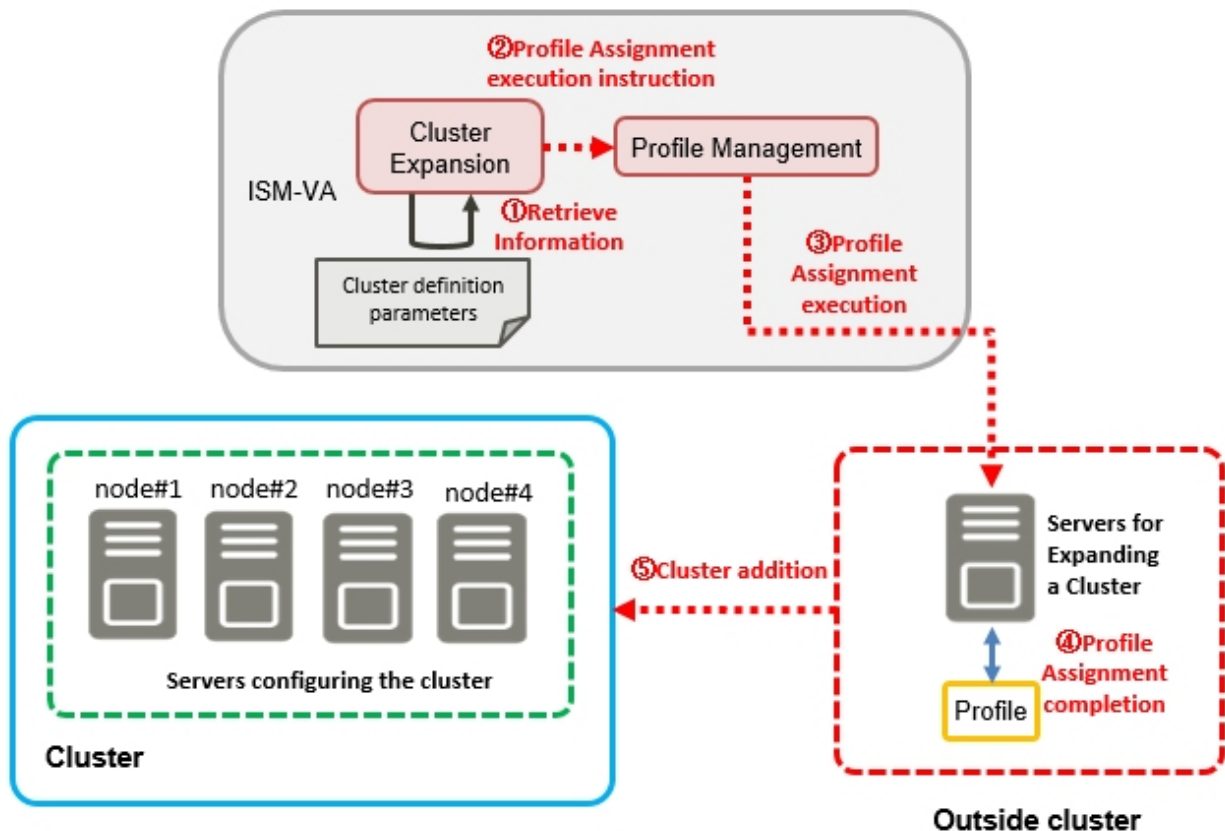
The OS setup script is a script that executes the settings required to connect to the OS of the servers for expanding a cluster during the Cluster Expansion processing.

## Note

- Create the policies before executing Cluster Expansion.
- The OS setup script used in Executing Script after Installation is specified automatically when executing Cluster Expansion. When creating profiles, do not specify anything in the "Executing Script after Installation" item. If it is specified, it will be overwritten by the OS setup script during the cluster expansion.

The relation diagram of Cluster Expansion and Profile Management is displayed.

Figure 2.24 Operation in link with Cluster Expansion and Profile Management



### 2.12.3.3 Cluster Definition Parameters

The Cluster Definition Parameters are the parameters used when executing Cluster Expansion. The setting information for the clusters or nodes configuring clusters to be expanded. Enter the parameters for the parts of the servers for expanding a cluster and execute.

If you want to store Cluster Definition Parameters in a device external to ISM (Management terminal), for example, you can export/import Cluster Definition Parameters as a text file written in JSON format. For detailed procedures, refer to "6.11 Export/Import/Delete Cluster Definition Parameters" in "Operating Procedures."

## Note

If you import and use Cluster Definition Parameters, you need to edit them.

For details of the Cluster Definition Parameters, refer to "ISM for PRIMEFLEX Parameter List."

### 2.12.3.4 Task list

Cluster Expansion is executed from the "Expand Cluster" wizard. The processing of the cluster expansion is registered as an ISM task. Confirm the current status of the task on the "Tasks" screen.

From the top of the Global Navigation Menu on the ISM GUI, select [Tasks] and Task List will be displayed in the "Tasks" screen. The task name of Cluster Expansion is "Cluster Expansion." From the task list when selecting [Task ID] whose task type is "Cluster Expansion," the task information and subtask list are displayed in the "Tasks" screen. The subtask lists are displayed for each server configuring a new cluster.

Each processing name displayed in the message column of the subtask list in the following format and its implemented contents are shown below.

<Processing name>:<Setting item name>

Table 2.12 PRIMEFLEX HS/PRIMEFLEX for VMware vSAN subtask processing list

Processing name	Implemented contents
Prep Check	Check the execution requirements for expanding a cluster.
OS Installation	Install an OS on the servers for expanding a cluster.
DNS Settings	Register DNS host record on the servers for expanding a cluster.
iRMC Settings	Execute the iRMC settings and ISM settings for the servers for expanding a cluster.
OS Settings	Execute the OS settings and ISM settings for the servers for expanding a cluster.
Cluster Settings	Execute the cluster settings for the servers for expanding a cluster.
Ism Settings	Execute the ISM settings for the servers for expanding a cluster.
ESXi Host Post Settings	Execute the OS settings (post-settings) for the servers for expanding a cluster.

Refer to "[Table 2.10 PRIMEFLEX HS/PRIMEFLEX for VMware vSAN automatic setting items list](#)" for the implemented contents.

Table 2.13 PRIMEFLEX for Microsoft Storage Spaces Direct subtask processing list

Processing name	Implemented contents
Prep Check	Check the execution requirements for expanding a cluster.
OS Installation	Install an OS on the servers for expanding a cluster.
iRMC Settings	Execute the iRMC settings and ISM settings for the servers for expanding a cluster.
OS Settings	Execute the OS settings and ISM settings for the servers for expanding a cluster.
Cluster Settings	Execute the cluster settings for the servers for expanding a cluster.
Ism Settings	Execute the ISM settings for the servers for expanding a cluster.

Refer to "[Table 2.11 PRIMEFLEX for Microsoft Storage Spaces Direct automatic setting item list](#)" for the implemented contents.

## 2.12.4 Firmware Rolling Update

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

Firmware Rolling Update is a function that uses the vMotion of the virtual machines on the nodes configuring the virtualized platform, or uses Live Migration (PRIMEFLEX for Microsoft Storage Spaces Direct) to execute Firmware Rolling Update without stopping operations.

This function reduces the workload of the customer by linking with Firmware Management of ISM and updating the firmware of all servers configuring the clusters.

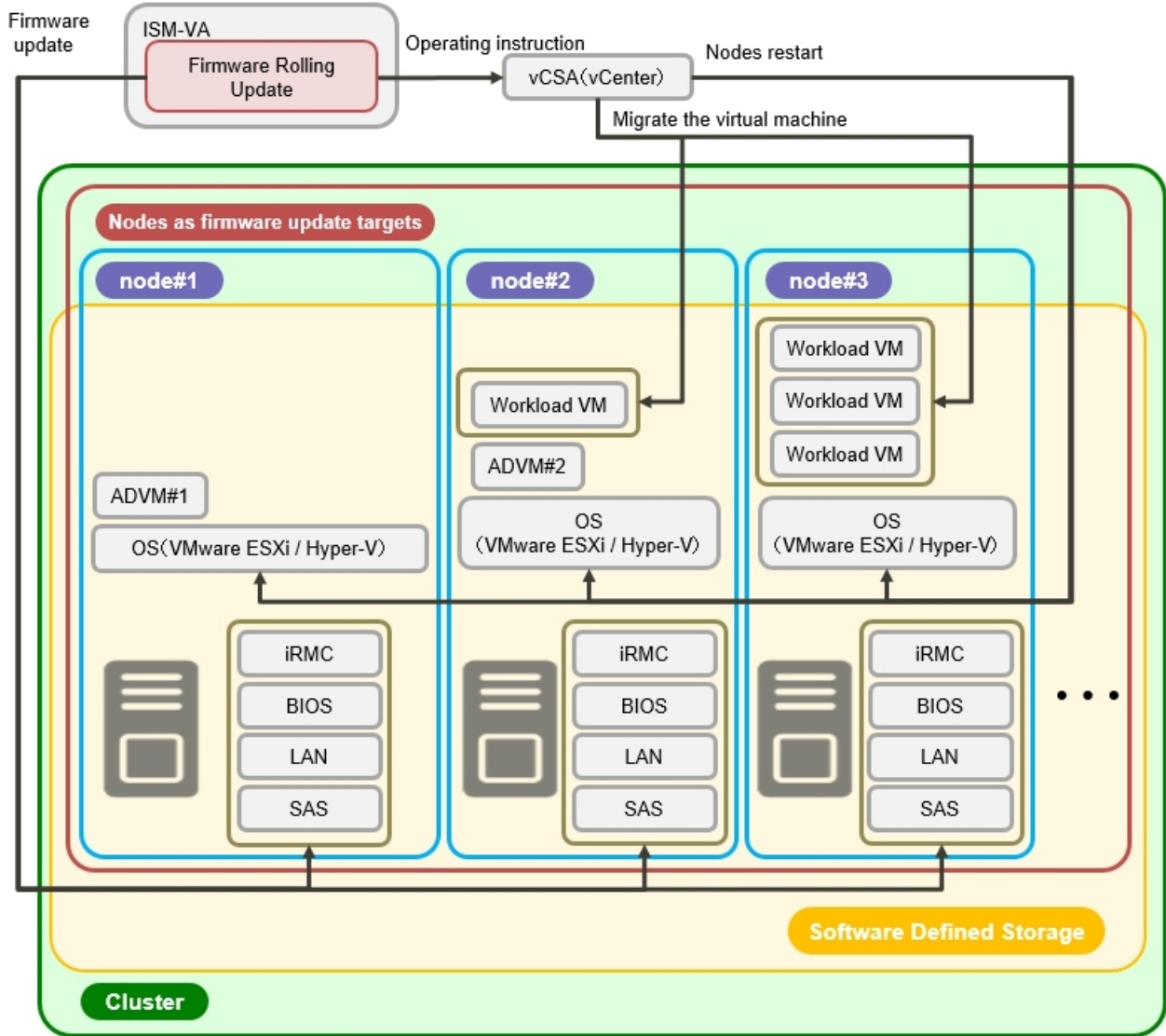
 Note

Before executing Firmware Rolling Update, you must select an evacuation server from the target cluster for the virtual machine.

The following is the firmware data supported by Firmware Rolling Update.

Type	Update Method
Server (iRMC)	Online Update
Server (BIOS)	Online Update

Figure 2.25 Overview of Firmware Rolling Update



### 2.12.4.1 Operation in link with Firmware Management

Firmware Rolling Update operates in link with Firmware Management and automatizes Firmware Rolling Update.

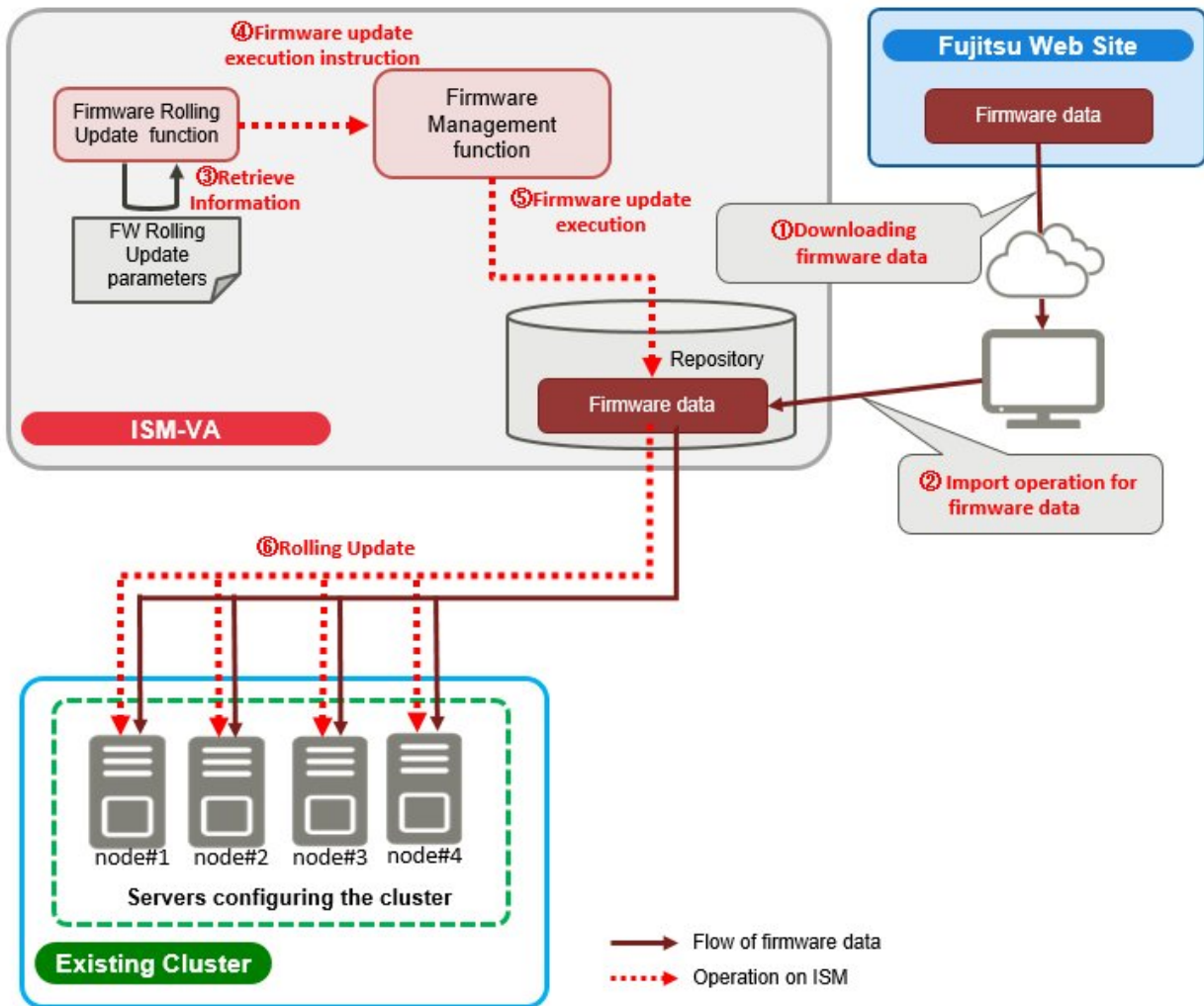
Among the firmware data imported in advance, the latest firmware will be applied.

## Note

- Before executing Firmware Rolling Update, import the firmware data into ISM.  
For the firmware data import, refer to "2.13.2 Repository Management."
- Even when there are some nodes on which Update Firmware of Firmware Management ends in an error, nodes updated normally will be rebooted and the firmware will be applied.

The following chart shows the relationship between Firmware Rolling Update and Firmware Management.

Figure 2.26 Relationship between Firmware Rolling Update and Firmware Management



### 2.12.4.2 Task list

Firmware Rolling Update is executed from the "FW Rolling Update" wizard. The processing of the Firmware Rolling Update is registered as an ISM task. Confirm the current status of the task on the "Tasks" screen.

From the top of the Global Navigation Menu on the ISM GUI, select [Tasks] and Task List will be displayed in the "Tasks" screen. The task name of Firmware Rolling Update is "Firmware Rolling Update." From the task list, when selecting the [Task ID] whose task type is "Firmware Rolling Update," the task information and subtask list are displayed on the "Tasks" screen. The subtask list is displayed for every Firmware Update target node.

Each processing name displayed in the message column of the subtask list in the following format and its implemented contents are shown below.

<Processing name>:<Setting item name>

Table 2.14 Online update subtask processes list

Processing name	Setting item name	Setting item contents
Firmware Rolling Update (Execute firmware update on the firmware update target nodes and restart of them)	<ol style="list-style-type: none"> <li>1. Prep Check</li> <li>2. Migrate VM to Another Node &amp; Set Maintenance Mode</li> <li>3. Migrate VM to Another Node &amp; Set Maintenance Mode</li> <li>4. Update Firmware (online)</li> <li>5. Shutdown Node</li> <li>6. Boot Node</li> <li>7. Unset Maintenance Mode &amp; Migrate VM to Target Node</li> <li>8. Unset Maintenance Mode &amp; Migrate VM to Target Node</li> <li>9. Post Check</li> </ol>	<ol style="list-style-type: none"> <li>1. Check the conditions for executing Firmware Rolling Update</li> <li>2. Migrate the node running on the target node to the evacuation node [Note 1]</li> <li>3. Set the node to Maintenance Mode</li> <li>4. Apply the firmware data Online</li> <li>5. Shutdown the node</li> <li>6. Start the node</li> <li>7. Release the Maintenance Mode of the node</li> <li>8. Return the node migrated to the evacuation node to the target node [Note 1]</li> <li>9. Check the post-requirements of Firmware Rolling Update</li> </ol>
Refresh Resource Information (Retrieves cloud management software information and node information)	<ol style="list-style-type: none"> <li>1. Refresh Resource Informations</li> <li>2. Refresh Virtual Inventory</li> </ol>	<ol style="list-style-type: none"> <li>1. Retrieve the cloud management software information</li> <li>2. Retrieve the node information</li> </ol>

[Note 1]: This is not executed when DRS is enabled in a vSAN cluster.

## 2.13 Functions of ISM Operating Platform

This section describes each function configuring the ISM operating platform.

- [2.13.1 User Management](#)
- [2.13.2 Repository Management](#)
- [2.13.3 Installation of Emulex OneCommand Manager CLI and Qlogic QConvergeConsole CLI](#)
- [2.13.4 Task Management](#)
- [2.13.5 ISM-VA Management](#)
- [2.13.6 Management of Cloud Management Software](#)
- [2.13.7 Shared Directory Management](#)
- [2.13.8 Link with ISM](#)
- [2.13.9 Linking with Other Software](#)

### 2.13.1 User Management

ISM users are managed as follows.

- A unique login name and a password are assigned to each user.
- Depending on the privileges called "user roles," access procedures to nodes and execution of the various functions are restricted.

- By grouping users (hereafter referred to as "user groups"), you can restrict the scope of access to each function separately for each user group.
- By grouping nodes (hereafter referred to as "node groups") and correlating them with user groups, you can restrict the scope of nodes that can be accessed by users.

The relationship between user groups and node groups are displayed in "Figure 2.27 Relationships between user groups, node groups, and roles."

Here, the following points are described:

- Types of user groups and access scope of users belonging to each group
- Types of user roles and operations executable by users having these roles
- Security Policy Settings
- Creating required users after initial setup of ISM
- Operations under User Management
- Operating in Link with Microsoft Active Directory or LDAP

### Types of user groups and access scope of users belonging to each group

You can define the access scope of users belonging to a user group by correlating user groups with node groups.

User group name	Managed nodes	Access scope
Administrator group	Manage all nodes	The administrator group has access to all nodes and node-related resources (such as logs). This user group serves the overall management of ISM.
Other than Administrator group	Manage all nodes	The administrator group has access to all nodes and node-related resources (such as logs). This user group serves the overall management of ISM.
	Nodes in the selected node group	Groups other than the administrator group have access to only those nodes and node-related resources (such as logs) that are within the node groups with which their own user group is correlated.
	No managed node	There are not any nodes or node-related resources (such as logs).

#### Point

In the following descriptions, consider user groups for which "Manage all nodes" is specified as managed nodes to be Administrator group.

#### Note

If the managed nodes are "Manage all nodes," it cannot be changed. Also, if the managed nodes are "Nodes in the selected node group" or "No managed node," it cannot be changed to "Manage all nodes."

### Types of user roles and operations executable by users having these roles

The types of operation that can be executed by users on nodes within their access scope are defined by their user roles as follows.



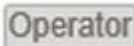





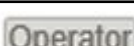

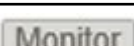
User Role	Type of access
Administrator role	Administrators can add, modify, delete, and view nodes, users, and all kinds of settings.
Operator role	Operators can modify and view nodes and all kinds of settings. They are not able to manage users.

User Role	Type of access
Monitor role	Monitors can view nodes and all kinds of settings. They are not able to manage users or to add, delete, or modify any nodes.

### Point

- For information on setting changes that can and cannot be made by operators, refer to the contents (indicated by icons) on the various functions that are provided in this manual. For information on the icon indications, refer to the description below.
- In the description below, users belonging to the Administrator group and carrying administrator roles will be described as "ISM Administrator."

In order to describe the access rights of users, the User Group to which a user belongs and the User Type according to the User Role they hold in these groups are classified as indicated below and are displayed by the following icons.

User Group to which user belongs	User Role held by user	Can execute	Cannot execute
Administrator group	Administrator role		
	Operator role		
	Monitor role		
Other groups (Other than Administrator group)	Administrator role		
	Operator role		
	Monitor role		

The attributes of users who can execute operations are as follows.

Example:



- When the display is as shown above, users with the following user attributes can execute operations:
  - Users who belong to an Administrator group and have an Administrator role or Operator role
  - Users who belong to a group other than an Administrator group and have an Administrator role or Operator role
- Users with a Monitor role indicated by the gray icon cannot execute the respective functions.

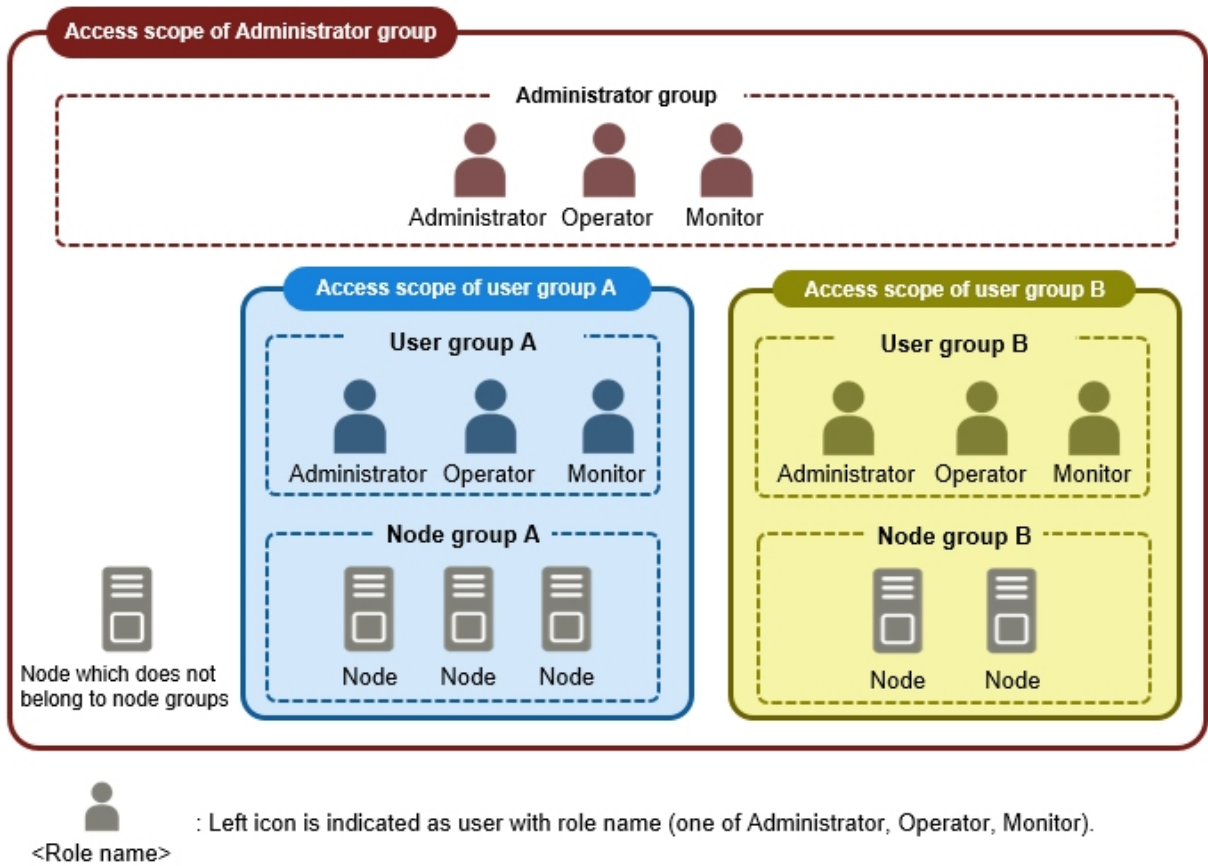
### Note

Users who belong to an Administrator group and have an Administrator role are special users (ISM administrator) who can manage ISM in its entirety.

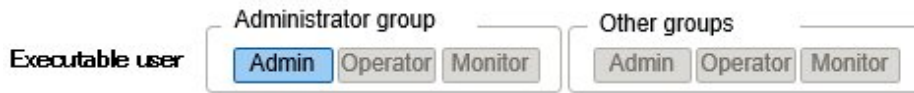
Users who belong to an Administrator group and have an Operator or Monitor role merely have different access scope, but otherwise the operations they can execute are the same as for users who have an Operator or Monitor role in a non-Administrator group.



Figure 2.27 Relationships between user groups, node groups, and roles



### Security Policy Settings



Execute the security policy settings 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 [Security Policy].
3. Select the [Edit] button to set the security policy.

For the security policy, there is the user password policy and the log in policy.

You can set passwords handled in User Management and log in restrictions.

You can set one security policy for the entire ISM. Safer operations become possible by setting a firm security policy. The setting items are described below.

#### User Password Policy

Item	Parameter	Operations after settings
Use Past Password	<ul style="list-style-type: none"> <li>- Allowed (Recommended)</li> <li>- Past n passwords prohibited (1 ≤ n ≤ 24)</li> </ul>	It is confirmed when setting a password on the "Add User" screen and "Edit User Settings" screen.
Password Length	1 - 32 (byte) (Recommended: 8 (bytes))	

Item	Parameter	Operations after settings
Password Character Type	<ul style="list-style-type: none"> <li>- No restrictions (Recommended)</li> <li>- Use at least n types of number, lowercase letter, uppercase letter, special character (2 n 4)</li> </ul>	
Same Password as User Name	<ul style="list-style-type: none"> <li>- Allowed</li> <li>- Prohibited (Recommended)</li> </ul>	
Prohibited Strings [Note 1]	Up to a maximum of 256 can be specified	
Period of Validity	<ul style="list-style-type: none"> <li>- Indefinitely</li> <li>- 1 - 365 (days) (Recommended: 90 (days))</li> </ul>	<p>If logging in with another setting than "Indefinitely," execute the following operations.</p> <ul style="list-style-type: none"> <li>- When the expiration date is reached The next action after expiration is executed.</li> <li>- When the expiration date has reached two weeks Warning messages are output.</li> <li>- Administrator A warning message will be output if the initial password has not been changed.</li> </ul>
Action after Expiration	<ul style="list-style-type: none"> <li>- Show warning message</li> <li>- Account lockout indefinitely (Recommended)</li> </ul>	

[Note 1]: Set a password that cannot be used. Passwords that match the set character string are forbidden.

### Point

If you select the [Default] button, the recommended values in the table above will be set.

### Note

- The things to be careful about for already created users, when updating to ISM 2.4 from a patch earlier than the ISM 2.0.0.d patch, are displayed below.
  - When you applied the patch, the expiration date for the passwords will be calculated from the time of the update.
  - The user password policy is set as follows.
    - Password Length: 1 (byte)
    - Password Character Type: No restrictions
    - Same Password as User Name: Allowed
    - Period of Validity: Indefinitely
    - Action after expiration: Show warning message
- The precautions for when [Period of Validity] is set to other than "Indefinitely" and [Action after Expiration] is set to "Account lockout indefinitely" are shown below.
  - The log in restrictions are limited to log in to ISM. Be careful, since log in to FTP or ISM-VA is not restricted.
  - The first log in to ISM succeeds after the password expiry date has passed. Change the password at this time. If the password is not changed, the log in will be locked indefinitely.

- When login has been locked indefinitely, if the password is reset by the ISM administrator, the lock is removed.
- The ISM administrator cannot be locked-out indefinitely. Only warning messages are output.

#### Login Policy

Item	Parameter	Description
Session Time	2 - 60 (minutes) (Default: 30 minutes)	The time after which the session will time out if there is no activity.
Account Lockout Threshold	6 - 256 (times) (Default: 6 times)	The threshold number of consecutive failed logins after which login will be temporarily prohibited.
Account Lockout Time	1 - 1440 (minutes) (Default: 30 minutes)	The time of temporary login prohibition after consecutive failed logins.

#### Note

The number of consecutive failed logins will be reset in the following circumstances.

- If login succeeded
- If the lock-out time since the last failed login has passed

### Creating required users after initial setup of ISM

#### Point

In the default settings of ISM, only users (ISM administrator) with an [Administrator Role] in [Administrator Groups] are registered.

User Name	Password	User Group Name	User Role	Usage
administrator	admin [Note]	Administrator	Administrator	Overall management of ISM

[Note]: Change the password before operating.

Create a user with the following procedure.

1. As an ISM administrator, log in to ISM-VA.
2. Create one or more node groups.  
For details, refer to "2.7.4.1 Add node groups" in "Operating Procedures."
3. Register the nodes that belong to each node group. (You can also register more nodes later.)  
For details, refer to "2.7.4.2 Edit node groups" in "Operating Procedures."
4. Create one or more user groups.  
For details, refer to "2.7.2.1 Add user groups" in "Operating Procedures."
5. Register the users that belong to each user group.  
For details, refer to "2.7.1.1 Add users" in "Operating Procedures."

### Operations under User Management

User Management is a function that is mainly used for the following purposes:

- Managing ISM users
- Managing user groups

- Authenticating ISM users
- Operating in link with Microsoft Active Directory or LDAP
- Managing node groups

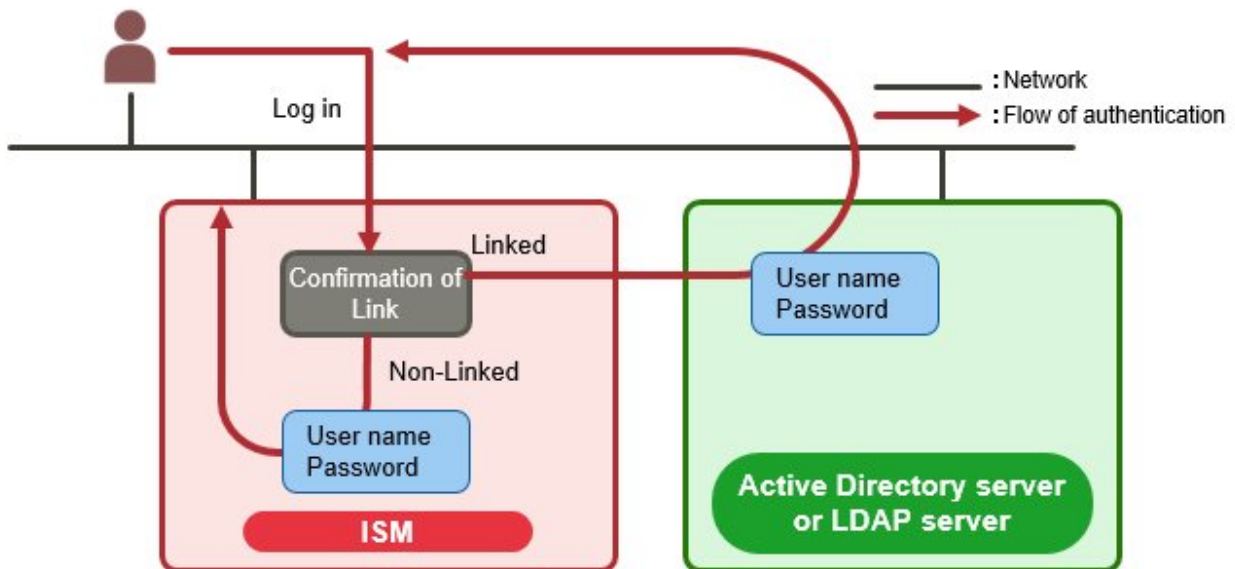
The target of operation in User Management vary with the operating user.

Operating user	Target of operation
Users who belong to an Administrator group and have an Administrator role	Operations can be performed for all existing user groups.
Users who belong to groups other than Administrator groups and have an Administrator role	Operations can be performed only for the user group to which the operating user belongs.

### Operating in Link with Microsoft Active Directory or LDAP

By linking ISM with Microsoft Active Directory or LDAP, you can integrate the management of users and passwords of multiple services. The following diagram gives an overview of a linked configuration.

Figure 2.28 Image of ISM in link with Microsoft Active Directory/LDAP



1. Log in as a user.
  - If the user is a target of linked operations:
    - Authentication is executed with Microsoft Active Directory or LDAP.
  - If the user is not a target of linked operations:
    - Authentication is executed with ISM.

### Note

- The administrator user cannot operate in link with Microsoft Active Directory or LDAP.
- Users whose user authentication method is "Infrastructure Manager(ISM)" cannot operate in link with Microsoft Active Directory or LDAP.
- You must set up a DNS server in ISM in advance if setting FQDN name as Microsoft Active Directory name or LDAP server name.
- If you cannot connect to the directory server with the content specified in [Settings] - [Users] - [LDAP Server Setting], an error will occur in the directory server information and setting will not be possible.

- A primary and two secondary servers can be specified as directory servers. In case that two servers are specified, if the currently used server cannot respond, the other server will be used.
- The following are the precautions for setting up a SSL certificate.
  - For the SSL certificate, set it after uploading it to the Administrator\ftp directory in advance.
  - After setup, delete the uploaded SSL certificate, since it is no longer required.
  - Specify the URL in the SSL certificate for the LDAP server name.
- The following are the precautions if you want to use SSL for the connection to the directory server.
  - Specify the LDAP user name from ldaps://.
  - For the port number, specify the port number for SSL transfer (for example 636).
  - Set the SSL certificate.
- When you change the password of the users specified by bind DN on the directory server, the change is not reflected in the settings of ISM. Change the password by setting the LDAP server on ISM.

## 2.13.2 Repository Management

The repository is a location used with ISM to store various kinds of resources. The resources are related to the user groups. The repository is mainly used for the following purposes:

- Storing of firmware data as well as the ServerView Suite Update DVD that are used for firmware updates  
Used in "[2.6 Firmware Management](#)."
- Storing of OS installation media that are used for installing OSES  
Used in "[2.4 Profile Management](#)."
- Storing of ServerView Suite DVD data that are used for installing OSES and Offline Update  
Used in "[2.4 Profile Management](#)" and "[2.6 Firmware Management](#)."



### Note

If the disk area in a repository is not enough, this results in a failure to store the various data for Repository Management. Refer to the following and allocate a sufficiently large disk area to the repository.

- [3.2.1.2 Estimation of required capacities for repositories](#)
- [3.7 Allocation of Virtual Disks](#)
- "2.7.2 Manage User Groups" in "Operating Procedures."

### 2.13.2.1 Storing and deleting firmware data



#### Storing firmware data

The following two procedures are available for storing firmware data to be applied on managed nodes in the repository:

- Importing ISO image files of the firmware data that are provided on DVD into the repository
- Importing the firmware data that are published on the FUJITSU website for each node into the repository

The firmware data to be used vary with the type of firmware update target. Prepare the DVD, firmware data shown in the following table. If the data are in DVD format, prepare the respective ISO image files.

Target firmware	Firmware Type (sort)	Firmware data to be used/Location from which to obtain
iRMC of PRIMERGY	iRMC	ServerView Suite Update DVD (11.15.09 version or later) [Note 1] Or the firmware data that can be downloaded from the following website <a href="http://support.ts.fujitsu.com/">http://support.ts.fujitsu.com/</a> [Note 2] <a href="http://support.ts.fujitsu.com/globalflash/ManagementController/">http://support.ts.fujitsu.com/globalflash/ManagementController/</a>
BIOS of PRIMERGY	BIOS	ServerView Suite Update DVD (11.15.09 version or later) [Note 1] Or the firmware data that can be downloaded from the following website <a href="http://support.ts.fujitsu.com/">http://support.ts.fujitsu.com/</a> [Note 2] <a href="http://support.ts.fujitsu.com/globalflash/SystemBoard/">http://support.ts.fujitsu.com/globalflash/SystemBoard/</a>
PCI Card	FC	ServerView Suite Update DVD (11.15.09 version or later) [Note 1] Or the firmware data that can be downloaded from the following website <a href="http://support.ts.fujitsu.com/globalflash/FibreChannelController/">http://support.ts.fujitsu.com/globalflash/FibreChannelController/</a>
	CNA	ServerView Suite Update DVD (11.15.09 version or later) [Note 1] Or the firmware data that can be downloaded from the following website <a href="http://support.ts.fujitsu.com/globalflash/LanController/">http://support.ts.fujitsu.com/globalflash/LanController/</a>
	SAS	ServerView Suite Update DVD (11.15.09 version or later) [Note 1] Or the firmware data that can be downloaded from the following website <a href="http://support.ts.fujitsu.com/globalflash/ScsiController/">http://support.ts.fujitsu.com/globalflash/ScsiController/</a>
	RAID	ServerView Suite Update DVD (11.15.09 version or later) [Note 1] Or the firmware data that can be downloaded from the following website <a href="http://support.ts.fujitsu.com/globalflash/ScsiController/">http://support.ts.fujitsu.com/globalflash/ScsiController/</a>
	LAN	ServerView Suite Update DVD (11.15.09 version or later) [Note 1] Or the firmware data that can be downloaded from the following website <a href="http://support.ts.fujitsu.com/globalflash/LanController/">http://support.ts.fujitsu.com/globalflash/LanController/</a>
PRIMEQUEST	Firmware of the server	The firmware data that can be downloaded from the following website <a href="http://support.ts.fujitsu.com/">http://support.ts.fujitsu.com/</a> [Note 2]
PRIMERGY BX Chassis MMB	MMB	The firmware data that can be downloaded from the following website <a href="http://support.ts.fujitsu.com/">http://support.ts.fujitsu.com/</a> [Note 2] <a href="http://support.ts.fujitsu.com/globalflash/BladeSystem/">http://support.ts.fujitsu.com/globalflash/BladeSystem/</a>
Network Switch Basic software	LAN Switch (SR-X model)	Contact your local Fujitsu customer service partner.
	LAN Switch (VDX model)	The firmware data that can be downloaded from the following website <a href="http://support.ts.fujitsu.com/">http://support.ts.fujitsu.com/</a>
	LAN Switch (CFX model)	Contact your local Fujitsu customer service partner.
	LAN Switch (PY CB Eth Switch model)	The firmware data that can be downloaded from the following website <a href="http://support.ts.fujitsu.com/">http://support.ts.fujitsu.com/</a> <a href="http://support.ts.fujitsu.com/globalflash/BladeSystem/">http://support.ts.fujitsu.com/globalflash/BladeSystem/</a>
	LAN Switch (Cisco Systems Nexus)	Contact your local Fujitsu customer service partner to receive it.

Target firmware	Firmware Type (sort)	Firmware data to be used/Location from which to obtain
	series, Cisco Systems Catalyst series)	
	FC Switch	The firmware data that can be downloaded from the following website <a href="http://support.ts.fujitsu.com/">http://support.ts.fujitsu.com/</a> [Note 2]
Storage Controller	ETERNUS DX/AF	The firmware data that can be downloaded from the following website <a href="http://support.ts.fujitsu.com/">http://support.ts.fujitsu.com/</a>

[Note 1]: To obtain the ServerView Suite Update DVD image, contact your local Fujitsu customer service partner.

[Note 2]: Download Flash File.

#### For importing the firmware data from DVD

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Firmware].
2. From the menu on the left side of the screen, select [Import].
3. From the [Actions] button on the [Import Data List] tab, select [Import DVD].
4. Select from the options in [File selection method].
  - Local  
Import an ISO image stored locally.
  - FTP  
Import an ISO image from the FTP server of ISM-VA.  
You must transfer the ISO image to the "<User group name>/ftp" directory in ISM-VA in advance.  
For FTP connection and how to transfer FTP, refer to "[2.1.2 FTP Access.](#)"
  - Shared Directory  
Import ISO image from a shared directory.  
You must mount the shared directory where the ISO image to be imported is saved in advance.  
For the shared directory settings and method for mounting it, refer to "[2.13.7 Shared Directory Management.](#)"
5. Specify the ISO image in [File Path].
6. Select the ISO image type in [File Type], then execute import with the [Apply] button.  
DVD import may take some time to complete. After starting the import, the operations are registered as ISM tasks. Confirm the current status of the task on the "Tasks" screen.  
When selecting [Tasks] from the top of the Global Navigation Menu on the GUI of ISM, the Task List is displayed.

#### Point

- The files you deployed on the FTP server of ISM-VA are no longer required after the import has finished. Use an FTP command to delete them.
- When you select "FTP" in [File selection method], if you check [Delete source file], the import source file on the FTP server will be deleted after the import has been completed.
- If you select "Shared Directory" in [File selection method], and if you check [Unmount shared directory], the shared directory is unmounted after the import has been completed.

For importing the firmware data downloaded from the Fujitsu web site

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Firmware].
2. From the menu on the left side of the screen, select [Import].
3. From the [Actions] button on the [Import Data List] tab, select [Import Firmware].
4. Select from the options in [File selection method].
  - Local  
Import the firmware data saved locally.
  - FTP  
Import firmware data from the FTP server of ISM-VA.  
You must transfer the firmware data to the "/<User group name>/ftp" directory in ISM-VA in advance.  
For FTP connection and how to transfer FTP, refer to "[2.1.2 FTP Access.](#)"
5. Specify the firmware data to be imported in [File Path].
6. Select the firmware type in [Type].
7. Select the firmware model in [Model Name].
8. Select the method for retrieving version of the firmware in [Version], then execute import with the [Apply] button.
  - Get automatically  
Version information is retrieved from the firmware when importing.  
With this option the firmware in the following table can be imported. If it cannot be imported, select "Enter manually" and execute the import.

Type	Model
iRMC	- PRIMERGY (server with iRMC S4, S5 mounted) - PRIMEQUEST 3800B
BIOS	- PRIMERGY (server with iRMC S3, S4, S5 mounted) - PRIMEQUEST 3800B [Note 1]

[Note 1]: Only items that mode is Offline for are imported.

- Enter manually  
Enter the firmware version manually when importing.  
Use the table below to enter the versions.

Type	Model	Version
iRMC	RX100 S8, CX2550 M1, BX920 S4, TX2550 M4, PRIMEQUEST 3800B etc.	iRMC and SDR versions [Note 1]
BIOS	RX100 S8, CX2550 M1, BX920 S4, TX2550 M4, PRIMEQUEST 3800B etc.	BIOS version [Note 1]
MMB	BX900 S2	Firmware version [Note 1]
PRIMEQUEST	PRIMEQUEST 2400S3 etc.	Version of the firmware of PRIMEQUEST [Note 1]
FC	LPe1250, LPe12002, MC-FC82E	BIOS and FW versions [Note 2]
	LPeXXX except for LPe1250 and LPe12002, MC-FC162E	Firmware version [Note 2]
	QLEXXX	BIOS version [Note 2]



Type	Model	Version
CNA	OCe10102, OCe14102 or MC-CNA112E	Firmware version [Note 1]
SAS	PSAS CP200i, PSAS CP400i, PSAS CP400e	Firmware version [Note 1]
RAID	PRAID CP400i, PRAID EP420e, PY SAS RAID Mezz Card 6Gb etc.	Firmware version [Note 1]
LAN	MCX415, MCX416 etc.	Firmware version [Note 1]
LAN Switch	SR-X model	Version of basic software [Note 1]
	VDX model	Firmware version [Note 1]
	CFX model	Firmware version [Note 1]
	PY CB Eth Switch/IBP 1Gb 36/12	Firmware version [Note 1]
	PY CB Eth Switch/IBP 10Gb 18/8	Firmware version [Note 1]
	PY CB Eth Switch 10/40 Gb 18/8+2	Firmware version [Note 1]
	Cisco Systems Nexus series	Version of NX-OS [Note 1]
	Cisco Systems Catalyst series	Version of IOS [Note 1]
FC Switch	Brocade FC Switch	Version of basic software [Note 2]
ETERNUS DX/AF	ETERNUS DX/AF model	Firmware version [Note 1]

[Note 1]: For information on the version, refer to the release notes.

[Note 2]: For information on the version, refer to the release notes or the file name.

## Point

- If you select "Local" in [File selection method], specify the ZIP folder where the firmware data is saved in [File Path] to import. If the firmware data is provided in ZIP format, unzip the file once. Again zip the folder created when unzipping and import it.
- If you select "FTP" in [File selection method], transfer the folder where the firmware data is saved to the FTP server of ISM-VA, then specify the transferred folder in [File Path] to import. If the firmware data is provided in ZIP format, unzip the file. Transfer the folder created when unzipping to ISM-VA and import it.
- If you are saving files on the FTP server of ISM-VA, use the FTP command or ftp client software (ffftp, WinSCP, or other) to transfer them. In this case, set it so that the character code is converted with UTF-8. Do not use Windows Explorer since the character code is not handled correctly.
- When you select "FTP" in [File selection method], if the import is not executed correctly or if the imported file is not displayed, execute the following procedure.
  1. Delete the imported firmware data and the files transferred to the FTP server on ISM-VA.
  2. Review the character code conversion settings.
  3. Redo the import.
- The files you deployed on the FTP server of ISM-VA are no longer required after the import has finished. Use an FTP command to delete them.
- If you select "BIOS" in [Type], multiple options, such as "RX2530 M4\_A1" or "RX2530 M4\_C1," may be displayed for the same model in the [Model Name] option.

For these, you must check which type of firmware data the node executing the firmware update is using, and adjust your selection accordingly.

Also, acquire and import firmware data of the same type as the firmware data used on the firmware update target.

What type of firmware data a node registered in ISM is using can be checked with the following procedure.

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes].
2. In the [Column Display] field on the "Node List" screen, select [Firmware].
3. Check the [Firmware Name] column.

---

### Deleting firmware data from repository

The following is a sample operation using the GUI.

1. From the Global Navigation Menu on the GUI of ISM, select [Structuring] - [Firmware].
2. From the menu on the left side of the screen, select [Import].
3. Execute one of the following.
  - If firmware data from the DVD was stored in repository:
    - a. Select [Import Data List] tab.
    - b. Select the checkboxes for the data to be deleted, then select the [Actions] button and select [Delete].
    - c. Execute the operations according to the instructions on the screen.
  - If firmware data downloaded from the FUJITSU website was stored in repository:
    - a. Select [Firmware Data] tab.
    - b. Select the checkboxes for the data to be deleted, then select the [Actions] button and select [Delete].
    - c. Execute the operations according to the instructions on the screen.

### 2.13.2.2 Storing and deleting OS installation files



### Storing OS installation files

As Profile Management uses the OS installation media you imported to the repository for installing OSes, the OS installation media are not directly used after the import.

To import the data, execute the following procedure.

1. Prepare an ISO image of the OS installation media. For ESXi, prepare a FUJITSU custom image.
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 [DVD Import].
4. From the [Actions] button, select [Import DVD].
5. Select from the options in [File selection method].
  - Local  
Import an ISO image stored locally.
  - FTP  
Import an ISO image from the FTP server of ISM-VA.  
You must transfer the ISO image to the "/<User group name>/ftp" directory in ISM-VA in advance.  
For FTP connection and how to transfer FTP, refer to "2.1.2 FTP Access."

- Shared Directory

Import ISO image from a shared directory.

You must mount the shared directory where the ISO image is saved in advance.

For the shared directory settings and method for mounting it, refer to "2.13.7 Shared Directory Management."

6. Specify the ISO image in [File Path].
7. Select the appropriate OS type in [Media Type], then execute import with the [Apply] button.

### Point

- The files you deployed on the FTP server of ISM-VA are no longer required after the import has finished. Use an FTP command to delete them.
- When you select "FTP" in [File selection method], if you check [Delete source file], the import source file on the FTP server will be deleted after the import has been completed.
- If you select "Shared Directory" in [File selection method], and if you check [Unmount shared directory], the shared directory is unmounted after the import has been completed.

### Deleting OS installation files from repository

The procedure for deletion is as follows:

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 [DVD Import].
3. Select the checkboxes for the data to be deleted, then select the [Actions] button and select [Delete].
4. Execute the operations according to the instructions on the screen.

### 2.13.2.3 Storing and deleting ServerView Suite DVD



### Storing of ServerView Suite DVD

When Profile Management installs an OS, it retrieves the programs for controlling the target node as well as the driver, application, and other files to be installed on the target node from the ServerView Suite DVD.

Import the ServerView Suite DVD that supports the target node and the OS to be installed in advance.

To import the data, execute the following procedure:

1. Prepare an ISO image of "ServerView Suite DVD."
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 [DVD Import].
4. From the [Actions] button, select [Import DVD].
5. Select from the options in [File selection method].
  - Local  
Import an ISO image stored locally.
  - FTP  
Import an ISO image from the FTP server of ISM-VA.

You must transfer the ISO image to the "/<User group name>/ftp" directory in ISM-VA in advance.

For FTP connection and how to transfer FTP, refer to "2.1.2 FTP Access."

- Shared Directory

Import ISO image from a shared directory.

You must mount the shared directory where the ISO image is saved in advance.

For the shared directory settings and method for mounting it, refer to "2.13.7 Shared Directory Management."

6. Specify the ISO image in [File Path].

7. Select [ServerView Suite DVD] in [Media Type], then execute import with the [Apply] button.

### Point

- The files you deployed on the FTP server of ISM-VA are no longer required after the import has finished. Use an FTP command to delete them.
- When you select "FTP" in [File selection method], if you check [Delete source file], the import source file on the FTP server will be deleted after the import has been completed.
- If you select "Shared Directory" in [File selection method], and if you check [Unmount shared directory], the shared directory is unmounted after the import has been completed.

## Deleting ServerView Suite DVD data from repository

The procedure for deletion is as follows:

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 [DVD Import].
3. Select the checkboxes for the data to be deleted, then select the [Actions] button and select [Delete].
4. Execute the operations according to the instructions on the screen.

## 2.13.3 Installation of Emulex OneCommand Manager CLI and QLogic QConvergeConsole CLI

---

### Note

- For executing a firmware update of a PCI card on Linux, the Emulex OneCommand Manager CLI or the QLogic QConvergeConsole CLI must be installed in the OS of the target server, and the PCI card information must be retrievable. For information on how to install and operate these CLIs, refer to the manuals for Emulex One Command Manager CLI and for QLogic QConvergeConsole CLI.  
For PCI cards that require installation of Emulex OneCommand Manager CLI and QLogic QConvergeConsole CLI, contact your local Fujitsu customer service partner.
- For executing a firmware update of a PCI card on Linux, the lspci command must be executable under Linux on the target server.

You should use the latest versions of the Emulex OneCommand Manager CLI or the QLogic QConvergeConsole CLI, respectively.

For information on the latest versions, contact your local Fujitsu customer service partner.

## 2.13.4 Task Management

---

In ISM, any processing that takes time is managed as a "Task." You can view the current status of all tasks at once on the "Tasks" screen instead of the respective operating screens of each task.

Also, you have to use the "Tasks" screen to abort (cancel) any ongoing processing.

On the "Tasks" screen, you can view processing of the tasks shown in the following table.

Function	Type of processing
Firmware Management	Import of firmware data Firmware update
Profile Management	Import of OS installation media Assignment of profiles Reassignment of profiles Release of profiles
Log Management	Collect Logs Delete Logs Create Download File
Network Management	Changing VLAN Settings
Virtual Resource Management	Refresh for Virtual Resource Information

### Procedure for displaying "Tasks" screen



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

## 2.13.5 ISM-VA Management

ISM-VA Management is a function used for installing, service operations, and maintenance of ISM.

Here, the following points are described:

- [Functions for use when installing ISM](#)
- [Functions for use in maintenance](#)

The commands you can use with ISM-VA Management are described in "[2.13.5.1 List of commands in ISM-VA Management.](#)"

### Functions for use when installing ISM

Function name	Overview of Function
Initial Setup	This function executes the basic setup from a hypervisor console after installing ISM-VA.  - Network settings - Time settings - Initial locale settings
License Settings	This function enables the ISM license key.
Certificate Activation	This function manages the certificates for access with web browsers.

### Functions for use in maintenance

Function name	Overview of Function
ISM-VA Service Control	This function can stop and restart ISM-VA as well as control the services that run internally.
Basic Settings	This function serves to modify the settings for ISM-VA after installation.  - Network Settings

Function name	Overview of Function
	<ul style="list-style-type: none"> <li>- Time settings</li> <li>- Locale setting</li> <li>- Virtual disk settings</li> <li>- Modification of Host Names</li> </ul>
Maintenance	<p>This function serves to execute all kinds of maintenance.</p> <ul style="list-style-type: none"> <li>- Confirmation of versions</li> <li>- Application of Patches</li> <li>- Collection of Archived Logs</li> <li>- Switching of debug flags</li> </ul>

### 2.13.5.1 List of commands in ISM-VA Management

The following list shows the commands in ISM-VA Management.

#### Console management menu

Function	Command
ISM-VA Basic Settings Menu	ismsetup

#### Network settings

Function	Command
Display of network devices	ismadm network device
Modification of network settings	ismadm network modify
Display of network settings	ismadm network show

#### Time settings

Function	Command
Display of time settings	ismadm time show
Display of available time zones	ismadm time list-timezones
Time zone setting	ismadm time set-timezone
Setting of date and time	ismadm time set-time
Enable/Disable NTP synchronization	ismadm time set-ntp
Adding of NTP server	ismadm time add-ntpserver
Removal of NTP server	ismadm time del-ntpserver

#### Locale and keymap settings

Function	Command
Display of locale and keymap	ismadm locale show
Display of available locales	ismadm locale list-locales
Locale setting	ismadm locale set-locale
Display of available keymaps	ismadm locale list-keymaps

Function	Command
Keymap setting	ismadm locale set-keymap

### License settings

Function	Command
Display of licenses	ismadm license show
Registration of licenses	ismadm license set
Deletion of license	ismadm license delete

### Certificate activation

Function	Command
Deployment of SSL server certificates	ismadm sslcert set
Display of SSL server certificates	ismadm sslcert show
Export of SSL server certificates	ismadm sslcert export
Creation of self-signed SSL server certificates	ismadm sslcert self-create

### ISM-VA service control

Function	Command
Restart of ISM-VA	ismadm power restart
Stop of ISM-VA	ismadm power stop
Modification of destination port number of ISM	ismadm service modify
Display of list of internal services	ismadm service show
Start of internal service individually	ismadm service start
Stop of internal service individually	ismadm service stop
Restart of internal service individually	ismadm service restart
Display of status of internal service individually	ismadm service status
Enabling of internal service individually	ismadm service enable
Disabling of internal service individually	ismadm service disable

### Virtual disk settings

Function	Command
Adding of LVM volume	ismadm volume add
Allocation of LVM volume to user group	ismadm volume mount
Cancel of allocation of LVM volume to user group	ismadm volume umount
Display of volume settings	ismadm volume show
Extension of LVM volume size	ismadm volume extend
Extension of size of LVM system volume	ismadm volume sysvol-extend
Removal of LVM volume	ismadm volume delete

### Maintenance

Function	Command
Collection of Archived Logs	ismadm system snap
Display of System Information	ismadm system show
Application of Patches	ismadm system patch-add
Application of Plug-in	ismadm system plugin-add
Upgrade of ISM-VA	ismadm system upgrade
Modification of Host Names	ismadm system modify
Switching the ISM RAS Log mode	ismadm system set-debug-flag
Backup of ISM	ismadm system backup
Restoration of ISM	ismadm system restore
ISM-VA Statistics Information Display	ismadm system stat

### Settings for core file collection directory

Function	Command
Display of collection directory	ismadm system core-dir-show
Collection directory settings	ismadm system core-dir-set
Clear collection directory	ismadm system core-dir-reset

### Alarm notification settings

Function	Command
Registration certificate for alarm notification mails	ismadm event import
Display certificate for alarm notification mails	ismadm event show
Deletion certificate for alarm notification mails	ismadm event delete

### MIB file settings

Function	Command
Registration of MIB files	ismadm mib import
Display of MIB files	ismadm mib show
Deletion of MIB files	ismadm mib delete

### Security settings

Function	Command
SSL/TLS enable status display	ismadm security show-tls
SSL/TLS enable setting	ismadm security enable-tls

### Settings for linking with other software

Function	Command
Registration certificate for link with other software	ismadm security import-software-cert
Display certificate for link with other software	ismadm security show-software-cert
Deletion certificate for link with other software	ismadm security delete-software-cert





## Note

ISM-VA must be restarted if the time interval settings were returned to a past time.

### 2.13.6 Management of Cloud Management Software

When you use the functions in link with cloud management software, register cloud management software with ISM.

The following is the supported cloud management software.

- VMware vCenter Server 5.5
- VMware vCenter Server 6.0
- VMware vCenter Server 6.5
- VMware vCenter Server 6.7
- Microsoft System Center 2012
- Microsoft System Center 2012R2
- Microsoft System Center 2016
- Microsoft Failover Cluster (Windows Server 2012) [Note 1]
- Microsoft Failover Cluster (Windows Server 2012R2) [Note 1]
- Microsoft Failover Cluster (Windows Server 2016) [Note 1]
- Microsoft Failover Cluster (Windows Server 2019) [Note 1]
- KVM (Red Hat Enterprise Linux)
- KVM (SUSE Linux Enterprise)
- IPCOM OS 1.x
- OpenStack (Red Hat Enterprise Linux)

[Note 1]: For Microsoft Failover Cluster, only the virtual machine registered for cluster roles are displayed.

#### 2.13.6.1 Registering cloud management software



The following is the operation procedure for registering new cloud management software.

1. From the Global Navigation Menu on the GUI of ISM, select [Settings] - [General] - [Cloud Management Software].
2. From the [Actions] button, select [Register].
3. Enter the information that is required for registration.
  - Cloud Management Software Name  
Set a name that is unique across the entire ISM system.
  - IP Address  
Set the IP address of the cloud management software.  
Register the cluster virtual IP address in the case of Microsoft Failover Cluster.  
For OpenStack, set the IP address of the controller node.

- Type

Select the type of cloud management software to be registered.

Also specify the version of Windows Server in the case of Microsoft Failover Cluster.

### Note

If Microsoft Failover Cluster was specified, you must set the domain name in [Account Information].

- Account Information

Set the domain name, account name, and password for the cloud management software.

Enter the domain name by using uppercase letters.

### Point

If the cloud management software is an OpenStack type, the project that registered the user will become the main project.

- URL

Set the URL for accessing the web management screen for the cloud management software.

If a cloud management software that provides a web management function was specified in [Type], the URL used to access the web management screen must be set.

- User Group Name

Select the name of the user group to be managed.

4. Select the [Register] button.

The cloud management software registered with Cloud Management Software List screen is displayed.

## 2.13.6.2 Retrieving information from cloud management software



In ISM, the following information running on the nodes can be retrieved.

- Virtual Machine Information

The virtual machine information retrieved from the cloud management software can be confirmed on the [Virtual Machines] tab of the Details of Node screen.

- Virtual Switch Information

The virtual switch information retrieved from the cloud management software can be confirmed on the "Network Map" screen.

It can be retrieved if the cloud management software type is a VMware vCenter Server, System Center, Microsoft Failover Cluster, or OpenStack. KVM is not supported.

- Virtual Router Information

The virtual router information retrieved from the cloud management software can be confirmed on the "Network Map" screen.

It can be retrieved if the cloud management software type is an OpenStack. VMware vCenter Server, System Center, Microsoft Failover Cluster, and KVM are not supported.

## Note

ISM manages information for the registered cloud management software, OS information of nodes and information for the virtual machines, virtual switches and virtual routers connected to it. Execute the settings respectively to retrieve virtual machine, virtual switch, and virtual router information.

ISM retrieves virtual machine, virtual switch, and virtual router information in 24 hour cycles. Follow the procedure below to retrieve the information at any time.

1. Retrieve node information for nodes that are managed with the cloud management software.
2. From the Global Navigation Menu on the GUI of ISM, select [Settings] - [General] - [Cloud Management Software].
3. Retrieve information using one of the following procedures.
  - If retrieving information from all cloud management software, select [Get Cloud Management Software Info] and then select [Run].
  - If limiting the items to be retrieved, select the cloud management software to be retrieved and select the [Actions] button - [Get Info] - [Run].

As soon as retrieval of the information is complete, a log with the Message ID "10021503" is exported to the [Events] - [Events] - [Operation Log]. If there is cloud management software where information could not be retrieved, a log will additionally be exported in [Events] - [Events] - [Operation Log]. Confirm that an error has not been exported, then confirm the information of the virtual machine, virtual switch, or virtual router.

## Note

- If registering both System Center and the Microsoft Failover Cluster registered in System Center in ISM, ISM will retrieve information from System Center, but information will not be retrieved from Microsoft Failover Cluster.
- In an environment using Microsoft Failover Cluster, if deleting a virtual machine from the Hyper-V manager, also delete this virtual machine from the failover cluster manager role.

### 2.13.6.3 Editing cloud management software



The following is the operation procedure for editing cloud management software information registered with ISM.

1. From the Global Navigation Menu on the GUI of ISM, select [Settings] - [General] - [Cloud Management Software], and then select the target cloud management software on the displayed "Cloud Management Software List" screen.
2. From the [Actions] button, select [Edit].
3. Edit the information.

Item	Description
Cloud Management Software Name	Set a name that is unique across the entire ISM system.
IP Address	Set the IP address of the cloud management software. For Microsoft Failover Cluster, set the virtual IP address of the cluster. For OpenStack, set the IP address of the controller node.
(Account Information)	Set the Domain Name, Account Name, Password and Port Number of the cloud management software.

Item	Description
URL	If the cloud management software provides a Web management function, set an URL to access the Web management screen.
User Group Name	Select a User Group Name to manage.

- Execute [Register] to make the contents of the information effective.

## 2.13.6.4 Deleting cloud management software



The following is the operation procedure for deleting cloud management software registered with ISM.

- From the Global Navigation Menu on the GUI of ISM, select [Settings] - [General] - [Cloud Management Software], and then select the target cloud management software on the displayed "Cloud Management Software List" screen.
- From the [Actions] button, select [Delete].
- Execute [Delete] to delete the cloud management software.

## 2.13.7 Shared Directory Management

Add shared directory used when importing DVD.

### 2.13.7.1 Adding shared directories



The following displays the procedure for adding a new shared directory.

- From the Global Navigation Menu on the GUI of ISM, select [Settings] - [General] - [Shared Directory].
- From the [Actions] button, select [Register].
- Enter the information that is required.

Item	Description
Host Name/IP Address	Set the IP address or host name of the shared directory.
Domain	Set the domain name of the shared directory. Set the domain name in capital letters.
Shared directory path	Set the path of the shared directory.
Type	Set the shared directory type from SMB/CIFS, NFS.
Account Name	Set the account name of the shared directory.
Password	Set the password of the shared directory.
User Group Name	Select the user group that the shared directory information belongs to.

- Select the [Register] button.

The added shared directory is displayed in the "Shared directory list" screen.



### Note

- The information of up to five shared directories can be added to each user group.

- If the shared directory cannot be mounted with the set shared directory information, an error will occur.

### 2.13.7.2 Editing shared directories



The following is the operation procedure for editing shared directory information registered with ISM.

1. From the Global Navigation Menu on the GUI of ISM, select [Settings] - [General] - [Shared Directory].
2. Execute one of the following.
  - Select the checkbox for the shared directory you want to edit, then select the [Actions] button and select [Edit].
  - Select the shared directory you want to edit and, when the information screen is displayed, select the [Actions] button and select [Edit].
3. Edit the information.

Item	Description
Host Name/IP Address	Set the IP address or host name of the shared directory.
Domain	Set the domain name of the shared directory. Set the domain name in capital letters.
Shared directory path	Set the path of the shared directory.
Type	Set the shared directory type from SMB/CIFS, NFS.
Account Name	Set the account name of the shared directory.
Password	Set the password of the shared directory.

4. Execute [Apply] to make the contents of the information effective.

#### Note

Shared directories cannot be edited if they are mounted.

### 2.13.7.3 Deleting shared directories



The following is the operation procedure for deleting shared directory registered with ISM.

1. From the Global Navigation Menu on the GUI of ISM, select [Settings] - [General] - [Shared Directory].
2. Execute one of the following.
  - Select the checkboxes of the shared directory you want to delete, then select the [Actions] button and select [Delete].
  - Select the shared directory you want to delete and, when the information screen is displayed, select the [Actions] button and select [Delete].
3. Select [Delete].

#### Note

Shared directories that are mounted cannot be deleted.

## 2.13.7.4 Mounting shared directories



The following is the operating procedure for mounting directory information registered with ISM.

1. From the Global Navigation Menu on the GUI of ISM, select [Settings] - [General] - [Shared Directory].
2. Execute one of the following.
  - Select the checkbox for the shared directory you want to mount, then select the [Actions] button and select [Mount].
  - Select the shared directory you want to mount and, when the information screen is displayed, select the [Actions] button and select [Mount].

### Note

- The following displays the privilege of the mounted directory.
  - Mount as read only.
  - SMB/CIFS  
Mount with the same user privilege as the privilege of the user group that created the shared directory information.
  - NFS  
Mount using root privilege.
- In the following cases it is unmounted.
  - ISM was restarted or stopped
  - The ISM service was stopped
- The user group carrying the mounted shared directory information cannot execute the following operations.
  - Changing user group names
  - Deleting user groups

## 2.13.7.5 Unmounting shared directories



The following is the operating procedure for unmounting directory information registered with ISM.

1. From the Global Navigation Menu on the GUI of ISM, select [Settings] - [General] - [Shared Directory].
2. Execute one of the following.
  - Select the checkbox for the shared directory you want to unmount, then select the [Actions] button and select [Unmount].
  - Select the directory you want to unmount and, when the information screen is displayed, select the [Actions] button and select [Unmount].

## 2.13.8 Link with ISM

---

### 2.13.8.1 Link display for other ISM status information

In ISM, the status information of the other ISM (Alarm Status/Status) can be displayed on the dashboard.

Links			Y
Tokyo DC	<span style="border: 1px solid red; padding: 2px;">🔔 3</span> <span style="border: 1px solid red; padding: 2px;">❌ 1</span> <span style="border: 1px solid red; padding: 2px;">❓ 5</span>	Tokyo	
Kawasaki DC	<span style="border: 1px solid yellow; padding: 2px;">🔔 2</span> <span style="border: 1px solid yellow; padding: 2px;">⚠️ 2</span>	Kawasaki	

For details of Status (Alarm Status/Status), refer to "2.1.1 GUI."

The following describes the operating procedure if displaying the status of other ISM on the dashboard.

1. Set a user that wants to display the status of other ISM on the dashboard.

In addition, this user is required to be registered in other ISM with the same user name and password.

- a. Log in to ISM as a user who belongs to an Administrator group and has an Administrator role.
- b. Edit the user that you want to display the status of the other ISM for on the dashboard by executing the following settings.
  - In [Link with ISM], select [Set this user as a link user]
  - Password

2. Register the CA certificate of the other ISM that you want to display.

For details, refer to "Registration of certificates" in "2.13.8.2 Certificate management for other ISM links."

3. Add [Links] to the dashboard on the GUI.

- a. From the Global Navigation Menu on the GUI of ISM, select [Dashboard].  
If [Links] is displayed, proceed to procedure f.  
If [Links] is not displayed, use the following procedure to add link.
- b. From the [☰] at the top of the screen, select [Add Widget].
- c. From the displayed [Add Widget] select [Links], then select the [Add] button.
- d. From the [☰], select [Change Layout].
- e. Select [Save] on [Edit Mode].
- f. Select the [Y] of [Links] displayed on the dashboard.
- g. Set the following in the "Widget settings: Links" screen.
  - Name: set the name you want to display in the widget.
  - URL: set the URL of the other ISM in the following way.  
https://<IP address of the target ISM or FQDN name>:<port number>
  - Description: Specify a description (comment) as you like.

Procedure to add widgets, and details on the widget contents, refer to the ISM online help.

## 2.13.8.2 Certificate management for other ISM links

Executable user	Administrator group	Other groups
	<span style="border: 1px solid gray; padding: 2px;">Admin</span> <span style="border: 1px solid gray; padding: 2px;">Operator</span> <span style="border: 1px solid gray; padding: 2px;">Monitor</span>	<span style="border: 1px solid gray; padding: 2px;">Admin</span> <span style="border: 1px solid gray; padding: 2px;">Operator</span> <span style="border: 1px solid gray; padding: 2px;">Monitor</span>

CA Certificates used if accessing other ISM are added in the link function of the widget.

## Registration of certificates

The following describes the operating procedure for adding new certificates.

1. From the Global Navigation Menu on the GUI of ISM, select [Settings] - [General] - [CA Certificate].
2. From the [Actions] button, select [Register].
3. Enter the information that is required.
  - Action after completion  
Select whether to delete the source file.
  - File Path  
Upload the CA certificate of the other ISM that you want to access and set up the uploaded file.
  - Host Name/IP Address  
Set the Host Name or IP Address of the other ISM that you want to access.
4. Select the [Register] button.  
Displaying the result screen, the registered certificate is displayed in the "CA Certificate List" screen.



- The certificate to register is the CA certificate. Regarding CA Certificates, refer to "[4.7.5 Download of CA Certificates.](#)"
- Whether access to the other ISM is possible with the registered certificate is not checked.

## Deleting certificates

The following is the operation procedure for deleting certificates registered with ISM.

1. From the Global Navigation Menu on the GUI of ISM, select [Settings] - [General] - [CA Certificate].
2. Execute one of the following.
  - Select the checkboxes of the certificates you want to delete, then select the [Actions] button and select [Delete].
  - Select the certificates you want to delete and, when the information screen is displayed, select the [Actions] button and select [Delete].
3. Execute [Delete] to delete the certificates.



Certificates can be deleted also if you are using the link function of the widget.

## 2.13.9 Linking with Other Software

---

From ISM, you can link with other software and display the information managed by the software in widgets on the dashboard on the ISM GUI.

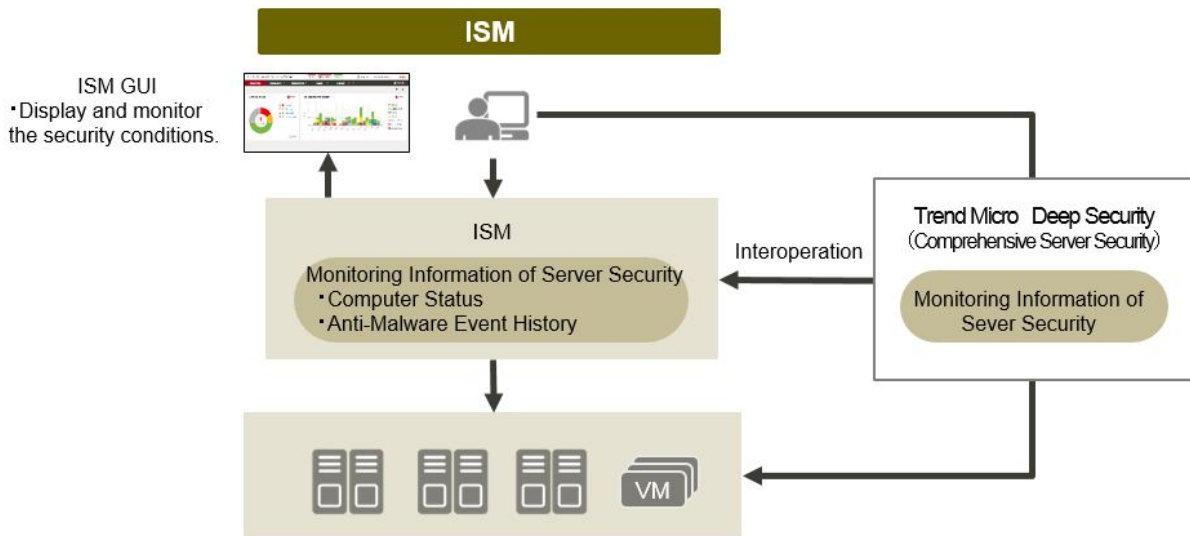
The following is the software that can be linked.

- Trend Micro Deep Security v10.0 or later  
An integrated server security software. Provides integrated security monitoring for physical machines and virtual machines.



Link with Deep Security Manager, which is the management module of Trend Micro Deep Security, to monitor the security status of the devices managed in ISM.

Figure 2.29 Image of link with Trend Micro Deep Security



The followings are the widgets that can be displayed on the dashboard on the ISM GUI.

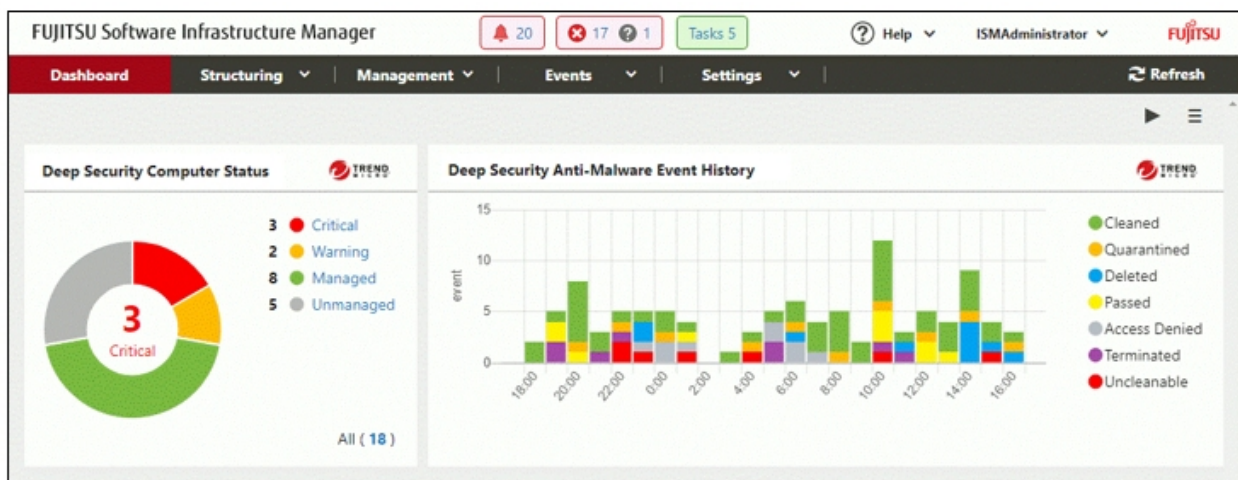
- Computer Status widget

Displays graphs of the security status of the computers managed by Deep Security Manager. If you select a graph, the Deep Security Manager GUI opens and you can check detailed information.

- Anti-Malware Event History widget

Displays chronological graphs of Anti-Malware Event History of Deep Security Manager. If you select a graph, the Deep Security Manager GUI opens and you can check detailed information.

Figure 2.30 Deep Security Link Widget



### 2.13.9.1 Preparations in advance for Deep Security Link

## Note

You must make preparations in advance for Deep Security. For details, refer to the documentation on Trend Micro's website. Note that you cannot use ISM links if the IP address of the Deep Security Manager is an IPv6 link local address.

1. Execute the following settings from the Deep Security Manager Web GUI.
    - a. Set the user account for Deep Security Manager.

Set the "Allow Access to web services API" in the access type of the user role.
    - b. Confirm the time zone of Deep Security Manager.

Select the user properties from the user name of the top of the screen. Take note of the displayed time zone.
- For details, refer to the documentation on the use of Deep Security REST API on Trend Micro's website.

2. Retrieve Deep Security Manager certificate.

Export the certificate from the Web browser. Select "Base 64 encoded X.509(.CER)" for the format of the export file.

## Point

The following is the export procedures for each Web browser. Display the Web GUI of Deep Security Manager in a Web browser, and then use the following procedure to export.

- For Internet Explorer
  1. Select the key icon in the address field, and then select "View certificates."
  2. From the [Details] tab, select [Copy to File].
  3. The Certificate Export Wizard opens. Specify the following and export.
    - "Base 64 encoded X.509(.CER)(S)" in "Export File Format"
    - File name and save location in "File to Export"
- For Google Chrome
  1. Select the key icon in the address field, and then select "Certificates."
  2. From the [Details] tab, select [Copy to File].
  3. The Certificate Export Wizard opens. Specify the following and export.
    - "Base 64 encoded X.509(.CER)(S)" in "Export File Format"
    - File name and save location in "File to Export"
- For FireFox
  1. Select the key icon in the address field. Select the host name of Deep Security Manager (IP address or FQDN), and then select [Show Details].
  2. Select [Show Certificates], and then select the [Details] tab.
  3. Select [Export]. Specify the following in "Save Certificate as File" and export.
    - The file type as "X.509 Certificates (PEM)"
    - File name and save location

## Note

Make sure to select "Base 64 encoded X.509(.CER)" for the format of the export file. Certificates in other formats cannot be used.

3. Upload a certificate file to ISM-VA.

For details on upload procedures, refer to "2.8 Upload Files to ISM-VA" in "Operating Procedures." When uploading, specify "Certificate for link with other software" for the file type.

4. Register a certificate in ISM-VA.

From the console, log in to ISM-VA as administrator and execute the following commands.

The execution example differs depending on the type of host name of Deep Security Manager (IP address or FQDN).

- For IPv4 address

```
# ismadm security import-software-cert -software TrendMicroDeepSecurity -type ipv4 -server <IPv4 address of Deep Security Manager> -file <Certificate file name>
```

- For IPv6 address

```
# ismadm security import-software-cert -software TrendMicroDeepSecurity -type ipv6 -server <IPv6 address of Deep Security Manager> -file <Certificate file name>
```

- For FQDN

```
# ismadm security import-software-cert -software TrendMicroDeepSecurity -type fqdn -server <FQDN of Deep Security Manager> -file <Certificate file name>
```

Example: If the host name of Deep Security Manager is in IPv4 format as "192.168.100.5," and the certificate file name is "DSManager.pem1"

```
# ismadm security import-software-cert -software TrendMicroDeepSecurity -type ipv4 -server 192.168.100.5 -file DSManager.pem1
```

### 2.13.9.2 Procedure to link with Deep Security

1. Log in to the GUI of ISM and open the dashboard screen.
2. Select [Language] from the user name displayed on the top right of the screen.
3. Set the same time zone as is set for Deep Security Manager.
4. From the [ ≡ ] at the top right side of the screen, select [Add Widget].
5. From the "Add Widget" screen, select the "Other widgets" panel.

The "Cooperated widgets with Trend Micro Deep Security" screen is displayed on the "Other Widgets" screen.

6. Select the "Deep Security Computer Status" panel or the "Deep Security Anti-Malware Event History" panel, and then select the [Add] button.
7. When displaying the Trend Micro widget for the first time, set the Deep Security Manager information. In the displayed screen, enter the following.

Item	Entered contents
Host Name	IP address or FQDN of Deep Security Manager
Account Name	User account of Deep Security Manager
Password / Password (for confirmation)	Password of Deep Security Manager
Port Number	Port number of Deep Security Manager Default is 4119. When changing from 4119, enter the changed port number.

8. After entering the information, select the [Apply] button.

If the information of Deep Security Manager has already been registered, a list of the registered Deep Security Managers will be displayed. Check the Deep Security Manager displayed by the widget and select the [Apply] button.

9. The widget is displayed on the dashboard.

For descriptions of the contents displayed in the widget, refer to the ISM online help.

 **Point**

- If there is a problem with the display of the Cooperated widgets with Trend Micro Deep Security, a message is displayed in the widget. The following are the messages displayed and their contents.

Message	Action
Register a certificate.	The certificate for Deep Security Manager has not been registered. Execute the procedures in " <a href="#">2.13.9.1 Preparations in advance for Deep Security Link</a> " and register the certificate in ISM.
Certificate file does not exist. Re-register a certificate.	The certificate file is not the certificate file of Deep Security Manager. Refer to " <a href="#">2.13.9.1 Preparations in advance for Deep Security Link</a> " and retrieve a certificate again, then register it in ISM.
Certificate file is not valid. Check the certificate file.	The certificate has expired or is not valid for other reasons. Refer to " <a href="#">2.13.9.1 Preparations in advance for Deep Security Link</a> " and retrieve a certificate again, then register it in ISM.
Login failed. Management software returned an error.	There is a problem with the connection to Deep Security Manager. The following are possible causes.  <ul style="list-style-type: none"> <li>- There is an error in the Deep Security user name or password entered on the ISM GUI.</li> <li>- There is an error in the format of the certificate file. Or the host information in the certificate file is not the host name of the connection target Deep Security.</li> <li>- There is an error in the communication with Deep Security.</li> <li>- The number of Deep Security sessions exceeds the number allowed.</li> </ul> For details on the cause, check the Deep Security system event.

If the error is not solved, or if messages other than the ones above are displayed, collect maintenance data for ISM and contact your local Fujitsu customer service partner.

- Whenever you select the link to the Deep Security link widget and the logon screen of Deep Security Manager is displayed, be sure to log on. Also, do not log out after you have logged on.

If you do not follow the note mentioned above, the following symptoms may occur. In this case, execute operations mentioned in the Action column below.

Symptom	Action
The Deep Security Manager screen turns white.	Enter the following URL in the address bar of the window in which the Deep Security Manager screen is displayed.  https://<IP address of Deep Security Manager>:<Port number of Deep Security Manager>  Log on to Deep Security Manager from the displayed logon screen.
The Deep Security Manger screen is displayed in the window that the GUI of ISM has been displayed.	If you select the [Back] button of the browser, the GUI of ISM is displayed.  If you select the link in the widget, the logon screen for Deep Security Manager is displayed. Log on to Deep Security Manager.

- After you log on to Deep Security Manager from the logon screen of Deep Security Manager, the Dashboard screen for Deep Security Manager may be displayed. In this case, select the link in the widget again. Detailed information will be displayed.

## 2.14 Operations When Deleting Nodes and When Modifying Groups

---

When you are going to delete a node or modify a group, execute the operations described below.

### Deleting nodes

Before you delete a node, complete the operations described below.

- If any tasks are being executed, wait until they have completed.
- Release any profiles assignments you have made.



.....  
If you delete a node while a profile assignment is active, this node will not be deleted. (The profile remains with an "Assigned" status.)  
Release the profile assignments individually.  
.....

### Modifying groups

Before you change the affiliation of a node from one node group to another or release a node from a node group, complete the operations described below.

- If any tasks are being executed on the relevant node, wait until they have completed.
- If any profile was applied to the relevant node, release the profile.
- Delete any schedules for log collection from the relevant node.
- Delete any saved logs that were retrieved from the relevant node.
- Delete any alarm settings of the relevant node.



- .....
- For profiles that were set by users who belong to a user group, these users will no longer be able to view and modify the profile settings. In such a case, the profile has to be deleted by a user belonging to an Administrator group.
  - If you forgot to delete any saved logs, revert the node temporarily to the former user group in order to be able delete the logs.
- .....

### Deleting User Groups

Before you delete a user group, complete the operations described below.

- Release any profiles assignments you have made.
- Delete all profiles, profile groups, policies, and policy groups that are included in the user group.
- Delete all imported OS media, SVS DVD data from the repository.
- Delete any schedules for log collection.
- Delete any saved logs.



.....  
For profiles and log-related operations that were set by users who belong to a user group, these users will no longer be able to view and modify the settings for profiles and log-related operations. In such cases, the settings have to be modified by a user belonging to an Administrator group.  
.....

## **Changing user group names**

Before you change the name of a user group, make sure that none of the following tasks are currently being executed.

- Firmware data import operations
- Firmware update operations

# Chapter 3 Installation of ISM

This chapter describes how to install ISM.

## Point

When using ISM for PRIMEFLEX for constructing a virtual platform system, refer to the following for the procedure to install ISM.

- When configuring a vSAN model  
"3. Installation of Virtualized Platform System" in "FUJITSU Integrated System PRIMEFLEX for VMware vSAN V1 Installation Guide"
- When configuring an S2D model  
"3. Installation of Virtualized Platform System" in "FUJITSU Integrated System PRIMEFLEX for Microsoft Storage Spaces Direct V1 Installation Guide"

## 3.1 Workflow for Installing ISM

This section describes the workflow for installing ISM.

### (1) Installation design

When you are going to install ISM, you have to execute the following tasks in preparation.

- Disk Resource Estimation
- Repository Setup
- Network Design
- Node Name Setup
- User setup

For the contents of the operation, refer to "[3.2 Installation Design for ISM.](#)"

### (2) Installation of ISM-VA

Install ISM-VA on a management server.

For information on the installation procedure, refer to "[3.3 Installation of ISM-VA.](#)"

### (3) Setup of ISM-VA environment

Set up the operating environment in which you installed ISM-VA.

For the contents of the environment setup procedure, refer to "[3.4 Environment Settings for ISM-VA.](#)"

### (4) Registration of license

Register the license that is required for using ISM.

For information on the tasks required to register the license, refer to "[3.5 Registration of Licenses.](#)"

### (5) Registration of users

Register the ISM users.

For information on the tasks to register users, refer to "[3.6 Registration of Users.](#)"

### (6) Allocation of virtual disks

Allocate virtual disks in order to extend the disk capacities of ISM-VA.

Refer to "[3.7 Allocation of Virtual Disks](#)" to allocate virtual disks to the entire ISM-VA and Administrator user groups.

### Note

After installation of ISM-VA, immediately execute virtual disk allocation for Administrator groups according to the procedure described in "[3.7.2 Allocation of Virtual Disks to User Groups](#)."

## (7) Registration of cloud management software

Register new cloud management software if you manage the virtual machines and virtual switches of the managed node.

For details on registering the cloud management software, refer to "[2.13.6 Management of Cloud Management Software](#)." Moreover, for pre-settings required to use Virtual Resource Management, refer to the following document. For details, contact your local Fujitsu customer service partner.

"Settings for Monitoring Target OS and Cloud Management Software"

## (8) Pre-Settings for Virtual Resource Management

Refer to "[3.8 Pre-Settings for Virtual Resource Management](#)."

## (9) Pre-Settings for Cluster Management

To use Cluster Management in ISM for PRIMEFLEX, you must set it up in advance.

For details on how to set it, refer to "[3.9 Pre-Settings for Cluster Management](#)."

## 3.2 Installation Design for ISM

Designing the installation in advance is important for having ISM operate smoothly. Design the following items.

- [3.2.1 Disk Resource Estimation](#)
- [3.2.2 Network Design](#)
- [3.2.3 Node Name Setup](#)
- [3.2.4 User Design](#)

### 3.2.1 Disk Resource Estimation

For the use of ISM, execute the usage capacity estimation of disk area and preliminary additional allocation described in the table below.

Usage	Data to be stored	Calculation procedure for capacity	Type	
			System area	User area
Log archive	Logs collected by Log Management and archived files when downloading  " <a href="#">2.5 Log Management</a> "	Calculate according to the number of nodes to collect logs for, log collection types, collection frequency and retention period  " <a href="#">3.2.1.1 Estimation of log storage capacity</a> "	Y [Note 1]	Y
Repository (Exclude ServerView Suite DVD)	DVD images and firmware data  " <a href="#">2.4 Profile Management</a> "  " <a href="#">2.6 Firmware Management</a> "	Calculate according to the number of DVDs to import and the volume of firmware data  " <a href="#">3.2.1.2 Estimation of required capacities for repositories</a> "	Y [Note 1]	Y



Usage	Data to be stored	Calculation procedure for capacity	Type	
			System area	User area
Repository (Only ServerView Suite DVD)	DVD image "2.4 Profile Management" "2.6 Firmware Management"	Calculate according to the number of DVDs to import  "3.2.1.2 Estimation of required capacities for repositories"	Y	-
Node management data	Data utilized by ISM for internal operation	Calculate according to the number of nodes to manage  "3.2.1.3 Estimation of node management data capacity"	Y	-
ISM RAS Logs	Logs utilized for investigation when occurring failures	Calculate according to the number of nodes to manage  "3.2.1.4 Estimation of ISM RAS log capacity"	Y	-
Maintenance data	Files taken when archiving ISM RAS logs  "4.16 MIB File Settings"	Calculate according to the generations to store the number of nodes to manage and the documents  "3.2.1.5 Estimation of maintenance data capacity"	Y [Note 1]	Y [Note 2]
ISM Backup/Restore	ISM Backup file  "4.4.2 Backup/restoration of ISM with the ISM-VA Management Command"	Calculate according to the number of nodes to manage  "3.2.1.6 Estimation of required capacities for ISM backup/restoration"	Y [Note 1]	Y [Note 2]

[Note 1]: If user group is allocated with an area, the allocated area is used in the user group. In user groups not allocated with an area, system area is used.

[Note 2]: They are exported to the repository area of the Administrator user group.

## Note

- Disk capacities cannot be extended dynamically during the operation of ISM-VA. Therefore, if disk space runs low during operation, this has an effect on the operation of log collection for Log Management as well as of repositories and backups. Consequently, it is important to estimate the disk capacity in advance to make sure it will not run low.

Create a virtual disk with the estimated capacity and allocate it to ISM-VA.

For creating virtual disk and allocating to a system area, refer to "3.7.1 Allocation of Virtual Disks to Entire ISM-VA."

For creating virtual disk and allocating to a user group, refer to "3.7.2 Allocation of Virtual Disks to User Groups."

- In order to avoid insufficient disk space, you should also design operations to include periodical deletion of repository, backup, and other data that are no longer required.
- The disk capacity currently used can be checked with the following procedure.

1. From the console as an administrator, log in to ISM-VA.
2. Check the disk utilization rate.

```
ismadm volume show -disk -r
```

Check /dev/mapper/centos-root.

Example:

```
# ismadm volume show -disk -r
Filesystem                Size  Used Avail Use% Mounted on
```

```

/dev/mapper/centos-root  31G  4.2G   27G  14% /
devtmpfs                3.9G    0   3.9G   0% /dev
tmpfs                   3.9G  4.0K   3.9G   1% /dev/shm
tmpfs                   3.9G  225M   3.7G   6% /run
tmpfs                   3.9G    0   3.9G   0% /sys/fs/cgroup
/dev/sda1               497M  172M   326M  35% /boot
tmpfs                   783M    0   783M   0% /run/user/1005
tmpfs                   783M    0   783M   0% /run/user/0
tmpfs                   783M    0   783M   0% /run/user/1001

  PV          VG      Fmt  Attr  PSize   PFree
  /dev/sda2  centos lvm2  a--  19.51g    0
  /dev/sda3  centos lvm2  a--  15.00g    0
#

```

### 3.2.1.1 Estimation of log storage capacity

The disk capacities for logs exported through Log Management depend on the number of managed nodes and on the period or frequency of log retention. In estimating the capacities, you should also take the possible number of additional node installations in the future into account.

In addition, estimate disk capacity used when downloading logs in the same way.

For information on how to estimate disk capacities for logs that are exported with Log Management, refer to "[A.3.3 General Standards for Disk Usage in Using Log Management.](#)"

### 3.2.1.2 Estimation of required capacities for repositories

In order to operate functions such as Profile Management or Firmware Management, you must prepare repositories in ISM-VA. In a repository, the following data are stored.

- Firmware data
- OS image files
- Work files

The disk capacities required for repositories vary with the types of OS to be installed on the managed nodes and the numbers of Update DVDs to be imported, but it is normal for them to use 10 GB and more. Refer to the table below when you estimate the required capacities.

Usage	Operation	Required capacity
Storage of firmware data	Import from Update DVD	Approximately 7 GB per Update DVD
	Import of other firmware data	Depends on data to be imported.
File storage for OS installation media	Import from Windows installation media	Approximately 3 to 8 GB per OS type Import of only the OS types to be installed with Profile Management is required.
	Import from VMware ESXi installation media	Approximately 0.5 GB per OS type Import of only the OS types to be installed with Profile Management is required.
	Import from Linux installation media	Approximately 4 GB per OS type
Storage of ServerView Suite DVD	Import from ServerView Suite DVD	Approximately 8 GB per ServerView Suite DVD
Creation and storage of files for work	None	Approximately 0.5 GB
Collection and storage of core files	Setting of ismadm system core-dir	Approximately 1 GB

## Point

- By correlating user groups and node groups, you can operate ISM separately for each node group. To do so, you have to prepare a separate repository for each user group. In this case, you must estimate the required disk capacities (excluding the one for the ServerView Suite DVD) for repositories only for the number of user groups.
- The ServerView Suite DVDs are stored in the system area. Depending on the number of ServerView Suite DVDs to be used, you must estimate the required disk capacity on the LVM volume in the system area.

### 3.2.1.3 Estimation of node management data capacity

According to the number of nodes to manage in ISM-VA, estimate disk capacity for node management data area.

The following is an estimation of the number of managed nodes and disk capacity required for the node management data area.

Number of managed nodes	Required disk capacity	
	When not monitoring the network statistics information	When monitoring the network statistics information
100 nodes or less	20 GB	25 GB
400 nodes or less	80 GB	100 GB
1000 nodes or less	200 GB	250 GB

For information on the network design, refer to "[2.7 Network Management](#)."

### 3.2.1.4 Estimation of ISM RAS log capacity

According to the number of nodes to manage in ISM-VA, change the ISM RAS log levels and estimate the disk capacity.

The following chart shows approximate values for the required disk capacities for various numbers of managed nodes and the corresponding log areas.

Number of managed nodes	ISM RAS log level	Required disk capacity
100 nodes or less	small (default)	10 GB
400 nodes or less	medium	40 GB
1000 nodes or less	large	100 GB

For details on how to switch the log level, refer to "[4.5.1.2 Switching the ISM RAS Log level](#)."

### 3.2.1.5 Estimation of maintenance data capacity

According to the number of nodes to manage in ISM-VA, change the ISM RAS log levels and estimate the disk capacity.

The following is an estimation of the number of managed nodes and required disk capacity for the maintenance data area.

Number of managed nodes	ISM RAS log level	Required disk capacity
100 nodes or less	Small (default)	15 GB
400 nodes or less	Medium	50 GB
1000 nodes or less	Large	120 GB

For details on how to switch the log level, refer to "[4.5.1.2 Switching the ISM RAS Log level](#)."

### 3.2.1.6 Estimation of required capacities for ISM backup/restoration

According to the number of nodes to manage in ISM-VA, estimate the disk capacity required for ISM backup/restore.

The following is an estimation of the number of managed nodes and required disk capacity for ISM backup/restore.

Number of managed nodes	Required disk capacity
100 nodes or less	15 GB
400 nodes or less	60 GB
1000 nodes or less	150 GB

## 3.2.2 Network Design

---

ISM uses the following two types of management LAN to manage servers:

Connect the network used in ISM to two types of management LANs.

- Networks connected to iRMC Management LAN

This type of network is mainly used for controlling servers or executing BIOS, iRMC, MMB or virtual IO settings.

- Networks connected to the onboard LAN or LAN card

This type of network is mainly used for OS installation and for establishing connections after OS installation.

Moreover, network connections are required for managing switches and storages. These can be either divided into physical and logical connections or used as one single integrated connection.



ISM-VA starts by default while the IP address "192.168.1.101" remains enabled. Be careful about overlapping with IP addresses of the other devices within the network.

You can avoid such IP address overlap by changing the IP address in the following procedure if an overlapped IP address is found.

1. Install ISM-VA on a hypervisor other than the one in the actual environment.
2. Change the IP address of ISM-VA.
3. Backup according to the procedure in "4.4 Backup and Restoration of ISM-VA."
4. Restore the ISM-VA that was backed up with hypervisor in the actual environment, according to the procedure described in "Restoration of ISM-VA with the Import Function."



- It is recommended that you prepare separate networks for service use (Production LANs) besides these management LANs.
- By correlating user groups and node groups, you can operate ISM separately for each node group. To do so, design separate networks for each node group. You can also set up firewalls around the network of each node group in order to separate data communication between groups and there by prevent viewing and manipulation of nodes that belong to other node groups.
- You can define only one network interface for ISM. If you are going to configure multiple networks, configure the router to enable communication between the networks.

## 3.2.3 Node Name Setup

---

Determine naming rules for nodes and profiles that will be required for node registration.

When you register a node, give it a unique name.

You can set up a maximum of 64 characters.

Note, however, that you cannot use the following characters.

Slash (/), Backslash (\), Colon (:), Asterisk (\*), Question mark (?), Double quotation ("), Angle brackets (<>), or Pipeline (|)

### 3.2.4 User Design

---

Set up appropriate user roles and user groups according to the actual tasks and functions of each user. It is recommended that you execute the user settings according to the actual tasks and functions of each user within the framework, setting up user roles according to such tasks as installation, monitoring, or maintenance of nodes, and setting up user groups organization-wise for only the actual users of each node resource.

If you are going to operate nodes separately for each user group, you should define a node that is operated and managed by a given user group as a node group and then correlate the user group with the node group. When you do so, you have to create a user with an Administrator role within the user group.

For details on user groups and users, refer to "[2.13.1 User Management](#)."

In order to ensure security in Node Management, it is also recommended that you design operations so that users are removed as soon as they have become obsolete, that passwords have to be changed at regular intervals, and so on.

For information on how to execute settings for user roles and user groups and on how to change passwords, refer to the ISM online help.

## 3.3 Installation of ISM-VA

---

The ISM software is supplied with a media pack of the products related to FUJITSU Software Infrastructure Manager.

Install ISM-VA according to the installation destination.

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

- [3.3.1 Installation on Microsoft Windows Server Hyper-V](#)
- [3.3.2 Installation on VMware vSphere Hypervisor](#)
- [3.3.3 Installation on KVM](#)

### 3.3.1 Installation on 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.
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."
4. On the "Choose Import Type" screen, select [Copy the virtual machine (create a new unique ID)], and then select [Next].
5. On the "Choose Destination" and "Choose 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].
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 how to convert, refer to the Hyper-V manual.

## 3.3.2 Installation 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.

- [Installation on VMware ESXi 5.5 or VMware ESXi 6.0](#)
- [Installation on VMware ESXi 6.5 or later](#)

### Installation on VMware ESXi 5.5 or VMware ESXi 6.0

1. Start vSphere Client and select [Deploy OVF Template] from the [File] menu.
2. On the source selection screen, select the ova file that is included in the DVD media, and then select [Next].
3. On the "Storage" screen, specify the location where the virtual machine is saved, and then select [Next].
4. On the "Disk Format" screen, select [Thick Provision Lazy Zeroed] or [Thick Provision Eager Zeroed], and then select [Next].
5. On the "Network Mapping" screen, select the network to be used by ISM, and then select [Next].
6. Select [Finish] to finish deployment of OVF templates.

### Installation 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. In the "Select creation type" screen, select [Deploy a virtual machine from an OVF or OVA file] and then select [Next].
3. In 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 select [Next].
4. In the "Select storage" screen, select the datastore to deploy to and select [Next].
5. In the "Deployment options" screen, select the network being used, select "Thick" for Disk provisioning and then select [Next].
6. In the "Ready to complete" screen, confirm the settings and then select [Finish] to complete deployment.

## 3.3.3 Installation 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
```



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 details 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].

## 3.4 Environment Settings for ISM-VA

---

Execute the initial setup after installing ISM-VA.

### 3.4.1 First Start of ISM-VA

---

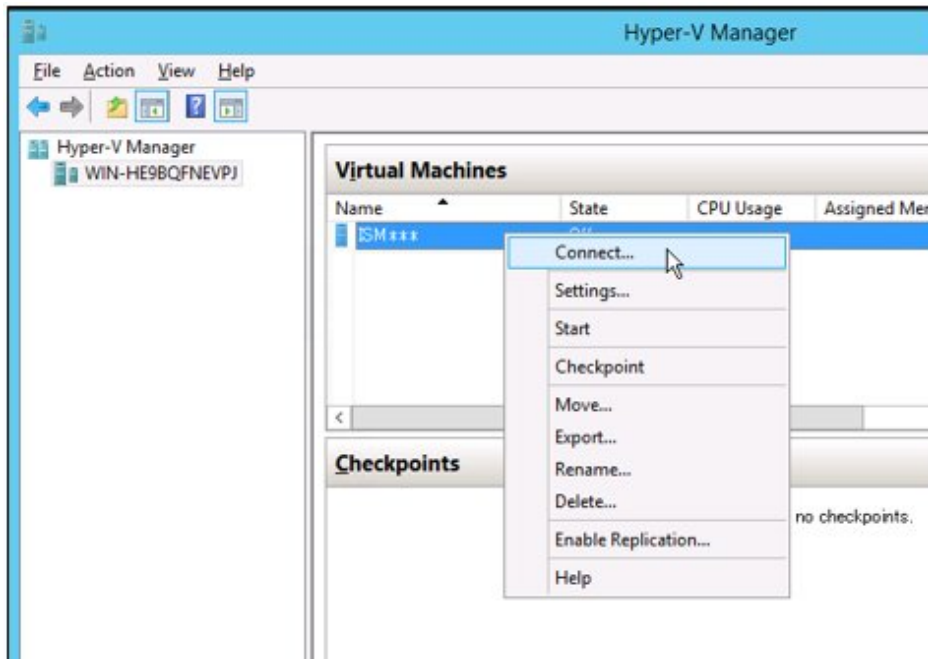
Use the respective function of the hypervisor on the installation destination to start up ISM-VA. Start up ISM-VA as a host OS user with administrator privileges.

The following procedures describe how to start up ISM-VA from Microsoft Windows Server Hyper-V, VMware vSphere Hypervisor, and KVM.

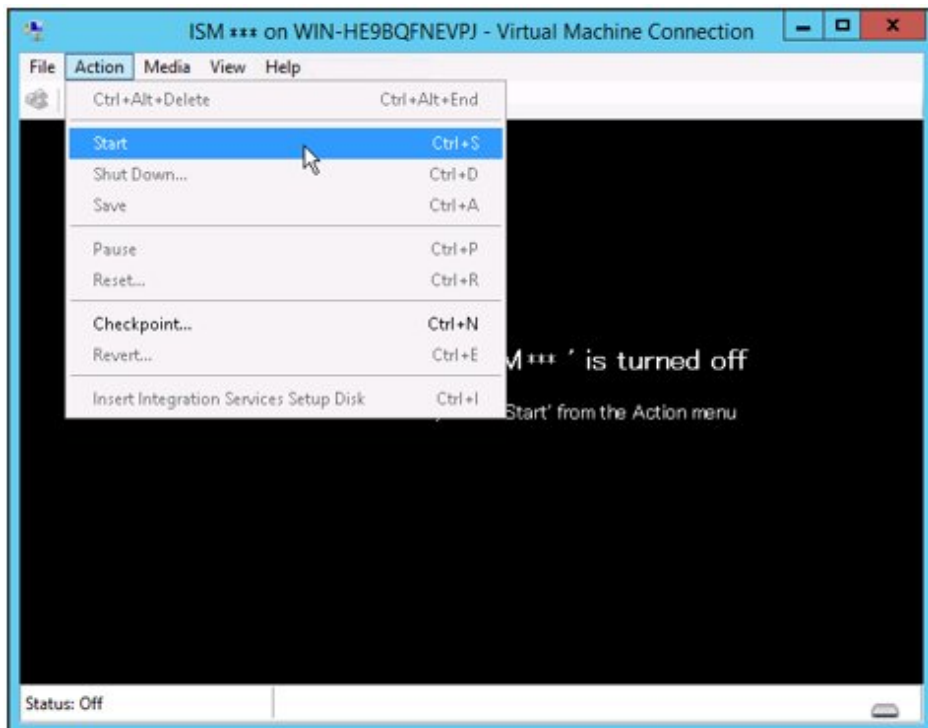
- [3.4.1.1 For ISM-VA running on Microsoft Windows Server Hyper-V \(First Time\)](#)
- [3.4.1.2 For ISM-VA running on VMware vSphere Hypervisor \(First Time\)](#)
- [3.4.1.3 For ISM-VA running on KVM \(First Time\)](#)

### 3.4.1.1 For ISM-VA running on Microsoft Windows Server Hyper-V (First Time)

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



2. On the "Virtual Machine Connection" screen, select [Start] from the [Action] menu to start ISM-VA.



### 3.4.1.2 For ISM-VA running on VMware vSphere Hypervisor (First Time)

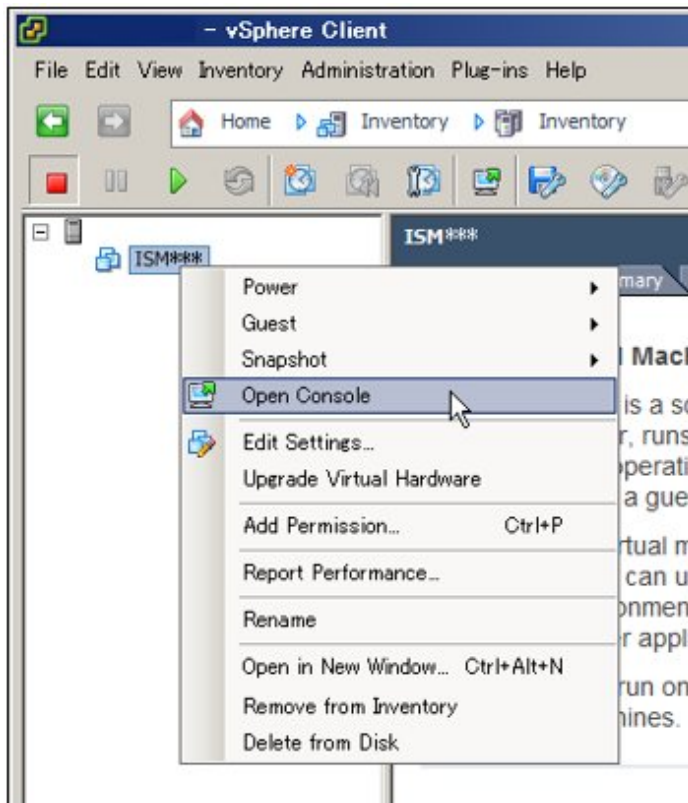
Procedures differ depending on the version of VMware ESXi. Refer to the specific reference for your version.

- [VMware ESXi 5.5 or VMware ESXi 6.0](#)
- [VMware ESXi 6.5 or later](#)

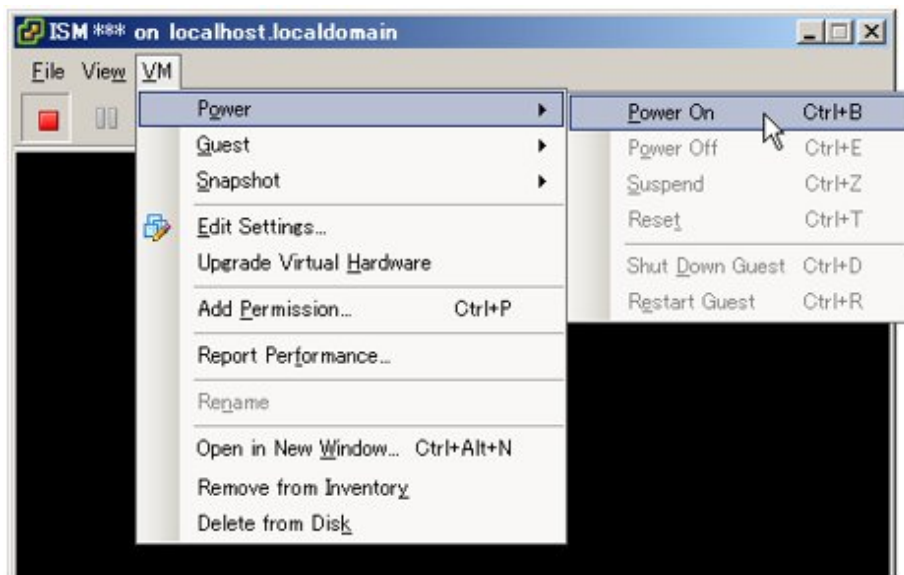


## VMware ESXi 5.5 or VMware ESXi 6.0

1. In vSphere Client, right-click on the installed ISM-VA, and then select [Open Console].

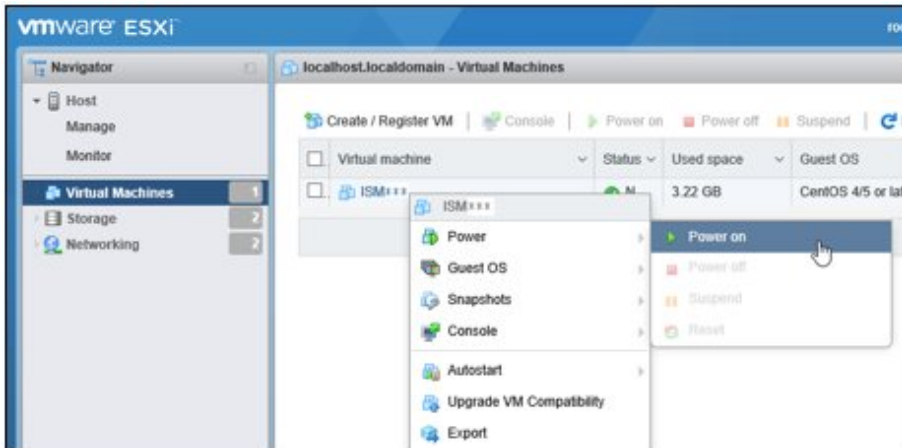


2. On the "Console" screen, select [Power] - [Power On] from the [VM] menu to start ISM-VA.

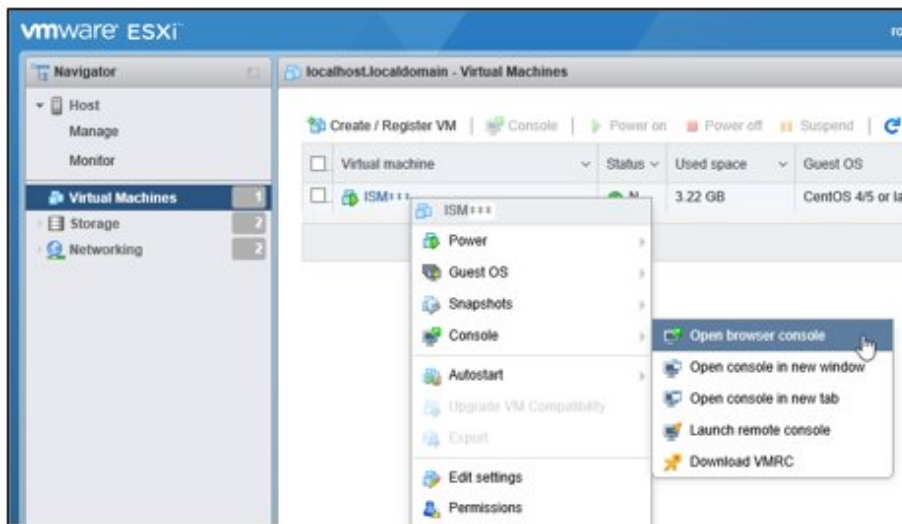


## VMware ESXi 6.5 or later

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



2. Right-click on the installed ISM-VA, and then select [Open browser console] or other console.



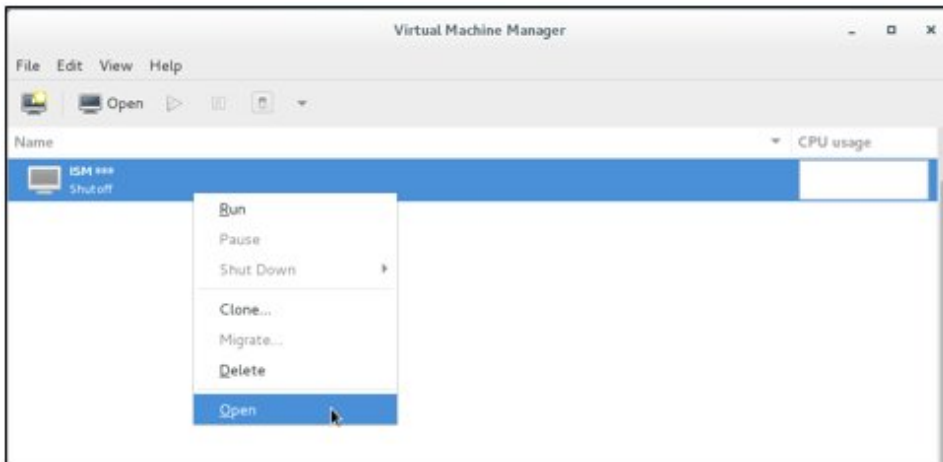
### Point

The following message may be displayed when starting up ISM-VA, but the ISM-VA settings are optimized to operate on VMware ESXi 5.5/6.0/6.5/6.7, so this is not a problem.

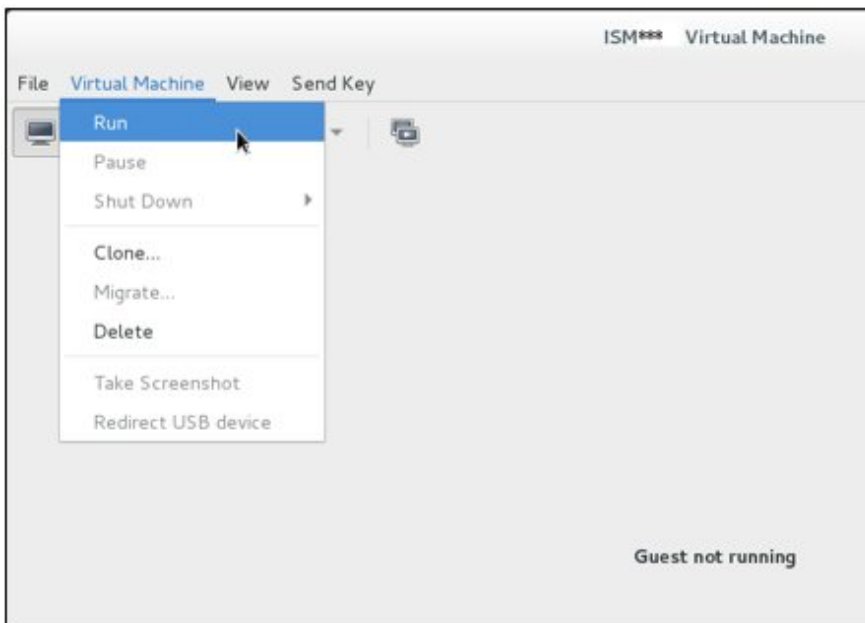
The configured guest OS (CentOS 4/5 or later (64-bit)) for this virtual machine does not match the guest that is currently running (CentOS 7 (64-bit)). You should specify the correct guest OS to allow for guest-specific optimizations.

### 3.4.1.3 For ISM-VA running on KVM (First Time)

1. In Virtual Machine Manager, right-click on the installed ISM-VA, and then select [Open].



2. On the "ISM-VA Virtual Machine" screen, select [Run] from the [Virtual Machine] menu to start ISM-VA.



## 3.4.2 Initial Setup of ISM-VA

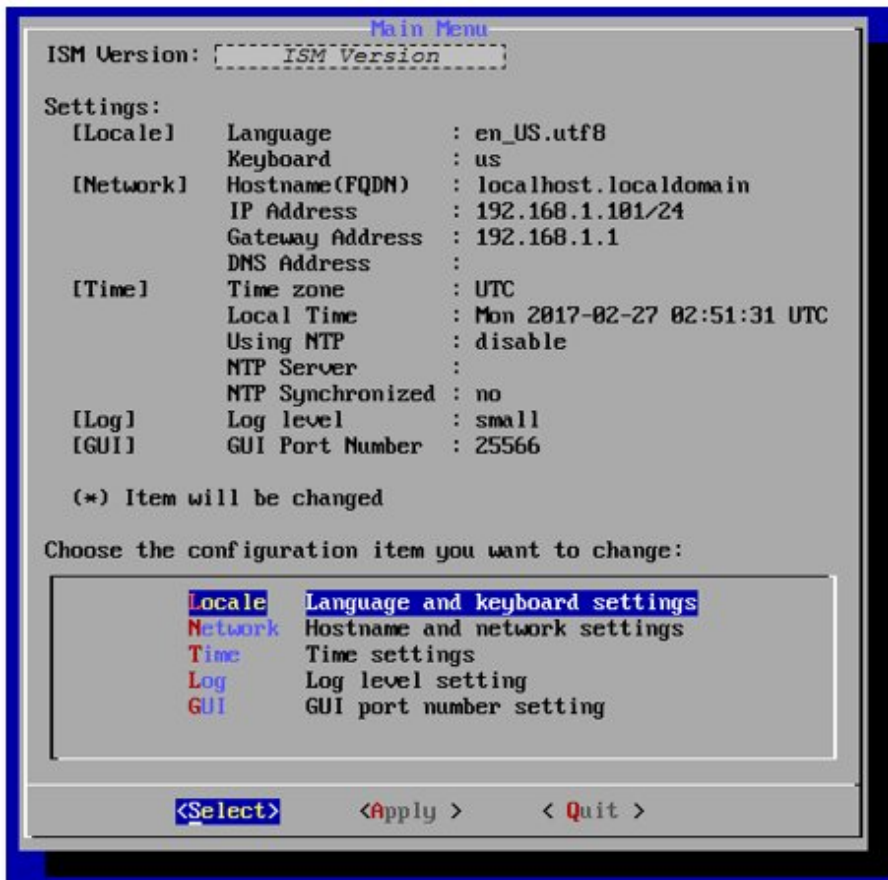
After starting ISM-VA, use the console basic setting menu or the ismadm commands to execute the basic setting menu for ISM-VA.

### 3.4.2.1 Initial setup using the Basic Setting Menu

1. Use the administrator account and the default password to log in to the console.
  - Administrator account: administrator
  - Default password: admin
2. Execute the following command to start the basic setting menu.

```
# ismsetup
```

The screen below is displayed.



3. Execute the ISM-VA settings.

In the basic setting menu, the following items can be set.

- Locale
- Network
- NTP server
- Log level
- Web GUI port number

For details on the basic setting menu, refer to "4.2 ISM-VA Basic Settings Menu."

When domain environment settings are required, execute Step 5 in "3.4.2.2 Initial setup using the ismadm command."

### 3.4.2.2 Initial setup using the ismadm command

1. Use the administrator account and the default password to log in to the console.

- Administrator account: administrator
- Default password: admin

2. From the console, execute the network settings.

- Confirm the LAN device names

```
# ismadm network device
DEVICE  TYPE      STATE      CONNECTION
eth0    ethernet  connected  eth0
lo      loopback  unmanaged  --
```

- Set up network and host name

```
# ismadm network modify <LAN device name> ipv4.method manual ipv4.addresses <IP address>/  
<Maskbit> ipv4.gateway <Gateway IP address> +ipv4.dns <DNS server>  
  
# ismadm system modify -hostname <Host name (FQDN)>
```

Example of command execution:

```
# ismadm network modify eth0 ipv4.method manual ipv4.addresses 192.168.1.101/24 ipv4.gateway  
192.168.1.1 +ipv4.dns 192.168.1.2  
  
You need to reboot the system to enable the new settings.  
Immediately reboots the system. [y/n]:  
  
# ismadm system modify -hostname ismva2.domainname  
You need to reboot the system to enable the new settings.  
Immediately reboots the system. [y/n]:
```

When command execution is complete, a confirmation message is displayed, prompting whether you want to reboot the system; enter "y" to reboot the system.

When executing the network settings and the host name settings at the same time, only reboot once after executing the latter settings.

The operations after executing the network/host name settings can be executed from both the hypervisor console as well as another console via SSH in the same ways. However, we recommend access via SSH for its good operability.

3. From the console, set the System Locale and the Keymap.

Use the following procedure to confirm the current settings.

```
# ismadm locale show  
System Locale: LANG=ja_JP.UTF-8  
VC Keymap: jp  
X11 Layout: jp
```

Use the following commands to change the current settings.

- Locale setting

```
# ismadm locale set-locale LANG=<Locale name>
```

Example of command execution:

```
# ismadm locale set-locale LANG=en_US.utf8
```

- Display of available <Locale name>

```
# ismadm locale list-locales
```

- Keymap setting

```
# ismadm locale set-keymap <Keymap name>
```

Example of command execution:

```
# ismadm locale set-keymap us
```

- Display of available <Keymap name>

```
# ismadm locale list-keymaps
```

Table 3.1 Keymap list

Language	Keymap Name
Japanese	jp
English	us
German	de-nodeadkeys
Chinese	cn
Korean	kr
Filipino	ph

Any modifications of System Locale become effective only after restarting ISM-VA.

4. From the console, set the date and time.

Use the following procedure to confirm the current settings.

```
# ismadm time show
  Local time: Thursday 2016-06-09 16:57:40 JST
  Universal time: Thursday 2016-06-09 07:57:40 UTC
  Time zone: Asia/Tokyo (JST, +0900)
  NTP enabled: no
  NTP synchronized: no
  RTC in local TZ: no
  DST active: n/a

NTP Servers:
506 Cannot talk to daemon
```

Use the following commands to change the current settings.

- Time zone setting

```
# ismadm time set-timezone <Time zone>
```

Example of command execution:

```
# ismadm time set-timezone America/New_York
```

- Display of available time zones

```
# ismadm time list-timezones
```

- Setting of date and time

```
# ismadm time set-time <Date> <Time>
```

Example of command execution:

```
# ismadm time set-time 2016-06-09 17:10:00
```

- Enable/Disable NTP synchronization

Enable

```
# ismadm time set-ntp 1
```

Disable

```
# ismadm time set-ntp 0
```

- Add/Remove NTP server

Add NTP server

```
# ismadm time add-ntpserver <NTP server>
```

Remove NTP server

```
# ismadm time del-ntpserver <NTP server>
```

5. From the console, set the domain environment.

This setting is not required if you do not use the domain environment.

- Adding of domain setting information

```
# ismadm kerberos add -d <Domain Name> -r <Realm> -n <Controller Name>
```

Example of command execution:

```
# ismadm kerberos add -d sample.local -r SAMPLE.LOCAL -n adsvr.sample.local
```

- Display of domain setting information

```
# ismadm kerberos show
```

- Going back to previous domain setting information

```
# ismadm kerberos restore
```

Unable to return to more than one previous state.

- Initialization of domain setting information

```
# ismadm kerberos init
```

## 3.5 Registration of 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 licenses for ISM, refer to "[1.1.2 Product System and Licenses](#)."

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

### Procedure of 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
# [Type] [Edition] [#Node] [Exp.Date] [Reg.Date] [Licensekey]
1 Server Adv. - - 2018-01-01 *****==
2 Node Adv. 10 - 2018-01-01 *****==
```

Table 3.2 Description of the exported command results

Item	Description
[Type]	Displays "Server" for a server license and "Node" for a node license.
[Edition]	Displays the type of license. - Adv.: ISM license - I4P: ISM for PRIMEFLEX license
[#Node]	Displays the number of nodes that can be managed on that license. Always displays a "-" if the license type is "Server."
[Exp.Date]	Displays the expiration date of the license. Always displays a "-" if it is unlimited.
[Reg.Date]	Displays the date and time when the license was registered.
[Licensekey]	Displays the character string of the registered license key.

4. Restart ISM-VA.

```
# ismadm power restart
```

### Register from the operating GUI of a Web browser

When registering a license for the first time

1. Implement "3.4.2 Initial Setup of ISM-VA."
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.



.....  
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.



If registering additional node licenses

From the GUI, log in as 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. Use the following procedure to register the 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 of licenses in "[4.8 License Settings](#)."

## 3.6 Registration of Users

---

Register the users required in order to operate ISM.

For details on how to register users, refer to "[2.13.1 User Management](#)."

## 3.7 Allocation of 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.



#### Point

For detailed procedures for the virtual disk creation and connection method, refer to "Operating Procedures."

### 3.7.1 Allocation of Virtual Disks to Entire ISM-VA

---

This section uses the Administrator group as an example to show 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).  
Create the virtual disks so as to be controlled by SCSI controllers.
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
```

## 3.7.2 Allocation of 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).  
Create the virtual disks so as to be controlled by SCSI controllers.
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 of command execution:

```

# 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

```

## 3.8 Pre-Settings for Virtual Resource Management

Operation monitoring for the virtualized platform can be executed by using Virtual Resource Management.

Management and monitoring for the virtual resource can be executed from the each management screen of the virtual resource on ISM GUI.

For the descriptions for the contents and displayed items of the GUI for Virtual Resource Management, refer to the ISM online help.



### Note

- For pre-settings for Virtual Resource Management, refer to "[A.1.2 Pre-settings for Virtual Resource Management.](#)"
- For the pre-settings for PRIMEFLEX for Microsoft Storage Spaces Direct, also execute the following settings for clusters.  
"Settings for Monitoring Target OS and Cloud Management Software" - "3.2.1. Settings When Using Domain User Account" - "(5) Kerberos delegation configuration for Active Directory."

## 3.9 Pre-Settings for Cluster Management

---

This section describes the settings required in advance for operation management of Cluster Management.

### 3.9.1 Pre-Settings for vSAN

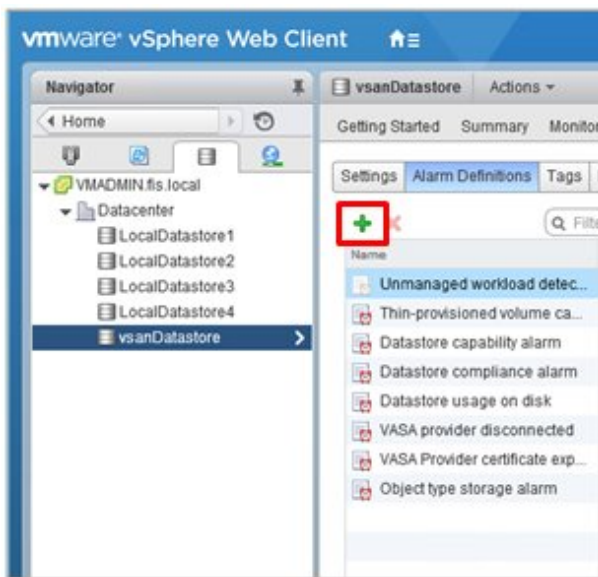
---

A vSAN alarm is required to be able to detect a datastore error when the network connection between hosts has been broken. Describes how to add vSAN alarm definitions.

1. Display the vSphere Web Client screen, select storage from [Home] - [Navigator], and then select the created vSAN datastore.

The following is if the vSAN datastore name is "vsanDatastore."

Select [Alarm Definition] (for vCenter Server Appliance 6.0 Update 2) from the [Management] tab on the right side of the displayed screen, or select [Problems] - [Alarm Definition] (for vCenter Server Appliance 6.5 or vCenter Server Appliance 6.7) from [Monitoring] and select [+].



- When the wizard screen is displayed, enter "Alarm name" and "Description" according to the following table, then select the [Next] button.

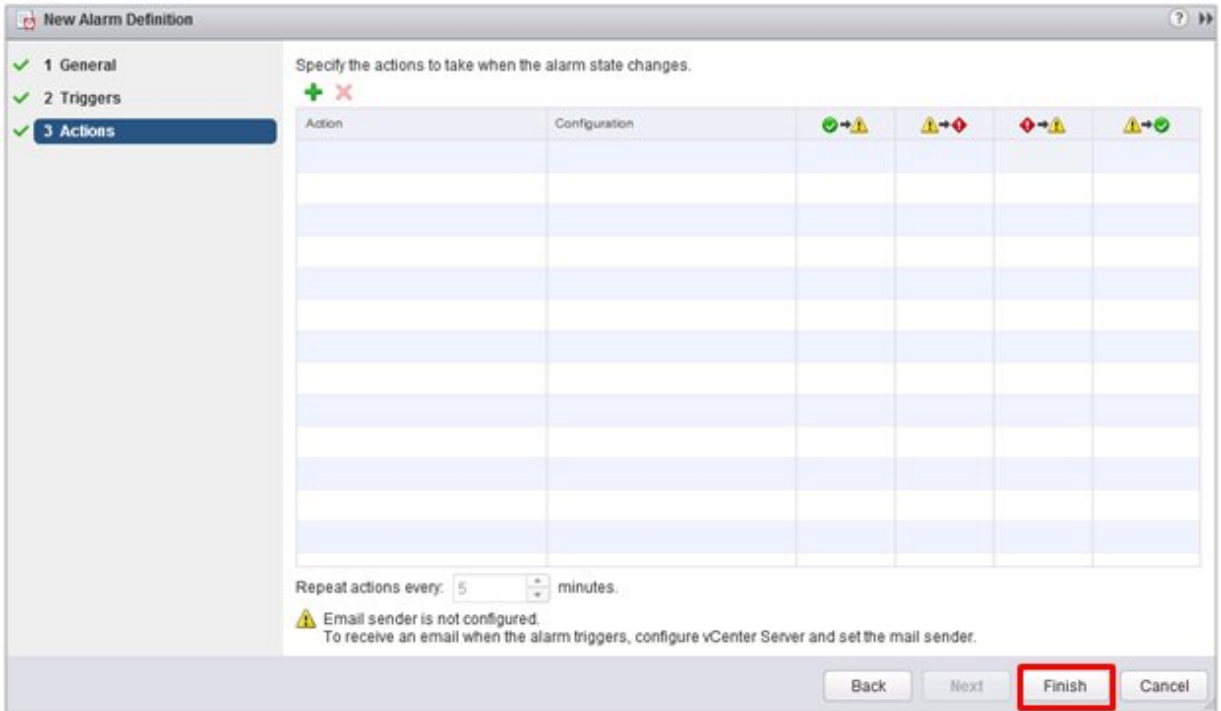
Item	Entered contents
Alarm name	Network connection between hosts
Description	Alarm for when the network between hosts has been disconnected

- Select [+] in the following screen, set each item according to the following table, then select the [Next] button.

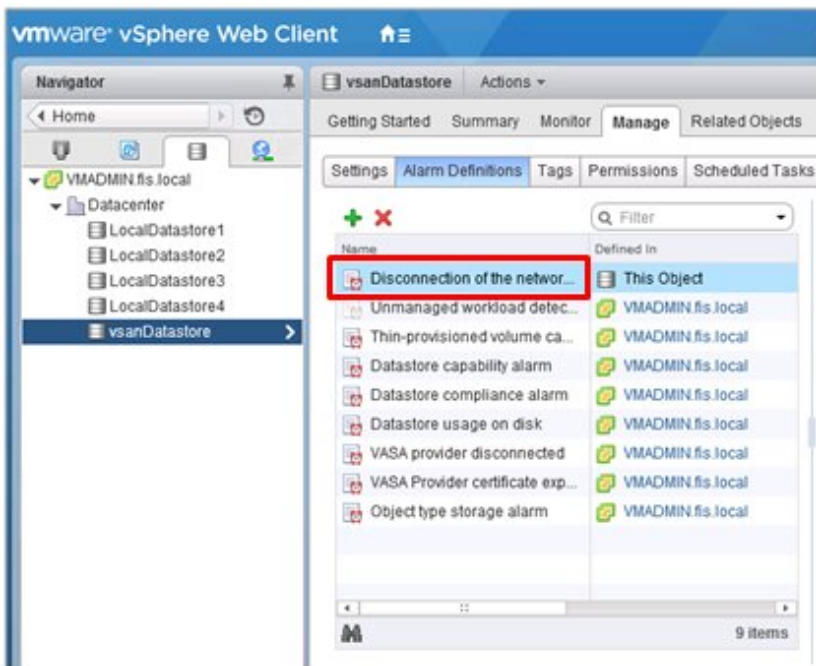
Trigger	Operator	Warning Condition	Critical Condition
Datastore State to All Hosts	is equal to	None	Disconnected

Item	Parameter
Trigger	Datastore State to All Hosts
Operator	Is equal to
Warning Conditions	None
Critical Conditions	Disconnected

4. Action is not required to be set. Select the [Finish] button (or the [Close] button).



When it is completed, the correct alarm definition is added to the alarm definition.



## 3.9.2 Pre-settings for Microsoft Storage Spaces Direct

To manage operation of PRIMEFLEX for Microsoft Storage Spaces Direct, you must execute the OS monitoring settings for ISM-VA and to enable CredSSP authentication all nodes configuring the storage pools. It is executed with the following procedures.

### Setting Windows OS monitoring from ISM

Execute the settings for monitoring Windows OS from ISM.

The information on the installation procedures are described in the following document. For details, contact your local Fujitsu customer service partner.

"Settings for Monitoring Target OS and Cloud Management Software"

- "2.1. Setting Procedure for Windows"
- "3.2. Setting Procedure for Microsoft Failover Cluster"

#### Note

- A domain user account is used for the operation management of PRIMEFLEX for Microsoft Storage Spaces Direct. Implement everything, including the procedure for when using the domain user account.
- Also execute the settings for clusters "3.2. Setting Procedure for Microsoft Failover Cluster" - "3.2.1. Settings When Using Domain User Account" - "(5) Kerberos delegation configuration for Active Directory."

### Settings to enable CredSSP authentication

Set CredSSP authentication to enabled for all nodes configuring the storage pool.

The nodes configuring the storage pool can be checked with the server manager or the failover cluster manager.

#### Note

If this setting is not executed, Virtual Resource Management for PRIMEFLEX for Microsoft Storage Spaces Direct cannot be used.

The following shows the procedure to execute the settings to enable CredSSP authentication.

1. Log in to the node as an ISM administrator (a user belonging to the Administrator group and having Administrator role), and start PowerShell with administrator privilege.
2. Execute the following commands.

```
Enable-WSManCredSSP -Role client -DelegateComputer <target node (full computer)name>
```

To specify all the full computer names in the domain, the wild card (\*) can be used.

Example of command execution:

```
Enable-WSManCredSSP -Role client -DelegateComputer *.pfdomain.local
```

If a message confirming whether or not to enable CredSSP authentication is displayed, enter "Y" and press the [Enter] key.

3. Continue by executing the following commands.

```
Enable-WSManCredSSP -Role server
```

If a message confirming whether or not to enable CredSSP authentication is displayed, enter "Y" and press the [Enter] key.

4. You can use the following command to check the enable setting of CredSSP authentication.

```
Get-WSManCredSSP
```

If a command result such as the following is displayed, the enable setting of CredSSP authentication is executed.

Example:

```
This computer is configured to permit the delegation of new certificate information for the next targets.  
wsman/*.pfdomain.local  
This computer is configured to receive certificate information from a remote client computer.
```

### 3.9.3 Pre-settings for ISM

---

Implement the settings required for ISM. Registration of the cloud management software and the OS information is executed.

#### Registering cloud management software

Register the cloud management software in ISM.

For details, refer to "[2.13.6 Management of Cloud Management Software](#)."

1. From the Global Navigation Menu on the GUI of ISM, select [Settings] - [General] - [Cloud Management Software].
2. From the [Actions] button, select [Register].
3. Enter the information that is required for registration.

For details on the information, refer to the ISM online help.



- For PRIMEFLEX for Microsoft Storage Spaces Direct the IP address representative of the cluster is set for the IP address.
- The tab specifies the following.
  - vSAN  
VMware vCenter Server 6.0, 6.5 or 6.7
  - PRIMEFLEX for Microsoft Storage Spaces Direct  
Microsoft Failover Cluster (Windows Server 2016 or Windows Server 2019)
- If you specified Microsoft Failover Cluster, make sure to enter the domain name in upper-case letters.

4. Select the [Register] button.

The cloud management software registered with Cloud Management Software List screen is displayed.

#### OS information registration

Register the OS information of the node.

The OS information includes information such as the OS type, IP addresses, and the account information that is required for connecting to the OS.



For PRIMEFLEX for Microsoft Storage Spaces Direct, refer to "[3.9.2 Pre-settings for Microsoft Storage Spaces Direct](#)."

1. From the Global Navigation Menu on the GUI of ISM, select [Management] - [Nodes].  
The "Node List" screen is displayed.
2. Select the name of the applicable node and select the [OS] tab.
3. From the [OS Actions] button, select [Edit OS Information].



4. Enter the information that is required for registration.

- The OS type and OS version specifies the following.

- For vSAN

- OS type: VMware ESXi

- OS version: 6.0, 6.5 or 6.7

- For Storage Spaces Direct

- OS type: Windows Server

- OS version: 2016 or 2019

- Enter OS IP address.

- In account, enter the local user account.

5. After entering the information, select the [Apply] button.

Confirm that "Basic Info" and "Information from OS" are displayed.



### Note

Leave it blank, without setting the domain name.

It is not required to set a domain name to use a local account for operations between ISM and the OS.

# Chapter 4 Operation of ISM

This chapter describes how to control ISM.

## 4.1 Start and Stop of ISM

Sometimes, it may be required to start up or stop ISM manually for maintenance or other reasons.

### 4.1.1 Start of ISM-VA

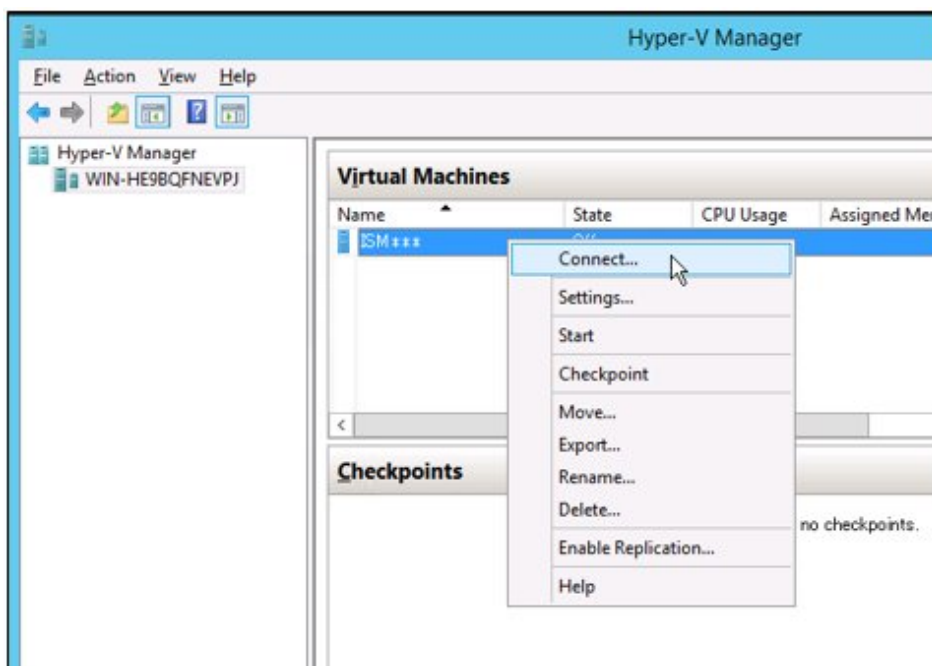
Use the respective function of the hypervisor on the installation destination to start up ISM-VA. Start up ISM-VA as a host OS user with administrator privileges.

The following procedures describe how to start up ISM-VA from Microsoft Windows Server Hyper-V, VMware vSphere Hypervisor, and KVM.

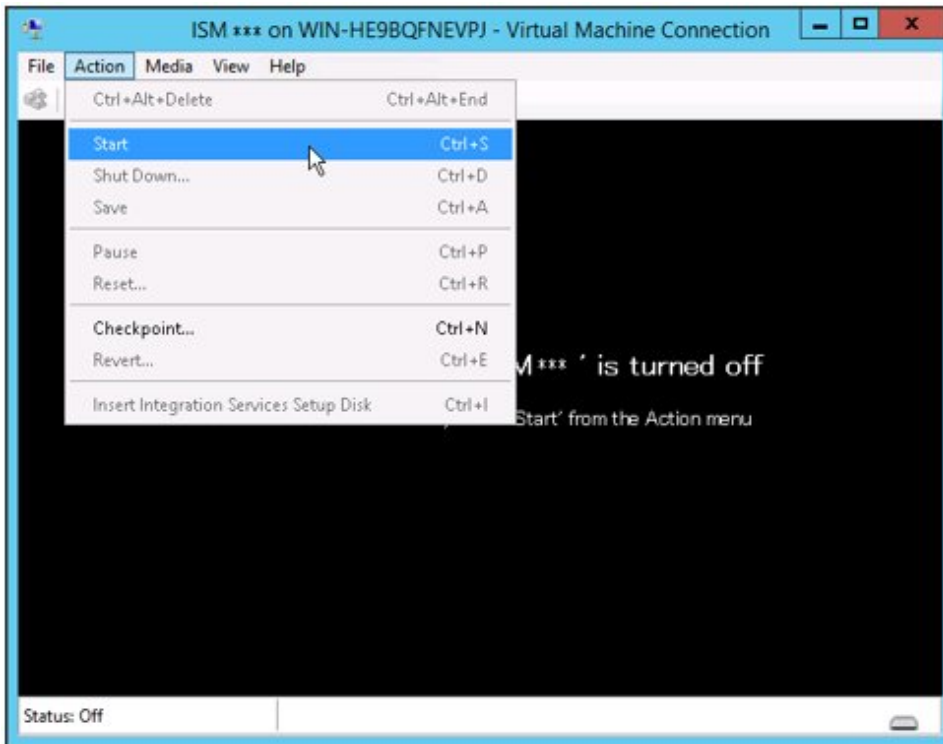
- [4.1.1.1 For ISM-VA running on Microsoft Windows Server Hyper-V \(after installation\)](#)
- [4.1.1.2 For ISM-VA running on VMware vSphere Hypervisor \(after installation\)](#)
- [4.1.1.3 For ISM-VA running on KVM \(after installation\)](#)

#### 4.1.1.1 For ISM-VA running on Microsoft Windows Server Hyper-V (after installation)

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



2. On the "Virtual Machine Connection" screen, select [Start] from the [Action] menu to start ISM-VA.



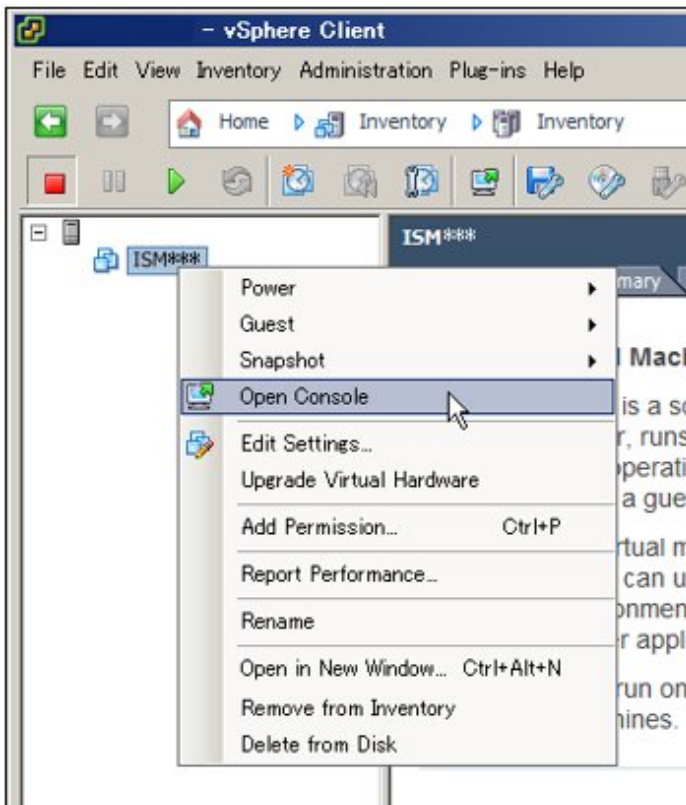
#### 4.1.1.2 For ISM-VA running on VMware vSphere Hypervisor (after installation)

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

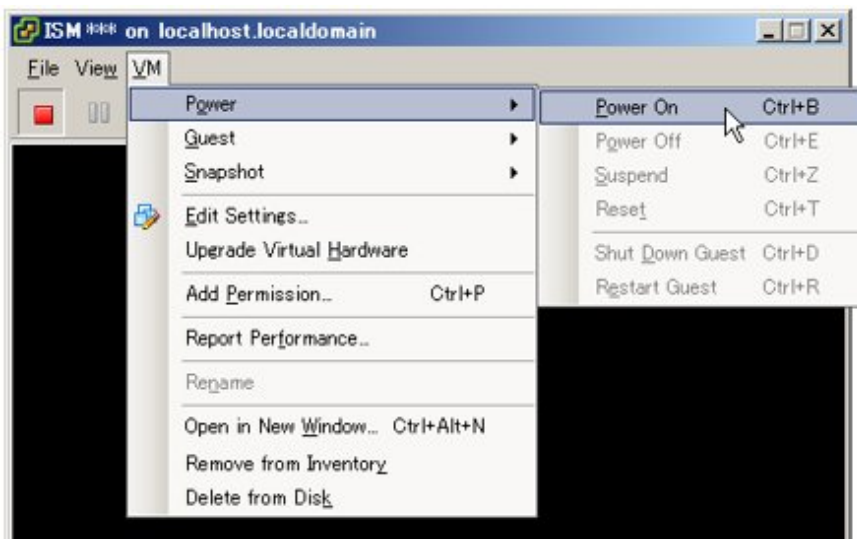
- [VMware ESXi 5.5 or VMware ESXi 6.0](#)
- [VMware ESXi 6.5 or later](#)

## VMware ESXi 5.5 or VMware ESXi 6.0

1. In vSphere Client, right-click on the installed ISM-VA, and then select [Open Console].

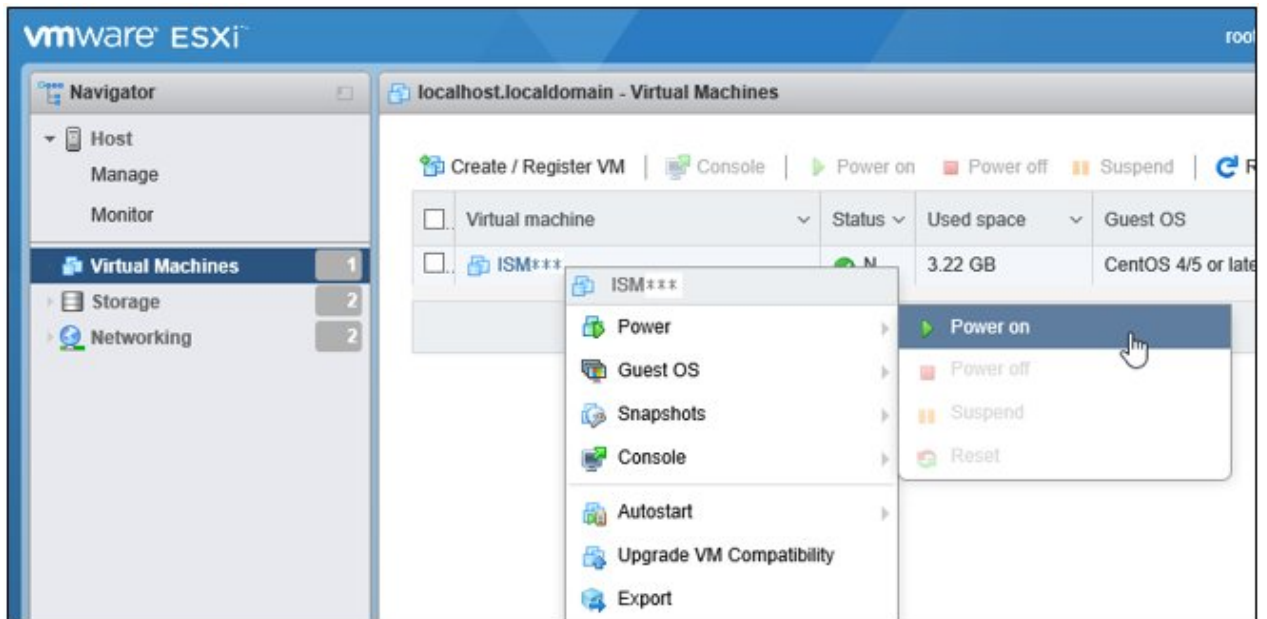


2. On the "Console" screen, select [Power] - [Power On] from the [VM] menu to start ISM-VA.

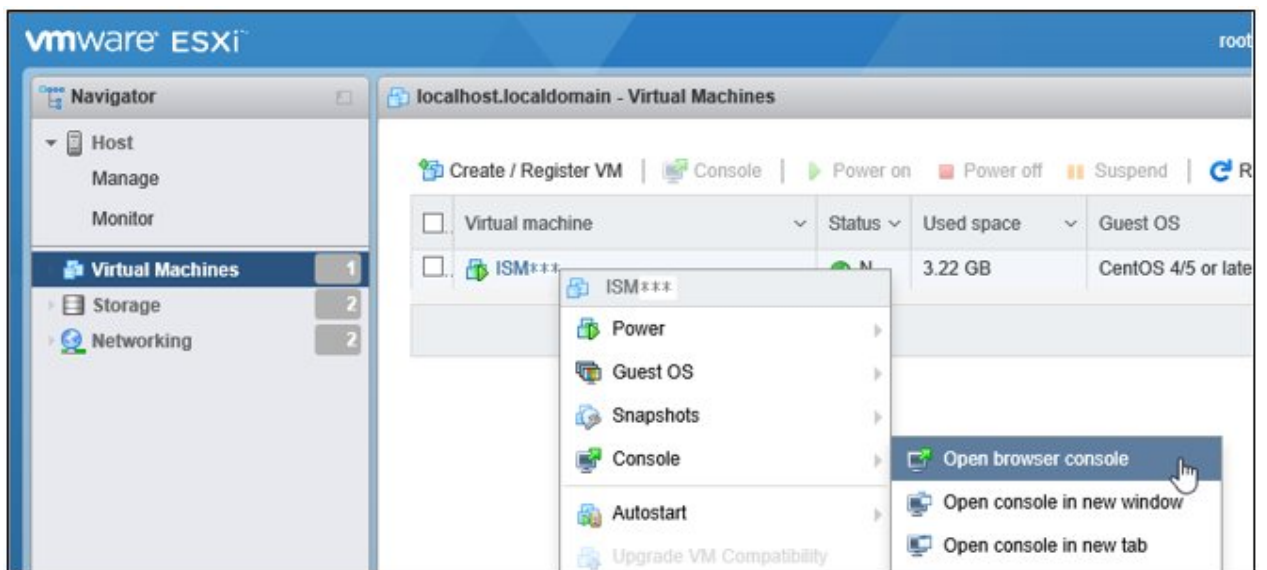


## VMware ESXi 6.5 or later

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

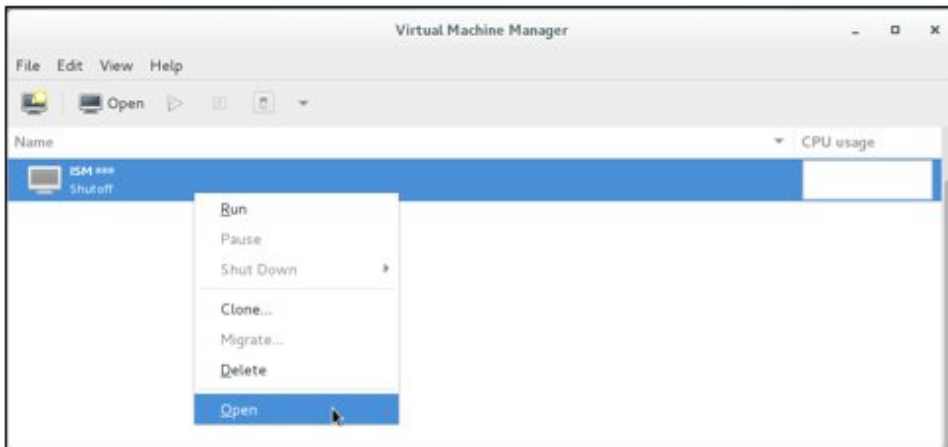


2. Right-click on the installed ISM-VA, and then select [Open browser console] or other console.

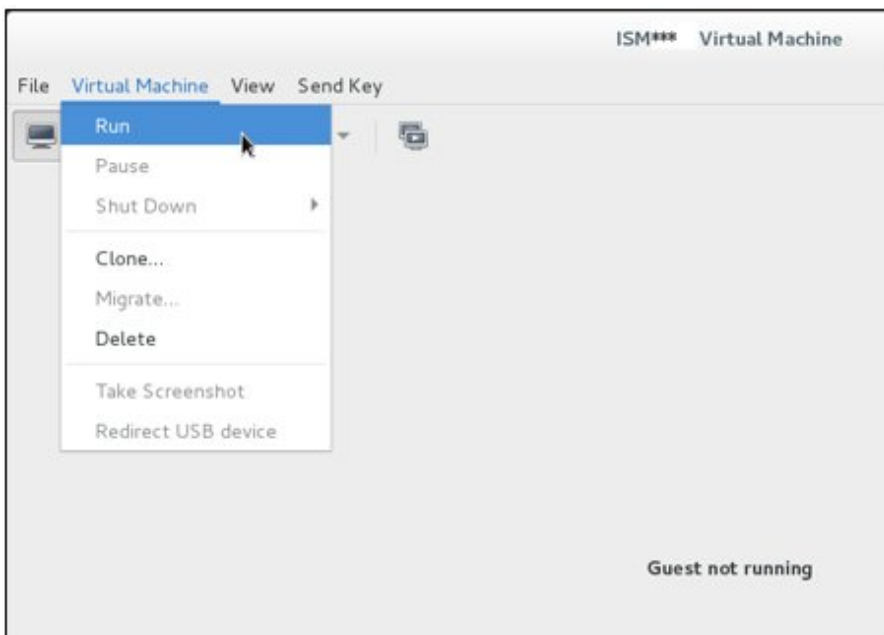


### 4.1.1.3 For ISM-VA running on KVM (after installation)

1. In Virtual Machine Manager, right-click on the installed ISM-VA, and then select [Open].



2. On the "ISM-VA Virtual Machine" screen, select [Run] from the [Virtual Machine] menu to start ISM-VA.



#### Point

Starting up ISM-VA may take several minutes to complete. Wait for a while, and then confirm that you can log in to the GUI.

### 4.1.2 Stop of ISM-VA

---

Use the ISM-VA command to terminate ISM-VA.

1. Start up the GUI.

Log in to the GUI as an ISM administrator.

2. Terminate all operations.

View the "Tasks" screen to confirm that all tasks are terminated.

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

- b. In the "Tasks" screen, check that the status has become "Completed" or "Cancellation completed."
- c. If there are tasks that are not either "Completed" or "Cancellation completed," then either wait for them to finish or cancel these tasks.

If you cancel the tasks, select the tasks running and then select [Cancel] from the [Actions] button. Cancel all tasks that are currently being executed.

Tasks of the "Updating firmware" (firmware update process) type may sometimes not be aborted by canceling. In such a case, you have to wait until processing finishes.

### Note

Terminating ISM-VA with any tasks still running may cause task processing to be interrupted with an error and result in incorrect operating behavior in later operations.

Therefore, be sure to either wait until all tasks finish, or cancel them manually and then, only when processing for canceling has finished, terminate ISM-VA.

3. Log out from the GUI of ISM, and then close the GUI.
4. Start up the console and log in as an ISM administrator.
5. To terminate ISM-VA, execute the termination command of ISM-VA.

```
# ismadm power stop
```

## 4.1.3 Restart of ISM-VA

Restarts of ISM-VA are mainly executed when applying patches in ISM-VA.

1. Terminate all ISM tasks, close the GUI, and then log in to the console.

For details on how to stop tasks and the GUI, refer to "[4.1.2 Stop of ISM-VA.](#)"

2. Execute the following command to restart ISM-VA.

```
# ismadm power restart
```

## 4.1.4 Start and Stop of ISM Service

As soon as you start up ISM-VA, the ISM service starts automatically.

To start and stop the ISM service, you have to log in to ISM-VA from the console as an administrator and execute the applicable ISM-VA commands.

### Start of ISM service

1. Execute the following command to start the ISM service.

```
# ismadm service start ism
```

### Stop of ISM service

1. Terminate all ISM tasks and close the GUI.

For details on how to stop tasks and the GUI, refer to "[4.1.2 Stop of ISM-VA.](#)"

2. Execute the following command to stop the ISM service.

```
# ismadm service stop ism
```

## 4.2 ISM-VA Basic Settings Menu

The basic settings for ISM-VA can easily be executed either through a selection menu or an item selection format.

Displayed below are the items that can be set in the ISM-VA basic settings menu.

Item		Settings/Display	Corresponding ismadm command
Locale	Language	Internal language setting	ismadm locale set-locale
	Keyboard	Keyboard map setting	ismadm locale set-keymap
Network	Hostname(FQDN)	Host name setting	ismadm network modify
	IP Address	IP address setting	
	Gateway Address	Gateway setting	
	DNS Address	DNS server setting	
Time	Time zone	Time zone setting	ismadm time set-timezone
	Local Time	Local time display	ismadm time show
	Using NTP	NTP Enabling/Disabling	ismadm set-ntp
	NTP Server	NTP server setting	ismadm add-ntpserver
			ismadm del-ntpserver
NTP Synchronized	NTP synchronization display	ismadm time show	
Log	Log level	ISM RAS Log level setting	ismadm system change-log-level
GUI	GUI port number	Web GUI connection port setting	ismadm service modify -port

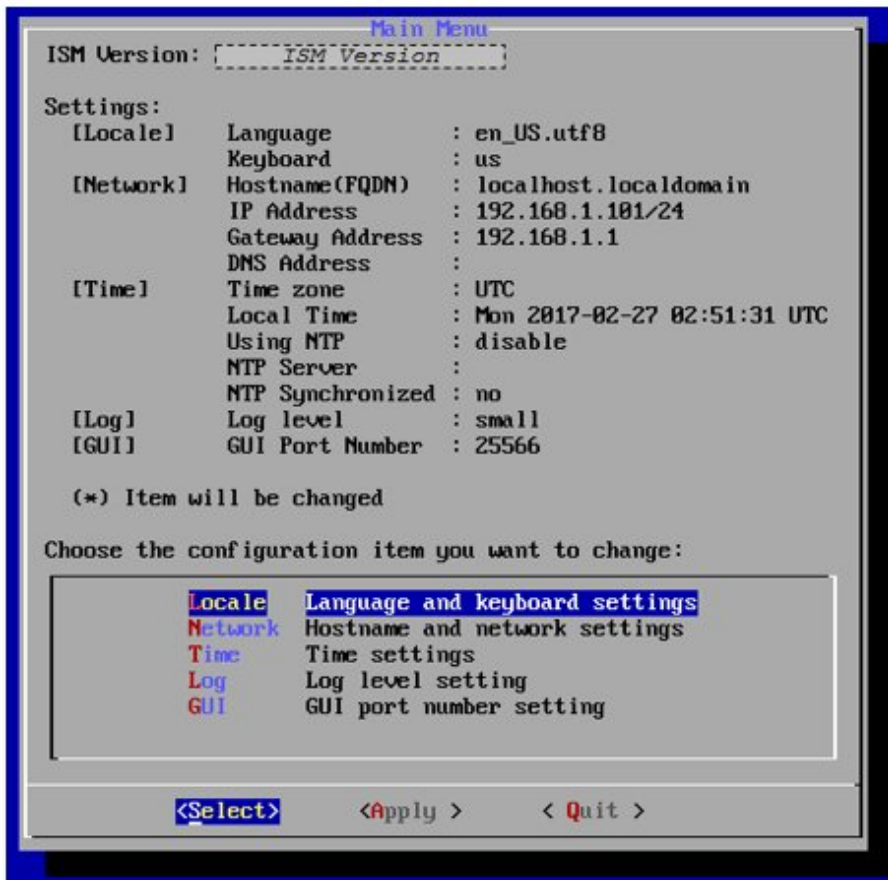
The following is the procedure for using the ISM-VA basic settings menu.

1. From the console as an administrator, log in to ISM-VA.
2. Start using the ISM-VA basic settings menu command.

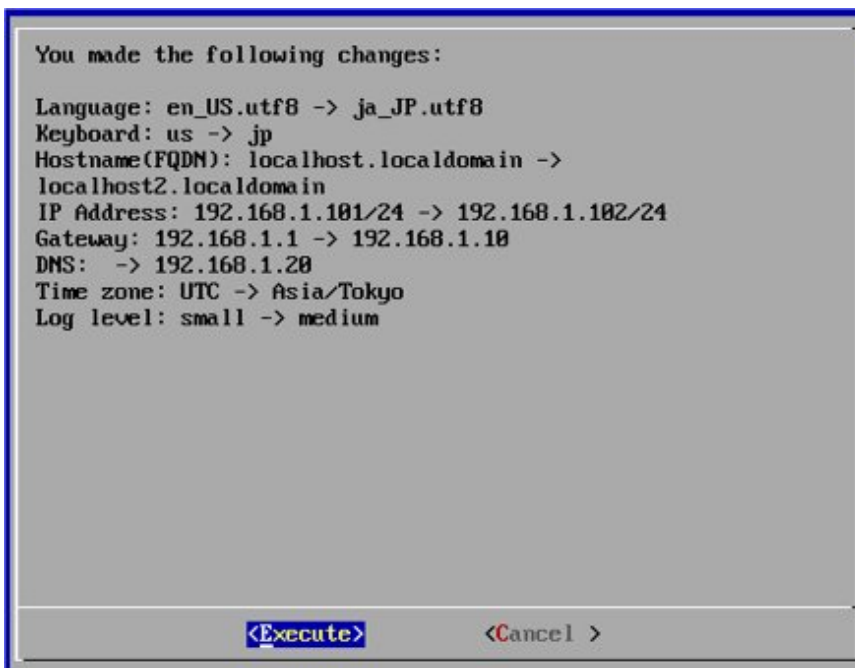
```
# ismsetup
```



The screen below is displayed.



3. Select the item you want to set and enter or select a setting value.
4. After entering a setting value, select [Apply].
5. Confirm the changes, and then select [Execute].



After the change processing has finished the change results are displayed.

6. To apply the changes, select [Reboot ISM-VA] and restart ISM-VA.



## 4.3 Modification of Destination Port Number

You can modify the destination port number (25566) that is used for connecting to the GUI from a web browser.

1. Log in to the console as an administrator.
2. Execute the following command to stop the ISM service.

```
# ismadm service stop ism
```

3. Execute the following command to modify the destination port of ISM.

```
# ismadm service modify -port <destination port number>
```

Example of command execution:

```
# ismadm service modify -port 35566
You need to reboot the system to enable the new settings.
Immediately reboots the system.[y/n]:
```

When command execution is complete, a confirmation message is displayed, prompting whether you want to restart; enter "y" to restart ISM-VA.

When the restart is complete, the GUI can be connected from the new destination port number.

## 4.4 Backup and Restoration of ISM-VA

The following methods can be used to back up/restore.

- [Backup/Restore ISM-VA with the Hypervisor](#)
- [Backup/Restore ISM with the ISM-VA Management Command](#)



### Note

When operating backup/restoration of ISM-VA, be careful of the following points.

- Operate back up with ISM-VA stopped.
- Any changes that were done after ISM has been backed up must be reflected after restoring.
- If the following links are used in ISM, determine if you must execute backup/restoration for each management server (management VM) at the same time.
  - If the domain users and the ISM users are linked

- If the information of the cloud management software is registered in ISM
- If you are using a backup software, back up/restore using the following functions provided by the backup software is not supported.
  - Functions that require an agent for the virtual machine (ISM-VA)
  - Restoration on file basis

## 4.4.1 Backup/restoration of ISM-VA with the Hypervisor



### Note

Before backup/restoration of ISM-VA, stop ISM-VA. For details on how to stop it, refer to ["4.1.2 Stop of ISM-VA."](#)

### Backup of ISM-VA with the Export Function

The export function of the hypervisor can be used to back up the entire ISM-VA.

For detailed procedures to export the hypervisor, refer to "Operating Procedures."

### Restoration of ISM-VA with the Import Function

Restore ISM-VA by using the procedure in ["3.3 Installation of ISM-VA"](#) to import the exported file.

## 4.4.2 Backup/restoration of ISM with the ISM-VA Management Command

Use the ISM-VA Management command to create a backup file that only has a part of the information.

It is different from the function of backup with the hypervisor, in that you can back up without turning off the ISM-VA. By limiting the backup targets it can be completed in less time, and the required external disk capacity is reduced. However, you must execute some environment settings, DVD imports and others again after it is restored.



### Point

Estimate the disk capacity required before the ISM backup/restoration. For an estimate of the required capacity, refer to ["3.2.1.6 Estimation of required capacities for ISM backup/restoration."](#)

For the ISM backup targets, refer to the following table.

Note: Y = Backup possible, N = Backup not possible

Target	Backup possible/not possible
ISM-VA setting information (setting items in the ISM-VA basic settings menu)	Y
Management data of nodes	Y
Management data of node groups	Y
Management data of accounts	Y
Management data of user groups	Y
Operation logs, audit logs, SNMP traps	Y
Profiles	Y
Power Capping settings [Note 1]	Y
Virtual disk allocation information [Note 2]	N
Repository [Note 3]	N

Target	Backup possible/not possible
Archived Logs, Node Logs [Note 3]	N
Files transferred to the "<User group name>/ftp" directory [Note 4]	N
Firmware Baseline definitions [Note 3]	N

[Note 1]: The Power Capping settings are backed up, but Power Capping is disabled. If using power capping after restoration of ISM, enable the power capping policy. For the procedure to enable power capping policies, refer to "6.4.3 Enable the Power Capping Policy of the Racks" in "Operation Procedures."

[Note 2]: After restoring ISM, the virtual disk allocation status is as follows. After restoring ISM, allocate virtual disks as required.

- The status of the allocated virtual disk to the entire ISM-VA will be back to the status of the ISM-VA that was backed up.
- The allocation of virtual disks is canceled for all user groups.

[Note 3]: The repository, Archived Logs, Node Logs, and Firmware Baseline definitions are deleted when executing restoration. After restoration, import the repository, collect logs, and create Firmware Baseline definitions again.

[Note 4]: The transferred files are deleted when executing restoration. However, the script file specified in the "Execute Script after Installation" item in Profile Management is backed up.

Restoration of the ISM backup file can only be executed for certain restoration destinations (ISM-VA backup).

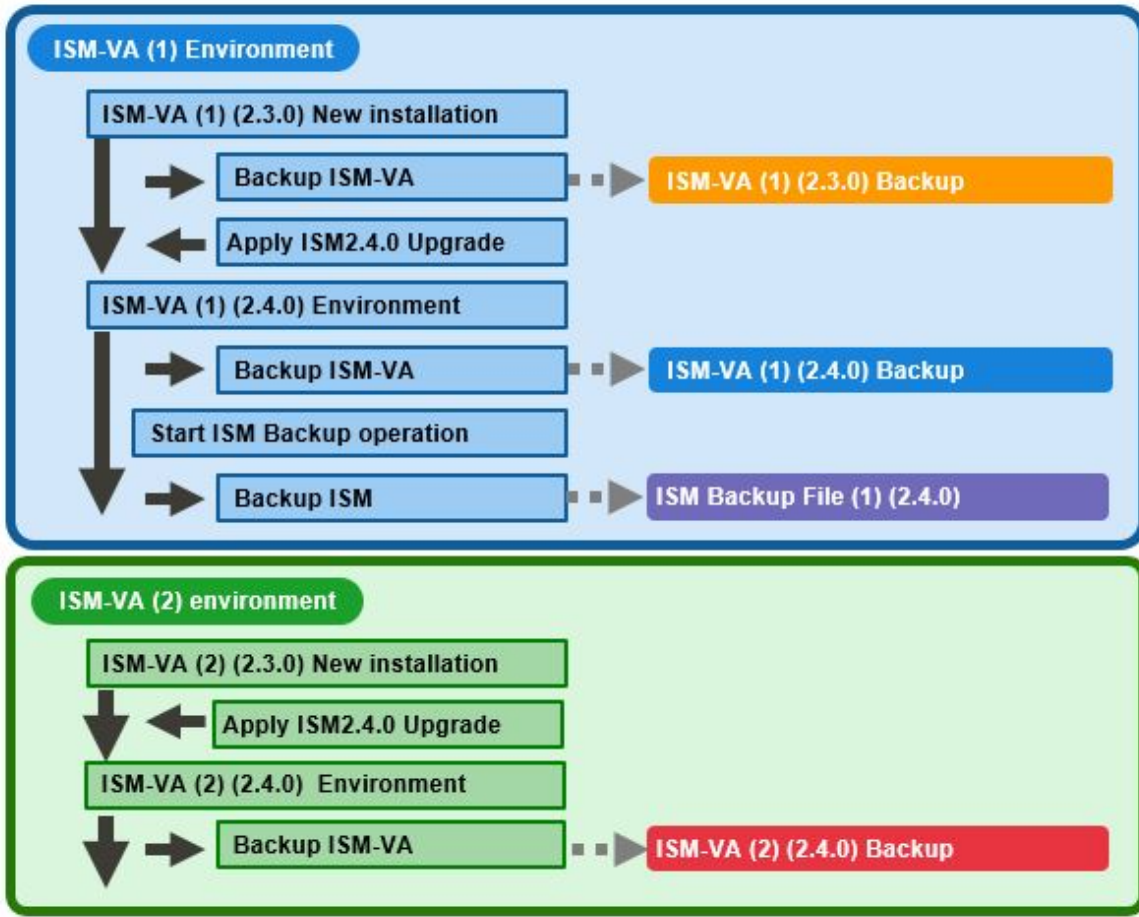
The requirements for ISM-VA that can be used as restoration destinations are as follows. Restoration for ISM-VA other than the ones below is not supported.

- The environment that backed up and restored ISM-VA before starting ISM backup
- The version of the backup of ISM-VA used as restoration destination and the version of the ISM backup file are the same

The following shows an example.

This section describes whether or not it is possible to restore the ISM backup file (1)(2.4.0) backed up in ISM-VA(1)(2.4.0).

The ISM backup file (1)(2.4.0) and each ISM-VA backup are the ones that has been retrieved using the following flow.



The following shows when it is possible and not possible to restore ISM backup file (1)(2.4.0).

Note: Y = Restoration possible, N = Restoration not possible

ISM-VA environment	ISM-VA restoration destination	Restoration possible/not possible
ISM-VA (1)	The environment where the ISM-VA(1)(2.4.0) backup was restored	Y [Note 1]
	The environment where the ISM-VA(1)(2.3.0) backup was restored	N [Note 2]
	The environment upgraded to ISM 2.4.0 where the ISM-VA(1)(2.3.0) backup was restored	N [Note 2]
ISM-VA (2)	The environment where the ISM-VA(2)(2.4.0) backup was restored	N [Note 3]

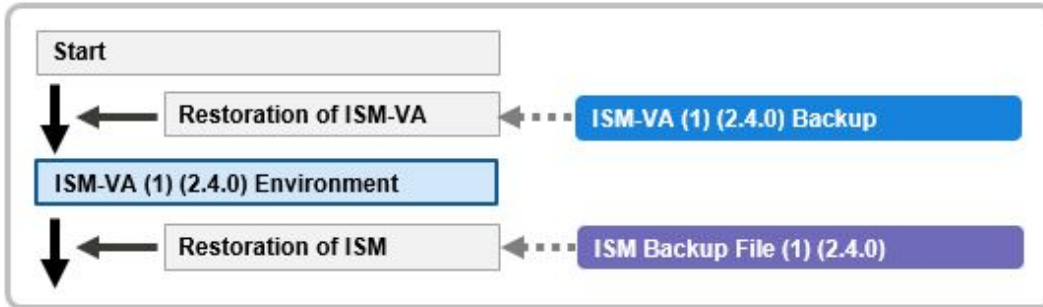
[Note 1]: For details, refer to "[ISM restoration for environments where the ISM-VA\(1\)\(2.4.0\) backup was restored.](#)"

[Note 2]: For details, refer to "[ISM restoration for environments where the ISM-VA\(1\)\(2.3.0\) backup was restored.](#)"

[Note 3]: For details, refer to "[ISM restoration for environments where the ISM-VA\(2\)\(2.4.0\) backup was restored.](#)"

### ISM restoration for environments where the ISM-VA(1)(2.4.0) backup was restored

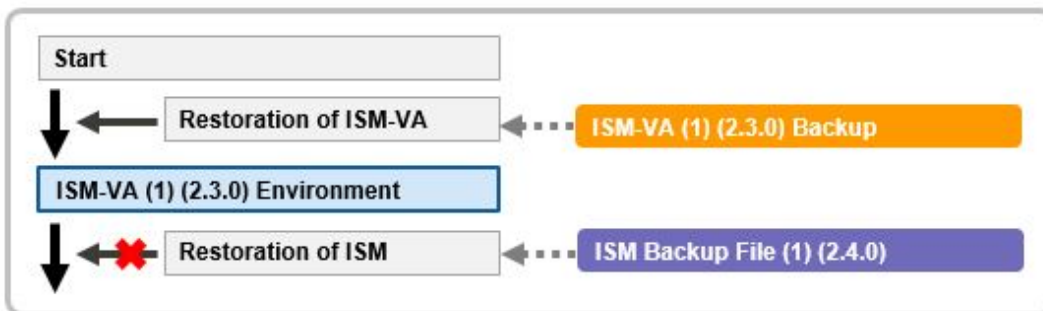
Restoration can be executed for the ISM backup file (1)(2.4.0) in an environment where the ISM-VA(1)(2.4.0) backup was restored.



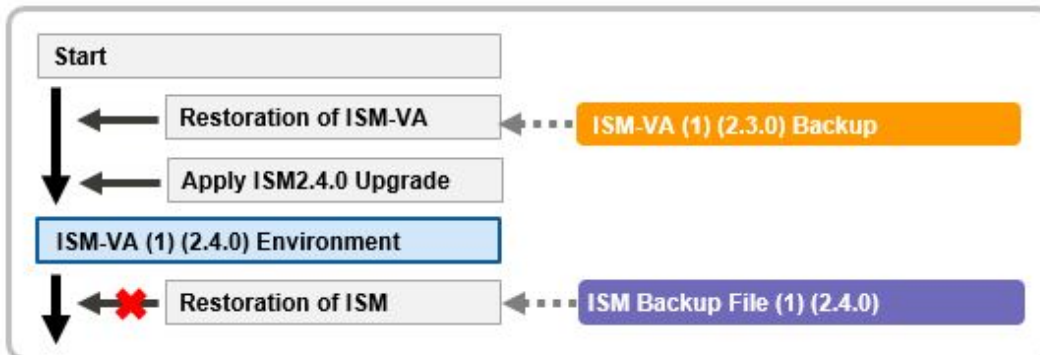
**ISM restoration for environments where the ISM-VA(1)(2.3.0) backup was restored**

Restoration of ISM backup file (1)(2.4.0) is not supported in an environment where the ISM-VA(1)(2.3.0) backup was restored.

ISM restoration is not supported for environments that were restored with an ISM-VA backup with of a different version than the ISM backup file.



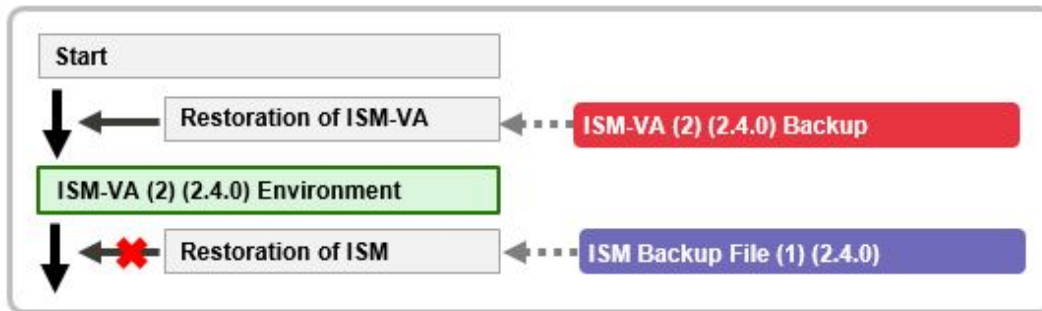
Also, after restoring an ISM-VA(1)(2.3.0) backup, restoration for an environment upgraded to ISM 2.4.0 is not supported either.



**ISM restoration for environments where the ISM-VA(2)(2.4.0) backup was restored**

Restoration of ISM backup file (1)(2.4.0) is not supported in an environment where the ISM-VA(2)(2.4.0) backup was restored.

ISM restoration is not supported for environments restored with an ISM-VA backup that is different from the ISM-VA created with the ISM backup file.



For details on the procedure, refer to "Operating Procedures."

#### 4.4.2.1 Backup of ISM

The following is the backup command of ISM.

```
# ismadm system backup
```

An example of ISM backup command execution is displayed below.

When you execute the command, the available disk capacity and the disk capacity required for ISM backup are displayed.

Confirm that there is enough available disk capacity, then in "Start backup process? [y/n]:" enter "y" and press the [Enter] key. When aborting the ISM backup, enter "n" and press the [Enter] key.



#### Note

If you execute backup with insufficient available disk capacity, this will result in an error.

Example of ISM backup command execution: (The sentences after the \* are not actually displayed on the screen.)

```
# ismadm system backup
[System Information]
Version : 2.4.0 (S2019xxxx-xx) *Version of the operating ISM-VA

[Disk Space Available]
System      : 27000MB      *Available disk capacity in the system (entire ISM-VA [Note 1])
/Administrator : 17000MB  *Available disk capacity in the /Administrator repository

[Disk Space Required]
System      : 1200MB      *Disk capacity required in the system (entire ISM-VA [Note 1])to
                        execute backup
/Administrator : 1200MB  *Disk capacity required in /Administrator repository to execute backup

Start backup process? [y/n]: *Select to execute/stop the backup

      (Backup process execution display)

Output file: /Administrator/ftp/ism<ISM version>-backup-<Backup date and time>.tar.gz
*Backup file name
```

[Note 1]: Including user group repositories not allocated to the virtual disks.

Since the backup file is output under "/Administrator/ftp" it can be read via FTP.

## Note

When you transfer backup files via FTP, transfer them in binary mode.

## Point

If the available disk capacity is not sufficient, take the following actions.

- If System is not sufficient, follow "4.6.2 Allocation of Additional Virtual Disks to Entire ISM-VA" and add virtual disks.
- If "/Administrator" is not sufficient, delete files that are not required, or follow "4.6.3 Allocation of Additional Virtual Disks to User Groups" and add virtual disks.

### 4.4.2.2 Restoration of ISM

Prepare the backup files to restore ISM in "/Administrator/ftp" in advance.

The backup files that can be specified in ISM restoration can be checked in "4.4.2.3 Display of backup file list."

The following is the ISM restore command. In <Backup file name>, specify the backup file saved in "/Administrator/ftp."

```
# ismadm system restore -file <Backup file name>
```

An example of ISM restore command execution is displayed below.

When you execute the command, the versions of ISV-VA and of the backup file, as well as the available disk capacity and the required disk capacity for ISM restoration are displayed.

Confirm that the versions of ISM-VA and the backup file are the same and that there is enough available capacity, then in "Start restore process? [y/n]:" enter "y" and press the [Enter] key. When aborting the ISM restoration, enter "n" and press the [Enter] key.

Example of ISM restore command execution: (The sentences after the \* are not actually displayed on the screen.)

```
# ismadm system restore -file ism2.4.0-backup-20190202102723.tar.gz
[System Information]
  Version : 2.4.0 (S2019xxxx-xx)      *Version of the operating ISM-VA

[Backup File Information]
  Version : 2.4.0 (S2019xxxx-xx)      *Version of the specified backup file

[Disk Space Available]
  System      : 45000MB                *Available disk capacity in the system (entire ISM-VA)

[Disk Space Required]
  System      : 2400MB                 *Disk capacity required in the system (entire ISM-VA)to execute restore

Start restore process? [y/n]: *Select to execute/stop the restoration
```

## Note

- When you transfer backup files via FTP, transfer them in binary mode.
- After executing the ismadm system restore command, you must restart ISM-VA. For details on the procedure, refer to "Operating Procedures."

### 4.4.2.3 Display of backup file list

Displays a list of the backup files saved under "/Administrator/ftp."

```
# ismadm system backup -list
```



or

```
# ismadm system restore -list
```

Example of the display of backup files list command execution: (The sentences after the \* are not actually displayed on the screen.)

```
# ismadm system backup -list
[System Information]
  Version : 2.4.0 (S2019xxxx-xx)      *Version of the operating ISM-VA

[Disk Space Available]
  System      : 45000MB                *Available disk capacity in the system (entire ISM-VA)

[Backup Files]
-----
  DIRECTORY   : /Administrator/ftp      *Directory where the backup file is saved
  FILE NAME   : ism2.4.0-backup-20190202102723.tar.gz *Backup file name
  FILE SIZE   : 200MB                   *Backup file size
  BACKUP SIZE : 1200MB                   *Size of the backed up ISM-VA information
  BACKUP DATE : 2019-02-02 10:27:23     *Backup date/time
  VERSION     : 2.4.0 (S2019xxxx-xx)    *Version of the backed up ISM-VA
-----
  DIRECTORY   : /Administrator/ftp
  FILE NAME   : ism2.4.0-backup-20190201151041.tar.gz
  FILE SIZE   : 150MB
  BACKUP SIZE : 1000MB
  BACKUP DATE : 2019-02-01 15:10:41
  VERSION     : 2.4.0 (S2019xxxx-xx)
```

## 4.5 Collection of Maintenance Data

You can collect the maintenance data that will be required for the investigation if a failure occurred.

### 4.5.1 ISM/ISM-VA Maintenance Data

The procedure to collect the maintenance data if the failure occurred in ISM is as follows.

Collect the required maintenance data depending on the purpose of investigation for the system operated by ISM.

Target of investigation	Person in charge	Maintenance data
Investigation of malfunctions in ISM and/or ISM-VA	Local Fujitsu customer service partner	ISM RAS Logs ISM-VA Operating System logs Database information

You can collect the maintenance data either separately according to the target of your investigation or collectively all together.

Maintenance data can only be collected by ISM administrators. ISM administrators provide the person in charge with the collected maintenance data.

#### Note

- Retrieving database information may take several hours to complete. Moreover, this requires large amounts of free disk space in ISM-VA. If you have to collect these kinds of data, or if you are going to collect multiply maintenance data together, follow the instructions of your local Fujitsu customer service partner.
- When you execute a command, the following message may sometimes be displayed on the hypervisor console, but this does not mean any problem.

```
blk_update_request:I/O error, dev fd0, sector 0
```

Output of logs used for failure investigation can be set as follows.

- [4.5.1.1 Switching the ISM RAS Log mode](#)
- [4.5.1.2 Switching the ISM RAS Log level](#)
- [4.5.1.3 Specification of core file collection directory](#)
- [4.5.1.4 How to collect ISM maintenance data](#)

### 4.5.1.1 Switching the ISM RAS Log mode

You can switch whether to output the details of ISM RAS Log for the failure investigation. Log output is disabled during initial installation.

1. From the console as an administrator, log in to ISM-VA.
2. Execute the command for switching the log for failure investigation on and off.
  - Enable log output

```
# ismadm system set-debug-flag 1
```

- Disable log output

```
# ismadm system set-debug-flag 0
```

### 4.5.1.2 Switching the ISM RAS Log level

You can switch export levels for logs to be used during failure investigation.

Switching the export level allows you to limit the sizes of logs to be exported. It is set to "small" during initial installation.

Log level	Approximate size of log to be exported	Number of managed nodes
small (default)	10 GB	100 nodes
medium	40 GB	400 nodes
large	100 GB	1000 nodes



#### Note

- Switching is only enabled from lower levels (settings with few managed nodes) to higher levels (settings with many managed nodes).
- After switching the log level, ISM-VA must be restarted.

1. From the console as an administrator, log in to ISM-VA.
2. Stop the ISM service.  
Stop the ISM service according to the procedure described in "[4.1.4 Start and Stop of ISM Service.](#)"
3. Execute the command for switching the level of the log for failure investigation.

- Switching to "medium"

```
# ismadm system change-log-level medium
```

- Switching to "large"

```
# ismadm system change-log-level large
```

4. Confirm the setting of the level of the log for failure investigation.  
To confirm the setting, you can use the command for displaying the system information.

```
# ismadm system show
ISM Version      : <Version>
GUI Port Number  : 25566
Hostname        : localhost
Log Level       : medium
```

The <Version> part shows the version of ISM-VA.

5. Execute the following command to restart ISM-VA.

```
# ismadm power restart
```

After starting ISM-VA, the new level of the log for failure investigation is effective.

### Point

You can also switch export levels for ISM RAS logs with "[4.2 ISM-VA Basic Settings Menu](#)."

## 4.5.1.3 Specification of core file collection directory

You can set a directory for collecting and as an archiving destination when exporting core file as maintenance data. If it is not set, an internal directory of system area in ISM-VA is used.

The exported core file is collected as a target of "[4.16 MIB File Settings](#)."

1. From the console as an administrator, log in to ISM-VA.
2. Execute a command for controlling the ISM-VA service.

- Display of collection directory

```
# ismadm system core-dir-show
Core Directory: Default Internal Directory
Store Size: 713596
```

The location of the core file collection directory currently set and the directory size of currently using are displayed.

If the collection directory location is not yet set, "Default Internal Directory" is displayed.

- Collection directory settings

```
# ismadm system core-dir-set -dir <directory>
```

Use ftp client to create a directory such as under /Administrator/ftp/ in advance, and then specify the directory.

Example:

```
# ismadm system core-dir-set -dir /Administrator/ftp/coredump/
```

### Note

Use the created collection directory as dedicated to core file export, and do not locate other files.

- Clear collection directory

```
# ismadm system core-dir-reset
```

Reverse the collection directory to unset status.

#### 4.5.1.4 How to collect ISM maintenance data

The procedures for retrieving maintenance data for ISM is either the procedure to retrieve from the GUI, or the procedure to execute a command to retrieve.

For details, refer to "8.2 Collect Maintenance Data" in "Operating Procedures."

### 4.5.2 ISM for PRIMEFLEX Maintenance Data

The following is the procedure for collecting the required maintenance data in case a failure occurs in the Virtual Platform Expansion function.

#### 4.5.2.1 Logs for Cluster Creation

The Cluster Creation log is as follows.

Maintenance data	Retrieving method
Cluster Creation log	Use the ISM-VA commands to collect it. For details, refer to " <a href="#">4.5.1.4 How to collect ISM maintenance data.</a> "
Execution log of the OS setting script executed after OS installation	<ul style="list-style-type: none"> <li>- PRIMEFLEX for VMware vSAN V1 Retrieve from the following location on the ESXi host. /vmfs/volumes/datastore1_error/post_script.log (Estimated capacity: About 30 KB)</li> <li>- PRIMEFLEX for Microsoft Storage Spaces Direct Retrieve from the following location on the Hyper-V host. C:\FISCRB\Log\post_script.log (Estimated capacity: About 30 KB)</li> </ul>
Execution log of the PowerShell script executed on the Windows Server	Retrieve from the following location on the Windows Server. <ul style="list-style-type: none"> <li>- Servers configuring a new cluster of PRIMEFLEX for Microsoft Storage Spaces Direct</li> <li>- PRIMEFLEX for VMware vSAN V1 DNS server</li> </ul> Retrieve all of the following files. C:\FISCRB\Log\ <file name="" of="" powershell="" script&gt;_yyyymmdd-hhmmssmmm.log<br=""></file> .log under C:\FISCRB\Log\

#### 4.5.2.2 Logs for Cluster Expansion

The Cluster Expansion log is as follows.

Maintenance data	Retrieving method
Cluster Expansion log	Use the ISM-VA commands to collect it. For details, refer to " <a href="#">4.5.1.4 How to collect ISM maintenance data.</a> "
Execution log of the OS setting script executed after OS installation	<ul style="list-style-type: none"> <li>- PRIMEFLEX HS V1.0/V1.1/PRIMEFLEX for VMware vSAN V1 version Retrieve it from the following location on the ESXi host. /vmfs/volumes/datastore1_error/post_script.log (Estimated capacity: About 30 KB)</li> <li>- PRIMEFLEX for Microsoft Storage Spaces Direct version</li> </ul>

Maintenance data	Retrieving method
	Retrieve it from the following location on the Hyper-V host. C:\FISCRB\Log\post_script.log (Estimated capacity: About 30 KB)
Execution log of the PowerShell script executed on the Windows Server	Retrieve it from the following location on the Windows Server. - Servers added when executing Cluster Expansion for the PRIMEFLEX for Microsoft Storage Spaces Direct version - DNS server of PRIMEFLEX HS V1.0/V1.1/PRIMEFLEX for VMware vSAN V1 version Retrieve all of the following files. C:\FISCRB\Log\ <file name="" of="" powershell="" script&gt;_yyyymmdd-hhmmssmmm.log<br=""></file> .log under C:\FISCRB\Log\

### 4.5.2.3 Logs for Cluster Management

The Cluster Management log is as follows.

Maintenance data	Retrieving method
Cluster Management log	Use the ISM-VA commands to collect it. For details, refer to " <a href="#">4.5.1.4 How to collect ISM maintenance data.</a> "
vSAN log	Retrieve the vc-support log from vCenter. For details, refer to " <a href="#">4.5.1.4 How to collect ISM maintenance data.</a> "

### 4.5.2.4 Logs for Firmware Rolling Update

The Firmware Rolling Update log is as follows.

Maintenance data	Retrieving method
Firmware Rolling Update log	Use the ISM-VA commands to collect it. For details, refer to " <a href="#">4.5.1.4 How to collect ISM maintenance data.</a> "

## 4.6 Management of Virtual Disks

You can cancel or newly add allocations of virtual disks.

### 4.6.1 Cancellation of Virtual Disk Allocations

The allocation of virtual disks allocated in "[3.7.2 Allocation of Virtual Disks to User Groups](#)" can be canceled.



#### Note

- On canceling an allocation, all data that were stored in the user group will be lost.
- Allocations of virtual disks to Administrator groups cannot be canceled.
- Allocations of virtual disks to the entire ISM-VA as executed according to "[3.7.1 Allocation of Virtual Disks to Entire ISM-VA](#)" cannot be canceled.

The following operating example shows how to cancel the allocation of a virtual disk to a user group named usrgrp1.

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

```
# ismadm service stop ism
```

3. Confirm that the virtual disk is allocated to usrgrp1.

```
# ismadm volume show -disk
Filesystem      Size  Used Avail  Use% Mounted on
/dev/mapper/centos-root 16G  2.5G  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/0
tmpfs           380M   0  380M   0% /run/user/1001
/dev/mapper/usrgrp1vol-lv 10G   33M   10G   1% 'RepositoryRoot' /usrgrp1

PV          VG          Fmt Attr PSize  PFree
/dev/sda2   centos      lvm2 a--  19.51g  0
/dev/sdb1   usrgrp1vol lvm2 a--  10.00g  0
```

In this example, the VG named `usrgrp1vol` is allocated to `usrgrp1`.

4. Specify the User Group Name and unmount the virtual disk.

```
# ismadm volume umount -gdir usrgrp1
```

5. Specify the Volume Name (`usrgrp1vol`) for `usrgrp1` and delete the virtual disk.

```
# ismadm volume delete -vol usrgrp1vol
Logical volume "usrgrp1vol" successfully removed.
```

6. Confirm the virtual disk settings.

Confirm that no virtual disk is set for `usrgrp1` and that the previously used directory `"/dev/sdb"` is now free.

```
# ismadm volume show -disk
Filesystem      Size  Used Avail  Use% Mounted on
/dev/mapper/centos-root 16G  2.5G  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/0
tmpfs           380M   0  380M   0% /run/user/1001
/dev/sdb1                               (Free)

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

7. Restart ISM-VA.

```
# ismadm power restart
```

## 4.6.2 Allocation of Additional Virtual Disks to Entire ISM-VA

Using the same procedure as in "[3.7.1 Allocation of Virtual Disks to Entire ISM-VA](#)," you can additionally allocate multiple virtual disks to the entire ISM-VA.

## 4.6.3 Allocation of Additional Virtual Disks to User Groups

You can allocate virtual disks in addition to the ones you allocated according to "3.7.2 Allocation of Virtual Disks to User Groups."

The following operating example shows how to allocate an additional virtual disk to a user group named usrgpr1.

1. Connect to the virtual disk.

Execute the operations in Step 1 of "3.7.2 Allocation of Virtual Disks to User Groups."

2. After starting up ISM-VA, log in to ISM-VA from the console as an administrator.
3. In order to allocate the additional 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.

```
# 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  169M  329M  34% /boot
/dev/mapper/usrgrp1vol-lv 10G  33M  10G   1% 'RepositoryRoot' /usrgrp1
tmpfs           380M   0  380M   0% /run/user/0
/dev/sdc                                     (Free)

PV              VG      Fmt Attr PSize PFree
/dev/sda2       centos lvm2 a-- 19.51g 0
/dev/sdb1       usrgpr1vol lvm2 a-- 10.00g 0
```

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

5. Execute the command for allocating additional virtual disks in order to allocate the added virtual disk to usrgpr1vol.

```
# ismadm volume extend -vol usrgpr1vol -disk /dev/sdc
Logical volume "/dev/mapper/usrgrp1vol-lv" resized.
```

6. Confirm the virtual disk settings.

Confirm that the newly added volume (/dev/sdc) is set for use by usrgpr1 (usrgpr1vol).

```
# 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
/dev/mapper/usrgrp1vol-lv 15G  33M  15G   1% 'RepositoryRoot' /usrgrp1
tmpfs           380M   0  380M   0% /run/user/0
tmpfs           380M   0  380M   0% /run/user/1001

PV              VG      Fmt Attr PSize PFree
/dev/sda2       centos lvm2 a-- 19.51g 0
/dev/sdb1       usrgpr1vol lvm2 a-- 10.00g 0
/dev/sdc1       usrgpr1vol lvm2 a-- 5.00g 0
```

7. Restart ISM-VA.

```
# ismadm power restart
```

## 4.7 Certificate Activation

---

### 4.7.1 Deployment of SSL Server Certificates

---

When using a SSL server certificate issued by an authentication authority concerning security, follow the procedure below to set it.

1. Transfer the SSL server certificate to ISM-VA.

Transfer destination: /Administrator/ftp

For information on how to transfer files using the GUI, refer to "4.22 File Upload Using the GUI."

For information on how to transfer files via FTP, refer to "2.1.2 FTP Access."

2. From the console as an administrator, log in to ISM-VA.
3. Deploy the SSL server certificate.

Execute the following command, specifying the "key" and "cert" files you transferred.

```
# ismadm sslcert set -key /Administrator/ftp/server.key -cert /Administrator/ftp/server.crt
```

4. Restart ISM-VA.

```
# ismadm power restart
```



You can create the unique SSL server certificate corresponding to the unique host name used in a local network on the Linux server with the openssl command installed, with use of the following commands.

```
# openssl genrsa -rand /proc/uptime 2048 > server.key
# openssl req -new -key server.key -x509 -sha256 -days 365 -set_serial $RANDOM -extensions v3_req -out server.crt
```

- Specify an arbitrary file name for the file name of the certificate (server.key/server.crt)
- Specify the effective days of the certificate for days option
- Specify the host name upon entering "Common Name" after executing openssl req command

### 4.7.2 Display of SSL Server Certificates

---

You can have the SSL certificates displayed that are enabled in ISM-VA.

1. From the console as an administrator, log in to ISM-VA.
2. Execute the command for displaying the SSL server certificates.

```
# ismadm sslcert show
```

### 4.7.3 Export of SSL Server Certificates

---

You can export the SSL certificates that are enabled in ISM-VA.

1. From the console as an administrator, log in to ISM-VA.
2. Execute the command for exporting the SSL server certificates.

```
# ismadm sslcert export -dir /Administrator/ftp
```

You can download the exported files via FTP.



## 4.7.4 Creation of Self-signed SSL Server Certificates

Create a self-signed SSL server certificate based on the IP address specified in ISM-VA or FQDN.

1. From the console as an administrator, log in to ISM-VA.
2. Execute the command for creating the self-signed SSL server certificates.

- For SSL accessing with IP address

```
# ismadm sslcert self-create -cnset ip
```

- For SSL accessing with FQDN

```
# ismadm sslcert self-create -cnset fqdn
```

3. Restart ISM-VA.

```
# ismadm power restart
```

## 4.7.5 Download of CA Certificates

You can download CA certificates from the following URL when self-signed SSL server certificates are created.

<https://<IP address of ISM-VA>:25566/ca.crt>

If you are using Internet Explorer or Google Chrome, execute [Save as] and change the file name to "ca.crt" for the displayed contents. When saving, select one of the following file types depending on the browser.

- Internet Explorer: [Text file (\*.txt)]
- Google Chrome: [All files]

Example of command execution: when downloading to a Linux server where the curl command has been installed

```
# curl -Ok https://192.168.10.20:25566/ca.crt
```

## 4.8 License Settings

You can register, display, and delete server licenses and node licenses in ISM-VA.

1. From the console as an administrator, log in to ISM-VA.
2. Execute a command for the license settings.

- Registration of license

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

- Display of licenses

```
# ismadm license show
```

Example of command execution:

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

Table 4.1 Description of the exported command results

Item	Description
[Type]	Displays "Server" for a server license and "Node" for a node license.
[Edition]	Displays the type of license.

Item	Description
	<ul style="list-style-type: none"> <li>- Adv.: ISM license</li> <li>- I4P: ISM for PRIMEFLEX license</li> </ul>
[#Node]	Displays the number of nodes that can be managed on that license. Always displays a "-" if the license type is "Server."
[Exp.Date]	Displays the expiration date of the license. Always displays a "-" if it is unlimited.
[Reg.Date]	Displays the date when the license was registered.
[Licensekey]	Displays the character string of the registered license key.

- Deletion of license

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

### Note

After registering or deleting licenses, ISM-VA must be restarted.

### Point

You can register licenses and check the displayed contents, including types, by selecting [Settings] - [General] - [License] from the Global Navigation Menu on the GUI of ISM.

## 4.9 Network Settings

You can execute and display the network settings.

1. From the console as an administrator, log in to ISM-VA.
2. Execute a command for the network settings.

- Display of network devices

```
# ismadm network device
```

- Modification of network settings

```
# ismadm network modify <LAN device name> ipv4.method manual ipv4.addresses <IP address>/<Maskbit> ipv4.gateway <Gateway IP address>
```

### Note

After modifying any network settings, ISM-VA must be restarted.

Example of command execution:

```
# ismadm network modify eth0 ipv4.method manual ipv4.addresses 192.168.1.101/24 ipv4.gateway 192.168.1.1
```

- Add DNS server

```
# ismadm network modify <LAN device name> +ipv4.dns <DNS server>
```

Example of command execution:

```
# ismadm network modify eth0 +ipv4.dns 192.168.1.2
```

- Delete DNS server

```
# ismadm network modify <LAN device name> -ipv4.dns <DNS server>
```

Example of command execution:

```
# ismadm network modify eth0 -ipv4.dns 192.168.1.2
```

- Display of network settings

```
# ismadm network show <LAN device name>
```

Example of command execution:

```
# ismadm network show eth0
```



.....  
You can also execute the network setting with "[4.2 ISM-VA Basic Settings Menu.](#)"  
.....

## 4.10 Alarm Notification Settings

---

You can register certificates to be used when sending alarm notifications from Monitoring.

### Registration of certificates for alarm notification mails

1. Transfer the certificates.

Transfer destination: <User group name>/ftp/cert

For information on how to transfer files using the GUI, refer to "[4.22 File Upload Using the GUI.](#)"

For information on how to transfer files via FTP, refer to "[2.1.2 FTP Access.](#)"

2. From the console as an administrator, log in to ISM-VA.
3. Execute the command for registering certificates for alarm notification mails.

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



.....  
To display and delete the certificates for alarm notification mails that are registered in ISM-VA, use the following command.  
.....

- Display of Certificates for Alarm Notification Mails

```
# ismadm event show -type cert
```

- Deletion of Certificates for Alarm Notification Mails

```
# ismadm event delete -type cert -file <Certificate file> -gid <User Group Name>
```

.....

## 4.11 ISM-VA Service Control

---

This function can stop and restart ISM-VA as well as control the services that run internally.

1. From the console as an administrator, log in to ISM-VA.

2. Execute a command for controlling the ISM-VA service.

- Restart ISM-VA

```
ismadm power restart
```

- Stop of ISM-VA

```
ismadm power stop
```

- Display of list of internal services

```
ismadm service show
```

- Start of internal service individually

```
ismadm service start <Service name>
```

Example of command execution: Start FTP server individually

```
# ismadm service start vsftpd
```

- Stop internal service individually

```
ismadm service stop <Service name>
```

Example of command execution: Stop FTP server individually

```
# ismadm service stop vsftpd
```

- Restart internal service individually

```
ismadm service restart <Service name>
```

Example of command execution: Restart FTP server individually

```
# ismadm service restart vsftpd
```

- Display of status of internal service individually

```
ismadm service status <Service name>
```

Example of command execution: Display FTP server status individually

```
# ismadm service status vsftpd
```

- Enable internal service individually

```
ismadm service enable <Service name>
```

Example of command execution: Enable FTP server individually

```
# ismadm service enable vsftpd
```

- Disable internal service individually

```
ismadm service disable <Service name>
```

Example of command execution: Disable FTP server individually

```
# ismadm service disable vsftpd
```

## 4.12 Display of System Information

You can have the internal system information of ISM-VA displayed from the console.

1. From the console as an administrator, log in to ISM-VA.
2. Execute the command for displaying the system information.

```
# ismadm system show
ISM Version      : <Version>
GUI Port Number  : 25566
Hostname         : localhost
Log Level        : small
```

The <Version> part shows the version of ISM-VA.

## 4.13 Modification of Host Names

---

You can modify the host name of ISM-VA.

1. From the console as an administrator, log in to ISM-VA.
2. Execute the command for modifying the host name.

```
# ismadm system modify -hostname <Host name (FQDN)>
```

Example of command execution:

```
# ismadm system modify -hostname ismva2.domainname
You need to reboot the system to enable the new settings.
Immediately reboots the system. [y/n]:
```

### Note

- Enter the host name in lowercase letters.
- After executing the command, a reboot is required.
- To modify the default host name "localhost," you have to follow the procedure described in "[4.7 Certificate Activation](#)" and deploy a certificate in ISM-VA that corresponds to the modified host name.

### Point

You can also modify the host name with "[4.2 ISM-VA Basic Settings Menu](#)."

## 4.14 Operation of Plug-in

---

You can apply and delete plug-in to/from ISM-VA, and display the plug-in applied to ISM-VA.

### 4.14.1 Application of Plug-in

---

1. Transfer the plug-in files to ISM-VA.

Transfer destination: /Administrator/ftp

For information on how to transfer files using the GUI, refer to "[4.22 File Upload Using the GUI](#)."

For information on how to transfer files via FTP, refer to "[2.1.2 FTP Access](#)."

Transfer the plug-in file in binary mode.

2. From the console as an administrator, log in to ISM-VA.
3. In order to apply plug-in, stop the ISM service temporarily.

Stop the ISM service according to the procedure described in "[4.1.4 Start and Stop of ISM Service](#)."

4. Execute the command for applying plug-in.

Execute the following command, specifying the plug-in file.

```
# ismadm system plugin-add -file <Plug-in file>
```

Example of command execution:

```
# ismadm system plugin-add -file /Administrator/ftp/FJSVsvism-ext-1.0.0-10.tar.gz
```

5. After applying the plug-in, restart ISM-VA.

```
# ismadm power restart
```

## 4.14.2 Display of Plug-in

---

Display of the applied plug-in version.

```
# ismadm system plugin-show
FJSVsvism-ext 1.0.0
```

It is displayed in "Plug-in name and version" format.



You can also display the information about plug-in with use of the command "ismadm system show" from ["4.12 Display of System Information."](#)

```
# ismadm system show
ISM Version      : <Version>
GUI Port Number  : 25566
Hostname         : localhost
Log Level        : small
Plugin           : FJSVsvism-ext 1.0.0
```

The <Version> part shows the version of ISM-VA.

Plugin displays the applied plug-in name and its version.

---

## 4.14.3 Deletion of Plug-in

---

Uninstall the applied plug-in.

1. Execute the command for deleting plug-in.

```
# ismadm system plugin-del -name <Plug-in Name>
```

The plug-in name is displayed with the command output in ["4.14.2 Display of Plug-in."](#)

Example of command execution:

```
# ismadm system plugin-del -name FJSVsvism-ext
Uninstall plugin <FJSVsvism-ext 1.0.0> ? [y/n]:
```

After executing the command, the uninstall plug-in confirmation screen is displayed.

2. Enter [y] to finalize the uninstallation.
3. After plug-in deletion, restart ISM-VA.

```
# ismadm power restart
```

## 4.15 ISM-VA Internal DHCP Server

---

You can use ISM-VA as a DHCP server by starting the ISM-VA internal DHCP services.

A DHCP server is required when using Profile Management for OS installation. It is possible to either use an external DHCP server or to use the procedure below to set up ISM as a DHCP server and to use that. (In this case you can select which DHCP server is used according to the operating procedure described in "[4.15.4 Switch of DHCP Servers.](#)")

If you use only the external DHCP server, the following settings are not required.

### 4.15.1 Settings for ISM-VA Internal DHCP Server

---

Set up the ISM-VA internal DHCP server. After the setup, the settings are made effective by stopping the DHCP services and starting them again.



Stop DHCP services and start them after changing the settings for the DHCP server.

For the methods to stop and start the service, refer to "[4.15.2 Operation of ISM-VA Internal DHCP Service.](#)"

To set up a DHCP server, you have two procedures. Set up the DHCP server with the either procedure according to your operation.

- Setup by specifying the parameter of `ismadm dhcpsrv` command  
This sets up for the DHCP server required for profile assignment of ISM-VA.
- Setup with conf file  
This sets up for general DHCP servers, regardless of the settings used in profile assignment of ISM-VA.

Setup by specifying the parameter of `ismadm dhcpsrv` command

```
# ismadm dhcpsrv set-simple -subnet <subnet>
                             -netmask <subnet mask>
                             -start <allocate start address>
                             -end <allocate end address>
                             -broadcast <broadcast address>
                             [-dns <DNS server IP address>]
                             [-gw <gateway IP address>]
```

You must enter the command in a single line.

You must specify the following parameters.

`-subnet`  
`-netmask`  
`-start`  
`-end`  
`-broadcast`

Example of command execution:

```
# ismadm dhcpsrv set-simple -subnet 192.168.1.0 -netmask 255.255.255.0 -start 192.168.1.150 -end
192.168.1.160 -broadcast 192.168.1.255 -dns 192.168.1.200 -gw 192.168.1.250

----- New Configuration -----
ddns-update-style none;
default-lease-time 86400;
max-lease-time 259200;

shared-network LOCAL-NET {
    subnet 192.168.1.0 netmask 255.255.255.0 {
```

```
range 192.168.1.150 192.168.1.160;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option vendor-class-identifier "PXEClient";
option domain-name-servers 192.168.1.200;
option routers 192.168.1.250;
    }
}
```

```
-----
Update DHCP configuration ? (Current settings are discarded)
[y/n]:
```

When command execution is complete, a message for confirming the value that you have set is displayed; enter "y" to confirm the setting.

#### Setup with conf file

Upload the conf file with description and feed the file with the command.

For information on how to transfer files using the GUI, refer to "[4.22 File Upload Using the GUI](#)."

For information on how to transfer files via FTP, refer to "[2.1.2 FTP Access](#)."

```
# ismadm dhcprsv set -file <conf file>
```

Example of command execution:

```
# ismadm dhcprsv set -file /Administrator/ftp/dhcpd.conf.new
```

## 4.15.2 Operation of ISM-VA Internal DHCP Service

You can start and stop the ISM-VA internal DHCP services and display their statuses.

- Confirmation of DHCP service status

```
# ismadm service status dhcpd
```

Command output

```
Active: active(running) :DHCP service active status
Active: inactive(dead) :DHCP service inactive status
/usr/lib/systemd/system/dhcpd.service; enable; :Settings to enable when booting ISM-VA
/usr/lib/systemd/system/dhcpd.service; disabled; :Settings not to enable when booting ISM-VA
```

- Manual startup of DHCP services

```
# ismadm service start dhcpd
```

### Note

- Set up for the DHCP server before you start the ISM-VA internal DHCP services.

For the method to set up the DHCP server, refer to "[4.15.1 Settings for ISM-VA Internal DHCP Server](#)."

- When the DHCP server is in "dead" state even in active settings, confirm if an error is shown with "[4.15.3 Confirmation of ISM-VA Internal DHCP Server Information](#)" - "Display of the DHCP server message."

- Manual stop of DHCP services

```
# ismadm service stop dhcpd
```

- Setup to enable DHCP services upon startup of ISM-VA

```
# ismadm service enable dhcpd
```



- Setup not to enable DHCP services upon startup of ISM-VA

```
# ismadm service disable dhcpd
```

### 4.15.3 Confirmation of ISM-VA Internal DHCP Server Information

---

You can display the ISM-VA internal DHCP server information.

You can execute the following: Display the contents of the currently-set DHCP server, Display messages of the DHCP server, Export the current set contents (conf file) to the location where ftp access is possible, and Export a sample conf file to the location where ftp access is possible.

- Display of the contents of the currently set DHCP server

```
# ismadm dhcpsrv show-conf
```

- Display of the DHCP server message

```
# ismadm dhcpsrv show-msg [-line]
```

20 lines are displayed when you execute it without option.

You can specify the number of displayed lines by specifying the option [-line].

Example of command execution:

```
# ismadm dhcpsrv show-msg -line 50
```

- Export of the current setting contents (conf file) to the location where ftp access is possible

```
# ismadm dhcpsrv export-conf -dir /Administrator/ftp
```

- Export a sample setting content (conf file) to the location where ftp access is possible

```
# ismadm dhcpsrv export-sample -dir /Administrator/ftp
```

### 4.15.4 Switch of DHCP Servers

---

When you use a DHCP server with Profile Management, you can switch use of the server between the ISM-VA internal DHCP server and the external DHCP server.

- Display of the current setting

```
# ismadm dhcpsrv show-mode
```

Command output

```
DHCP mode: local    :ISM-VA internal DHCP server is used in Profile function.
DHCP mode: remote  :The external DHCP server is used in Profile function.
```

- Switching of the settings

- Setting up so that a profile is assigned with use of the ISM-VA internal DHCP server

```
# ismadm dhcpsrv set-mode local
```

- Setting up so that a profile is assigned with use of the external DHCP server

```
# ismadm dhcpsrv set-mode remote
```

## 4.16 MIB File Settings

---

You can import MIB files that allow you to execute arbitrary trap reception in ISM-VA.

## Registration of MIB files

1. Transfer an MIB file.

Transfer destination: /Administrator/ftp/mibs

For information on how to transfer files using the GUI, refer to "[4.22 File Upload Using the GUI.](#)"

For information on how to transfer files via FTP, refer to "[2.1.2 FTP Access.](#)"

2. From the console as an administrator, log in to ISM-VA.
3. Execute MIB file registration command.

```
# ismadm mib import
```

### Point

You can display and delete the MIB files registered on ISM-VA by using the following commands.

- Display of MIB Files

```
# ismadm mib show
```

- Deletion of MIB Files

```
# ismadm mib delete -file <MIB file name>
```

## 4.17 Application of Patches

You can apply patches to ISM-VA.

### Note

Back up ISM-VA before applying patches.

For the backup procedure, refer to "[2.1.2 Export ISM-VA](#)" in "[Operating Procedures.](#)"

1. Transfer the patch files to ISM-VA.

Transfer destination: /Administrator/ftp

Patch files (tar.gz format) are included in the published files (zip format).

Decompress the published files to obtain the patch files.

For information on how to transfer files using the GUI, refer to "[4.22 File Upload Using the GUI.](#)"

For information on how to transfer files via FTP, refer to "[2.1.2 FTP Access.](#)"

Transfer the correction file in binary mode.

2. From the console as an administrator, log in to ISM-VA.
3. In order to apply patches, stop the ISM service temporarily.

Stop the ISM service according to the procedure described in "[4.1.4 Start and Stop of ISM Service.](#)"

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/SVISM_V200S20160606-02.tar.gz
```

5. After applying patches, restart ISM-VA.

```
# ismadm power restart
```

## 4.18 Upgrade of ISM-VA

---

If you need to upgrade ISM, contact your local Fujitsu customer service partner.



If you want to upgrade from V1.0 - V1.5 to V2.4, contact your local Fujitsu customer service partner.

After acquiring the upgrade file, use the following procedure to upgrade.



Back up ISM-VA before upgrading.

For the back up procedure, refer to "2.1.2 Export ISM-VA" in "Operating Procedures."

1. Transfer the upgrade files to ISM-VA.

Transfer destination: /Administrator/ftp

Check the names of the upgrade files in the readme.txt or readme\_en.txt file saved in the upgrade program.

For information on how to transfer files using the GUI, refer to "4.22 File Upload Using the GUI."

For information on how to transfer files via FTP, refer to "2.1.2 FTP Access."

2. From the console as an administrator, log in to ISM-VA.
3. In order to execute upgrade, stop the ISM service temporarily.

Stop the ISM service according to the procedure described in "4.1.4 Start and Stop of ISM Service."

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
```

## 4.19 ISM-VA Statistics Information Display

---

You can display statistics information of the CPU utilization rate, memory utilization rate, and swap utilization number for ISM-VA.

### 4.19.1 Overview of Statistics Information Display

---

You can summarize and display all data (about one month's data) collected by the hour.

```
# ismadm system stat
```

Table 4.2 Output contents

Display Item	Description
DATE	Date
CPU-avg	Average CPU utilization rate
CPU-max	Maximum CPU utilization rate
MEM-total	Physical memory capacity (MB) allocated to ISM-VA
MEM-avg	Average memory utilization rate (except the cache used by the OS)
MEM-max	Maximum memory utilization rate (except the cache used by the OS)
SWAP-avg	Average swap utilization number per second
SWAP-max	Maximum swap utilization number per second

Example of command execution:

```
# ismadm system stat
  DATE      CPU-avg  CPU-max  MEM-total MEM-avg  MEM-max  SWAP-avg  SWAP-max
2018/04/01  32.43   35.18   7823     57.96   58.71    0.00     0.00
2018/04/02  32.85   36.99   7823     57.52   58.66    0.00     0.00
2018/04/03  33.00   38.33   7823     56.14   58.17    0.00     0.00
2018/04/04  32.64   38.65   7823     54.22   55.22    0.00     0.00
2018/04/05  32.64   37.76   7823     53.84   54.97    0.00     0.00
2018/04/06  29.90   37.72   7823     54.62   56.28    0.00     0.00
2018/04/07  18.75   44.33   7823     55.01   56.13    0.00     0.00
```

## 4.19.2 Network Statistics Information Display

You can display the data of the specified date by the hour. The date can be specified individually or in a range. The detailed data for all dates collected with the "all" specification is displayed.

```
# ismadm system stat -date {DATE or all}
```

Table 4.3 Output contents

Display Item	Description
DATE	Date
HOUR	Hour (hour)
CPU-avg	Average CPU utilization rate
CPU-max	Maximum CPU utilization rate
MEM-total	Physical memory capacity (MB) allocated to ISM-VA
MEM-avg	Average memory utilization rate (except the cache used by the OS)
MEM-max	Maximum memory utilization rate (except the cache used by the OS)
SWAP-avg	Average swap utilization number per second
SWAP-max	Maximum swap utilization number per second

- Example of execution (for individual specification):

```
# ismadm system stat -date 2018/04/01,2018/04/02,2018/04/03
  DATE      HOUR      CPU-avg  CPU-max  MEM-total MEM-avg  MEM-max  SWAP-avg  SWAP-max
2018/04/01 00:00   31.57   33.87   7823     54.31   54.76    0.00     0.00
2018/04/01 01:00   31.97   34.25   7823     54.26   54.80    0.00     0.00
2018/04/01 02:00   32.13   34.13   7823     54.25   54.88    0.00     0.00
```

- Example of execution (for range specification):

```
# ismadm system stat -date 2018/04/01-2018/04/05
  DATE      HOUR      CPU-avg  CPU-max  MEM-total MEM-avg  MEM-max  SWAP-avg  SWAP-max
2018/04/01 00:00    31.57   33.87   7823     54.31   54.76    0.00     0.00
2018/04/01 01:00    31.97   34.25   7823     54.26   54.80    0.00     0.00
2018/04/01 02:00    32.13   34.13   7823     54.25   54.88    0.00     0.00
```

- Example of execution (when specifying all):

```
# ismadm system stat -date all
  DATE      HOUR      CPU-avg  CPU-max  MEM-total MEM-avg  MEM-max  SWAP-avg  SWAP-max
2018/04/01 00:00    31.57   33.87   7823     54.31   54.76    0.00     0.00
2018/04/01 01:00    31.97   34.25   7823     54.26   54.80    0.00     0.00
2018/04/01 02:00    32.13   34.13   7823     54.25   54.88    0.00     0.00
```

### 4.19.3 Real Time Information Display

You can summarize the currently operating information at intervals of one second and displays them for the specified number of times. The number of times that can be specified is in the range between 1 and 600.

```
# ismadm system stat -real {COUNT}
```

Table 4.4 Output contents

Display Item	Description
DATE	Date
TIME	Time
CPU-avg	Average CPU utilization rate
MEM-total	Physical memory capacity (MB) allocated to ISM-VA
MEM-avg	Average memory utilization rate (except the cache used by the OS)
SWAP-avg	Average swap utilization number per second

Example of command execution:

```
# ismadm system stat -real 10
  DATE      TIME      CPU-avg  MEM-total  MEM-avg  SWAP-avg
2018/04/10 08:00:25    0.51    7823     63.28    0.00
2018/04/10 08:00:26    1.02    7823     63.28    0.00
2018/04/10 08:00:27    1.52    7823     63.28    0.00
2018/04/10 08:00:28    0.51    7823     63.28    0.00
2018/04/10 08:00:29    1.52    7823     63.28    0.00
2018/04/10 08:00:30    2.02    7823     63.29    0.00
2018/04/10 08:00:31    1.02    7823     63.29    0.00
2018/04/10 08:00:32    1.51    7823     63.29    0.00
2018/04/10 08:00:33    1.02    7823     63.29    0.00
2018/04/10 08:00:34    1.52    7823     63.29    0.00
```

### 4.19.4 Output Statistics Information File

You can output the same contents that is displayed on the screen to a file.

Use Overview of Statistics Information Display, Detailed Statistics Information Display and the Real Time Information Display combined together.

Output location: /Administrator/ftp/ismva\_stat.txt

```
# ismadm system stat -file
```

```
# ismadm system stat -date {DATE or all} -file
```

```
# ismadm system stat -real {COUNT} -file
```

## 4.20 Change of the SSL/TLS Protocol Version

You can set the available SSL/TLS protocol versions.

1. From the console, log in to ISM-VA as an administrator.
2. Execute the command to set SSL/TLS to be enabled.

```
# ismadm security enable-tls TLSv1.1,TLSv1.2  
You need to reboot the system to enable the new settings. Immediately reboots the system. [y/n]:
```

When command execution is complete, a confirmation message prompting whether you want to restart is displayed.

3. Enter "y" to restart ISM-VA.

After the restart the specified SSL/TLS protocol version can be used.



### Note

- When executing the command, specify the versions that are permitted to be used separated with a comma (not a space).

The following versions can be specified.

SSLv3, TLSv1, TLSv1.1, TLSv1.2

- After executing the command, a reboot is required.
- The following is set by default.

ISM environment	SSL/TLS versions that can be used
Update/upgrade from a version earlier than ISM 2.3.0	SSLv3, TLSv1, TLSv1.1, TLSv1.2
Starts from ISM 2.3.0 or later	TLSv1.2

## 4.21 Settings for Links with Other Software

You can register certificates used when linking to other software.

1. Transfer the certificate.

Transfer destination: /Administrator/ftp/software/cert

For information on how to transfer files using the GUI, refer to "[4.22 File Upload Using the GUI.](#)"

For information on how to transfer files via FTP, refer to "[2.1.2 FTP Access.](#)"

2. From the console, log in to ISM-VA as an administrator.
3. Execute a command to register certificates used when linking to other software.

```
# ismadm security import-software-cert -software <Software name> -type <ipv4, ipv6 or fqdn> -  
server <IP address or FQDN of the server where you installed the software> -file <Certificate  
file name>
```

The following are the software names that can be specified.

Types of software	Software name specified in software
Trend Micro Deep Security	TrendMicroDeepSecurity

## Note

- For the certificate used in linking with Trend Micro Deep Security, select "Base 64 encoded X.509(.CER)" from the certificate export wizard in your Web browser. Selected and retrieved certificates other than "Base 64 encoded X.509(.CER)" cannot be used.
- To register the certificate used for Link with Trend Micro Deep Security, you must set the information of Trend Micro Deep Security in the widget.

## Point

To display and delete the certificates for linking to other software that are registered in ISM-VA, use the following command.

- Display certificate for link with other software

```
# ismadm security show-software-cert -software <Software name>
```

- Deletion certificate for link with other software

```
# ismadm security delete-software-cert -software <Software name> -type <ipv4, ipv6 or fqdn> -server <IP address or FQDN of the server where you installed the software>
```

## 4.22 File Upload Using the GUI

Using the GUI, the files used by the various functions in ISM can be uploaded to and deleted from the storage location in ISM-VA.

- The file storage location is the same as the storage location of the upload by FTP. For details, refer to "[2.1.2 FTP Access](#)."
- For the method to upload files, refer to "2.8 Upload Files to ISM-VA" in "Operating Procedures."

## Point

When using the GUI, the following operations cannot be executed. Perform them with FTP.

- Downloading the files in the file storage location
- New creation, renaming, and deletion of the file storage directory

# Chapter 5 Maintenance of Nodes

This chapter describes the maintenance of nodes.

## 5.1 Maintenance Mode

If you have to execute maintenance of a node after detecting a failure, it is recommended to enable Maintenance Mode on the target node in the ISM.

As alarm detection and background processing in ISM is restricted for nodes that Maintenance Mode is enabled, this prevents alarms from being issued repeatedly for the failed node.

The operating behavior of ISM while a node is in Maintenance Mode is as follows.

Affected function	Operating behavior in Maintenance Mode
Sensor Threshold Monitoring	Retrieval of current sensor statuses is stopped.
SNMP Trap Monitoring	Traps are received and recorded in the trap logs, but alarms are not issued.
Get Node Information	Retrieval of node information, which is periodically executed by ISM, is stopped. If required, retrieve the node information manually.
Node Log Collection	Scheduled log collections are skipped. If required, collect the Node Logs manually.

### Point

During Maintenance Mode, all functions other than those stated above remain available. For example, while a node is in Maintenance Mode, you can still execute the following operations:

- Assignment, reassignment, and release of profiles
- Firmware updates
- Manual collection of node information
- Manual collection of Node Logs

### Procedure for enabling Maintenance Mode

1. Open the Details of Node screen.
2. From the [Actions] button, select [Enable Maintenance Mode].

When the screen for confirmation is displayed, confirm the node name and select [Yes].

### Procedure for disabling Maintenance Mode

1. Open the Details of Node screen.
2. From the [Actions] button, select [Disable Maintenance Mode].

### Note

- Enable/Disable Maintenance Mode for PRIMEQUEST also enables/disables Maintenance Mode for the partitions and extension partitions under it. You can not specify a partition or extension partition and enable/disable Maintenance Mode.
- Enable/Disable Maintenance Mode for VCS Fabric (Brocade VCS Fabric) also enables/disables Maintenance Mode for the VDX fabric switch under it. You can not specify a VDX Fabric Switch to enable/disable Maintenance Mode for.



## 5.2 Investigation of Errors

---

In ISM, malfunctions are detected separately on each node.

For information that is more detailed than what is stated in the [Events] - [Events] - [Operation Log], you must access and investigate the respective devices directly.

# Appendix A Instructions for Manage and Operate Nodes

This chapter describes information on pre-settings and environmental settings, as well as settings of nodes to be managed or operated and their reference information required to use ISM.

## A.1 ISM Environmental Settings

### A.1.1 DHCP/PXE Settings in Using Profile Management/Firmware Management

When using the following functions, use the PXE boot function.

- Using Profile Management to install an OS on a server
- Using Firmware Management to execute Online Update of a server or an installed IO card.

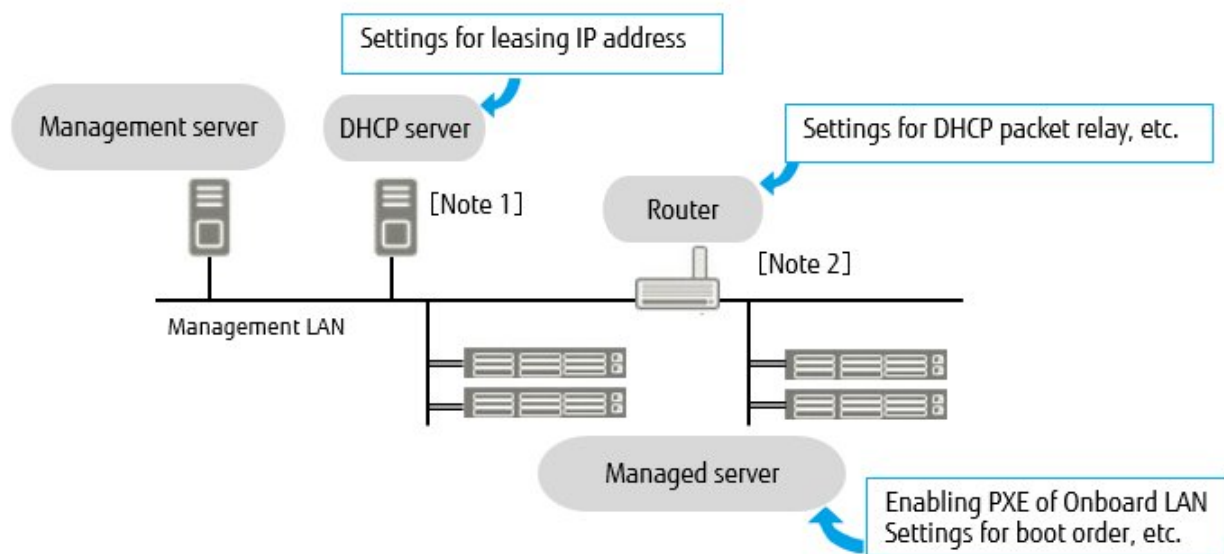
To operate PXE correctly, adequate prior preparation for managed server (node) and network configurations are required. This section provides information on the required operations for PXE boot.

Please note that for profile assignment other than OS installation and execution of firmware online update, the operations described in this section are not required.

#### Network configuration example

An example of network configuration in using PXE boot function and major preparatory operations are described below.

Figure A.1 Network configuration example



[Note 1]: Instead of preparing an external DHCP server, you can use the DHCP server function in the ISM-VA (management server). You can choose to use either the external DHCP server or the DHCP server in the managed server.

[Note 2]: If the network segment is not split, a router is not required.

#### Required preparatory operations

##### Managed Server

You can use the onboard LAN port [Note 1] or LAN card for the PXE boot function.

Change BIOS settings as required and enable PXE boot from the LAN port. [Note 2]

[Note 1]: Depending on the model of managed server, it may be described as "Dynamic LoM."

[Note 2]: You can specify the LAN port in the "PXE boot port" settings of each node.



**Pre-settings:**

- Configure so that the LAN port and PXE function are enabled.  
For onboard, these settings items are set as Enabled in factory shipment. Reset the settings items to Enabled if they have been changed to Disabled. For LAN cards, refer to the manuals, etc., of the respective cards.
- If PXE boot is set to Enabled for multiple network ports, check the settings of BIOS boot order and set the boot order so that the highest priority of ISM is given to the LAN port used for PXE boot in the network ports.

**DHCP Server/Router**

You can either enable the DHCP function in the ISM-VA or operate the DHCP server in the same network segment as the management server and set so that the appropriate IPv4 address can be leased to the PXE boot LAN port. Note that the lease period must be set equal to or greater than 60 minutes.

For example: The scope settings when ISM-VA is connected with 192.168.1.100/24

- Lease range: 192.168.1.128 to 192.168.1.159
- Lease period: 8 days

If the managed server is connected with the network of a different segment, set up a router so that the DHCP packets, etc., required for PXE boot can be transferred to each other between the segments.

Likewise, set up the variety of ports used by ISM so that their communication is available.

**ISM (Management Server)**

There is no specific setting for PXE boot. Follow this manual to execute the procedures below.

- Allocating virtual disk(s) to overall ISM-VA/allocating virtual disk(s) to user groups
- Importing OS installation DVD (For OS installation)
- Importing ServerView Suite Update DVD (For Office update)
- Importing ServerView Suite DVD
- Registering managed server in ISM

When registering in ISM, register the iRMC user with "OEM" or "Administrator" authorization.

## **A.1.2 Pre-settings for Virtual Resource Management**

---

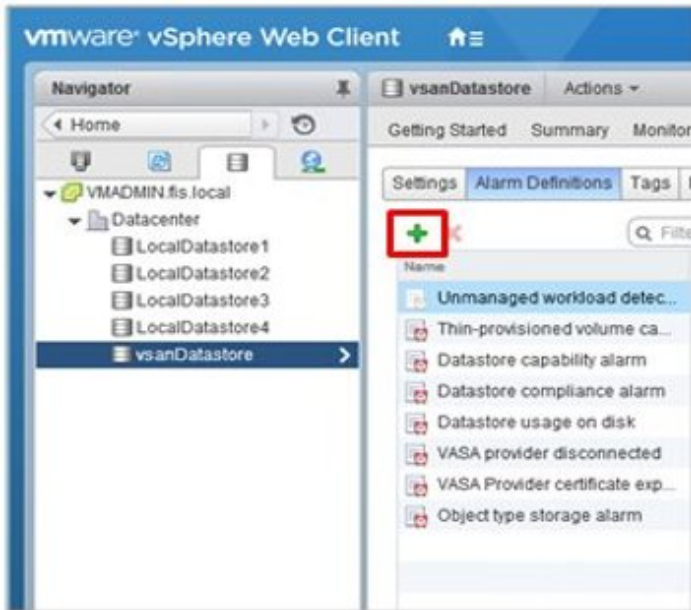
Operations of virtualization platform can be monitored by using Virtual Resource Management. This section provides information about pre-settings required for Virtual Resource Management.

**Pre-settings for VMware vSAN**

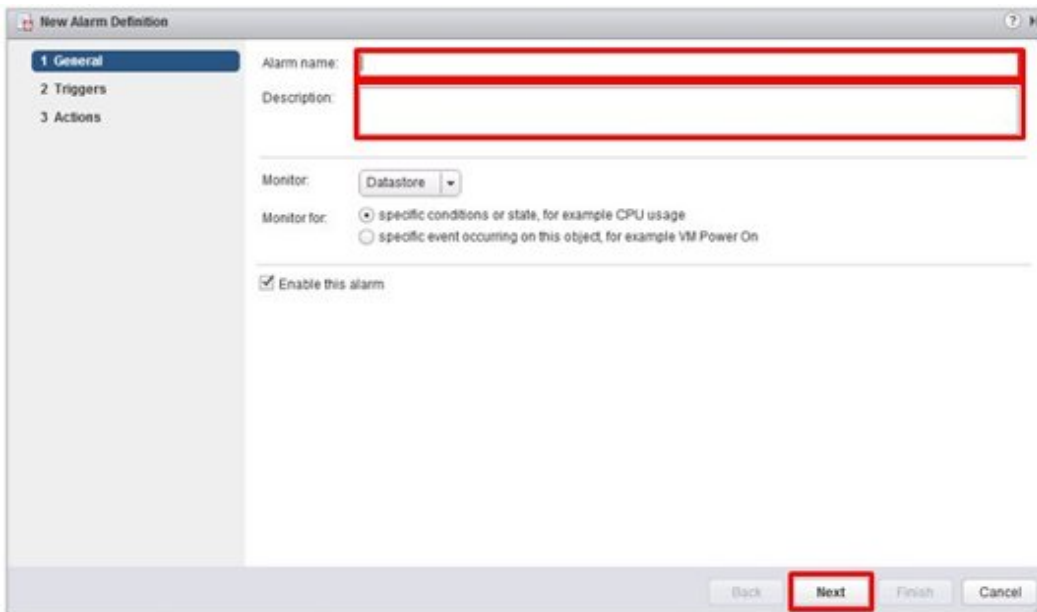
VMware vSAN alarm definition is required to enable the detection of vSAN datastore errors caused by a network disconnection between the vSAN hosts. The procedure below describes how to add vSAN alarm definitions.

1. Open the vSphere Web Client screen, from [Home] - select storage and select the created vSAN datastore.

From the [Management] tab (or from the [Monitor] tab and select [Issues] in case of vCenter Server Appliance 6.5), select [Alarm Definitions] on the right side of the displayed screen, and then select [+].

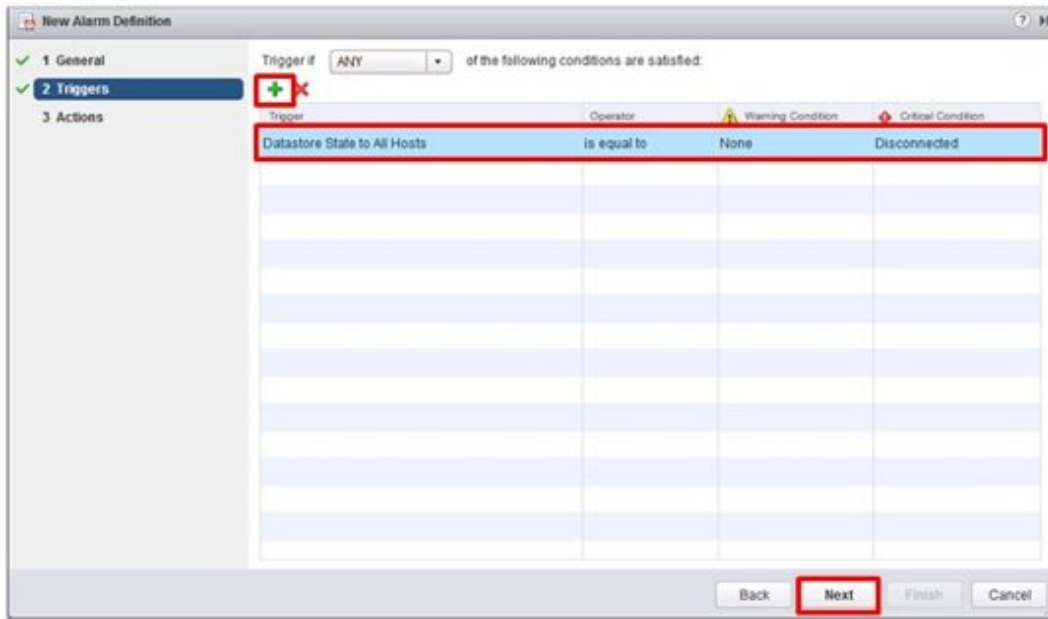


2. When the wizard screen is displayed, fill in [Alarm name] and [Description] as in the following chart, and then select the [Next] button.



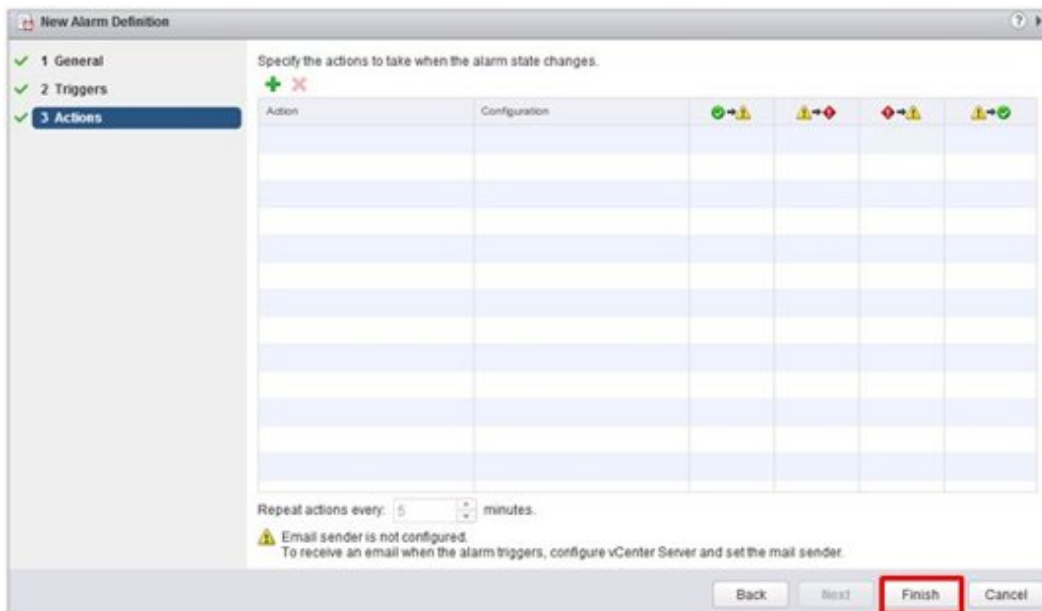
Item	Content
Alarm name	Network disconnection between hosts
Description	Alarm when the network between the hosts is disconnected.

3. Select the [+] in the following screen, then set the items as in the following chart and select the [Next] button.

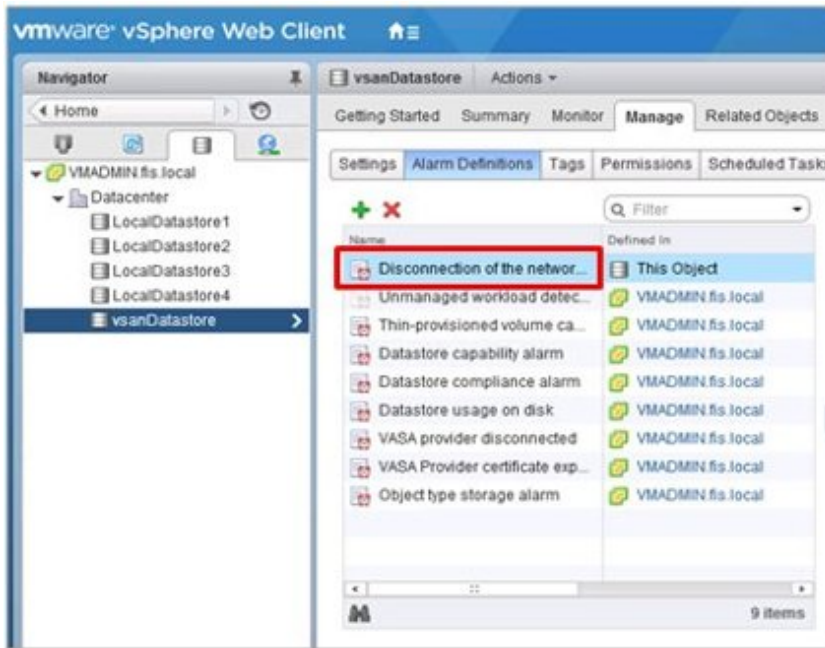


Item	Parameter
Trigger	Datastore Status to All Hosts
Operator	is equal to
Warning requirements	None
Maximum requirements	Disconnected

4. No need to set Actions. Select the [Finish] button.



The new definition is added to the alarm definitions when completed.



### Pre-settings for Storage Spaces Direct

For operation management of Microsoft Storage Spaces Direct, you must set ISM-VA to enable OS monitoring and CredSSP authentication for all the nodes configuring the storage pools. Use the following procedures for setting.

#### Settings for ISM-VA

Execute the settings for OS monitoring from ISM. For the setting procedure, refer to "2.1. Setting Procedure for Windows" in "Settings for Monitoring Target OS and Cloud Management Software."

#### Settings for nodes

Enable CredSSP authentication for all the nodes configure the storage pools.



If you do not execute these settings, Virtual Resource Management cannot be used for Storage Spaces Direct.

The nodes configure the storage pools can be checked from the Server Manager and the Failover Cluster Manager.

1. Log in to the node as a user with domain administrator privileges and start PowerShell.
2. Execute the following command.

```
Enable-WSManCredSSP -Role client -DelegateComputer <Target node (Computer) name>
```

Wild card (\*) can be used to specify all of the computer names in a domain.

Example:

```
Enable-WSManCredSSP -Role client -DelegateComputer *.pfdomain.local
```

3. And then, execute the following command.

```
Enable-WSManCredSSP -Role server
```

### A.1.3 Notes on MIB File Import

This section describes the notes on MIB file import in ISM.

## About the format of MIB

By describing the specific format for the annotation in the trap definition, it is possible to indicate the severity of MIB etc., but it may not be processed as defined depending on the contents. This section describes the format of MIB to be imported.

The annotation format of the Trap definition (TRAP-TYPE/NOTIFICATION-TYPE) of MIB conforms to the format proposed by Novell NMS.

Examples:

```
sniScVoltageTooHigh TRAP-TYPE
ENTERPRISE sniServerMgmt
VARIABLES {
trapServerName,
trapTime,
trapCabinetNumber,
trapObjectNumber,
trapString
}
DESCRIPTION
    "Power supply voltage is too high."
--#TYPE      "Voltage too high"
--#SUMMARY  "Power supply voltage %d (%s) in cabinet %d at server %s is too high."
--#SEVERITY   CRITICAL
 ::= 652
```

Table A.1 Description of comment field

Comment	Description
--#TYPE	Short name for the Trap. This name can be up to 40 characters long. It is used as a part of the trap message in ISM.
--#SUMMARY	Description of the trap with placeholders and format information for the actual parameters for trap transmission. It is used as a part of the trap message in ISM.
--#ARGUMENTS	List of parameters to substitute in the SUMMARY string. Parameters are substituted in the order in which they appear in the list. Each element of the list is the index (zero-based) of the parameter in the VARIABLES clause.
--#SEVERITY	Default severity assigned to the trap. This can be one of the following: <ul style="list-style-type: none"> <li>- INFORMATIONAL</li> <li>- MINOR</li> <li>- MAJOR</li> <li>- CRITICAL</li> </ul>

### Note

- If --#TYPE is not defined, the object name is substituted.
- If --#SUMMARY is not defined, the contents of DESCRIPTION is substituted.
- If --#SEVERITY is not defined or if the severity type other than INFORMATIONAL/MINOR/MAJOR/CRITICAL is defined, the severity of the trap is handled as INFORMATIONAL.

## Countermeasure for when Unknown trap was received

At the time of the trap reception, if the corresponding MIB is not registered, the severity is displayed as Unknown and the incorrect message will be displayed. If you receive the Unknown trap, import the latest MIB and update the data. If you still receive the Unknown trap even after the update, confirm that there are no abnormalities in the target devices. However, if you receive traps from nodes that are not managed in ISM, the message will not be correctly displayed.

## A.2 Details of Managed Nodes Settings

### A.2.1 List of Available Port Numbers

ISM needs to communicate with devices. This section provides the information required on the available port numbers for communications. You must set these according to your device type or environment.

Table A.2 Available port numbers for ISM for each target device

Target Device	Function	Protocol	Available Port
PRIMERGY (RX/BX/CX/TX) PRIMEQUEST 3000B IPCOM VX2 (except PRIMERGY CX1430 M1)	Retrieval of node information	IPMI/HTTPS	623/443
	Monitoring	IPMI	623
	Trap reception	SNMP (Trap)	162
	Firmware update	IPMI/TFTP	623/69
	Log collection	IPMI/SSH/HTTPS	623/22/443
	Profile assignment (general)	IPMI	623
		HTTP	80
		HTTPS	443
	Profile assignment (only upon OS installation)	FTP	21
		DHCP	67
		TFTP	69
SMB		445	
PXE		4011	
ISM-original	9213		
PRIMERGY CX1430 M1	Retrieval of node information	IPMI/HTTPS	623/443
	Monitoring	IPMI	623
	Firmware update		
PRIMERGY BX Chassis (MMB)	Retrieval of node information	SNMP/SSH	161/22
	Monitoring	SNMP/SSH	161/22
	Trap reception	SNMP (Trap)	162
	Firmware update	SNMP/SSH/TFTP	161/22 69
	Log collection	SSH	22
PRIMEQUEST 2000Type3 PRIMEQUEST 3000E	Retrieval of node information	SNMP/IPMI	161/623
	Monitoring	SNMP/IPMI	161/623
	Trap reception	SNMP (Trap)	162
	Firmware update	FTP/SSH	21/22
	Log collection	IPMI	623
ETERNUS DX/AF	Retrieval of node information	SNMP/SSH	161/22
	Monitoring	SNMP	161
	Trap reception	SNMP (Trap)	162
	Firmware update	FTP/SSH	21/22
	Log collection	FTP/SSH	21/22



Target Device	Function	Protocol	Available Port
	Profile assignment	SSH	22
ETERNUS NR (NetApp)	Retrieval of node information	SNMP/SSH	161/22
	Monitoring	SNMP/HTTPS	161/443
	Trap reception	SNMP (Trap)	162
	Firmware update	-	-
	Log collection	SSH/HTTPS	22/443
	Profile assignment	-	-
SR-X	Retrieval of node information	SNMP/SSH	161/22
	Monitoring	SNMP	161
	Trap reception	SNMP (Trap)	162
	Firmware update	FTP/SSH	21/22
	Log collection	SSH	22
	Profile assignment	SSH	22
PSWITCH 2048P/T PSWITCH 4032P	Retrieval of node information	SNMP/SSH	161/22
	Monitoring	SNMP	161
	Trap reception	SNMP (Trap)	162
	Firmware update	FTP/SSH	21/22
	Log collection	SSH	22
	Profile assignment	SSH	22
VDX	Retrieval of node information	SSH	22
	Monitoring	SNMP	161
	Trap reception	SNMP (Trap)	162
	Firmware update	FTP/SSH	21/22
	Log collection	SSH	22
	Profile assignment	SSH	22
Catalyst 3750-X Nexus 5000 Series Arista 7000 Family	Retrieval of node information	SSH	22
	Monitoring	SNMP	161
	Trap reception	SNMP (Trap)	162
CFX2000F/R PRIMERGY Switch Blade/Converged Fabric Switch Blade (10Gbps 18/8+2)	Retrieval of node information	SSH	22
	Monitoring	SNMP	161
	Trap reception	SNMP (Trap)	162
	Firmware update	FTP/SSH	21/22
	Log collection	SSH	22
	Profile assignment	SSH	22
PRIMERGY BX Switch Blade (1Gbps/ 10Gbps)	Retrieval of node information	SSH	22
	Monitoring	SNMP	161
	Trap reception	SNMP (Trap)	162
	Firmware update	FTP/TFTP	21/69
		SSH	22

Target Device	Function	Protocol	Available Port
	Log collection	SSH	22
PRIMERGY BX LAN Pass-Thru Blade	Retrieval of node information	SNMP	161
	Monitoring		(communicate with MMB)
	Trap reception	SNMP (Trap)	162
Brocade FC Switch	Retrieval of node information	SSH	22
	Monitoring	SNMP	161
	Trap reception	SNMP (Trap)	162
PRIMERGY BX FC Switch Blade	Retrieval of node information	SSH	22
	Monitoring	SNMP	161
	Trap reception	SNMP (Trap)	162
	Firmware update	SSH	22
	Log collection	SSH	22
Asetek Rack CDU	Retrieval of node information	SNMP	161
Schneider Electric Metered Rack Mount PDU	Monitoring	SNMP	161
Schneider Electric Smart-UPS	Trap reception	SNMP (Trap)	162

Table A.3 Available port numbers for ISM for each target OS

Target OS	Function	Protocol	Available Port
Windows	Retrieval of OS information	WSMAN	5986
	Monitoring	WSMAN	5986
	Firmware update	-	-
	Log collection	WSMAN	5986
Linux	Retrieval of OS information	SSH	22
	Monitoring	SSH	22
	Firmware update	SSH	22
	Log collection	SSH	22
VMware ESXi	Retrieval of OS information	vSphere API/CIM	443/5989
	Monitoring	vSphere API	443
	Firmware update	-	-
	Log collection	REST	443

## A.2.2 Details of Node Settings

To manage nodes with the use of ISM, you must set up the connection information on the node side. This section provides the required connection information for set up.

### Connection information

To establish a connection with the nodes, and before performing node registration, the following settings are required on the node side. For more information, refer to the manuals of the respective devices.

Note: Y = Required, - = Not required

Node	Connection Information			
	IPMI Account [Note 1]/ Password	SSH Account/ Password	Information Required to Enter for SNMP [Note 2]	HTTPS Account/ Password
PRIMERGY(RX/CX/TX) (Except for CX1430 M1)	Y	-	-	- [Note 4]
PRIMERGY CX1430 M1	Y	-	-	Y
PRIMEQUEST 2000Type3	Y	Y	Y	-
PRIMEQUEST 3000E	Y	Y	Y	-
PRIMEQUEST 3000B	Y	-	-	- [Note 4]
ETERNUS DX/AF	-	Y	Y	-
ETERNUS NR	-	Y	Y	-
SR-X	-	Y	Y	-
PSWITCH 2048P/T PSWITCH 4032P	-	Y	Y	-
VDX	-	Y	Y	-
Brocade FC Switch	-	Y	Y	-
Cisco Catalyst	-	Y	Y	-
Cisco Nexus	-	Y	Y	-
Arista 7000 Family	-	Y	-	-
PRIMERGY BX Chassis (MMB)	-	Y	Y	-
PRIMERGY BX Server Blade	Y	-	-	-
PRIMERGY BX Switch Blade (1Gbps/10Gbps)	-	Y	Y	-
PRIMERGY BX LAN Pass-Thru Blade	-	-	- [Note 3]	-
PRIMERGY BX FC Switch Blade	-	Y	Y	-
PRIMERGY Switch Blade/ Converged Fabric Switch Blade (10Gbps 18/8+2)	-	Y	Y	-
CFX2000F/R	-	Y	Y	-
AsetekRackCDU	-	-	Y	-
SchneiderElectric Metered RackMountPDU	-	-	Y	-
SchneiderElectric Smart-UPS	-	-	Y	-

For the models which are confirmed for operation, contact your local Fujitsu customer service partner.

[Note 1]: Use the account with administrator access privilege or OEM.

[Note 2]: For SNMP v1 or v2, you must enter the community name.

For SNMP v3, you must enter the user name, security level, authentication protocol (when authentication is used), authentication password (when authentication is used), encrypted protocol (when encryption is used), encrypted password (when encryption is used).

[Note 3]: PRIMERGY BX LAN Pass-Thru Blade requires connection information settings of the chassis (MMB).

[Note 4]: You can only specify HTTPS port number. The account/password will be the same as its IPMI.

## Required settings for management

Confirm the following settings in addition to the connection information settings.

### [PRIMERGY]

When you are using the iRMC S4 firmware version 9.00 or later for the PRIMERGY S8/M1/M2/M3 generation server, you must change the IPMI Privileges and Permissions of Web UI of iRMC to retrieve the SAS card information of the ISM node details. Execute the following procedure to change the IPMI Privileges and Permissions.

1. [User Management] - [iRMC S4 User Management] - [IPMI Privileges/Permissions] - mark the checkbox of [Redfish Enabled].
2. [User Management] - [iRMC S4 User Management] - [IPMI Privileges/Permissions] - change the box of [Redfish Role] to Administrator.

### [SR-X]

Enable LLDP settings

### [VDX]

- Enable LLDP settings
- Set the IP address of the management LAN port for each switch
- Disable AG mode

### [Arista 7000 Family]

Enable LLDP settings

### [ETERNUS DX/AF]

As the port connecting to ISM, use the maintenance port of Control Module.

(If connecting to a remote port, the firmware update function, the log collection function and profile assignment function may not work.)

### [PRIMEQUEST 2000 Type3, PRIMEQUEST 3000E]

- For the MMB account settings (account settings for IPMI connection) for ISM, use the account that registered in the Web UI [Network Configuration] - [Remote Server Management] of PRIMEQUEST.
- For the SSH account settings for ISM, use the account that registered in the WEB UI [User Administration] - [User List] of PRIMEQUEST. The access privileges must be administrator or CE.

### [PRIMERGY BX]

- Switch Blade: Enable LLDP settings
- Fibre Channel Switch Blade: Enable SW-MIB settings

Example of command execution:

```
snmpconfig --enable mibCapability -mib_name SW-MIB
```

- When the power of the Chassis is OFF, information cannot be retrieved from MMB. Therefore, the relation between the server blade and connection blade look temporarily cancelled. When the status of the power is ON, select the chassis, go to the [Action] button - [Get Node information] and execute the operation.

## Required settings for notification

Make the settings for SNMP traps in addition to the settings for connection information and for required information for management.

For details, refer to the manuals of the respective devices.

For the devices listed below, Engine ID is automatically input when selecting the target node in Trap Reception settings.

Note: Y = Supported, - = Not supported

Node	Availability of Automatic input of Engine ID
PRIMERGY(RX/CX/TX)	Y
PRIMEQUEST 2000Type3	-
PRIMEQUEST 3000E	Y
PRIMEQUEST 3000B	Y
ETERNUS DX/AF	Y
ETERNUS NR	-
SR-X	Y [Note 1]
PSWITCH 2048P/T PSWITCH 4032P	Y
VDX	Y
Brocade FC Switch	Y
Cisco Catalyst	Y
Cisco Nexus	Y
PRIMERGY BX Chassis (MMB)	-
PRIMERGY BX Server Blade	Y
PRIMERGY BX Switch Blade (1Gbps/10Gbps)	Y [Note 1]
PRIMERGY BX LAN Pass-Thru Blade	-
PRIMERGY BX FC Switch Blade	Y
PRIMERGY Switch Blade/Converged Fabric Switch Blade (10Gbps 18/8+2)	Y [Note 1] [Note 2]
CFX2000F/R	Y [Note 1] [Note 2]
AsetekRackCDU	-
SchneiderElectricMetered RackMountPDU	-
SchneiderElectricSmart-UPS	-

[Note 1]: When SNMP v3 Engine ID is not set for the following devices and selecting the target node in the ISM Trap Reception settings, the Engine ID is not automatically input. To automatically input the Engine ID, set the SNMP v3 Engine ID for the devices in advance.

- PRIMERGY BX Switch Blade (10Gbps)
- PRIMERGY Switch Blade/Converged Fabric Switch Blade (10Gbps 18/8+2)
- CFX2000F/R
- SR-X

[Note 2]: When fabric is configured and SNMP v3 Engine ID has been set for the devices, set each Engine ID with the same values in the whole fabric.

## A.3 Details of Other Settings

---

### A.3.1 ETERNUS DX/AF Drive Enclosure Display

---

ISM is capable of managing drive enclosures connected to a control enclosure of ETERNUS DX/AF as its nodes.

This section provides the required setting information to manage drive enclosures.

## Registration of drive enclosure

A drive enclosure is automatically registered with ISM as its node by the following procedure.

1. Register the controller enclosure of ETERNUS DX/AF with ISM as its node and a drive enclosure connected.
2. After completion of node information retrieval of the controller enclosure, the drive enclosure is displayed on a node list.

## Details of node information of drive enclosure

The details of node information of the drive enclosure is displayed in the details of node information of the controller enclosure in ISM.

## Status of drive enclosure

The drive enclosure status is always displayed as "Unknown." This is because the drive enclosures are intensively managed by a controller enclosure. Refer the controller enclosure node information.

## Deletion of drive enclosure

Drive enclosure is deleted from a node list in the following cases.

- Controller enclosure node information retrieval is executed after a drive enclosure is cut off from the controller enclosure.
- The node of the controller enclosure is deleted from ISM.

## A.3.2 General Standards for Firmware Update Time

It may take time to update firmware with the use of the Firmware Manager of ISM. This section provides guideline standards for the time required to update firmware.

When making plans to update firmware, refer the times described below. Moreover, interrupting the firmware update before completion should be avoided.



### Note

The times described below indicate the time taken for updating the current firmware with standard configurations. Since the time may vary depending on the firmware version, network configurations and/or network load conditions, it is recommended to plan with enough margin, including time to address unexpected troubles.

Table A.4 General standards for firmware update time

Target of Firmware Update	Standard Time/Unit	Note
Firmware update of iRMC in PRIMERGY	Online update 10 to 20 min.	
	Offline update 15 to 30 min.	If the server is set to be turned ON after the firmware is assigned, it takes an additional 15 minutes.
Firmware update of BIOS in PRIMERGY	Online update 1 to 2 min.	To assign firmware, you must take into account the extra time for powering the server ON/OFF.
	Offline update 15 to 30 min.	If the server is set to be turned ON after the firmware is assigned, it takes an additional 15 minutes.
Firmware update of iRMC in PRIMEQUEST 3800B	Online update 10 to 20 min.	
Firmware update of BIOS in PRIMEQUEST 3800B	Online update 5 to 15 min.	To assign firmware, you must take into account the extra time for powering the server ON/OFF.
Firmware update of PRIMEQUEST 2000 series, 3000 series	70 to 130 min.	

Target of Firmware Update	Standard Time/Unit	Note
PRIMERGY BX900S2 MMB	10 to 20 min.	The time noted in the left is the time taken per MMB.
Firmware update of network switch SR-X	2 to 10 min.	
Firmware update of fabric switch CFX2000R/F, converged fabric switch blade	10 to 20 min.	
Firmware update of converged switch VDX	15 to 30 min.	
Firmware update of PSWITCH 2048P/T, PSWITCH 4032P	20 to 30 min.	
Firmware update of LAN switch blade	10 to 20 min.	
Firmware update of Cisco Systems Nexus series	30 to 50 min.	
Firmware update of Cisco Systems Catalyst series	10 to 20 min.	
Firmware update of FC switch blade	10 to 20 min.	
Firmware update of PCI card	Online update 5 to 15 min.	To assign firmware, you must take into account the extra time for powering the server ON/OFF. The time noted in the left is the time taken per card.
	Offline update 15 to 20 min.	The time noted in the left is the time taken per card.
Firmware update of ETERNUS DX/AF series	10 to 60 min.	When a unified environment exists and multiple controller enclosures are installed, the update time will be longer.

### A.3.3 General Standards for Disk Usage in Using Log Management

ISM is capable of periodically collecting logs from nodes and accumulating them on ISM-VA by using the Log Management. This section provides the information on the area for accumulating the collected logs and general standards for accumulated data amount.

The collected logs are accumulated on the log storage area on a virtual disk(s) allocated to user groups. See allocation of virtual disk to each user group of ISM-VA.

#### Note

- The following are the default settings for log retention period and the number of generations.

Change the log retention period and the number of generations as required.

Archived Logs	Node Logs (data for download/data for log search)
7 Generations	30 days

- The capacity described on this document is reference value for specific configurations and operations. The capacity can vary greatly depending on the actual use conditions.

#### Type of managed logs and their accumulation area

Log Management creates archived logs, node logs (data for download) and node logs (data for log search) after the collection of logs.

Each of the above logs is accumulated in the following log storage areas.

Log Type	Storage Area
Archived Logs	Log storage area for the user group related to the node group to which a node belongs [Note 1]
Node Logs (data for download)	

Log Type	Storage Area
Node Logs (data for log search)	Log storage area for Administrator group [Note 2]

[Note 1]: If a node group is not related to a user group, these logs are accumulated in the log storage area of Administrator group.

[Note 2]: The node logs (data for log search) of all nodes are accumulated in the log storage area of the Administrator group. Even if a node group is related to a user group(s) other than the Administrator group, these logs are accumulated in the log storage area of the Administrator group.

### General standards for log capacity

[Capacity for Archived Logs]

Table A.5 General standard for one generation per node

Log Collection Target		Standard Capacity	
Hardware	Server	PRIMERGY	1 KB
		PRIMEQUEST 3000B	1 KB
		IPCOM VX2	1 KB
	Chassis	PRIMERGY BX	100 KB
		PRIMEQUEST 3000E	50 KB
	Connection Blade	Ethernet Switch	100 KB
		Fibre Channel Switch	10 MB
	Switch	SR-X	50 KB
		CFX	100 KB
		PSWITCH 2048P/T	350 KB
		PSWITCH 4032P	
		VDX	50 MB
		Cisco Catalyst	1 MB
		Cisco Nexus	1 MB
	Storage	ETERNUS DX/AF	10 MB
ETERNUS NR (NetApp) Cluster		100 KB	
ETERNUS NR (NetApp) Chassis		500 MB	
Operating system	Windows	5 MB	
	Linux	5 MB	
	VMware ESXi	3 MB	
	IPCOM OS	50 MB	
ServerView Suite	ServerView Agents	Windows: 10 MB	
	ServerView Agentless Service	Linux: 80 MB	
	ServerView RAID Manager		

[Capacity for Node Logs (data for download)]

Table A.6 General standard for 30 days' worth per node

Log Collection Target		Standard Capacity	
Hardware	Server	PRIMERGY	50 KB
		PRIMEQUEST 3000B	50 KB
		IPCOM VX2	50 KB



Log Collection Target			Standard Capacity
	Chassis	PRIMERGY BX	50 KB
		PRIMEQUEST 3000E	500 KB
	Connection Blade	Ethernet Switch	100 KB
		Fibre Channel Switch	50 KB
	Switch	SR-X	100 KB
		CFX	100 KB
		PSWITCH 2048P/T	150 KB
		PSWITCH 4032P	
		VDX	100 KB
		Cisco Catalyst	50 KB
		Cisco Nexus	50 KB
Storage	ETERNUS DX/AF	100 KB	
	ETERNUS NR (NetApp) Cluster	200 KB	
Operating system	Windows		1 MB
	Linux		1 MB
	VMware ESXi		4 MB
	IPCOM OS		1 MB

[Capacity for Node Logs (data for log search)]

Table A.7 General standard for 30 days' worth per node

Log Collection Target			Standard Capacity
Hardware	Server	PRIMERGY	500 KB
		PRIMEQUEST 3000B	500 KB
		IPCOM VX2	500 KB
	Chassis	PRIMERGY BX	500 KB
		PRIMEQUEST 3000E	500 KB
	Connection Blade	Ethernet Switch	1 MB
		Fibre Channel Switch	500 KB
	Switch	SR-X	1 MB
		CFX	1 MB
		PSWITCH 2048P/T	1 MB
		PSWITCH 4032P	
		VDX	1 MB
		Cisco Catalyst	500 KB
		Cisco Nexus	500 KB
	Storage	ETERNUS DX/AF	1 MB
ETERNUS NR (NetApp) Cluster		2 MB	
Operating system	Windows		15 MB
	Linux		15 MB
	VMware ESXi		50 MB

Log Collection Target		Standard Capacity
	IPCOM OS	15 MB

## Appendix B Uninstallation of ISM-VA

Uninstall ISM-VA according to the installation destination.

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

- [Uninstalling from Microsoft Windows Server Hyper-V](#)
- [Uninstalling from VMware vSphere Hypervisor 5.5 or VMware vSphere Hypervisor 6.0](#)
- [Uninstalling from VMware vSphere Hypervisor 6.5 or later](#)
- [Uninstalling from KVM](#)

### Uninstalling from Microsoft Windows Server Hyper-V

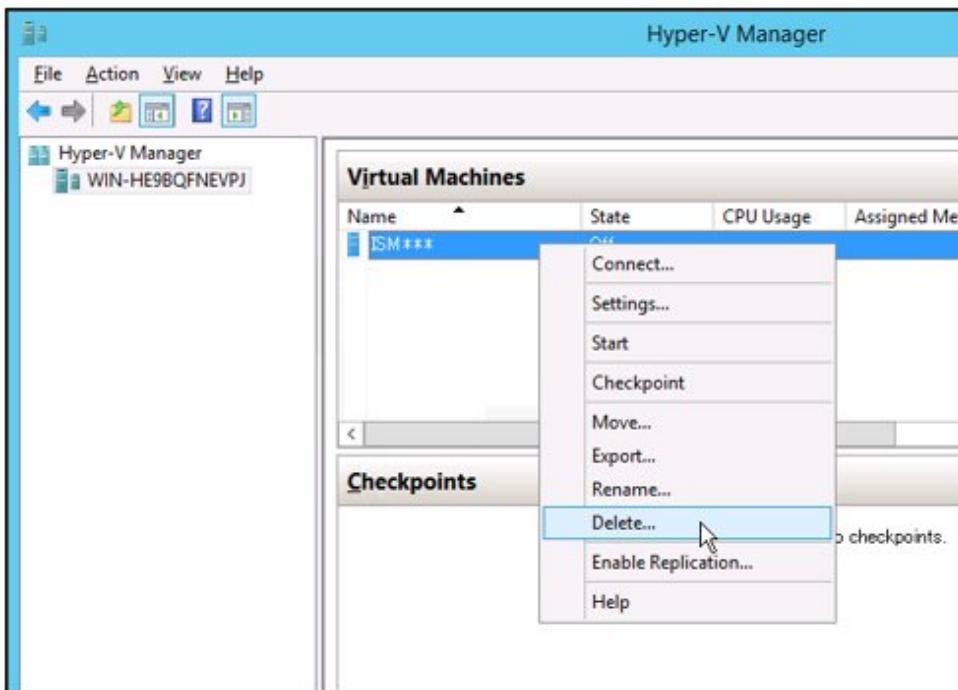
1. Stop ISM-VA.

For details, refer to "[4.1.2 Stop of ISM-VA.](#)"

2. Start Hyper-V Manager, right-click on the installed ISM-VA, and then select [Settings].

Take a memo of the displayed storage location of the virtual hard disk that is allocated to the ISM-VA and of the corresponding file name.

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



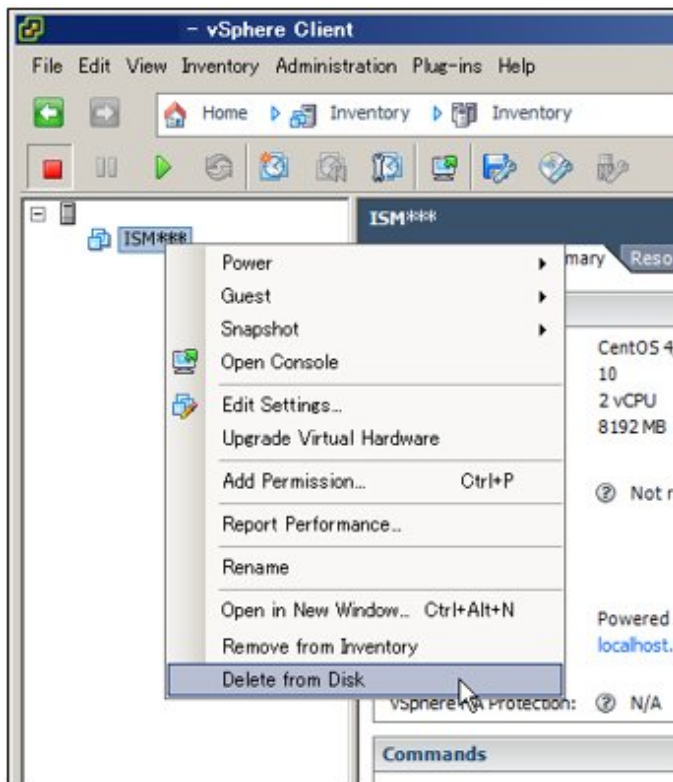
4. Use Explorer to remove the virtual hard disk for which you took the memo in Step 2.

### Uninstalling from VMware vSphere Hypervisor 5.5 or VMware vSphere Hypervisor 6.0

1. Stop ISM-VA.

For details, refer to "[4.1.2 Stop of ISM-VA.](#)"

2. Start vSphere Client, right-click on the installed ISM-VA, and then select [Delete from Disk].

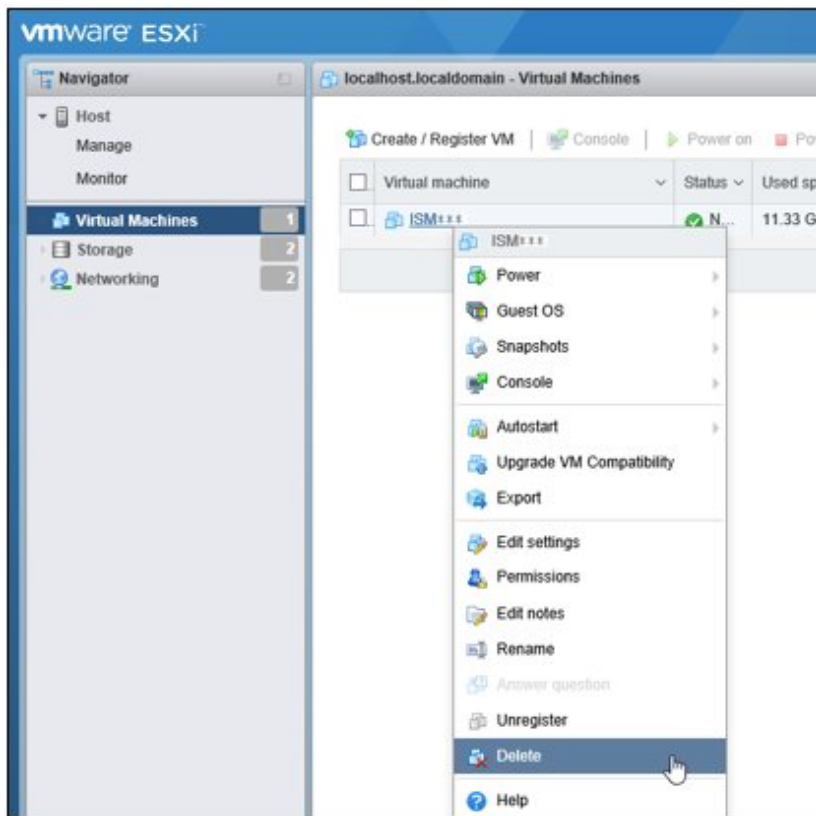


## Uninstalling from VMware vSphere Hypervisor 6.5 or later

1. Stop ISM-VA.

For details, refer to "[4.1.2 Stop of ISM-VA.](#)"

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

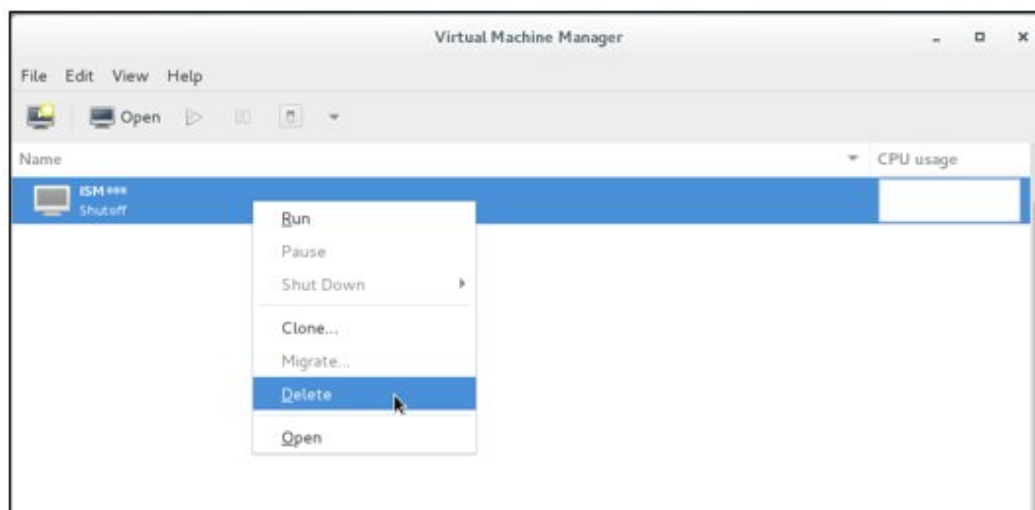


## Uninstalling from KVM

1. Stop ISM-VA.

For details, refer to "[4.1.2 Stop of ISM-VA.](#)"

2. Start Virtual Machine Manager, right-click on the installed ISM-VA, and then select [Delete].



## Appendix C Successor Cluster Expansion

This chapter describes the process for adding servers that will become successors in PRIMEFLEX.

### C.1 Successor Cluster Expansion Requirements

PRIMEFLEX, which is a Hyper-converged infrastructure (HCI) product, can add successor servers in addition to the same generation servers of the ones at the time of purchase.

#### C.1.1 Addable Successor Servers

For each PRIMEFLEX, the generations of addable servers are as follows.

PRIMEFLEX model name	Generation of the servers for expanding a cluster	
	PRIMERGY M2 series	PRIMERGY M4 series
PRIMEFLEX HS V1.0	It is addable because it is the same server generation as the one at the time of purchase.	It is addable because it is the successor model of the one at the time of purchase.
PRIMEFLEX HS V1.1		

For each PRIMEFLEX of the type at the time of purchase, models of addable servers are as follows.

Add models that use vSAN with successor type servers used at the time of purchase.

Server type at time of purchase	Type of server for expanding a cluster		
	PRIMERGY RX2530 M4	PRIMERGY RX2540 M4	PRIMERGY CX2560 M4
PRIMERGY RX2530 M2	Successor servers for the servers at the time of purchase can be added with ISM for PRIMEFLEX.	Servers are not addable.	Servers are not addable.
PRIMERGY RX2540 M2	Servers are not addable.	Successor servers for the servers at the time of purchase can be added with ISM for PRIMEFLEX.	Servers are not addable.
PRIMERGY CX2550 M2	Servers are not addable.	Servers are not addable.	Successor servers for the servers at the time of purchase can be added with ISM for PRIMEFLEX.

#### C.1.2 Network Configuration

For adding a successor model server, you must match the physical/logical network configuration to the server at the time of purchase.

Since 10GBase-T, or 10GBase can be selected for the network interface of the existing servers (PRIMERGY RX2530 M2/PRIMERGY RX2540 M2), select the same port for the PCI card and port expansion options of the servers for expanding a cluster (PRIMERGY RX2530 M4/PRIMERGY RX2540 M4).

For the network interface of the existing server (PRIMERGY CX2550 M2), you can select 1GBase-T or 10GBase. Therefore, select the same port for both the port expansion option for a server (PRIMERGY CX2560 M4) for expanding a cluster and the PCI card.

Item	Existing server and Network configuration		Servers for expanding a cluster and Network configuration	
Server	PRIMERGY RX2530 M2 /PRIMERGY RX2540 M2	PRIMERGY RX2550 M2	PRIMERGY RX2530 M4 /PRIMERGY RX2540 M4	PRIMERGY RX2560 M4

Item	Existing server and Network configuration		Servers for expanding a cluster and Network configuration	
Network Configuration	<ul style="list-style-type: none"> <li>- Port expansion option: 10G x2 ports</li> <li>- PCI: 10G x2 ports</li> </ul>	<ul style="list-style-type: none"> <li>- Port expansion option: 1G x2 ports</li> <li>- PCI: 10G x2 ports</li> </ul>	<ul style="list-style-type: none"> <li>- Onboard 1G x2 ports</li> <li>- Port expansion option: 10G x2 ports</li> <li>- PCI: 10G x2 ports</li> </ul>	<ul style="list-style-type: none"> <li>- Onboard 1G x1 port</li> <li>- Port expansion option: 1G x2 ports</li> <li>- PCI: 10G x2 ports</li> </ul>

Figure C.1 Network configuration when adding PRIMERGY RX2530 M4 in a PRIMERGY RX2530 M2 environment

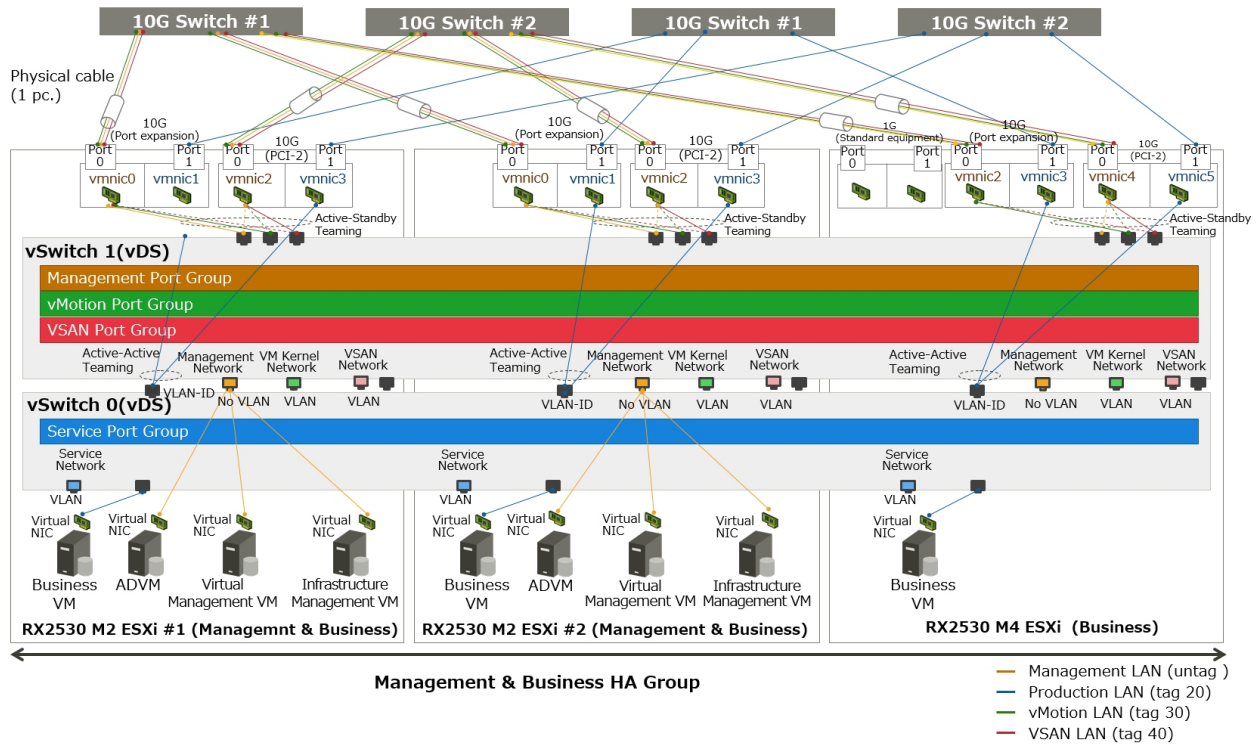
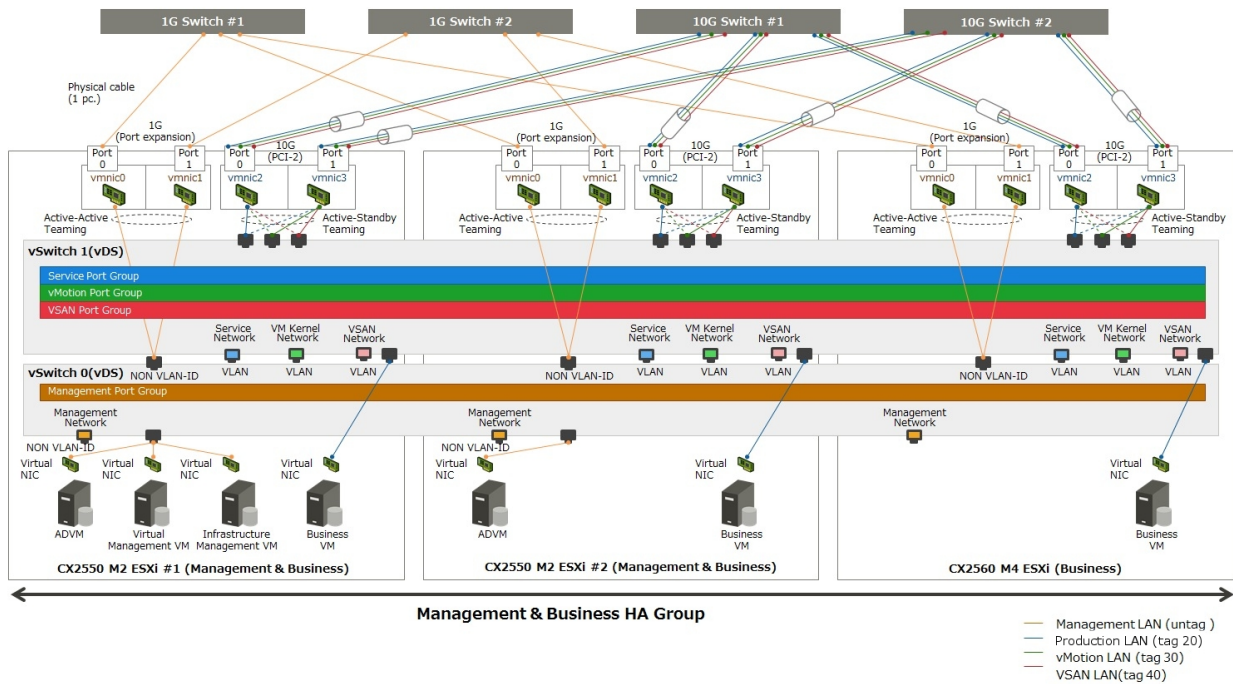


Figure C.2 Network configuration when adding PRIMERGY CX2560 M4 in a PRIMERGY CX2550 M2 environment



### C.1.3 Hardware Requirements

With SDS, it is recommended to add servers with hardware with the same configuration as the existing server. However, if the generation of the existing server differs from that of the servers for expanding a cluster, it may not be possible to execute the same configuration.

This part describes the policy for selecting the hardware configuration of the server for expanding a cluster for the existing server.

The following are the options that are relevant for the existing servers and the servers for expanding a cluster.

- Base unit
- CPU
- Memory
- HDD
- SSD
- On board LAN (Flexible LOM)
- SAS controller card
- Option card (LAN card that is required to be mounted)

#### Note

- For the relevant options, it is recommended to select them according to the policy of this document. If you select an option that does not match the policy of this document, performance may be affected. The recommended configuration of the servers for expanding a cluster can be confirmed by the configurator.
- For the irrelevant options, select them according to the installation conditions of each server and your environment.

The following is the details of each option.



## Base unit

The server types listed in "[C.1.1 Addable Successor Servers](#)" can be used for addition.

## CPU

If the CPU generations that can be mounted on existing servers and servers for expanding a cluster are different, it is recommend that CPUs mounted in the servers for expanding a cluster have CPUs equal to or higher than those mounted in existing servers.

"CPUs equal to or higher than the CPU" means that the both number of cores and clocks are equal to or higher than the CPU mounted in the existing server.

The number of CPUs is to be the same as that of existing servers.

Depending on the CPU mounted in the existing server, there may be cases in which there are no CPUs equal to or higher than the CPUs that can be mounted in the servers for expanding a cluster. In that case, it is recommended to execute the operation in different clusters separately from the existing server.

If servers with non-equivalent CPUs are added to the same cluster, the throughput of the virtual machine may be affected depending on the position of the virtual machine or virtual machine component.

## Memory

Install the memory to be installed in the servers for expanding a cluster so that it is to be greater than the total capacity of installed memory per 1 node of the existing server.

If the memory of the same model name can be arranged, it is recommended to install the same units with the same model name.

If there is no memory of the same model name, there is no problem even if the capacity per unit memory and the number of units mounted are different from the destination place to be added.

## HDD (Capacity)

It is recommended to mount the same model name/number of units for HDD mounting to the servers for expanding a cluster if you can arrange the same HDD model name as the existing server.

If the HDD with the same model name as the existing server is not supported by the servers for expanding a cluster, use HDD with equal or higher performance, and mount it so that the disk capacity is over the existing server.

All the HDDs mounted on the servers for expanding a cluster must be the same model name.

HDD with equal or higher performance is an HDD that satisfies the following requirements. If there are multiple HDDs that satisfy the requirements, select the HDD of which "rotation number" is close to the servers for expanding a cluster.

Item	Condition
HDD type (nearline SAS, SAS and others)	Same as the existing servers
Rotation number (rpm)	Same as or exceeding the existing servers
Sector size	Same as the existing servers

As for the disk capacity and the number of mounted HDD, install the disk capacity so that it will be more than the existing server per server for expanding a cluster.

There are the following configurations for the HDD installation pattern.

If there are multiple HDD mounted patterns satisfying the requirements, this order is recommended: Configuration 1 > Configuration 2 = Configuration 3 > Configuration 4.

However, the number of mounted HDDs as SDS must be satisfied.

Configuration	Item	
	Disk capacity (per one HDD)	Number installed
Configuration 1	Same as the existing servers	Same number as the existing servers
Configuration 2	HDD which has more capacity than that of existing server and the least capacity	Same number as the existing servers

Configuration	Item	
	Disk capacity (per one HDD)	Number installed
Configuration 3	HDD which has less capacity than that of existing server and the greatest capacity SSD	The capacity of each server is the minimum number above the existing number of servers (More number than existing servers)
Configuration 4	HDD which has more capacity than that of existing server and the least capacity	The capacity of each server is the minimum number above the existing number of servers (Less number than existing servers)

Examples of HDD installation are shown below.

Example 1:

HDD configuration of the existing servers (vSAN): 900 GB x 4 units

- If the disk of the server for expanding a cluster is 400 GB, 900 GB, 1 TB, or 2 TB, it will be the 900 GB x 4 units of configuration 1.
- If the disk of the server for expanding a cluster is 400 GB, 1 TB, or 2 TB, it will be the 1 TB x 4 units of configuration 2.
- If the disk of the server for expanding a cluster is 400 GB or 600 GB, it will be the 600 GB x 6 units of configuration 3.
- If the disk of the server for expanding a cluster is 2 TB, it will be the 2 TB x 2 units of configuration 4.

Example: 2

HDD configuration of the existing servers (vSAN): 600 GB x 2 units

- If the disk of the server for expanding a cluster is 400 GB or 1.2 TB, the configuration will be the 400 GB x 3 units, that is configuration 3 (Since the number of mounted HDDs should be two or more, 1.2 TB x 1 unit configuration is not acceptable).

## SSD (Cache / Capacity)

It is recommended to mount the same model name/number of units for SSD mounting to the server for expanding a cluster if you can arrange the same SSD model name as the existing server.

If the SSD with the same model name as the existing server is not supported by the server for expanding a cluster, use SSD with equal or higher performance, and mount it so that the disk capacity is over the existing server.

For the product class, the same as the existing server is recommended, but it can be changed according to your environment.

All the SSD mounted on the server for expanding a cluster must be the same model name.

An SSD with equal or higher performance is an SSD that satisfies the following requirements.

Item	Condition
Data transfer rate (SAS 12 Gbps and others)	Same as the existing servers
Recording method (MLC and others)	Same as the existing servers

As for the disk capacity and the number of mounted SSD, install the disk capacity so that it will be more than the existing server per server for expanding a cluster.

There are the following configurations for the installation pattern.

If there are multiple SSD mounted patterns satisfying the requirements, this order is recommended: Configuration 1 > Configuration 2 = Configuration 3 > Configuration 4.

However, the number of mounted SSDs as each SDS must be satisfied.

Configuration	Item		
	Disk capacity (Per one SSD)	Number installed	Product class (Write assurance value)
Configuration 1	Same as the existing servers	Same number as the existing servers	The same number as the existing servers is recommended
Configuration 2	SSD which has more capacity than that of existing server and the least capacity	Same number as the existing servers	
Configuration 3	SSD which has less capacity than that of existing server and the greatest capacity SSD	Number that makes the capacity per server more than the existing servers (More number than existing servers)	
Configuration 4	SSD which has more capacity than that of existing server and the least capacity	The capacity of each server is the minimum number above the existing number of servers (Less number than existing servers)	

### Onboard LAN (Flexible LOM)

Select the option with communication speed / number of port described in "[C.1.2 Network Configuration](#)."

### SAS controller card

Select the same model name if the same model name of existing server is available.

If you do not have it, select the successor model of the card mounted to the existing server.

### Option card (LAN card that is required to be mounted)

The LAN card that is to be mounted so that the network configuration of the server for expanding a cluster can be the same as in the existing server.

Select a card that satisfies the requirements described in "[C.1.2 Network Configuration](#)."

The network interface (10GBase/10GBase-T) must be the same as the existing server.

### Options other than the above

For options other than the above, they can be selected according to the requirements of each PRIMEFLEX or your environment.

## C.1.4 Software Requirements

You must install the same version of software for both existing servers and servers for expanding a cluster.

### Software Version

If the software installed to the existing server is not supported by the server for expanding a cluster, update the software of existing server before adding the server.

The update policy for the software installed to each PRIMEFLEX are as follows.

Table C.1 Update policy (For vSAN)

Software name	Where to install	Edition
VMware vSphere	Server for expanding a cluster	Install a version that is supported by both the servers for expanding a cluster and the existing servers.
	Existing servers	Select the same version for both the servers for expanding a cluster and the existing servers (including build numbers).
vSAN	Server for expanding a cluster	Install a version that is supported by both the servers for expanding a cluster and the existing servers.
	Existing servers	Select the same version for both the servers for expanding a cluster and the existing servers (including build numbers).

Software name	Where to install	Edition
vCenter Server (vCSA)	Virtual Admin VM	Install the same version as VMware vSphere or a later version.
Windows Server (ADVM)	ADVM	Install the version at the time of purchase.
ISM for PRIMEFLEX	Infrastructure Admin VM	Install a version which supports VMware vSphere/vSAN of both the server for expanding a cluster and the existing servers.
ServerView RAID Manager	ADVM	Install a version which supports VMware vSphere of both the server for expanding a cluster and the existing servers.

## Products to be arranged

The following describes the software products that must be arranged for the server for expanding a cluster.

The following are the software products required to be arranged for the vSAN model.

Software products	Relevant to existing server	Alternative
VMware vSphere License	Yes	Required
vSAN License	Yes	Required
vCenter Server License	None	Optional
Windows Server License	None	Optional
ISM for PRIMEFLEX Media Pack	None	Not required
ISM for PRIMEFLEX Server License	None	Not required
ISM for PRIMEFLEX Node License	None	Required

Details of each software product are as follows.

- VMware vSphere License

Arrange the same license (edition, support level [weekday 24Hours]) as the one installed to the existing server. As for supporting period, it is changeable according to customers' requirements.

- vSAN License

Arrange the same license (edition, support level [weekday 24Hours]) as the one installed to the existing server. As for supporting period, it is changeable according to customers' requirements.

- vCenter Server License

It is not relevant to the configuration of existing server. Arrange it if you install 2 or more of vCenter Server.

- Windows Server License

It is not relevant to the configuration of existing server. Arrange it if required.

- ISM for PRIMEFLEX Media Pack

It is not required to additionally arrange ISM for PRIMEFLEX Media Pack for servers for expanding a cluster.

- ISM for PRIMEFLEX Server License

It is not required to additionally arrange ISM for PRIMEFLEX Server License for servers for expanding a cluster.

- ISM for PRIMEFLEX Node License

It is not relevant to the configuration of existing server. Arrange the node license for the number of servers for expanding a cluster.

## C.2 Successor Cluster Expansion

Execute Cluster Expansion with successor models according to the following work flow.

Table C.2 Successor Cluster Expansion Flow

Procedure for cluster expansion		Tasks
1	<a href="#">Preparations</a>	<ul style="list-style-type: none"> <li>- Sizing of Admin VM</li> <li>- Update of software and firmware</li> <li>- Settings related to the CPU compatibility</li> </ul>
2	<a href="#">Cluster Expansion with ISM for PRIMEFLEX</a>	Execution of Cluster Expansion

## C.2.1 Preparations

This section describes preparations before you execute Cluster Expansion.

### Sizing of Admin VM

Resources of Infrastructure Admin VM, Virtual Admin VM and ADVN may be insufficient according to the number of servers to be added.

If resources of each VM are insufficient, add physical/virtual resources.

Although you add servers in order to increase resources, securing the resource of ISM-VA and vCSA in advance is still required.

If the physical resources of the management and workload server are insufficient, add the physical memory/disk to the management & workload server.

Refer to the manual of each software for the resource amount required for the number of registered nodes and the procedure to change the resource amount.

The resource amount of the Admin VM at factory settings and the number of registerable nodes in each model are as follows.

Model name	Admin VM name/Software name	Resource amount			Number of registerable nodes
		CPU	Memory	Disk	
PRIMEFLEX HS V1.0	Infrastructure Admin VM (ISM for PRIMEFLEX)	4vCPU	8 GB	136 GB	400 nodes
	Virtual Admin VM (vCenter Server Appliance)	2vCPU	10 GB	120 GB	Host: 10 units Virtual machine: 100 units
PRIMEFLEX HS V1.1	Infrastructure Admin VM (ISM for PRIMEFLEX)	4vCPU	8 GB	136 GB	400 nodes
	Virtual Admin VM (if Small is selected) (vCenter Server Appliance)	4vCPU	16 GB	290 GB	Host: 100 units Virtual machine: 1000 units

### Update of software and firmware

Update the following as required so that hypervisor version and patch version of servers for expanding a cluster and existing server are the same.

For the updating procedure, refer to the manual of each software.

- PRIMERGY Firmware
- Hypervisor version and patch version
- vCSA version (for vSAN)
- ISM for PRIMEFLEX version
- RAID Manager version (for vSAN)

## Settings related to the CPU compatibility

To execute live migration between servers with different CPU generations, settings are required for each model.

In VMware, in order to execute live migration between hosts with different processor generations, you must set EVC (Enhanced vMotion Compatibility) for the cluster. When it is enabled, CPU functions that affect vMotion's compatibility are masked, and some applications may behave unexpectedly.

For details of the EVC and how to set it, refer to "vCenter Server and Host Management" below.

<https://docs.vmware.com/en/VMware-vSphere/6.5/vsphere-esxi-vcenter-server-651-host-management-guide.pdf>

When activating the EVC function, if the virtual machine is started at a level higher than the CPU level set in the EVC, vMotion will not work between hosts on the cluster that has EVC enabled if the virtual machine is not adjusted to the set level.

The CPU level for the virtual machine gets the CPU information from the host at the time of starting the virtual machine. Therefore, if you are running the virtual machine at a high CPU level, restarting the virtual machine is required.

If EVC is set at the level equivalent to the CPU level of the currently running virtual machine, EVC is enabled without stopping the virtual machine.

## C.2.2 Cluster Expansion with ISM for PRIMEFLEX

---

For cluster expansion with ISM for PRIMEFLEX, refer to the following.

- " 6.9 Expand a Cluster for PRIMEFLEX HS/PRIMEFLEX for VMware vSAN" in "Operating Procedures."

## Appendix D Troubleshooting

This appendix describes the major causes and countermeasures for errors and unexpected behavior in ISM operation.

### Symptom: Registration of a discovered node fails.

#### Causes and countermeasures

Check the serial number of the discovered node. If the node is already registered, delete the node and register it again.

### Symptom: When registering nodes after editing IP address, the error "Registration of nodes discovered manually failed. IP address cannot be changed. The specified IP address already exists." is displayed.

#### Causes and countermeasures

When registering nodes after editing IP address, execute ping to the changed IP address and execute it after checking that there is no response.

For iRMC S3 generation PRIMERGY, ping to IP addresses might result in success a few minutes before and after changing.

### Symptom: GUI login fails with "Session Time Out" for ISM that was normally used, and the symptom occurs even after ISM-VA restart.

The following messages are output in the console screen of the hypervisor.

```
[55490.269659] XFS (dm-0): Internal error xfs_bmap_read_extents(1) at line 1321 of file fs/xfs/libxfs/xfs_bmap.c. Caller xfs_iread_extents+0x75/0xd0 [xfs]
[55490.272852] XFS (dm-0): Corruption detected. Unmount and run xfs_repair
[55490.275983] ffff8801ecb6e000: 42 4d 41 50 00 00 00 82 00 00 00 00 7a 2e fc BMAP.....z..
[55490.277488] ffff8801ecb6e010: ff ff ff ff ff ff ff ff 00 00 00 00 03 a5 20 00 .....
[55490.278907] ffff8801ecb6e020: 00 00 10 a1 ae 80 00 80 00 00 00 00 03 a6 20 00 .....
[55490.280367] ffff8801ecb6e030: 00 00 10 a1 c5 80 00 30 00 00 00 00 03 a6 80 00 .....0.....
[55490.281844] XFS (dm-0): Internal error xfs_bmap_read_extents(1) at line 1321 of file fs/xfs/libxfs/xfs_bmap.c. Caller xfs_iread_extents+0x75/0xd0 [xfs]
[55490.284837] XFS (dm-0): Corruption detected. Unmount and run xfs_repair
[55490.286288] ffff8801ecb6e000: 42 4d 41 50 00 00 00 82 00 00 00 00 7a 2e fc BMAP.....z..
[55490.287727] ffff8801ecb6e010: ff ff ff ff ff ff ff ff 00 00 00 00 03 a5 20 00 .....
[55490.289073] ffff8801ecb6e020: 00 00 10 a1 ae 80 00 80 00 00 00 00 03 a6 20 00 .....
[55490.290441] ffff8801ecb6e030: 00 00 10 a1 c5 80 00 30 00 00 00 00 03 a6 80 00 .....0.....
[55490.291716] XFS (dm-0): Internal error xfs_bmap_read_extents(1) at line 1321 of file fs/xfs/libxfs/xfs_bmap.c. Caller xfs_iread_extents+0x75/0xd0 [xfs]
[55490.294744] XFS (dm-0): Corruption detected. Unmount and run xfs_repair
[55490.296176] ffff8801ecb6e000: 42 4d 41 50 00 00 00 82 00 00 00 00 7a 2e fc BMAP.....z..
[55490.297620] ffff8801ecb6e010: ff ff ff ff ff ff ff ff 00 00 00 00 03 a5 20 00 .....
[55490.299035] ffff8801ecb6e020: 00 00 10 a1 ae 80 00 80 00 00 00 00 03 a6 20 00 .....
[55490.300401] ffff8801ecb6e030: 00 00 10 a1 c5 80 00 30 00 00 00 00 03 a6 80 00 .....0.....
[55490.301766] XFS (dm-0): Internal error xfs_bmap_read_extents(1) at line 1321 of file fs/xfs/libxfs/xfs_bmap.c. Caller xfs_iread_extents+0x75/0xd0 [xfs]
```

#### Causes and countermeasures

- ISM does not operate normally due to corruption of the virtual disk of ISM-VA.

Corruption of virtual disk might occur if hardware is in physical error and the server operating ISM-VA or ISM-VA itself is compulsorily stopped.

- If you have the ISM-VA already backed up, restore and use it.  
If you do not execute backup, install it newly.

### Symptom: For one of the following functions, the error "Communication with server failed," is displayed when executing an operation to import a file.

- [Structuring] - [Profiles] - [Actions] - [Import] - [Browse] button

- From [Structuring], select [Import] from the menu on the left side of the screen, then select the [Import Data List] tab - [Actions] - [Import DVD] - [Browse] button
- From [Structuring], select [Import] from the menu on the left side of the screen, then select the [Import Data List] tab - [Actions] - [Import Firmware] - [Browse] button
- From [Structuring], select [Import] from the menu on the left side of the screen, then select the [ServerView Suite] tab - [Actions] - [Import DVD] - [Browse] button

### Causes and countermeasures

- Confirm the files in the FTP folder and subfolders for the user group to which the user belongs; the files names should not contain any character coding other than UTF-8.
- Confirm the current status of data communication between ISM and the client.

---

### Symptom: Failure in confirming status and control of node

#### Causes and countermeasures

- Confirm that the network between the target node and ISM is operating correctly.
- Confirm whether the power cable is connected to the respective device and whether power is supplied.
- Confirm whether the IP address registered in ISM matches that of the respective device (or OS). Especially after modifying any IP addresses, you should confirm that you did not forget to change the registration information in ISM.
- Check whether the user accounts registered in ISM match those in the respective device (or OS). Especially after modifying any passwords, you should confirm that you did not forget to change the registration information in ISM.
- Confirm that no other ISM function is being in use for the node to be manipulated with ISM (for example, starting a profile assignment while a firmware update is in progress).

---

### Symptom: File downloads fail when using Internet Explorer 11.

#### Causes and countermeasures

File downloads may fail depending on your Internet Explorer settings. Modify your settings as follows:

On the [Internet Options] - [Security] tab, select the [Custom level] button and change the setting for [Downloads] - [File download] to [Enable].

---

### Symptom: Fails to register Microsoft Active Directory as LDAP server settings.

#### Causes and countermeasures

When you register Active Directory registered a large number of user information (for example, 1,000 or more), check that environment variable called "MaxPageSize" in Active Directory has the value according to the registered user information.

## Firmware Management

---

### Symptom: When updating the firmware, the target firmware cannot be specified.

#### Causes and countermeasures

- Firmware data must be imported and loaded in advance. If you have not imported them yet, execute an import first.
- If you are importing firmware individually and there is an error in the specified information such as firmware type or model name, the firmware will not be displayed as firmware that supports the specified node. Confirm the information on the repository screen. If it contains any errors, delete it from the repository first, and then import the firmware with the correct information.
- As you cannot downgrade the firmware to a previous version, firmware versions older than the current one on the node are not displayed in the Latest Version column. Check the version of the current version on the node and of the firmware you imported.

---

### Symptom: Online Update of the PCI card fails



## Causes and countermeasures

For Online Update the operating behavior of firmware on PCI cards depends on the OS of the server on which each PCI card is mounted. Refer to the documentation that is supplied with the firmware data or by the source from which you obtained the firmware data to confirm whether it is compatible with the relevant server OS.

Use Offline Update if the firmware data does not support the OS of the server.

---

### Symptom: The text in the release notes is not correctly displayed.

## Causes and countermeasures

Depending on the encoding settings in your browser, the release notes may sometimes not be correctly displayed. Check your encoding settings.

---

### Symptom: Firmware updates for ETERNUS DX/AF models fail.

## Causes and countermeasures

Possibly, the conditions for enabling the Update Mode are not fulfilled.

Refer to the precautions PDF file "Matrix of Versions for Which Firmware Updates Are Executable," which is provided together with the firmware data, to confirm whether your environment fulfills the conditions for enabling the Update Mode.

---

### Symptom: Offline Update fails.

## Causes and countermeasures

- When using Offline Update, the ServerView Suite DVD and the ServerView Suite Update DVD must have been imported. Confirm that the ServerView Suite DVD or the ServerView Suite Update DVD has been imported.
- Possibly, there is any error in the environment settings for running PXE boot. Confirm the following:
  - Whether DHCP servers are able to lease appropriate IP addresses
  - Whether, by any error, the PXE function is disabled in the BIOS settings of the node
  - Whether the onboard LAN or LAN card of the node is connected to ISM

## Profile Management

---

### Symptom: An error occurs in assigning, reassigning, or release a profile on a PRIMERGY server.

## Causes and countermeasures

You executed the profile assignment operation with the power of the target node being on. For profile assignment on PRIMERGY, be sure to execute the operation after turning the power off.

---

### Symptom: An error occurs in assigning, reassigning, or releasing a profile on a switch or storage.

## Causes and countermeasures

Executing these settings from ISM may sometimes result in an error when there are ongoing connections to the target node from sources other than ISM via SSH or the web. When you are going to operate a node from ISM, log out from external connections beforehand.

---

### Symptom: An error occurs when installing an OS with Profile Management.

## Causes and countermeasures

- The OS installation media to be installed were not yet imported. Import the installation media for the OS to be installed before you execute profile assignment.
- The ServerView Suite DVD that supports the installation target node and the type of OS was not yet imported. Import the ServerView Suite DVD that supports the installation target node and the type of OS before you execute profile assignment. If no version is specified for the ServerView Suite DVD to be used within the profile, the latest imported DVD is used. If you are using older device models and/or OSes, set the version of the DVD to be used within the profile.

- Possibly, there is any error in the environment settings for running PXE boot. Confirm the following:
  - Whether DHCP servers are able to lease appropriate IP addresses
  - Whether, by any error, the PXE function is disabled in the BIOS settings of the node
  - Whether the onboard LAN or LAN card of the node is connected to ISM

---

**Symptom: An error occurs when importing an exported profile or policy.**

**Causes and countermeasures**

If you import a profile or policy without any changes to the same ISM from which you exported it, an error occurs as a profile or policy of the same name already exists. Edit the "Profile Name" within the file to be imported, modifying the respective profile name or policy name.

## **Network Management**

---

**Symptom: No connection information is displayed on the Network Map.**

**Causes and countermeasures**

In order to retrieve and display connection information with ISM, it is first required to enable the LLDP function of each node. Enable LLDP with reference to the instruction manual or other documentation for the node. For nodes that support no LLDP, set up the connection information manually on the ISM screen.

---

**Symptom: The information displayed on the Network Map is outdated or incorrect.**

**Causes and countermeasures**

- The contents displayed on the Network Map are equivalent to the information at the time you last executed [Update network information] on the GUI screen. Execute [Update network information].
- Whenever an item such as the port status of a node has changed, execute [Get Node Information] and then [Update network information].

---

**Symptom: The virtual connection relationships are not displayed on the Network Map or there are errors in the displayed contents.**

**Causes and countermeasures**

To display the connection relationships between the virtual switches and the virtual machines, you must register the OS information of the cloud management software and of the managed target nodes to ISM.

Check that the cloud management software information is properly registered and the OS information of the managed node is properly registered.

---

**Symptom: Fails to change the VLAN settings.**

**Causes and countermeasures**

- The network switch must be accessible from ISM. Confirm that the switch is operating normally and that it can be accessed from ISM.
- Depending on the network switch device type there are reserved VLAN IDs. Check that the VLAN ID to be changed is not the registered VLAN ID of the network switch to be set up.

---

**Symptom: Fails to change link aggregation settings.**

**Causes and countermeasures**

- The network switch must be accessible from ISM. Confirm that the switch is operating normally and that it can be accessed from ISM.
- Depending on the network switch device type, the LAG Name and Mode that can be set differently. Check the LAG name and Mode can be set by the device specification.

## Log Management

---

### Symptom: Node logs of a node are collected incorrectly or not at all.

#### Causes and countermeasures

- Execute it again after some time when the log collection fails because of influence of the connection status or other.
- When you have newly registered a node, log collection is not yet set to be executed. Set a schedule for log collection under [Log Collection Settings].
- If the status on the [Log Collection Settings] tab on the Details of Node screen is "Exempt" and no action button for log collection is displayed, either the node is a device not eligible for log collection, or, at a point immediately after node registration, the device information was not yet obtained. If the target node is eligible for log collection, wait for a few minutes before you refresh the screen.
- Confirm the [Target] of the log type you specify for log collection. For schedule settings, confirm that the [Enable schedule execution] checkbox is selected.
- If you are able to collect logs by executing [Collect Logs] on the GUI screen but not with the schedule settings you made, it is possibly caused by the node power being off at the time of scheduled execution. Check the contents of the schedule.
- If the total volume of the log file exceeds the upper limit (size limit) set in the user group settings, new log files cannot be saved. From the Global Navigation Menu, check the [Operation Log] in [Events] - [Events] and if either of the items below can be found in the log collection timing, delete some of the collected logs to reduce the data volume.
  - During log collection for node (<node name>) Archived Log for the user group (User group name) exceeded the capacity (xxMB) set for log retention.
  - During log collection for node (<node name>) Node Log (download data) for the user group (<User group name>) exceeded the capacity (xxMB) set for log retention.
  - During log collection for node (<node name>) Node Log (log discovery data) exceeded the capacity (xxMB) set for log retention.

---

### Symptom: Settings for log collection of a node cannot be set.

#### Causes and countermeasures

If the node status is "Exempt," check whether the node actually supports log collection. If the status is "Exempt" although the node supports log collection, maybe ISM did not yet obtain the node information, so confirm the network connection with the node and the node property settings, and then execute [Get Node Information].

---

### Symptom: "Operating System" and "ServerView Suite" cannot be specified in log collection of a node.

#### Causes and countermeasures

- When the OS information of a target node is not registered yet, or not yet obtained with ISM, it cannot be specified. Register the OS information before you execute [Get Node Information].
- Depending on the type of OS, you may not be able to specify "ServerView Suite" as it may not be eligible for information retrieval.